A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

OpenScape Business V3

Administratordokumentation
11/2025

A31003-P3030-M100-63-0019

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Inhalt

1 Versionsgeschichte von Änderungen 39
1.1 Versionsgeschichte von Verbesserungen/Fixes 57

2 Einführung und wichtige Hinweise 67
2.1 Über diese Dokumentation 67
2.1.1 Dokumentationen und Zielgruppen 67
2.1.2 Struktur der Administratoren-Dokumentation 69
2.1.3 Arten von Themen 71
2.1.4 Darstellungskonventionen 72
2.2 Sicherheits- und Warnhinweise 72
2.2.1 Warnhinweise: Gefahr 73
2.2.2 Warnhinweise: Warnung 74
2.2.3 Warnungen: Vorsicht 75
2.2.4 Warnhinweise: Hinweis 76
2.2.5 Länderspezifische Sicherheitshinweise 76
2.2.5.1 Sicherheitshinweise für Australien 76
2.2.5.2 Sicherheitshinweise für Brasilien 77
2.2.5.3 Sicherheitshinweise für USA 77
2.2.5.4 Sicherheitshinweise für Kanada 80
2.3 Wichtige Hinweise 81
2.3.1 Verhalten in Notfällen 81
2.3.2 Bestimmungsgemäßer Gebrauch 82
2.3.3 Sachgemäße Entsorgung und Recycling 82
2.3.4 Normen und Richtlinien bezüglich der Installation 83
2.3.4.1 Anschluss von OpenScape Office X an den Versorgungsstromkreis 83
2.3.4.2 Anschließen von OpenScape Business S und OpenScape Business UC Booster Server an den Stromversorgungskreis 84
2.3.4.3 Geschirmte Verkabelung für LAN- und WAN-Anschlüsse von OpenScape Business X 84
2.3.4.4 Brandschutzanforderungen 85
2.3.4.5 Blitzschutzanforderungen 85
2.3.4.6 Kennzeichnungen für OpenScape Business X 86
2.3.5 Hinweise zu Störaussendung und Funkstörung von OpenScape Business X 86
2.3.6 Datenschutz und Datensicherheit 86
2.3.7 Technische Vorschriften und Konformität von OpenScape Business X 87
2.3.7.1 CE-Konformität 87
2.3.7.2 Konformität mit US- und kanadischen Normen 88
2.3.7.3 Konformität mit internationalen Normen 88
2.3.8 Betriebsbedingungen 88
2.3.8.1 Betriebsbedingungen OpenScape Business X 88
2.3.8.2 Betriebsbedingungen OpenScape Business S und OpenScape Business UC Booster Server 89

3 Systemübersicht 90
3.1 Highlights 90
3.2 Unified Communications 90
3.2.1 UC-Funktionen (Überblick) 91
3.2.2 Benutzerzugriff auf UC-Funktionen (UC Clients) 98
3.2.3 Integration in Geschäftsanwendungen 101
3.3 OpenScape Business Modelle 102
3.3.1 Vertriebliche Ausbaustufen 102
3.3.2 UC Hardware Modelle 105
3.3.3 UC Booster Hardware 106

3.3.4 UC Software Modelle (Softswitch)..... 107
3.3.5 Aufbau und Umweltbedingungen..... 107
3.3.6 Unterstützte Telefone..... 108
3.4 Weiterführende Informationen..... 109
3.4.1 Unterstützte Sprachen..... 109
3.4.2 Internet-Links..... 111

4 Administrationskonzept..... 113
4.1 OpenScape Business Assistant (WBM)..... 113
4.1.1 Voraussetzungen für das WBM..... 113
4.1.2 Startseite des WBM..... 113
4.1.3 Einführung in das WBM..... 115
4.1.3.1 So melden Sie sich bei der WBM an..... 117
4.1.3.2 Wie Sie sich vom WBM abmelden..... 117
4.1.4 WBM-Benutzerverwaltung..... 118
4.1.4.1 Wie Sie einen Administrator hinzufügen..... 120
4.1.4.2 Wie Sie einen Administrator bearbeiten..... 121
4.1.4.3 Wie Sie das eigene Administratorpasswort ändern..... 121
4.1.4.4 Wie Sie einen Administrator löschen..... 122
4.1.4.5 So ändern Sie ein Manager E Administrator-Kennwort..... 122
4.1.5 Wizards..... 122
4.1.5.1 Wizards – Grundinstallation..... 123
4.1.5.2 Wizards – Netzwerk / Internet..... 123
4.1.5.3 Assistenten – Telefone / Abonnenten..... 123
4.1.5.4 Wizards – Zentrale Telefonie..... 124
4.1.5.5 Wizards – User-Telefonie..... 125
4.1.5.6 Wizards – Sicherheit..... 125
4.1.5.7 Wizards – UC Smart (nur mit UC Smart)..... 126
4.1.5.8 Wizards – UC Suite (nur mit UC Suite)..... 126
4.1.5.9 Assistenten – Globales Verzeichnis..... 127
4.1.5.10 Assistenten - Cloud Services..... 127
4.1.6 Service-Center..... 127
4.1.6.1 Service Center – **Dokumente**..... 127
4.1.6.2 Service Center – **Software** 128
4.1.6.3 Service Center – **Inventory** > **System**..... 128
4.1.6.4 Service Center – **Inventory** > **Rufnummern**..... 128
4.1.6.5 Service Center – **Inventory** > **Netzwerkübersicht**..... 128
4.1.6.6 Service-Center – **Software-Update**..... 129
4.1.6.7 Service-Center – **Email-Weiterleitung**..... 129
4.1.6.8 Service-Center – **Remote-Zugang**..... 129
4.1.6.9 Service-Center – **Restart / Reload**..... 129
4.1.6.10 Service-Center – **Diagnose** > **Status**..... 129
4.1.6.11 Service-Center – **Diagnose** > **Event Viewer**..... 129
4.1.6.12 Service-Center – **Diagnose** > **Trace**..... 129
4.1.6.13 Service-Center – Diagnose > Service-Protokoll..... 129
4.1.7 Experten-Modus..... 130
4.1.8 Online-Hilfe..... 130
4.1.8.1 Wie Sie die Online-Hilfe kontextsensitiv aufrufen..... 130
4.2 Manager E..... 130
4.2.1 Wie Sie den KDS in den Manager E laden..... 132
4.2.2 Wie Sie den KDS in das System zurücksichern..... 132

5 Ersteinrichtung von OpenScape Business X..... 133
5.1 Voraussetzungen für die Erstinstallation..... 134
5.2 Komponenten..... 135
5.3 Rufnummernplan..... 136

5.4 IP-Adressen-Schema....137
5.5 Erstinbetriebnahme....139
5.5.1 Wie Sie das Kommunikationssystem starten....139
5.5.2 Wie Sie den Admin-PC mit dem Kommunikationssystem verbinden....140
5.5.3 Wie Sie das WBM starten....141
5.6 Integration ins Kunden-LAN....143
5.6.1 Wie Sie den Wizard Erstinstallation starten....143
5.6.2 Systemeinstellungen....144
5.6.2.1 Wie Sie das Display-Logo und die Produktbezeichnung festlegen....144
5.6.2.2 Wie Sie die IP-Adressen festlegen (optional)....145
5.6.2.3 So legen Sie Richtungsnamen fest....146
5.6.3 DHCP-Einstellungen....146
5.6.3.1 So deaktivieren Sie den internen DHCP-Server....147
5.6.3.2 So aktivieren und konfigurieren Sie den internen DHCP-Server....147
5.6.3.3 So aktivieren Sie DHCP nur für Mitel/Unify Geräte....149
5.6.4 Länder- und Zeiteinstellungen....150
5.6.4.1 Wie Sie das Länderkennzeichen und die Sprache für Event-Logs auswählen....151
5.6.4.2 Wie Sie die DECT-Systemkennung eingeben....152
5.6.4.3 Wie Sie das Datum und die Uhrzeit manuell einstellen....152
5.6.4.4 Wie Sie das Datum und die Uhrzeit von einem SNTP-Server beziehen....153
5.6.5 UC-Lösung....154
5.6.5.1 Wie Sie die UC-Lösung festlegen....154
5.6.6 Anschluss des Kommunikationssystems ans Kunden-LAN....155
5.6.6.1 Wie Sie das Kommunikationssystem ans Kunden-LAN anschließen....155
5.7 Basiskonfiguration....156
5.7.1 Wie Sie den Wizard Basisinstallation starten....156
5.7.2 Systemrufnummern und Vernetzung....157
5.7.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben....157
5.7.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben....158
5.7.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren....159
5.7.3 Teilnehmerdaten....160
5.7.3.1 Wie Sie die Teilnehmerdaten anzeigen....162
5.7.3.2 Wie Sie alle Rufnummern löschen....162
5.7.3.3 Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen....163
5.7.3.4 Teilnehmerdaten über eine XML-Datei importieren....163
5.7.3.5 Anzeigen von Massendaten....164
5.7.4 ISDN-Konfiguration....165
5.7.4.1 Wie Sie den Anschluss von ISDN-Teilnehmern konfigurieren....166
5.7.4.2 Wie Sie den ISDN-Anlagenanschluss konfigurieren....166
5.7.4.3 Wie Sie den ISDN-Mehrgeräteanschluss konfigurieren....167
5.7.4.4 Wie Sie die ISDN-Konfiguration deaktivieren....167
5.7.5 Internetzugang....168
5.7.5.1 Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren....170
5.7.5.2 Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren....171
5.7.5.3 Internet-Zugang über vorkonfigurierten ISP konfigurieren....172
5.7.5.4 Internet-Zugang über Standard-ISP PPPoE konfigurieren....174
5.7.5.5 Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren....176
5.7.5.6 Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port....179
5.7.5.7 Wie Sie den Internet-Zugang deaktivieren....180
5.7.6 Internet-Telefonie....180
5.7.6.1 Vordefinierten ITSP konfigurieren....182
5.7.6.2 Wie Sie Internet-Telefonie deaktivieren....186
5.7.7 Teilnehmer....187

5.7.7.1 ISDN-Teilnehmer konfigurieren 187
5.7.7.2 Analoge Teilnehmer konfigurieren 190
5.7.7.3 UP0-Teilnehmer konfigurieren 193
5.7.7.4 Wie Sie DECT-Teilnehmer konfigurieren 196
5.7.7.5 Wie Sie IP- und SIP-Teilnehmer konfigurieren 199
5.7.8 Konfiguration von UC Suite 202
5.7.8.1 So konfigurieren Sie die UC Suite 202
5.7.9 Konfiguration der UC Smart Sprachboxen 203
5.7.9.1 Wie Sie die UC Smart Sprachboxen konfigurieren 203
5.7.10 Konferenz-Server-Einstellungen 204
5.7.10.1 Wie Sie die Konferenz-Server-Einstellungen ändern 204
5.7.11 E-Mail-Versand (optional) 205
5.7.11.1 E-Mail-Versand konfigurieren 205
5.8 Abschließende Tätigkeiten 208
5.8.1 Wie Sie die Lizenzen aktivieren und zuordnen 209
5.8.2 Wie Sie den UC Smart Client zur Installation bereitstellen 211
5.8.3 Wie Sie die UC Suite Clients zur Installation bereitstellen 211
5.8.4 Wie Sie eine Datensicherung durchführen 213
5.9 Inbetriebnahme der IP-Telefone 213
5.9.1 Wie Sie ein IP-Telefon konfigurieren 215
5.9.2 Wie Sie ein SIP-Telefon konfigurieren 216
5.10 Diagnose-Traces für einen Fehlerfall erfassen 218
5.11 Neuflash 219

6 Ersteinrichtung von OpenScape Business S 222
6.1 Voraussetzungen für die Ersteinrichtung 222
6.2 Komponenten 225
6.3 IP-Adressen-Schema 226
6.4 Rufnummernplan 227
6.5 Installation der Kommunikationssoftware 227
6.5.1 Wie Sie die Kommunikationssoftware installieren 229
6.6 Inbetriebnahme 231
6.6.1 Wie Sie den Wizard Erstinstallation starten 231
6.6.2 Systemeinstellungen 232
6.6.2.1 Wie Sie das Sie das Anzeigelogo und den Produktnamen festlegen 232
6.6.2.2 Wie wählen Sie den Ländercode und die Sprache für Trace-Protokolle aus 233
6.6.2.3 Wie Sie einen weiteren LAN-Anschluss als WAN-Schnittstelle aktivieren 234
6.6.2.4 Wie ändern Sie den Wahlplan auf 4 Ziffern 235
6.6.3 UC-Lösung 236
6.6.3.1 Wie Sie die UC-Lösung festlegen 236
6.7 Basiskonfiguration 237
6.7.1 Wie Sie den Wizard Basisinstallation starten 237
6.7.2 Systemrufnummern und Vernetzung 238
6.7.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben 238
6.7.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben 239
6.7.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren 240
6.7.2.4 Wie Sie die Upstream-Strecke Ihrer Internetverbindung konfigurieren 241
6.7.3 Teilnehmerdaten 241
6.7.3.1 Wie Sie die Teilnehmerdaten anzeigen 243
6.7.3.2 Wie Sie alle Rufnummern löschen 243
6.7.3.3 Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen 244
6.7.3.4 Teilnehmerdaten über eine XML-Datei importieren 244
6.7.4 Internetzugang 245
6.7.4.1 Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port 245
6.7.5 Internet-Telefonie 246

6.7.5.1 Vordefinierten ITSP konfigurieren....247
6.7.5.2 Wie Sie Internet-Telefonie deaktivieren....252
6.7.6 Teilnehmer....252
6.7.6.1 Wie Sie IP- und SIP-Teilnehmer konfigurieren....252
6.7.7 Konfiguration von UC Suite....255
6.7.7.1 So konfigurieren Sie die UC Suite....256
6.7.8 Konfiguration der UC Smart Sprachboxen....256
6.7.8.1 Wie Sie die UC Smart Sprachboxen konfigurieren....257
6.7.9 Konferenz-Server-Einstellungen....257
6.7.9.1 Wie Sie die Konferenz-Server-Einstellungen ändern....257
6.7.10 E-Mail-Versand (optional)....258
6.7.10.1 E-Mail-Versand konfigurieren....258
6.8 Abschließende Tätigkeiten....261
6.8.1 Wie Sie die Lizenzen aktivieren und zuordnen....262
6.8.2 Wie Sie den UC Smart Client zur Installation bereitstellen....264
6.8.3 Wie Sie die UC Suite Clients zur Installation bereitstellen....264
6.8.4 Wie Sie eine Datensicherung durchführen....265
6.9 Inbetriebnahme der IP-Telefone....266
6.9.1 Wie Sie ein IP-Telefon konfigurieren....267
6.9.2 Wie Sie ein SIP-Telefon konfigurieren....268
6.10 Deinstallation der Kommunikationssoftware....270
6.10.1 Wie Sie die Kommunikationssoftware deinstallieren....270
6.11 Verwendete Ports....270
6.12 Diagnose-Traces für einen Fehlerfall erfassen....273
6.13 Neuflash....274

7 Ersteinrichtung OpenScape Business UC Booster....277
7.1 Voraussetzungen für die Ersteinrichtung....279
7.2 Sicherung der Konfigurationsdaten des Kommunikationssystems....282
7.2.1 Wie Sie eine Datensicherung durchführen....282
7.3 Inbetriebnahme UC Booster Card....283
7.3.1 Montage der UC Booster Card....283
7.3.2 Konfiguration der UC Booster Card....283
7.3.3 Software-Update für die UC Booster Card....284
7.3.3.1 Wie Sie ein Software-Update durchführen....284
7.4 Inbetriebnahme UC Booster Server....285
7.4.1 Installation der Kommunikationssoftware....285
7.4.1.1 Wie Sie die Kommunikationssoftware installieren....286
7.4.2 Konfiguration des UC Booster Servers....288
7.4.2.1 IP-Adresse des Kommunikationssystems bekannt geben....288
7.4.3 Software-Update für die UC Booster Server....290
7.5 Basiskonfiguration....291
7.6 Abschließende Tätigkeiten....291
7.7 Deinstallation der Kommunikationssoftware....292
7.7.1 Wie Sie die Kommunikationssoftware deinstallieren....292
7.8 Hochrüstung von UC Booster Card auf UC Booster Server....292
7.9 Verwendete Ports....294

8 Lizenzierung....297
8.1 Lizenzierungsverfahren....298
8.2 Lizenzen....300
8.2.1 Basislizenz....301
8.2.2 Benutzerlizenzen....302
8.2.3 User-orientierte Lizenzen....303
8.2.4 Systemlizenzen....305
8.2.5 Evaluierungslizenzen....307

8.2.6 Upgrade-Lizenzen ... 309
8.2.7 Vorschläge für Lizenzkombinationen ... 309
8.3 Lizenzierung eines Kommunikationssystems (Standalone) ... 312
8.3.1 CLS Connect ... 313
8.3.1.1 Aktivierung von CLS Connect ... 313
8.3.1.2 Umschaltung von CLS Connect ... 314
8.3.2 Lizenzaktivierung (Standalone) ... 314
8.3.2.1 Wie Sie Lizenzen online aktivieren (Standalone) ... 315
8.3.2.2 Wie Sie Lizenzen offline aktivieren (Standalone) ... 316
8.3.3 Lizenzzuordnung (Standalone) ... 317
8.3.3.1 Teilnehmer lizenzieren (Standalone) ... 319
8.3.3.2 Wie Sie Leitungen lizenzieren (Standalone) ... 322
8.4 Lizenzierung mehrerer Kommunikationssysteme (Netzverbund) ... 323
8.4.1 Lizenzaktivierung (Netzverbund) ... 325
8.4.1.1 Wie Sie Lizenzen offline aktivieren (Netzverbund) ... 325
8.4.1.2 Wie Sie Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen ... 327
8.4.2 Lizenzzuordnung (Netzverbund) ... 328
8.4.2.1 Wie Sie Teilnehmer lizenzieren (Netzverbund) ... 330
8.4.2.2 Wie Sie Leitungen lizenzieren (Netzverbund) ... 333
8.4.2.3 Wie Sie Systemlizenzen einem Knoten zuordnen ... 333
8.4.2.4 Wie Sie die Systemlizenz "Networking" einem Knoten zuordnen ... 334
8.5 Lizenzinformationen ... 334
8.5.1 Lizenzinformationen ohne Netzverbund (Standalone) ... 335
8.5.1.1 Wie Sie Lizenzinformationen anzeigen ... 335
8.5.2 Lizenzinformationen im Netzverbund ... 335
8.5.2.1 Wie Sie alle Lizenzen des Netzverbundes anzeigen ... 336
8.5.2.2 Wie Sie die an einen Knoten gebundenen Lizenzen anzeigen ... 336
8.5.2.3 Wie Sie alle im Netzverbund gemeinsam genutzten Lizenzen anzeigen ... 337
8.5.2.4 Wie Sie Teilnehmer- und User-orientierte Lizenzen knotenabhängig anzeigen ... 337
8.6 Lizenzprofilzuordnung ... 337
8.6.1 Wie Sie ein Lizenzprofil hinzufügen ... 338
8.6.2 Wie Sie ein Lizenzprofil bearbeiten ... 339
8.6.3 Wie Sie Teilnehmern ein Lizenzprofil zuordnen ... 339
8.6.4 Wie Sie ein Lizenzprofil löschen ... 340
8.7 Rehost nach Hardwaretausch ... 341
8.7.1 Wie Sie einen Rehost nach einem Hardwaretausch ausführen ... 342
8.8 Lizenzserver (Central License Server, CLS) ... 342
8.8.1 Wie Sie die IP-Adresse des Lizenzservers abfragen oder ändern ... 342
8.8.2 So überprüfen Sie die Verbindung zum Central License Server (CLS) ... 343
8.9 Lizenzagent (Customer License Agent, CLA) ... 343
8.9.1 Wie Sie eine Verbindung zum lokalen Lizenzagenten konfigurieren ... 344
8.9.2 Wie Sie die Verbindung zum zentralen Lizenzagenten ändern ... 344
8.10 Locking ID und Advanced Locking ID ... 344
8.10.1 Wie Sie die Locking ID des Kommunikationssystems abfragen ... 346
8.10.2 Wie Sie die Locking ID des Soft Switches abfragen ... 346
8.10.3 Wie Sie die Advanced Locking ID des Soft Switches abfragen ... 346
8.11 So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) ... 346
8.12 So migrieren Sie den Master-Knoten eines vernetzten Systems von V2-Mainboard zu V3-Mainboard ... 348
8.13 So migrieren Sie den Slave-Knoten eines vernetzten Systems von V2-Mainboard zu V3-Mainboard ... 349
8.14 Migration von HiPath 3000 Systemen auf OSBiz V3 Software mit V3 Mainboard ... 349
8.15 Aktualisierung von V2 auf V3 mit **CLS Connect** ... 350
8.16 Aktualisierung von V2 auf V3 ohne **CLS Connect** ... 350

9 Integration ins interne Datennetz (LAN) ... 352
9.1 LAN-Schnittstelle ... 352
9.1.1 IP-Adresse und Netzmaske der LAN-Schnittstelle ... 352

9.1.1.1 Wie Sie IP-Adresse und Netzmaske der Hardware-Plattform ändern....353
9.1.1.2 Wie Sie IP-Adresse der UC Booster Card ändern....354
9.1.1.3 Wie Sie IP-Adresse und Netzmaske des Softswitches ändern....354
9.1.2 Interner IP-Adressbereich der LAN-Schnittstelle....355
9.1.2.1 Wie Sie den internen IP-Adressbereich der Hardware-Plattform ändern....355
9.1.2.2 Wie Sie den internen IP-Adressbereich der Hardware-Plattform zurücksetzen....356
9.2 DHCP....356
9.2.1 DHCP-Relay-Agent....356
9.2.1.1 So konfigurieren Sie die Hardwareplattform als DHCP-Relay-Agent....356
9.2.2 DHCP-Server....357
9.2.2.1 Aktivieren und Konfigurieren des DHCP-Servers der Hardwareplattform....359
9.2.2.2 So deaktivieren Sie den DHCP-Server der Hardwareplattform....360
9.2.2.3 Wie Sie den DHCP-Server des Softswitches aktivieren und konfigurieren....361
9.2.2.4 Wie Sie den DHCP-Server des Softswitches deaktivieren....362
9.2.2.5 So aktivieren Sie DHCP nur für Mitel/Unify Geräte....362
9.3 DNS - Namensauflösung....363
9.3.1 Externen DNS-Server festlegen....365
9.4 IP-Routing....365
9.4.1 Wie Sie den Default Router aktivieren oder deaktivieren....366
9.4.2 Wie Sie eine statische Route hinzufügen....366
9.4.3 Wie Sie statische Routen löschen....367
9.5 Deployment Service (DLI und DLS)....367
9.5.1 Wie Sie einen externen DLS-Server im internen DHCP-Server konfigurieren....370
9.5.2 Wie Sie den internen DLI aktivieren....370
9.5.3 Wie Sie das Kommunikationssystem als Deployment und Licensing Client konfigurieren....371

10 Anbindung an Service-Provider....372
10.1 Internetzugang....372
10.1.1 Internet-Zugang über einen externen Internet-Router....374
10.1.1.1 Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren....375
10.1.1.2 Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren....376
10.1.1.3 Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port....377
10.1.2 Internet-Zugang über Internet-Modem....378
10.1.2.1 Wie Sie den Internet-Zugang über einen vorkonfigurierten ISP konfigurieren....379
10.1.2.2 Wie Sie den Internet-Zugang über einen Standard-ISP PPPoE konfigurieren....381
10.1.2.3 Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren....383
10.1.3 WAN-Schnittstelle....386
10.1.4 DynDNS....386
10.1.4.1 Wie Sie den DynDNS-Service konfigurieren....387
10.1.4.2 Wie Sie den Mail-Exchanger definieren....389
10.2 Amtszugang über ITSP....389
10.2.1 Konfiguration eines ITSP....391
10.2.1.1 Vordefinierten ITSP konfigurieren....393
10.2.1.2 So fügen Sie ein neues ITSP hinzu....399
10.2.1.3 Wie Sie Multisite über ITSP konfigurieren....406
10.2.1.4 So speichern Sie eine vorkonfigurierte ITSP-Vorlage als neue Vorlage....407
10.2.1.5 Wie Sie eine vorkonfigurierte ITSP-Vorlage anpassen....408
10.2.1.6 Wie Sie eine vorkonfigurierte ITSP-Vorlage manuell aktualisieren....408
10.2.2 STUN (Simple Traversal of UDP over NAT)....409
10.2.2.1 Wie Sie den STUN-Modus festlegen....410
10.3 Amtszugang über digitale und analoge Leitungen....410
10.3.1 Leitungen....410
10.3.1.1 Wie Sie den ISDN-Amtszugang konfigurieren....412

10.3.1.2 Wie Sie einen analogen Amtszugang konfigurieren....413
10.3.1.3 Wie Sie alle Leitungen anzeigen....414
10.3.1.4 Wie Sie eine einzelne Leitung anzeigen....414
10.3.1.5 Wie Sie eine Leitungskennzahl ändern....414
10.3.1.6 Wie Sie eine MSN einer Leitung zuweisen....415
10.3.1.7 ISDN-Protokoll ändern....415
10.3.1.8 Wie Sie den B-Kanal-Belegungsmodus ändern....415
10.3.1.9 Wie Sie das Wahlverfahren ändern....416
10.3.2 Richtungen....416
10.3.2.1 Wie Sie die Richtungszuordnung ändern....419
10.3.2.2 Wie Sie den Richtungsnamen ändern....420
10.3.2.3 Wie Sie die Richtungskennzahl ändern....420
10.3.2.4 Wie Sie eine Überlaufrichtung bei deaktiviertem LCR konfigurieren....420
10.3.2.5 Wie Sie eine Überlaufrichtung bei aktiviertem LCR konfigurieren....421
10.3.2.6 Wie Sie die Belegungsart konfigurieren....421
10.3.2.7 Wie Sie die Anlagenrufnummer kommend und gehend eintragen....421
10.3.2.8 Wie Sie das Format der übermittelten Rufnummer konfigurieren....422
10.3.2.9 Wie Sie die Art der übermittelten Rufnummer konfigurieren....422
10.3.2.10 Wie Sie das Richtungs-Präfix konfigurieren....422
10.3.2.11 Wie Sie eine Richtung für die Vernetzung definieren und eine zweite Amtskennziffer eintragen....423
10.3.3 Wähltonüberwachung....423
10.3.3.1 Wie Sie die Verzögerungszeit der Wähltonüberwachung konfigurieren....424
10.3.3.2 Wie Sie die Wähltonüberwachungszeit konfigurieren....425
10.3.3.3 Wie Sie die Ziffernwahlzeit konfigurieren....425
10.3.3.4 Wie Sie die Auswertung des zweiten Wähltons aktivieren oder deaktivieren....426
10.4 Priorisierung der Amtsholung bei aktiviertem LCR....426
10.4.1 Wie Sie die Amtsholung priorisieren....427

11 Teilnehmer....428
11.1 Rufnummernplan....428
11.1.1 Standard-Rufnummernplan....429
11.1.2 Individueller Rufnummernplan....430
11.1.2.1 Wie Sie Standard-Rufnummern löschen oder ändern....431
11.1.2.2 Wie Sie spezielle Standard-Rufnummern ändern....432
11.1.2.3 Wie Sie Rufnummern und Teilnehmerdaten importieren....432
11.2 Anforderungen an die LAN-Telefonie....433
11.2.1 Audio-Codecs....434
11.2.1.1 Wie Sie Audio-Codec-Parameter konfigurieren....434
11.2.1.2 Wie Sie Audio-Codec-Parameter einem Ziel zuordnen....435
11.2.2 Übertragung von Tönen nach RFC2833....436
11.2.2.1 Wie Sie die Übertragung von Fax- und Modem-Tönen nach RFC2833 aktivieren oder deaktivieren....436
11.2.2.2 Wie Sie die Übertragung von DTMF-Tönen nach RFC2833 aktivieren oder deaktivieren....437
11.2.3 Quality of Service....437
11.2.3.1 Wie Sie Quality of Service konfigurieren....439
11.3 IP-Teilnehmer....440
11.4 SIP-Stationen....441
11.5 UP0-Teilnehmer....443
11.6 DECT-Teilnehmer....444
11.7 Mitel SIP DECT-Teilnehmer....445
11.8 ISDN-Teilnehmer....445
11.8.1 Wie Sie die S_0-Schnittstelle für ISDN-Teilnehmer konfigurieren....447
11.8.2 Wie Sie nur eingerichtete Nummern für MSN zulassen....448
11.9 Analoge Teilnehmer....449
11.10 Virtuelle Teilnehmer....450

11.11 Tastenprogrammierung 451
11.11.1 Wie Sie die Funktionstasten der Systemtelefone programmieren.... 452
11.12 Teilnehmer-Profile.... 453
11.13 Konfiguration der Teilnehmer....454
11.13.1 IP-Teilnehmer konfigurieren 456
11.13.2 Wie Sie SIP-Teilnehmer konfigurieren.... 459
11.13.3 UP0-Teilnehmer konfigurieren.... 463
11.13.4 Wie Sie DECT-Teilnehmer konfigurieren.... 466
11.13.5 So konfigurieren Sie Mitel SIP-DECT-Teilnehmer über die Bereitstellung....470
11.13.5.1 So konfigurieren Sie SIP-Teilnehmer über den Expertenmodus.... 472
11.13.6 ISDN-Teilnehmer konfigurieren....473
11.13.7 Analoge Teilnehmer konfigurieren....475
11.13.8 Wie Sie den Namen der Teilnehmer ändern....478
11.14 Konfiguration der Teilnehmer-Profile 479
11.14.1 Wie Sie ein neues Teilnehmer-Profil anlegen....480
11.14.2 Wie Sie Teilnehmer-Profile und deren Mitglieder anzeigen.... 481
11.14.3 Wie Sie Mitglieder zu einem Teilnehmer-Profil hinzufügen....481
11.14.4 Wie Sie Mitglieder aus einem Teilnehmer-Profil löschen....482
11.14.5 Wie Sie ein einzelnes Teilnehmer-Profil exportieren oder importieren....482
11.14.6 Wie Sie die Werte und Einstellungen eines Teilnehmer-Profils ändern....483
11.14.7 Wie Sie alle Teilnehmer-Profile exportieren oder importieren....484
11.15 Konfiguration der Authentifizierungsdaten am SIP-Telefon....485
11.15.1 Wie Sie die Authentifizierungsdaten über das WBM des SIP-Telefons konfigurieren....485
11.15.2 Wie Sie die Authentifizierungsdaten am Display des SIP-Telefons konfigurieren....487
11.16 Export von Teilnehmerdaten....488
11.16.1 Wie Sie die Teilnehmerdaten exportieren.... 489

12 UC Smart....490
12.1 Grundeinstellungen für UC Smart.... 491
12.1.1 Wie Sie UC Smart aktivieren.... 491
12.1.2 Wie Sie UC Smart konfigurieren....492
12.1.3 Wie Sie die applikationsgesteuerten Konferenzen konfigurieren....493
12.1.4 Wie Sie die IP-Adressen von Komponenten des Systems ermitteln....494
12.1.5 Wie Sie den Status von UC Smart ermitteln.... 494
12.2 UC Smart Clients....495
12.2.1 myPortal @work.... 495
12.2.1.1 Voraussetzungen für myPortal @work.... 497
12.2.1.2 Benutzerkonfiguration für myPortal@work.... 499
12.2.1.3 Konfigurationsschritte zur Nutzung von myPortal @work über das Internet.... 506
12.2.1.4 Weitere Konfigurationshinweise & Einstellungen.... 508
12.2.1.5 Leitfaden zur Fehlerbehebung....510
12.2.1.6 Weitere Hinweise....512
12.3 Benutzer von UC Smart.... 512
12.3.1 Wie Sie Benutzer von UC Smart konfigurieren.... 513
12.3.2 Wie Sie für einen Benutzer von UC Smart das Kennwort ändern....513
12.4 Anwesenheitsstatus (Präsenz)....514
12.5 Verzeichnisse und Journal.... 515
12.5.1 Verzeichnisse....515
12.5.1.1 Verzeichnisse für Systemtelefone konfigurieren....516
12.5.2 Internes Verzeichnis....517
12.5.2.1 Wie Sie die Anzeige eines Teilnehmers im internen Verzeichnis aktivieren oder deaktivieren.... 517
12.5.3 Favoritenliste.... 518
12.5.4 Systemverzeichnis....518
12.5.5 Unified-Verzeichnis....518
12.5.5.1 Leistungsmerkmale.... 519
12.5.5.2 Regeln und Konventionen.... 522

12.5.5.3 Funktionale Grenzen....523
12.5.5.4 Unified-Verzeichnis in vernetzten Systemen....524
12.5.6 Journal....525
12.6 Anrufe....525
12.6.1 Rufnummernformate....525
12.6.2 Voraussetzungen für den Empfang von VoIP-Anrufen auf myPortal to go mit CallKit auf Ihrem iPhone....526
12.7 Konferenzen....526
12.8 Web Collaboration....528
12.8.1 Wie Sie die Verbindung zum Web Collaboration Server (Public Server) konfigurieren....529
12.8.2 Wie Sie die Verbindung zum Web Collaboration Server deaktivieren....530
12.9 Instant Messaging....530
12.9.1 Instant Messaging....530
12.10 Sprachbox (SmartVM)....530
12.10.1 Konfiguration der Sprachbox (SmartVM)....533
12.10.1.1 Wie Sie die Sprachbox deaktivieren oder aktivieren....534
12.10.1.2 Wie Sie die Sprachbox (SmartVM) konfigurieren....534
12.10.1.3 Wie Sie eine Standardmailbox für einen Teilnehmer hinzufügen....535
12.10.1.4 Wie Sie die Berechtigungsgruppe für einen Sprachbox-Port ändern....536
12.10.1.5 Wie Sie die Struktur des Telefonmenüs der Sprachbox ändern....536
12.10.1.6 Wie Sie einzelne Begrüßungen laden, sichern und löschen....537
12.10.1.7 Wie Sie Begrüßungen und Nachrichten sichern und wiederherstellen....537
12.10.2 Benachrichtigungsdienst für neue Nachrichten....538
12.10.2.1 Wie Sie die E-Mail-Benachrichtigung aktivieren oder deaktivieren....539

13 UC Suite....540
13.1 Grundeinstellungen für UC Suite....540
13.1.1 UC Suite aktivieren....541
13.1.2 Wie Sie die Berechtigung von systemseitig eingeleiteten UC-Anrufe einschränken....541
13.2 UC Suite Clients....541
13.2.1 myPortal for Desktop....542
13.2.2 myPortal @work....543
13.2.3 myPortal for Outlook....543
13.2.4 Fax Printer....543
13.2.5 myAttendant....544
13.2.6 Voraussetzungen für UC Suite PC-Clients....544
13.2.7 Silent Installation/Deinstallation für UC Suite PC-Clients....548
13.2.7.1 Wie Sie eine Silent Installation durchführen....549
13.2.7.2 Wie Sie eine Silent Deinstallation durchführen....550
13.2.8 Automatische Updates....551
13.3 Benutzer und Benutzer-Profile von UC Suite....551
13.3.1 Benutzer von UC Suite....552
13.3.1.1 Wie Sie einen Benutzer von UC Suite konfigurieren....555
13.3.1.2 Wie Sie einen Benutzer von UC Suite zurücksetzen....555
13.3.1.3 Wie Sie einen Benutzer von UC Suite als Agenten konfigurieren (myAgent)....555
13.3.1.4 Anwesenheitsstatus für einen Benutzer von UC Suite ändern....556
13.3.1.5 Kennwort für einen Benutzer von UC Suite ändern....556
13.3.1.6 Kennwortlänge für Benutzer von UC Suite ändern....557
13.3.2 Benutzer-Profile der UC Suite....557
13.3.2.1 Wie Sie ein Benutzer-Profil von UC Suite hinzufügen....559
13.3.2.2 Wie Sie ein Benutzer-Profil von UC Suite ändern....559
13.3.2.3 Wie Sie die Benutzer-Profile von UC Suite anzeigen....560
13.3.2.4 Wie Sie Mitglieder zu einem Benutzer-Profil von UC Suite hinzufügen....560
13.3.2.5 Wie Sie Mitglieder aus einem Benutzer-Profil von UC Suite löschen....560
13.3.2.6 Wie Sie ein Benutzer-Profil von UC Suite löschen....561
13.4 Anwesenheitsstatus und CallMe-Dienst....561

13.4.1 Anwesenheitsstatus (Präsenz)....561
13.4.2 CallMe-Dienst....564
13.4.3 Statusbezogene Anrufumleitung....565
13.4.4 Regelbasierte Anrufumleitung....565
13.5 Verzeichnisse und Journal....566
13.5.1 Verzeichnisse....566
13.5.1.1 Verzeichnisse für Systemtelefone konfigurieren....569
13.5.2 Internes Verzeichnis....570
13.5.2.1 Wie Sie die Anzeige analoger Teilnehmer im internen Verzeichnis aktivieren oder deaktivieren....570
13.5.2.2 Wie Sie die Suche im internen Verzeichnis aktivieren oder deaktivieren....571
13.5.3 Externes Verzeichnis....571
13.5.3.1 CSV-Datei vom lokalen Dateisystem in das externe Verzeichnis importieren....572
13.5.3.2 Zugriff auf eine externe Datenbank für das externe Verzeichnis hinzufügen....574
13.5.3.3 CSV-Datei aus dem externen Verzeichnis exportieren....575
13.5.4 Externes Offline-Verzeichnis (LDAP)....575
13.5.4.1 Wie Sie ein externes Offline-Verzeichnis (LDAP) für PC-Clients hinzufügen....576
13.5.4.2 Wie Sie ein externes Offline-Verzeichnis (LDAP) für PC-Clients löschen....577
13.5.4.3 Wie Sie ein externes Offline-Verzeichnis (LDAP) für Systemtelefone hinzufügen....577
13.5.5 Systemverzeichnis....578
13.5.6 Unified-Verzeichnis....578
13.5.6.1 Leistungsmerkmale....579
13.5.6.2 Regeln und Konventionen....582
13.5.6.3 Funktionale Grenzen....583
13.5.6.4 Unified-Verzeichnis in vernetzten Systemen....584
13.5.6.5 So importieren Sie Kontakte in Unified Directory....585
13.5.6.6 So bearbeiten oder hinzufügen Sie neue Unified Directory-Kontakte....586
13.5.7 Abteilungen....587
13.5.7.1 Abteilung hinzufügen....587
13.5.7.2 Teilnehmer einer Abteilung zuordnen....587
13.5.7.3 Abteilung bearbeiten....588
13.5.7.4 Wie Sie eine Abteilung entfernen....588
13.5.8 Favoritenliste....588
13.5.9 Journal....589
13.5.9.1 Maximale Aufbewahrungsdauer für das Journal ändern....590
13.6 Anrufe....591
13.6.1 Desktop-Wahl und Clipboard-Wahl....591
13.6.2 PopUp-Fenster....592
13.6.3 Aufzeichnen von Anrufen....592
13.6.3.1 Aufzeichnung von Anrufen aktivieren oder deaktivieren....592
13.6.3.2 Ansage für Aufzeichnung aktivieren oder deaktivieren....593
13.6.3.3 Hinweiston für eine Aufzeichnung aktivieren oder deaktivieren....593
13.7 Konferenzen....594
13.7.1 Konferenzmanagement....594
13.7.1.1 Wie Sie die Einwahlnummer für einen virtuellen Konferenzraum ändern....598
13.7.1.2 Mehrere externe Konferenzteilnehmer zulassen oder verhindern....598
13.7.1.3 Wie Sie den Konferenzton aktivieren oder deaktivieren....599
13.7.1.4 Wie Sie die Zeitspanne für automatisches Beenden von Konferenzen ändern....599
13.7.1.5 Wie Sie Details zu einer gespeicherten Konferenz abfragen....600
13.7.1.6 Wie Sie eine gespeicherte Konferenz löschen....600
13.7.1.7 Konfiguration der Aufzeichnung von Konferenzen....600
13.7.2 Ad-hoc-Konferenz....601
13.7.3 Geplante Konferenz....601
13.7.4 Permanente Konferenz....603
13.7.5 Offene Konferenz....604
13.8 Web Collaboration....605

13.8.1 Wie Sie die Verbindung zum Web Collaboration Server (Custom Server) konfigurieren....606
13.8.2 Wie Sie die Verbindung zum Web Collaboration Server (Public Server) konfigurieren....607
13.8.3 Wie Sie die Verbindung zum Web Collaboration Server deaktivieren....608
13.9 Instant Messaging....608
13.9.1 Sofortnachricht versenden....608
13.9.1.1 Sofortnachrichten aktivieren oder deaktivieren....609
13.10 AutoAttendant....609
13.10.1 Persönlicher AutoAttendant....610
13.11 Sprach- und Faxnachrichten....610
13.11.1 Voicemail-Postfach....610
13.11.1.1 Wie Sie die Rufnummer der Sprachbox konfigurieren....612
13.11.1.2 Wie Sie die Rufweiterschaltung zur Sprachbox konfigurieren....613
13.11.1.3 Parameter der Sprachbox konfigurieren....613
13.11.1.4 Wie Sie die Aufbewahrungsdauer für Sprachnachrichten konfigurieren....614
13.11.1.5 Kennwortabfrage der Sprachbox aktivieren oder deaktivieren....614
13.11.1.6 Wie Sie eine Info für empfangene Sprachnachrichten konfigurieren....614
13.11.1.7 Wie Sie die Briefkastentaste für die Abfrage von Sprachnachrichten konfigurieren....615
13.11.2 Ansagen der Sprachbox....615
13.11.2.1 Ansage für die Sprachbox importieren....617
13.11.2.2 Sprache für Ansagen der Sprachbox ändern....617
13.11.3 Faxbox....618
13.11.3.1 Wie Sie eine Faxbox für Teilnehmer hinzufügen....618
13.11.3.2 Wie Sie den Dateityp für gespeicherte Faxnachrichten (UC Suite) konfigurieren....619
13.11.4 Senden von Faxnachrichten mit Fax Printer....619
13.11.4.1 Zentrales Fax-Deckblatt hinzufügen....620
13.11.4.2 Zentrales Fax-Deckblatt bearbeiten....621
13.11.4.3 Kopfzeile für Fax Printer hinzufügen....621
13.11.4.4 Kopfzeile für Fax Printer ändern....621
13.11.4.5 Wie Sie eine Kopfzeile für Fax Printer löschen....622
13.11.5 Benachrichtigungsdienst für neue Nachrichten (UC Suite)....622
13.11.6 E-Mail-Versand....623
13.11.6.1 E-Mail-Versand konfigurieren....623
13.11.7 SMS-Template....624
13.11.7.1 SMS-Template hinzufügen....625
13.11.7.2 SMS-Template bearbeiten....626
13.11.7.3 Wie Sie ein SMS-Template entfernen....627
13.11.8 Fax over IP (T.38 / G.711-Fax)....627
13.11.8.1 Wie Sie Fax over IP (T.38-Fax) aktivieren oder deaktivieren....628
13.12 Überblick über Integration von Microsoft Office 365....628
13.12.1 OpenScape Business-System unter Verwendung von einfacher Authentifizierung mit Microsoft Office 365 verbinden....629
13.12.2 OpenScape Business-System unter Verwendung von moderner Authentifizierung mit Microsoft Office 365 verbinden....635
13.12.3 So überprüfen Sie, ob die Funktionen der Microsoft Office 365-Integration konfiguriert sind....635

14 Funktionen am Telefon....637
14.1 Anrufen....637
14.1.1 Ziffernwahl....637
14.1.2 Blockwahl....637
14.1.3 Keypad-Wahl....637
14.1.4 Wahlendeerkennung....638
14.1.5 Editieren der Wahl....638
14.1.5.1 Wie Sie das Editieren der Wahl aktivieren oder deaktivieren....639
14.1.6 Wahlwiederholung....639
14.1.6.1 Wie Sie die automatische Wahlwiederholung aktivieren oder deaktivieren....640
14.1.7 Kurzwahl zentral KWZ....640

14.1.7.1 Wie Sie ein Kurzwahlziel hinzufügen ... 642
14.1.7.2 Kurzwahlziele aus einer XML-Datei importieren ... 642
14.1.7.3 Wie Sie Kurzwahlziele in eine XML-Datei exportieren ... 643
14.1.7.4 Wie Sie Kurzwahlziele bearbeiten ... 643
14.1.8 Kurzwahl individuell (KWI) ... 644
14.1.9 Direktruf ... 644
14.1.10 Direktansprechen / Direktantworten ... 645
14.1.10.1 Wie Sie den Direktansprechschutz für Teilnehmer aktivieren oder deaktivieren ... 646
14.1.11 Assoziierte Wahl ... 646
14.1.12 Leitungsvormerken ... 647
14.1.12.1 Wie Sie Leitungsvormerken aktivieren oder deaktivieren ... 647
14.1.13 Privatleitung ... 648
14.2 Anrufsignalisierung, Rufnummernanzeige ... 648
14.2.1 Unterschiedliche Anrufsignalisierung ... 648
14.2.2 Calling Line Identification Presentation (CLIP) ... 649
14.2.2.1 Wie Sie einstellbare CLIP aktivieren oder deaktivieren ... 649
14.2.3 Calling Line Identification Restriction (CLIR) ... 650
14.2.3.1 Wie Sie die Unterdrückung der Teilnehmerrufnummer aktivieren oder deaktivieren ... 650
14.2.4 Connected Line Identification Presentation (COLP) ... 651
14.2.4.1 Wie Sie die Rufnummernübermittlung des Angerufenen aktivieren oder deaktivieren ... 651
14.2.5 Rufnummernunterdrückung des Angerufenen (COLR) ... 651
14.2.6 CLIP no screening (Übermittlung kundenspezifischer Rufnummerninformationen) ... 652
14.2.6.1 Wie Sie CLIP no screening konfigurieren ... 652
14.2.7 CLIP für analoge Endgeräte ... 653
14.2.8 Stiller Ruf / Ruhe ... 653
14.2.9 Rufnummernumwertung in Namen bei Kurzwahl zentral ... 653
14.3 Funktionen während der Verbindung ... 653
14.3.1 Halten ... 653
14.3.2 Parken ... 654
14.3.3 Rückfrage ... 655
14.3.4 Makeln ... 655
14.3.5 Übergeben ... 655
14.3.6 Wiederanruf ... 656
14.3.7 Call Supervison ... 657
14.3.7.1 Wie Sie Call Supervision für einen Teilnehmer aktivieren oder deaktivieren ... 658
14.3.8 Diskretes Ansprechen ... 658
14.3.9 Live Call Recording (Voice Recording; Sprachaufzeichnung) ... 660
14.4 Steuern der Erreichbarkeit ... 661
14.4.1 Anrufumleitung ... 661
14.4.1.1 Wie Sie eine Rufweiterschaltung konfigurieren ... 663
14.4.2 Anrufumleitung (CF) ... 665
14.4.2.1 Wie Sie Anrufumleitung über analoge Amtsleitungen aktivieren oder deaktivieren ... 666
14.4.2.2 Wie Sie eine Anrufumleitung nach Anrufumleitung zum externernen Ziel aktivieren oder deaktivieren ... 667
14.4.3 Anrufumleitung nach Zeit ... 667
14.4.4 Rufweiterschaltung im Amt (nicht für USA) ... 668
14.4.5 Rufzuordnung ... 668
14.4.5.1 Wie Sie eine Rufzuordnung konfigurieren ... 668
14.4.6 Rufzuschaltung ... 669
14.4.7 Anrufe abweisen ... 670
14.4.8 Zurückstellen eines Anrufs ... 670
14.4.9 Anrufschutz ... 671
14.5 Optimieren der Kommunikationsabläufe ... 671
14.5.1 Rückruf ... 672
14.5.2 Anklopfen ... 673
14.5.2.1 Wie Sie Anklopfen aktivieren oder deaktivieren ... 674

14.5.2.2 Wie Sie sofortiges Anklopfen durch Vermittlungsplatz aktivieren oder deaktivieren....674
14.5.3 Aufschalten....675
14.5.3.1 Wie Sie einen internen Teilnehmer für das Aufschalten berechtigen....675
14.5.3.2 Wie Sie den Abwurfplatz für das Aufschalten berechtigen....676
14.5.4 Abwesenheitstexte....676
14.5.4.1 Wie Sie einen Abwesenheitstext ändern....676
14.5.5 Mitteilungstexte....677
14.5.5.1 Wie Sie einen Mitteilungstext ändern....677
14.5.6 Assoziierte Dienste....677
14.5.6.1 Wie Sie Assoziierte Dienste aktivieren oder deaktivieren....678
14.5.7 DISA....678
14.5.7.1 Wie Sie die DISA-Berechtigung für einen Teilnehmer aktivieren oder deaktivieren....679
14.5.7.2 Wie Sie eine DISA-Nummer konfigurieren....680
14.5.7.3 Wie Sie den DISA-Sicherheitsmodus konfigurieren....680
14.5.8 Flex Call/Mobile PIN....681
14.5.9 Relocate/Rufnummerntausch....681
14.5.9.1 Wie Sie Relocate/Rufnummertausch systemweit freigeben....682
14.5.10 Rücksetzen aktivierter Leistungsmerkmale....682
14.5.11 Prozeduren....682
14.5.12 Weckeinrichtung und Termine....684
14.6 Übersicht über Funktionen und Codes....684

15 Arbeiten im Team (Gruppen)....689
15.1 Anrufübernahmegruppe, Gruppenruf und Sammelanschluss....689
15.1.1 Anrufübernahmegruppe....689
15.1.2 Gruppenruf....691
15.1.3 Gruppennummer....695
15.1.4 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Wizards....699
15.1.4.1 Wie Sie eine Anrufübernahmegruppe konfigurieren....699
15.1.4.2 Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen....700
15.1.4.3 Wie Sie einen Gruppenruf (Gruppe) hinzufügen....700
15.1.4.4 Wie Sie einen Gruppenruf (Gruppe) ändern....702
15.1.4.5 Wie Sie einen Gruppenruf (Gruppe) löschen....703
15.1.4.6 Wie Sie ein Mitglied zum Gruppenruf (Gruppe) hinzufügen oder löschen....703
15.1.4.7 Wie Sie einen Sammelanschluss hinzufügen....704
15.1.4.8 Wie Sie einen Sammelanschluss ändern....705
15.1.4.9 Wie Sie einen Sammelanschluss löschen....706
15.1.4.10 Wie Sie ein Mitglied zum Sammelanschluss hinzufügen oder löschen....706
15.1.5 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Experten-Modus....707
15.1.5.1 Wie Sie die Anzeige der Rufnummer und des Namens des Anrufers aktivieren oder deaktivieren....707
15.1.5.2 Wie Sie den Aufmerksamkeitston aktivieren oder deaktivieren....708
15.1.5.3 Wie Sie die Anrufübernahme von Wiederanrufen aktivieren oder deaktivieren....708
15.1.5.4 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) hinzufügen....709
15.1.5.5 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) anzeigen oder ändern....710
15.1.5.6 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) löschen....710
15.1.5.7 Wie Sie ein Mitglied zum Gruppenruf (Freifall oder Anklopfen) hinzufügen oder löschen....710
15.1.5.8 Wie Sie den Anklopfschutz für Gruppenmitglied ein- oder ausschalten....711
15.2 Teamschaltung / Team-Gruppe und Chef/Sekretär / Top-Gruppe....712
15.2.1 Teamschaltung / Team-Gruppe....712
15.2.2 Chef/Sekretär / Top-Gruppe....716
15.2.3 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Wizards....720
15.2.3.1 Wie Sie eine Teamschaltung / Team-Gruppe hinzufügen....721

15.2.3.2 Wie Sie eine Teamschaltung / Team-Gruppe ändern....722
15.2.3.3 Wie Sie eine Teamschaltung / Team-Gruppe löschen....723
15.2.3.4 Wie Sie eine Chef/Sekretär- / Top-Gruppe hinzufügen....724
15.2.3.5 Wie Sie eine Chef/Sekretär- / Top-Gruppe ändern....725
15.2.3.6 Wie Sie eine Chef/Sekretär- / Top-Gruppe löschen....726
15.2.4 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Experten-Modus....726
15.2.4.1 Wie Sie ein Mitglied zur Teamschaltung / Team-Gruppe hinzufügen oder löschen....727
15.2.4.2 Wie Sie ein Mitglied einer Teamschaltung / Team-Gruppe ändern....727
15.2.4.3 Wie Sie die Eigenschaften der Mitglieder einer Teamschaltung / Team-Gruppe ändern....728
15.2.4.4 Wie Sie die Telefon-Tastenbelegung für Teamschaltung / Team-Gruppe ändern....728
15.2.4.5 Wie Sie eine Faxbox zur Teamschaltung / Team-Gruppe hinzufügen....729
15.2.4.6 Wie Sie ein Mitglied zur Chef/Sekretär / Top-Gruppe hinzufügen oder löschen....729
15.2.4.7 Wie Sie ein Mitglied einer Chef/Sekretär / Top-Gruppe ändern....730
15.2.4.8 Wie Sie die Eigenschaften der Mitglieder einer Chef/Sekretär / Top-Gruppe ändern....730
15.2.4.9 Wie Sie eine Faxbox zur Chef/Sekretär / Top-Gruppe hinzufügen....731
15.3 Basic-MULAP und Chef-MULAP....731
15.3.1 Basis-MULAP....731
15.3.2 Chef-MULAP....734
15.3.3 Konfiguration von Basic-MULAPs und Chef-MULAPs....737
15.3.3.1 Basic-MULAP hinzufügen....737
15.3.3.2 Wie Sie Basic-MULAP anzeigen oder ändern....738
15.3.3.3 Wie Sie eine Basic-MULAP löschen....738
15.3.3.4 Wie Sie ein Mitglied zur Basic-MULAP hinzufügen oder löschen....739
15.3.3.5 Wie Sie ein Mitglied einer Basic-MULAP ändern....739
15.3.3.6 Chef-MULAP hinzufügen....740
15.3.3.7 Wie Sie eine Chef-MULAP anzeigen oder ändern....740
15.3.3.8 Wie Sie eine Chef-MULAP löschen....741
15.3.3.9 Wie Sie ein Mitglied zur Chef-MULAP hinzufügen oder löschen....741
15.3.3.10 Wie Sie ein Mitglied einer Chef-MULAP ändern....742
15.3.3.11 Basic-MULAP in Gruppe hinzufügen....742
15.4 Sprachbox-Gruppe und Faxbox-Gruppe....743
15.4.1 Sprachbox-Gruppe....743
15.4.2 Faxbox-Gruppe....744
15.4.3 Konfiguration von Sprachbox-Gruppen und Faxbox-Gruppen....744
15.4.3.1 Wie Sie eine Sprachbox-Gruppe hinzufügen....745
15.4.3.2 Wie Sie eine Sprachbox-Gruppe anzeigen oder ändern....745
15.4.3.3 Wie Sie eine Sprachbox-Gruppe löschen....746
15.4.3.4 Wie Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen oder löschen....746
15.4.3.5 Wie Sie ein Mitglied einer Sprachbox-Gruppe ändern....746
15.4.3.6 Faxbox-Gruppe konfigurieren....747
15.4.3.7 Wie Sie eine Faxbox-Gruppe anzeigen oder ändern....748
15.4.3.8 Faxbox-Gruppe löschen....748
15.4.3.9 Mitglied zur Faxbox-Gruppe hinzufügen oder löschen....748
15.5 Direktansprechen für Gruppen....749
15.5.1 Durchsage an Gruppe....749
15.5.2 Übergabe an Gruppe aus Durchsage....750
15.6 Anrufverteilung (UCD Uniform Call Distribution)....750
15.6.1 Anrufverteilung / UCD-Gruppe....751
15.6.1.1 Wie Sie eine Anrufverteilung / UCD-Gruppen konfigurieren....752
15.6.2 UCD-Agenten....753
15.6.2.1 Wie Sie UCD-Agenten hinzufügen oder löschen....755
15.6.3 Nachbearbeitung....755
15.6.3.1 Wie Sie die automatische Nachbearbeitungszeit ändern....756
15.6.4 Priorisierte Anrufordnung....756
15.6.4.1 Wie Sie die Priorisierung der Anrufordnung ändern....757

15.6.5 UCD-Anrufe automatisch annehmen..... 757
15.6.5.1 Wie Sie das automatische Annehmen von UCD-Anrufen ändern..... 758
15.6.6 UCD-Warteschlange..... 758
15.6.6.1 Wie Sie eine UCD-Warteschlange ändern..... 759
15.6.7 UCD-Überlauf..... 760
15.6.7.1 Wie Sie den UCD-Überlauf ändern..... 760
15.6.8 UCD-Nachtschaltung..... 761
15.6.9 Ansagen / Wartemusik bei UCD..... 761
15.6.9.1 Wie Sie Ansagen / Wartemusik bei UCD ändern..... 762
15.6.10 Übergabe an UCD-Gruppen..... 762
15.6.10.1 Wie Sie die Wiederanrufzeit für übergebene Gespräche an UCD-Gruppen ändern..... 763
15.6.11 Auslösen von UCD-Anrufen über analoge Leitungen..... 763
15.6.11.1 Wie Sie die Auslösezeit für UCD-Anrufe über analoge Leitungen ändern..... 764

16 Anruf-Routing..... 765
16.1 Berechtigungen (Wahlkontrolle)..... 765
16.1.1 Berechtigungsgruppen und Berechtigungsklassen..... 765
16.1.1.1 Wie Sie den Namen einer Berechtigungsgruppe ändern..... 766
16.1.1.2 Wie Sie die Berechtigungsklassen einer Berechtigungsgruppe ändern..... 766
16.1.1.3 Wie Sie alle Teilnehmer einer Berechtigungsgruppe anzeigen..... 767
16.1.2 Erlaubnis- und Verbotslisten..... 767
16.1.2.1 Wie Sie eine Notrufnummernliste erstellen..... 768
16.1.2.2 Wie Sie eine Erlaubnis- und eine Verbotsliste erstellen..... 769
16.1.2.3 Wie Sie weitere Erlaubnislisten erstellen..... 769
16.1.2.4 Wie Sie weitere Verbotslisten erstellen..... 770
16.1.2.5 Wie Sie alle Rufnummern einer Verbotsliste anzeigen..... 770
16.1.2.6 Wie Sie alle Rufnummern einer Erlaubnisliste anzeigen..... 770
16.1.2.7 Wie Sie den Auswertungsfilter für eine Verbotsliste ändern..... 771
16.1.3 Blacklist..... 771
16.1.3.1 Wie Sie im Experten-Modus in eine Blacklist für kommende Gespräche erstellen..... 772
16.1.3.2 Bearbeiten/Löschen von Rufnummern in der Blacklist..... 773
16.1.3.3 Anzeige von Rufnummern in der Blacklist..... 774
16.1.3.4 Wie Sie in der Einrichtung eine Blacklist für kommende Gespräche erstellen..... 774
16.1.4 Nachtschaltung..... 775
16.1.4.1 Wie Sie Berechtigungen für die manuelle Nachtschaltung vergeben..... 776
16.1.4.2 Wie Sie Berechtigungen für die manuelle Nachtschaltung löschen..... 776
16.1.4.3 Zeitgesteuerte Nachtschaltung konfigurieren..... 777
16.1.4.4 Wie Sie einen Sondertag für die zeitgesteuerte Nachtschaltung konfigurieren..... 777
16.1.4.5 Wie Sie einen Sondertag für die zeitgesteuerte Nachtschaltung löschen..... 778
16.1.5 Automatische Berechtigungsumschaltung nach Zeit..... 778
16.1.5.1 Zeitplan..... 779
16.1.6 VBZ (Verkehrsbeziehungen)..... 780
16.1.6.1 VBZ-Gruppen (Verkehrsbeziehungsgruppen)..... 780
16.1.6.2 Zuordnung der KWZ-Nummern zu VBZ-Gruppen..... 781
16.1.6.3 Wie Sie Teilnehmer einer VBZ-Gruppe zuweisen..... 781
16.1.6.4 Wie Sie die Leitung einer VBZ-Gruppe zuweisen..... 782
16.1.6.5 Wie Sie die VBZ-Matrix ändern..... 782
16.1.7 Zentrales Codeschloss, Berechtigungsumschaltung..... 782
16.1.8 Individuelles Codeschloss (Telefon abschließen)..... 783
16.1.8.1 Wie Sie das individuelle Codeschloss zurücksetzen..... 783
16.1.9 R-Gesprächsschutz je Amtsleitung (nur für Brasilien)..... 784
16.1.10 R-Gesprächsschutz je Teilnehmer (nur für Brasilien)..... 784
16.2 LCR (Least Cost Routing, Leitweglenkung)..... 784
16.2.1 LCR-Funktionalität..... 784
16.2.1.1 Wie Sie die LCR freigeben..... 787
16.2.2 LCR-Wahlplan..... 788

16.2.2.1 Wie Sie den Wahlplan bearbeiten....789
16.2.3 LCR-Wegetabelle....790
16.2.3.1 Wie Sie Wegetabellen bearbeiten....790
16.2.4 LCR-Berechtigung....791
16.2.4.1 Wie Sie die LCR-Berechtigung vergeben und ändern....792
16.2.5 LCR-Wahlregeln....792
16.2.5.1 Wie Sie Wahlregeln bearbeiten....794
16.2.6 Netzanbieter....794
16.2.7 Gezielte Belegung von Amtsleitungen....795
16.2.7.1 Wie Sie die Kennzahl für gezielte Belegung von ISDN-Amtsleitungen konfigurieren....796
16.2.7.2 Wie Sie Kennzahlen für die gezielte Amtsbelegung anzeigen....796
16.3 Wahlbewertung und Call-Routing....797
16.3.1 Überblick Call Routing / LCR....798
16.3.2 Flußdiagramm Wahlbewertung....800
16.3.3 Call Routing und LCR im Netzverbund....801
16.3.3.1 Dediziertes Gateway....803
16.3.4 Szenarien: Wahlbewertung und Call Routing....804
16.3.4.1 Teilnehmer A ruft Teilnehmer B über Internrufnummer....805
16.3.4.2 Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer....805
16.3.4.3 Teilnehmer A ruft externen Teilnehmer über Amt....806
16.3.4.4 ISDN-Amt ruft Teilnehmer A....807
16.3.4.5 Sonderkonfigurationen....808
16.3.4.6 Teilnehmer A ruft Teilnehmer C über Internrufnummer....809
16.3.4.7 Teilnehmer A ruft Teilnehmer C über öffentliche Rufnummer im Netzverbund....810
16.3.4.8 ISDN-Amt ruft Teilnehmer C....813
16.3.4.9 ISDN-Amt Gateway 1 ruft Teilnehmer D....814
16.3.4.10 Teilnehmer D ruft externen Teilnehmer über Amt....817
16.4 Notrufe....819
16.4.1 Röchelschaltung / Hotline....820
16.4.1.1 Wie Sie einen Hotlineziel konfigurieren und ändern....821
16.4.1.2 Wie Sie die Röchelzeit ändern....821
16.4.1.3 Wie Sie Röcheln oder Hotline für einen Teilnehmer konfigurieren....821
16.4.2 Leitungstrennung für einen Notruf....822
16.4.2.1 Wie Sie die Leitungstrennung für einen Notruf aktivieren oder deaktivieren....822
16.4.3 Nur für USA, Kanada: Notrufdienst E911....823
16.4.3.1 Wie Sie CLIP / Lin bearbeiten....823
16.4.4 Notrufe in Kombination mit Mobile Logon....823
16.4.4.1 Konfiguration des Notrufszenarios....824
16.4.5 Notrufdienst E112 (für Europa)....826
16.4.5.1 Wie Sie eine ITSP Loc-ID zu einem Teilnehmer hinzufügen....827
16.5 Anrufsteuerungsdienst (Call Admission Control)....827
16.5.1 Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP....827
16.5.2 Einschränkung des Bandbreitenbedarfs bei Gateway-Gesprächen....828
16.5.3 Einschränkung der Anzahl der Gespräche in Vernetzungszenarien....828
16.6 Gemeinschaftsanlage....828
16.6.1 Kurzwahl zentral in Gemeinschaftsanlagen....830

17 Attendants....831
17.1 AutoAttendant....831
17.1.1 Company AutoAttendant (UC Smart)....833
17.1.1.1 Wie Sie einen eingerichteten Company AutoAttendant konfigurieren....834
17.1.1.2 Wie Sie einen neuen Company AutoAttendant einrichten....835
17.1.2 Company AutoAttendant (UC Suite)....837
17.1.2.1 Zeitpläne....837
17.1.2.2 Vorlagen (Templates)....845
17.2 OpenStage Attendant....847

17.3 OpenScape Business Attendant..... 848
17.3.1 OpenScape Business BLF..... 851
17.3.2 Einrichtebeispiele für OpenScape Business Attendant, OpenScape Business BLF..... 852
17.3.2.1 Szenario 1: OpenScape Business Attendant an ein OpenScape Business Einzelsystem angeschlossen..... 852
17.3.2.2 Szenario 2: Zwei oder mehr OpenScape Business Attendants, die an ein OpenScape Business Einzelsystem angeschlossen sind..... 858
17.3.2.3 Szenario 3: OpenScape Business Vernetzung mit jeweils eigenen OpenScape Business Attendants (netzweite BLF und Anwesenheitsstatus über WSI)..... 860
17.3.2.4 Szenario 4: OpenScape Business-Vernetzung mit zentralem OpenScape Business Attendant (netzweite BLF und Anwesenheitsstatus über WSI)..... 860
17.3.2.5 Szenario 5: OpenScape Business BLF an einem OpenScape Business Einzelsystem..... 861
17.3.2.6 Szenario 6: OpenScape Business BLF an einem OpenScape Business Netzverbund (BLF und Anwesenheitsstatus über WSI)..... 863
17.4 myAttendant..... 863
17.4.1 Teilnehmerverwaltung..... 865
17.4.2 Nachrichtencenter 865
17.4.3 Szenario 1: Wie Sie myAttendant an einem OpenScape Business Einzelsystem einrichten..... 866
17.4.4 Szenario 2: Wie Sie zwei oder mehrere myAttendants an einem OpenScape Business Einzelsystem einrichten..... 867
17.4.5 Szenario 3: Wie Sie ein OpenScape Business-Netzwerk mit zentralem myAttendant einrichten..... 868
17.5 Abwurfplatz..... 869
17.5.1 Wie Sie Abwurfplatz und Abwurfkriterien konfigurieren..... 871
17.5.2 Wie Sie einen zentralen Abwurfplatz konfigurieren..... 872
17.5.3 Wie Sie Abwurf bei Codeschloss konfigurieren..... 872
17.5.4 Abwurf bei Ansage konfigurieren..... 872

18 Multimedia Contact Center..... 873
18.1 Contact Center Clients..... 873
18.1.1 myAgent..... 874
18.1.2 Voraussetzungen für myAgent..... 875
18.1.3 myReports..... 877
18.1.3.1 Wie Sie myReports-Administrator-Kennwort zurücksetzen..... 879
18.1.4 Voraussetzungen für myReports..... 879
18.1.5 Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients..... 881
18.2 Agenten..... 882
18.2.1 Berechtigungsabhängige Funktionen für Agenten..... 882
18.2.2 Bevorzugte Agenten..... 883
18.2.3 Agent in mehreren Warteschlangen..... 884
18.2.4 Contact Center Pausen..... 884
18.2.5 An- und Abmeldung des Agenten per Telefon..... 884
18.3 Warteschlangen und Zeitpläne..... 888
18.3.1 Warteschlangen..... 888
18.3.2 Zeitpläne..... 890
18.3.3 Nachbearbeitung..... 899
18.3.4 Servicegrad..... 899
18.3.5 Wandanzeige (Wallboard)..... 900
18.3.6 Agentenrückruf..... 900
18.4 VIP-Betreuung..... 900
18.4.1 VIP-Anruferpriorität..... 900
18.4.2 VIP-Rufliste..... 901
18.5 Rückfalllösung (Fallback-Lösung)..... 901
18.6 Konfiguration des Contact Centers..... 905
18.6.1 Beispiel für eine Contact-Center-Konfiguration..... 905
18.6.1.1 Wie Sie UCD-Gruppen für das Beispiel-Contact-Center konfigurieren..... 907

18.6.1.2 Wie Sie eine Rückfalllösung (Fallback-Lösung) für das Beispiel-Contact-Center konfigurieren....908
18.6.1.3 Wie Sie einen Teilnehmer als Agent für das Beispiel-Contact-Center konfigurieren....909
18.6.1.4 Ansagen für das Beispiel-Contact-Center aufnehmen....910
18.6.1.5 Ansagen für das Beispiel-Contact-Center laden....911
18.6.1.6 Den Zeitplan Standard Schedule XYZ für das Beispiel-Contact-Center hinzufügen....911
18.6.1.7 Den Zeitplan Standard Schedule Hotline für das Beispiel-Contact-Center hinzufügen....916
18.6.1.8 Warteschlangen für das Beispiel-Contact-Center hinzufügen....918
18.6.1.9 Agenten den Warteschlangen des Beispiel-Contact-Centers zuordnen....921
18.6.2 Vorgehensweise bei der Konfiguration....922
18.6.2.1 Wie Sie UCD-Gruppen für das Contact Center konfigurieren....923
18.6.2.2 Wie Sie einen Teilnehmer als Agent konfigurieren....923
18.6.2.3 Individuelle Ansage für das Contact Center aufnehmen....924
18.6.2.4 Individuelle Ansage für das Contact Center laden....925
18.6.2.5 Zeitplan hinzufügen....925
18.6.2.6 Zeitplan ändern....929
18.6.2.7 Zeitplan löschen....930
18.6.2.8 Regel (CCV) als PDF-Datei speichern....931
18.6.2.9 Regel (CCV) als Backup-Datei herunterladen....931
18.6.2.10 Heruntergeladene Regel (CCV) in einem Sicherungsdateiformat hochladen....932
18.6.2.11 Warteschlange hinzufügen....932
18.6.2.12 Warteschlange ändern....936
18.6.2.13 Wie Sie eine Warteschlange aktivieren oder deaktivieren....939
18.6.2.14 Wie Sie einen Pilot für eingehende Faxnachrichten in Warteschlangen konfigurieren....939
18.6.2.15 Wie Sie Sollwerte für Servicegrad festlegen....940
18.6.2.16 Wie Sie die VIP-Anruferpriorität festlegen....940
18.6.2.17 Wie Sie eine VIP-Rufliste bearbeiten....941
18.6.2.18 Bevorzugten Agenten festlegen....942
18.6.2.19 Wie Sie einen bevorzugten Agenten löschen....943
18.6.2.20 Contact Center-Pause hinzufügen....943
18.6.2.21 Wie Sie eine Contact Center-Pause ändern....944
18.6.2.22 Contact Center-Pause löschen....944
18.6.2.23 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" hinzufügen....944
18.6.2.24 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" ändern....945
18.6.2.25 Nachbearbeitungsgrund für "Einfache Nachbearbeitung" löschen....945
18.6.2.26 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" hinzufügen....946
18.6.2.27 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" ändern....947
18.6.2.28 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" löschen....947
18.6.2.29 Warteschlange einen Agenten zuordnen....948
18.6.2.30 Agenten aus einer Warteschlange entfernen....949
18.7 Hinweise zum Einsatz des Contact Centers....949
18.7.1 Einschränkungen beim Betrieb des Contact Centers....949
18.8 Hinweise zum Einsatz von DECT-Telefonen....952
18.9 Berichte....953
18.9.1 Vordefinierte Berichtsvorlagen....954

19 Mobility....955
19.1 Integrierte Mobilitätslösungen....955
19.2 Mobilität unterwegs....955
19.2.1 myPortal to go....956
19.2.1.1 Voraussetzungen:myPortal to go....958
19.2.2 Mobility Entry....959
19.2.3 Vergleich Mobile Clients und Mobility Entry....961
19.2.4 Abhängigkeiten für Mobile Clients und Mobility Entry....963
19.2.5 One Number Service....964
19.2.6 Dual-Mode-Telefonie....965

19.2.7 Konfiguration von myPortal to go und Mobility Entry 965
19.2.7.1 Wie Sie ein GSM-Mobiltelefon integrieren..... 966
19.2.7.2 Wie Sie ein Dual-Mode-Telefon (GSM/WLAN) mit HFA- oder SIP-Client integrieren..... 968
19.2.7.3 Wie Sie die Web-Schnittstelle für Mobiltelefone und Web-Clients aktivieren..... 970
19.2.7.4 Wie Sie die Mobiltelefon-Integration löschen..... 970
19.3 Mobilität im Büro..... 971
19.3.1 Desk Sharing..... 971
19.3.2 Integrierte Cordless-Lösung..... 972
19.3.2.1 Systemübersicht..... 973
19.3.2.2 Cordless-Baugruppenanschaltung..... 974
19.3.2.3 Systemausbau..... 975
19.3.2.4 Cordless/DECT-Telefone..... 976
19.3.2.5 Bedeutung der Ergebnisse beim Test des Funkbereichs..... 977
19.3.3 Konfiguration der integrierten Cordless-Lösung..... 979
19.3.3.1 Wie Sie die DECT-Systemkennung eingeben und weitere Cordless-Parameter (systemweite Daten) konfigurieren..... 979
19.3.3.2 Wie Sie Cordless-Basisstationen konfigurieren..... 980
19.3.3.3 Wie Sie DECT-Telefone erstmalig konfigurieren..... 981
19.3.3.4 Wie Sie ein DECT-Telefon (OpenStage/Gigaset-Mobilteil) an Cordless anmelden..... 982
19.3.3.5 Wie Sie weitere DECT-Telefone hinzufügen..... 983
19.3.3.6 Wie Sie DECT-Telefone löschen..... 984
19.3.3.7 Wie Sie die Multi-SLC-Parameter konfigurieren..... 984
19.3.3.8 Wie Sie die Daten zu den Basisstationen abfragen..... 985
19.3.3.9 Wie Sie den Hinweiston der Message Waiting Indication (MWI) für DECT-Telefone aktivieren..... 985
19.3.3.10 Wie Sie den Anmeldestatus der DECT-Telefone abfragen..... 986
19.3.4 Cordless IP..... 986
19.3.5 WLAN-Telefone und Access Points..... 987
19.3.5.1 Anforderungen an das WLAN..... 987
19.4 Heim-Mobilität..... 987
19.4.1 Konfiguration für VPN..... 988
19.4.2 Konfiguration für SIP-Gerät@Home..... 989
19.4.3 Konfiguration für Systemgerät@Home..... 991
19.4.4 Wie Sie Gerät@Home aktivieren..... 993
19.4.5 Software-Update für Systemgerät (HFA) @Home..... 993
19.4.6 Wie Sie einen STUN-Server für Gerät@Home angeben..... 995

20 Sicherheit..... 996
20.1 Firewall..... 996
20.1.1 Porthandling..... 996
20.1.1.1 Portfreigabe..... 997
20.1.1.2 Wie Sie die Portfreigabe konfigurieren..... 998
20.1.1.3 Port-Verwaltung..... 998
20.1.1.4 Wie Sie globale Port-Manager-Einstellungen ändern..... 998
20.1.2 NAT..... 999
20.1.2.1 Wie Sie eine NAT-Regel konfigurieren..... 1000
20.1.2.2 Wie Sie mehrere NAT-Regeln mit dem NAT-Tabelleneditor konfigurieren..... 1000
20.1.2.3 Wie Sie eine NAT-Regel löschen..... 1001
20.1.3 Application Firewall..... 1002
20.1.3.1 Wie Sie die Konfiguration der Application Firewall anzeigen..... 1003
20.1.3.2 Wie Sie Dienste über die Application Firewall einschränken..... 1003
20.1.3.3 Wie Sie die Konfiguration der Application Firewall löschen..... 1004
20.1.4 Diensteverwaltung (OpenScape Business S)..... 1004
20.1.4.1 Wie Sie Dienste hinzufügen oder sperren..... 1004
20.2 Signaling- und Payload-Encryption (SPE)..... 1005
20.2.1 Wie Sie SPE Unterstützung aktivieren oder deaktivieren..... 1007

20.2.2 Wie Sie SPE-Sicherheitseinstellungen ändern..... 1007
20.2.3 Wie Sie ein SPE-Zertifikat und den privaten Schlüssel importieren (PKCS#12)..... 1007
20.2.4 Wie Sie das SPE CA-Zertifikat importieren..... 1008
20.2.5 Wie Sie SPE für einen Teilnehmer aktivieren oder deaktivieren..... 1008
20.3 Virtual Private Network VPN 1009
20.3.1 Anforderungen für VPN..... 1010
20.3.2 Anbindung von Teleworkern über VPN..... 1012
20.3.2.1 Wie Sie die Anbindung von Teleworkern über VPN konfigurieren..... 1013
20.3.2.2 Wie Sie die Teleworker-Daten exportieren..... 1015
20.3.3 Vernetzung von Kommunikationssystemen über VPN..... 1015
20.3.3.1 Wie Sie die Vernetzung über VPN konfigurieren..... 1016
20.3.3.2 Wie Sie Topologie-Daten einer VPN-Vernetzung exportieren und importieren..... 1018
20.3.4 VPN - Sicherheitsmechanismen..... 1019
20.3.5 VPN - Zertifikate..... 1021
20.3.5.1 VPN - Wie Sie Lightweight-CA-Zertifikate generieren..... 1023
20.3.5.2 VPN - Zertifikatsverwaltung - Wie Sie ein Zertifikat anzeigen..... 1023
20.3.5.3 VPN - Wie Sie ein Trusted CA-Zertifikat importieren (X.509)..... 1024
20.3.5.4 VPN - Peer Zertifikate - Wie Sie eine Zertifikatsanforderung (CSR) generieren..... 1024
20.3.5.5 VPN - Peer Zertifikate - Wie Sie ein Zertifikat (PKCS#12) generieren..... 1025
20.3.5.6 VPN - Wie Sie ein Peer Zertifikat importieren (PKCS#12)..... 1026
20.3.6 VPN-Clients..... 1026
20.3.6.1 NCP VPN Client Einstellungen..... 1027
20.3.6.2 Wie Sie einen NCP VPN Client konfigurieren..... 1029
20.3.6.3 Wie Sie einen Shrew Soft VPN Client konfigurieren..... 1030
20.3.6.4 Wie Sie einen iOS oder Android VPN Client konfigurieren..... 1031
20.3.6.5 Wie Sie einen Mac OS-X VPN Client konfigurieren..... 1031
20.3.7 VPN - Dienste..... 1032
20.3.7.1 VPN - Aktive Dienste - Wie Sie alle IPsec-Dienste anzeigen..... 1032
20.3.7.2 VPN - Aktive Dienste - Wie Sie einen speziellen IPsec-Dienst anzeigen..... 1032
20.3.7.3 VPN - Konfigurierte Dienste - Wie Sie alle IPsec-Dienste anzeigen..... 1033
20.3.7.4 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst ändern..... 1033
20.3.7.5 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst umbenennen..... 1034
20.3.7.6 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst löschen..... 1034
20.3.8 VPN-Tunnel..... 1034
20.3.8.1 VPN - Aktive Tunnel - Wie Sie allgemeine Tunneldaten anzeigen..... 1034
20.3.8.2 VPN - Aktive Tunnel - Wie Sie Regeln für alle Tunnel anzeigen..... 1035
20.3.8.3 VPN - Konfigurierte Tunnel - Wie Sie allgemeine Tunneldaten anzeigen..... 1035
20.3.8.4 VPN - Konfigurierte Tunnel - Wie Sie Regeln für alle Tunnel anzeigen..... 1036
20.3.8.5 VPN - Wie Sie einen konfigurierten Tunnel hinzufügen..... 1036
20.3.9 VPN-Regeln..... 1038
20.3.9.1 VPN - Aktive Regeln - Wie Sie Regeln anzeigen..... 1038
20.3.9.2 VPN - Aktive Regeln - Wie Sie spezielle Regel anzeigen..... 1039
20.3.9.3 VPN - Konfigurierte Regeln - Wie Sie alle Regeln anzeigen..... 1039
20.3.9.4 VPN - Konfigurierte Regeln - Wie Sie eine Regel hinzufügen..... 1040
20.3.9.5 VPN - Wie Sie eine Regel ändern..... 1040
20.3.9.6 VPN - Wie Sie eine Regel für die Gegenrichtung hinzufügen..... 1041
20.3.9.7 VPN - Wie Sie eine Regel löschen..... 1041
20.3.10 PKI-Server..... 1042
20.3.10.1 VPN - Wie Sie den PKI-Server anzeigen..... 1042
20.3.10.2 VPN - Wie Sie einen PKI-Server hinzufügen..... 1042
20.4 Zertifikatshandling..... 1042
20.4.1 Einführung..... 1043
20.4.2 CA-Zertifikat generieren..... 1045
20.4.3 Wie Sie ein selbstsigniertes Zertifikat generieren..... 1045
20.4.4 Zertifikatsanforderungen (CSR) generieren..... 1046
20.4.5 Server-Zertifikat importieren (PKCS#12)..... 1048

20.4.6 Server-Zertifikat importieren (PEM)..... 1048
20.4.7 Wie Sie Zertifikate anzeigen..... 1049
20.4.8 Wie Sie ein Zertifikat löschen..... 1049
20.4.9 Wie Sie ein Zertifikat exportieren (X.509)..... 1050
20.4.10 Wie Sie ein verlängertes Zertifikat importieren (X.509)..... 1050
20.4.11 Wie Sie ein Zertifikat aktivieren..... 1050
20.4.12 Zertifikatshandling für Booster Server..... 1051
20.5 Web Sicherheit..... 1052
20.5.1 Verbindungen zum Web-Server..... 1052
20.5.1.1 Wie Sie die Verbindungen zum Web-Server konfigurieren (UC Suite)..... 1052
20.5.1.2 Wie Sie die Verbindungen zum Web-Server konfigurieren (UC Smart)..... 1052
20.5.2 Admin-Protokoll..... 1053
20.5.2.1 Wie Sie das Admin.-Protokoll laden..... 1053
20.5.2.2 Wie Sie die Admin.-Protokoll-Sprache ändern..... 1053
20.6 SQL-Sicherheit..... 1054
20.6.1 Einzelknoten..... 1054
20.6.2 Mehrfachknoten..... 1054
20.6.3 Wie Sie die SQL-Datenbankkennwörter konfigurieren..... 1055
20.7 Schutz vor SIP-Attacken (SIP Attack Protection)..... 1056

21 Vernetzung von OpenScape Business..... 1058
21.1 Vernetzungsplan..... 1059
21.1.1 Homogene und inhomogene Netze..... 1059
21.1.1.1 Wie Sie die Übersicht aller OpenScape Business Knoten anzeigen..... 1060
21.1.2 Single- und Multi-Gateway..... 1060
21.2 Netzweite Leistungsmerkmale..... 1061
21.2.1 Netzweite Leistungsmerkmale der UC-Lösungen..... 1061
21.2.2 Netzweite Voice-Leistungsmerkmale..... 1064
21.3 Lizenzierung eines Netzverbundes..... 1065
21.4 Anforderungen an die Vernetzung..... 1065
21.4.1 Anforderungen an die LAN-Vernetzung..... 1066
21.4.2 Rufnummernplan im Netz..... 1068
21.4.2.1 Wahl von öffentlichen Rufnummern im Netz..... 1069
21.5 Wegeoptimierung (Path Replacement)..... 1069
21.5.1 Wie Sie die Wegeoptimierung (Path Replacement) aktivieren oder deaktivieren..... 1070
21.6 Vernetzungsszenarien..... 1070
21.6.1 Abhängigkeiten und Einschränkungen..... 1071
21.6.2 Vernetzung von mehreren OpenScape Business X..... 1072
21.6.2.1 Wie Sie die Basisinstallation für Knoten 1 (Master) konfigurieren..... 1076
21.6.2.2 Wie Sie die Vernetzung für Knoten 1 (Master) konfigurieren..... 1077
21.6.2.3 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren..... 1077
21.6.2.4 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren..... 1078
21.6.2.5 Wie Sie die Vernetzungsfunktion für den Master kontrollieren..... 1079
21.6.2.6 Wie Sie Richtungen und Richtungsparameter konfigurieren (ISDN-Amt für den Master)..... 1079
21.6.2.7 Wie Sie Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Master)..... 1080
21.6.2.8 Wie Sie LCR für die Vernetzung konfigurieren (Master)..... 1080
21.6.2.9 Wie Sie die Richtung und Richtungsparameter konfigurieren (Slave)..... 1081
21.6.2.10 Wie Sie LCR für die Vernetzung konfigurieren (Slave)..... 1082
21.6.3 Vernetzung von OpenScape Business X mit OpenScape Business S (Single Gateway)..... 1083
21.6.3.1 Wie Sie die Basisinstallation für Knoten 1 (Master) konfigurieren..... 1089
21.6.3.2 Wie Sie die Vernetzung für Knoten 1 (Master) konfigurieren..... 1090
21.6.3.3 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren..... 1091
21.6.3.4 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren..... 1092
21.6.3.5 Wie Sie die Basisinstallation für Knoten 3 (Slave) konfigurieren..... 1092
21.6.3.6 Wie Sie die Vernetzungsfunktion für den Master kontrollieren..... 1093
21.6.3.7 Vernetzung konfigurieren für Knoten 3 (Slave)..... 1094

21.6.3.8 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 3, Slave)....1094
21.6.3.9 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 2)....1096
21.6.3.10 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 1, Master)....1097
21.6.3.11 Wie Sie Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Knoten 1)....1098
21.6.3.12 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 1)....1098
21.6.4 Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway)....1100
21.6.4.1 Wie Sie die Basisinstallation für Knoten 4 (OpenScape Business S, Master) konfigurieren....1108
21.6.4.2 Wie Sie die Vernetzung für Knoten 4 (Master) konfigurieren....1109
21.6.4.3 Wie Sie die Basisinstallation für Knoten 1 (Slave) konfigurieren....1110
21.6.4.4 Wie Sie die Vernetzung für Knoten 1 (Slave) konfigurieren....1111
21.6.4.5 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren....1111
21.6.4.6 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren....1112
21.6.4.7 Wie Sie die Basisinstallation für Knoten 3 (Slave) konfigurieren....1113
21.6.4.8 Wie Sie die Vernetzung für Knoten 3 (Slave) konfigurieren....1114
21.6.4.9 Wie Sie die Vernetzungsfunktion für den Master kontrollieren....1115
21.6.4.10 Wie Sie ein Multi-Gateway für Knoten 4 (Master) konfigurieren....1115
21.6.4.11 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 1, Slave)....1116
21.6.4.12 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 1, Slave)....1116
21.6.4.13 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 2, Slave)....1118
21.6.4.14 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 2, Slave)....1119
21.6.4.15 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 3, Slave)....1121
21.6.4.16 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 3, Slave)....1121
21.6.4.17 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 4, Master)....1123
21.6.4.18 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 4, Master)....1124
21.6.5 Vernetzung von OpenScape Business in Hosting-Umgebungen....1127
21.6.6 Vernetzung von OpenScape Business X und OpenScape 4000....1130
21.6.7 Vernetzung von OpenScape Business X und OpenScape Voice....1137
21.6.8 Anbindung von externen Anschaltungen an OpenScape Business über SIP-Interconnection....1140
21.6.9 Offene Nummerierung in OpenScape Business X Netzwerken....1142
21.6.9.1 Wie Sie die offene Nummerierung konfigurieren....1143
21.6.10 Vernetzung über ISDN....1144
21.6.11 OpenScape Business Netzverbund mit zentralem ITSP-Amtsanschluss....1146
21.7 Zentraler Abwurfplatz im Netzverbund (nicht für USA)....1148
21.7.1 Wie Sie einen zentralen Abwurfplatz im Multi-Gateway-Netzverbund konfigurieren....1149
21.8 Presence Manager....1150
21.9 Synchronisationsstatus im Netzverbund....1151
21.9.1 Manuelle Synchronisierung im Netzverbund....1152
21.9.2 Wie Sie eine Synchronisierung manuell starten....1152
21.10 Überlebensfähigkeit....1152
21.10.1 Wie Sie Survivability konfigurieren....1155
21.11 Entfernung eines Knotens aus dem Netzverbund....1156

22 Anschaltungen....1157
22.1 Analoges Ansagegerät....1157
22.1.1 Wie Sie ein analoges Ansagegerät hinzufügen....1158
22.1.2 Wie Sie die Ansageverzögerung ändern....1158
22.2 Türsprechstelle und Türöffner....1159
22.2.1 DoorLine a/b T01-T04....1159
22.2.1.1 Wie Sie den Teilnehmerport der Doorline a/b T01-T04 konfigurieren....1160
22.2.1.2 Wie Sie die Nebenstelle für die Doorline a/b T01-T04 konfigurieren....1161
22.2.2 DoorCom Analog....1161
22.2.2.1 Wie Sie den Teilnehmerport der DoorCom Analog konfigurieren....1162
22.2.2.2 Wie Sie die Nebenstelle für die DoorCom Analog konfigurieren....1162
22.2.3 Türfreisprecheinrichtung mit Verstärker (TFE-S)....1162
22.2.3.1 Wie Sie die Türsprechstelle konfigurieren....1164
22.2.4 Lautsprecher....1164

22.2.4.1 Wie Sie die analoge Teilnehmer-Schnittstelle für einen Lautsprecher konfigurieren..... 1165
22.2.4.2 Wie Sie die analoge Teilnehmer-Schnittstelle für den Anschluss eines Verstärker am TFE S Modul konfigurieren..... 1166
22.3 Aktoren..... 1166
22.3.1 Wie Sie einen Aktor konfigurieren..... 1168
22.4 Sensoren..... 1169

23 Application Connectivity..... 1171
23.1 CSTA..... 1171
23.1.1 Wie Sie die Portnummer für CSTA ändern..... 1173
23.1.2 Wie Sie den CMD für die Nutzung von TAPI 120 aktivieren oder deaktivieren..... 1174
23.1.3 Wie Sie den DSS-Server für die Nutzung von netzweiten DSS-Tasten aktivieren oder deaktivieren..... 1175
23.1.4 Wie Sie den CSP aktivieren oder deaktivieren..... 1175
23.1.5 Wie Sie Media Extension Bridge aktivieren oder deaktivieren..... 1176
23.2 OpenScape Business TAPI 120/170..... 1176
23.2.1 OpenScape Business TAPI 120..... 1177
23.2.2 OpenScape Business TAPI 170..... 1182
23.3 Web Services Interface..... 1187
23.4 Open Directory Service..... 1188
23.4.1 Wie Sie Open Directory Service aktivieren oder deaktivieren..... 1193
23.4.2 Wie Sie Open Directory Service neu starten..... 1193
23.4.3 Kennwort für Zugriff auf Open Directory Service konfigurieren..... 1193
23.4.4 ODBC-ODBC Bridge Server konfigurieren..... 1194
23.4.5 Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen..... 1196
23.4.6 Vorschau auf LDAP-Suchergebnis für Open Directory Service durchführen..... 1199
23.4.7 Wie Sie eine externe Datenquelle für Open Directory Service löschen..... 1199
23.5 Active Directory Integration Service..... 1200
23.5.1 Wie Sie die den Active Directory Service konfigurieren..... 1201
23.6 Application Launcher..... 1202
23.6.1 Voraussetzungen für Application Launcher..... 1203
23.6.2 Profil mit Konfigurationsdaten von Application Launcher..... 1204
23.6.2.1 Wie Sie das Profil mit Konfigurationsdaten von Application Launcher bereitstellen..... 1204
23.7 myPortal for Teams im Überblick..... 1204
23.7.1 myPortal for Teams konfigurieren..... 1205
23.7.2 So laden Sie myPortal for Teams in den Teams-Speicher hoch..... 1206
23.8 Unify Phone..... 1206
23.8.1 Unify Phone-Konnektivität konfigurieren..... 1207
23.8.2 Wie konfigurieren Sie die Unify Phone-Benutzerinstanz..... 1208
23.8.3 Unify Phone-Benutzer verwalten..... 1208
23.8.3.1 Wie Sie Unify Phone-Benutzer erstellen..... 1209
23.8.3.2 Wie fügen Sie bestehende Unify Phone-Benutzer hinzu..... 1209
23.8.3.3 Unify Phone-Benutzerdetails bearbeiten..... 1211
23.8.3.4 Wie entfernen oder löschen Sie Unify Phone-Benutzer..... 1211
23.8.3.5 Wie Sie alternative Nummern und Anruf-Routing für das Unify Phone-Interworking einrichten..... 1212
23.9 Let's Encrypt-Dienst..... 1212
23.9.1 Wie konfigurieren Sie den Let's Encrypt-Dienst..... 1213
23.10 CloudLink Service..... 1214
23.10.1 So konfigurieren Sie den Cloud Link-Dienst..... 1214
23.10.2 So öffnen Sie die CloudLink Daemon-Webschnittstelle..... 1215
23.10.3 So konfigurieren Sie die CloudLink Dämon-Webschnittstelle..... 1215
23.10.4 So aktivieren/konfigurieren Sie den SIP-Connector für die Verbindung mit Workflow Studio..... 1216
23.11 CloudLink-Pilotnummern..... 1217
23.11.1 So konfigurieren Sie CloudLink-Pilotnummern..... 1217

24 Accounting..... 1218
24.1 Verbindungsdaten..... 1218
24.1.1 Erfassung von Verbindungsdaten..... 1218
24.1.1.1 Wie Sie die Erfassung von Verbindungsdaten aktivieren oder deaktivieren..... 1219
24.1.1.2 Wie Sie die Protokollierung der Verbindungsdauer aktivieren oder deaktivieren..... 1219
24.1.1.3 Wie Sie die Protokollierung von Geldbeträgen oder Tarifeinheiten konfigurieren..... 1220
24.1.1.4 Wie Sie Tariffaktor, Währung und Rechengenauigkeit konfigurieren..... 1220
24.1.1.5 Wie Sie die Protokollierung der letzten vier Ziffern aktivieren oder deaktivieren..... 1221
24.1.1.6 Wie Sie die Protokollierung gehender Anrufe ohne Verbindung aktivieren oder deaktivieren... 1221
24.1.1.7 Wie Sie die Protokollierung kommender Verbindungen aktivieren oder deaktivieren..... 1222
24.1.1.8 Wie Sie das Verbindungsprotokoll aktivieren oder deaktivieren..... 1222
24.1.1.9 Wie Sie die Protokollierung der MSN aktivieren oder deaktivieren..... 1223
24.1.1.10 Wie Sie das Dezimalformat aktivieren oder deaktivieren..... 1223
24.1.2 Projektkennzahlen..... 1223
24.1.2.1 Wie Sie eine Projektkennzahl konfigurieren..... 1224
24.1.2.2 Wie Sie ein PKZ-Prüfverfahren konfigurieren..... 1225
24.1.2.3 Wie Sie die Wahlwiederholung mit PKZ aktivieren oder deaktivieren..... 1225
24.2 Anzeige und Übertragung von Verbindungsdaten..... 1226
24.2.1 Übermittlung von Geldbeträgen (nicht für USA)..... 1226
24.2.1.1 Wie Sie die Übermittlung von Geldbeträgen konfigurieren..... 1226
24.2.2 Anzeige der Verbindungskosten am Telefon..... 1227
24.2.3 Anzeige der Verbindungsdauer am Telefon..... 1227
24.2.3.1 Wie Sie die Anzeige der Verbindungsdauer aktivieren oder deaktivieren..... 1228
24.2.4 Übertragung von Verbindungsdaten..... 1228
24.2.4.1 Wie Sie das Format auswählen..... 1235
24.2.4.2 Wie Sie die Übertragung von Verbindungsdaten über HTTPS aktivieren oder deaktivieren..... 1235
24.3 Kostenkontrolle..... 1235
24.3.1 Hinweis auf teure Verbindungswege..... 1235
24.3.1.1 Wie Sie einen Hinweis auf einen teuren Verbindungsweg konfigurieren..... 1236
24.3.2 Schutz vor Gebührenbetrug..... 1236
24.3.2.1 Wie Sie den Schutz vor Gebührenmissbrauch aktivieren oder deaktivieren..... 1236
24.4 Accounting-Tools..... 1237
24.4.1 Accounting Manager..... 1237
24.4.2 Teledata Office..... 1237

25 Wartung..... 1238
25.1 Telefonie-Konfiguration..... 1238
25.1.1 Datum und Uhrzeit..... 1238
25.1.1.1 Wie Sie Datum und Uhrzeit manuell konfigurieren..... 1239
25.1.1.2 Wie Sie die Zeitzone einstellen..... 1239
25.1.1.3 Wie Sie das Datumsformat konfigurieren..... 1240
25.1.2 SNTP..... 1240
25.1.2.1 Wie Sie das Datum und die Uhrzeit von einem SNTP-Server beziehen..... 1240
25.1.3 Telefon-Logos..... 1241
25.1.3.1 Telefon-Logo ins System laden..... 1241
25.1.3.2 Wie Sie ein Telefon-Logo an Systemtelefone verteilen..... 1242
25.1.3.3 Wie Sie ein Telefon-Logo löschen..... 1242
25.1.4 Kundenindividuelle Displayanzeige..... 1242
25.1.4.1 Wie Sie die kundenindividuelle Displayanzeige (System-Name) ändern..... 1243
25.1.5 Mehrsprachige Textausgabe..... 1243
25.1.6 Flexible Menüs..... 1243
25.1.6.1 Wie Sie das flexible Menü ändern..... 1243
25.1.7 Wartemusik..... 1244
25.1.7.1 Wie Sie interne Wartemusik importieren..... 1245
25.1.7.2 Wie Sie die Funktion der internen Wartemusik konfigurieren..... 1246
25.1.7.3 Wie Sie die interne Wartemusik für jede VBZ-Gruppe ändern..... 1246

25.1.8 Ansagen....1247
25.1.8.1 So konfigurieren Sie die Ansagen (UC Suite & UC Booster)....1248
25.1.8.2 So konfigurieren Sie die Ansagen (UC Smart)....1249
25.1.9 Teilnehmer-zu-Teilnehmer Zeichengabe....1249
25.1.10 Sprachkanal-Signalisierungsschutz....1250
25.1.11 Zeitparameter....1250
25.1.12 Steuerung von Centrex-Leistungsmerkmalen....1250
25.1.12.1 Wie Sie die Steuerung von Centrex-Leistungsmerkmalen aktivieren oder deaktivieren....1250
25.2 Sichern und Wiederherstellen....1251
25.2.1 Backup-Sets....1252
25.2.1.1 Wie Sie sich Backup-Sets anzeigen lassen....1252
25.2.1.2 Wie Sie Backup-Sets löschen....1253
25.2.2 Backup-Medien....1253
25.2.2.1 Backup-Medium hinzufügen....1254
25.2.2.2 Backup-Medium bearbeiten....1255
25.2.2.3 Wie Sie ein Backup-Medium löschen....1256
25.2.3 Sofortiges Sichern....1256
25.2.3.1 Wie Sie ein Backup-Set sofort sichern....1257
25.2.4 Zeitgesteuertes Sichern....1258
25.2.4.1 Wie Sie ein Backup-Set zeitgesteuert sichern....1258
25.2.5 Wiederherstellen....1259
25.2.5.1 Wie Sie ein Backup-Set wiederherstellen....1259
25.3 Updates....1260
25.3.1 Nutzung eines lokalen Webservers....1262
25.3.1.1 Wie Sie den Zugang zum lokalen Web-Server konfigurieren....1262
25.3.2 Update des Kommunikationssystems....1263
25.3.2.1 Wie Sie das System über einen Webserver aktualisieren....1264
25.3.2.2 Wie Sie das System über ein USB-Medium aktualisieren....1266
25.3.2.3 System über einen Datei-Upload aktualisieren....1267
25.3.2.4 Wie Sie das System über ein USB-Medium ohne WBM-Zugriff aktualisieren....1268
25.3.3 Update der Systemtelefone....1269
25.3.3.1 Wie Sie die Telefonsoftware ins System laden....1270
25.3.3.2 Wie Sie die Telefonsoftware an Systemtelefone verteilen....1270
25.3.3.3 Wie Sie die Telefonsoftware löschen....1271
25.3.3.4 Wie Sie die automatische Verteilung der Telefonsoftware aktivieren oder deaktivieren....1271
25.3.3.5 Automatisches Reflashing konfigurieren....1271
25.3.4 Software-Status....1273
25.3.4.1 Wie Sie den Software-Status abfragen....1273
25.4 Restart, Reload, Shutdown....1273
25.4.1 Restart (Neustart) von OpenScape Business....1274
25.4.1.1 Wie Sie einen Restart (Neustart) von OpenScape Business auslösen....1275
25.4.2 Reload von OpenScape Business....1275
25.4.2.1 Wie Sie einen Reload von OpenScape Business auslösen....1276
25.4.3 Shutdown (Herunterfahren) von OpenScape Business X....1277
25.4.3.1 Wie Sie OpenScape Business X herunterfahren....1277
25.4.4 PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X....1277
25.4.4.1 Wie Sie eine PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X konfigurieren....1277
25.4.5 Restart (Neustart) der UC Booster Card (Application Board OCAB)....1278
25.4.5.1 Wie Sie einen Restart (Neustart) der UC Booster Card (Application Board OCAB) auslösen....1278
25.4.6 Reload der UC Booster Card (Application Board OCAB)....1279
25.4.6.1 Wie Sie einen Reload der UC Booster Card (Application Board OCAB) auslösen....1279
25.4.7 Restart (Neustart) der UC Applikation....1280
25.4.7.1 Wie Sie einen Restart (Neustart) der UC Applikation auslösen....1280
25.5 Inventory-Management....1280
25.5.1 Systemstatus....1280

25.5.1.1 Wie Sie den Teilnehmer-Status abfragen....1281
25.5.1.2 Wie Sie den Verbindungsaufbau-Status abfragen....1282
25.5.1.3 Wie Sie den ITSP-Status abfragen....1283
25.5.1.4 Wie Sie IP-Adressen anzeigen....1283
25.5.2 Inventar....1284
25.5.2.1 Wie Sie das Inventory von OpenScape Business X abfragen....1285
25.5.2.2 Wie Sie das Inventory von OpenScape Business S abfragen....1287
25.6 Automatische Aktionen....1287
25.6.1 Automatische Aktion Garbage Collection....1287
25.6.1.1 Wie Sie die automatische Aktion Garbage Collection ändern....1288
25.6.1.2 Wie Sie die automatische Aktion Garbage Collection starten (aktivieren)....1289
25.6.1.3 Wie Sie die automatische Aktion Garbage Collection stoppen (deaktivieren)....1289
25.6.2 Automatische Aktion DLS Notification....1289
25.6.2.1 Wie Sie die automatische Aktion DLS Notification ändern....1290
25.6.2.2 Wie Sie die automatische Aktion DLS Notification starten (aktivieren)....1290
25.6.2.3 Wie Sie die automatische Aktion DLS Notification stoppen (deaktivieren)....1291
25.6.3 Warnmechanismus für SDHC-Kartenlebensdauer....1291
25.6.3.1 Benachrichtigung bei Fehlern in SDHC-Karte festlegen....1293
25.6.3.2 Automatische Aktion Warnmechanismus für SDHC-Lebensdauer starten....1293
25.6.3.3 SDHC-Karte klonen und wechseln....1294
25.6.3.4 Datei für SDHC-Datensicherung erstellen....1295
25.6.3.5 Austausch der SDHC-Karte....1298
25.7 Power Management....1300
25.7.1 Wie Sie das Power-Management aktivieren oder deaktivieren....1301
25.7.2 Wie Sie den Ethernet-Link-Modus der LAN-Schnittstellen ändern....1301
25.8 Überwachung und Wartung von OpenScape Business....1302
25.8.1 Prüfen einer Netzwerkverbindung von OpenScape Business X....1302
25.8.1.1 Wie Sie Ping senden....1303
25.8.1.2 Wie Sie Traceroute testen....1303
25.8.2 SNMP (Simple Network Management Protocol)....1303
25.8.2.1 Wie Sie alle Communities anzeigen....1316
25.8.2.2 Wie Sie eine Community hinzufügen....1317
25.8.2.3 Wie Sie eine Community ändern....1317
25.8.2.4 Wie Sie eine Community löschen....1318
25.8.2.5 Wie Sie Traps anzeigen....1318
25.8.2.6 Wie Sie Details eines Traps anzeigen....1319
25.8.3 Manuelle Aktionen....1319
25.8.3.1 Wie Sie Diagnosedaten / Diagnose-Protokolle herunterladen....1321
25.8.4 Traces....1322
25.8.4.1 Wie Sie eine Systemtrace-Protokolldatei herunterladen....1329
25.8.4.2 Wie Sie eine Systemtrace-Protokolldatei löschen....1330
25.8.4.3 Trace-Einstellungen auf Standardwerte festlegen....1330
25.8.4.4 Wie Sie alle Trace-Profile anzeigen....1331
25.8.4.5 Wie Sie ein Trace-Profil starten oder stoppen....1332
25.8.4.6 Wie Sie die Trace-Format-Konfiguration anzeigen oder ändern....1332
25.8.4.7 Wie Sie die Trace-Ausgabe-Interfaces anzeigen oder ändern....1333
25.8.4.8 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll anzeigen oder ändern....1333
25.8.4.9 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll herunterladen oder öffnen....1333
25.8.4.10 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll löschen....1334
25.8.4.11 Wie Sie M5T-Trace-Komponenten anzeigen....1334
25.8.4.12 Wie Sie eine M5T-Trace-Komponente starten oder stoppen....1335
25.8.4.13 Wie Sie M5T-Trace-Komponenten ändern....1335
25.8.4.14 Wie Sie den Secure Trace starten oder stoppen....1335
25.8.4.15 Wie Sie den Status des Secure Trace abfragen....1336
25.8.4.16 Wie Sie das Passwort für den Secure Trace ändern....1336
25.8.4.17 Wie Sie das Zertifikat für den Secure Trace aus einer X.509-Datei importieren....1337

25.8.4.18 Wie Sie die H.323-Stack-Trace-Konfiguration anzeigen oder ändern..... 1337
25.8.4.19 Wie Sie H.323-Module ändern..... 1337
25.8.4.20 Wie Sie das H.323-Stack-Trace-Protokoll herunterladen oder öffnen..... 1338
25.8.4.21 Wie Sie das H.323-Stack-Trace-Protokoll löschen..... 1338
25.8.4.22 Wie Sie den Lizenz-Komponenten-Trace ändern..... 1339
25.8.4.23 Wie Sie Details eines Trace-Profils anzeigen..... 1339
25.8.4.24 Wie Sie alle Trace-Profile stoppen..... 1339
25.8.4.25 Wie Sie ein Trace-Profil hinzufügen..... 1340
25.8.4.26 Wie Sie Trace-Komponenten anzeigen..... 1340
25.8.4.27 Wie Sie Details einer Trace-Komponente anzeigen..... 1341
25.8.4.28 Wie Sie eine Trace-Komponente starten oder stoppen..... 1341
25.8.4.29 Wie Sie alle Trace-Komponenten stoppen..... 1341
25.8.4.30 Trace-Einstellungen auf Standardwerte festlegen..... 1342
25.8.4.31 Wie Sie Trace-Komponenten ändern..... 1342
25.8.4.32 Automatische Weiterleitung von Systemprotokolldateien..... 1343
25.8.4.33 Kernel Crash-Datendienst starten..... 1343
25.8.4.34 Kernel Crash-Datendienst anhalten..... 1344
25.8.4.35 Wie Sie den Medienserver-Trace starten..... 1344
25.8.4.36 Wie Sie den Medienserver-Trace anhalten..... 1345
25.9 TCP-Dump..... 1345
25.9.1 Wie Sie einen TCP-Dump starten..... 1345
25.9.2 Wie Sie einen TCP-Dump stoppen..... 1346
25.9.3 Wie Sie einen TCP-Dump löschen..... 1346
25.10 RPCAP-Dämon..... 1346
25.10.1 Wie Sie den RPCAP-Dämon aktivieren..... 1347
25.10.2 Wie Sie den RPCAP-Dämon deaktivieren..... 1347
25.11 Ereignisse..... 1347
25.11.1 Wie Sie die Event-Protokollierung über LAN ändern..... 1349
25.11.2 Wie Sie eine Event-Protokolldatei herunterladen..... 1350
25.11.3 Wie Sie eine Event-Protokolldatei löschen..... 1350
25.11.4 Wie Sie E-Mail-Einstellungen für Events ändern..... 1350
25.11.5 Wie Sie die Event-Reaktionstabelle anzeigen..... 1351
25.11.6 Wie Sie Reaktionseinstellungen eines Events ändern..... 1351
25.11.7 Wie Sie Reaktionseinstellungen mehrerer Events ändern..... 1352
25.11.8 Wie Sie Diagnose Logs herunterladen oder öffnen..... 1353
25.11.9 Wie Sie Diagnose Logs löschen..... 1353
25.11.10 Wie Sie die Ziele für die Alarm-Signalisierung festlegen..... 1354
25.12 Konfigurationsdaten für die Diagnose..... 1354
25.12.1 Wie Sie Konfigurationsdaten für die Diagnose erzeugen..... 1355
25.13 Card Manager..... 1356
25.13.1 Wie Sie mit dem Card Manager die Kommunikationssoftware auf die M.2 SATA SSD schreiben.. 1357
25.13.2 Kommunikationssoftware mit dem Card Manager auf die SDHC-Karte schreiben..... 1359
25.13.3 Wie Sie mit dem Card Manager die Kommunikationssoftware auf die OCAB-Festplatte schreiben..... 1361
25.14 Überwachung und Wartung der UC Suite..... 1363
25.14.1 Protokollierung..... 1363
25.14.1.1 Aufzeichnung der Systemprotokolle aktivieren oder deaktivieren..... 1365
25.14.1.2 Aufzeichnung der Client-Logs systemweit aktivieren oder deaktivieren..... 1365
25.14.1.3 Wie Sie die Aufzeichnung der Client-Logs teilnehmerindividuell aktivieren oder deaktivieren..... 1366
25.14.1.4 Ablagepfad für Client-Log-Dateien konfigurieren..... 1366
25.14.1.5 Zentrales Speichern der Client-Logs auf der Festplatte aktivieren oder deaktivieren..... 1367
25.14.1.6 Wie Sie Client Logs aller internen Teilnehmer herunterladen..... 1367
25.14.2 Benachrichtigung..... 1368
25.14.2.1 So konfigurieren Sie E-Mail-Benachrichtigungen über Systemfehler..... 1370
25.14.3 Wartung..... 1371

25.14.3.1 Tageszeit für die Wartung konfigurieren....1372
25.14.3.2 Aufbewahrungszeit für Protokolldateien konfigurieren....1373
25.14.3.3 Sofortige Systemwartung durchführen....1373
25.14.3.4 Aufbewahrungszeit für Contact-Center-Daten konfigurieren....1373
25.15 Überwachung der UC Smart....1374
25.15.1 Wie Sie den aktuellen Status der UC Smart abrufen....1374
25.16 Remote Services....1374
25.16.1 RSP.servicelink....1375
25.16.1.1 Wie Sie das RSP.servicelink-Plugin installieren, konfigurieren und registrieren....1378
25.16.1.2 Wie Sie das RSP.servicelink-Plugin aktivieren....1379
25.16.1.3 Wie Sie das RSP.servicelink-Plugin deaktivieren....1380
25.16.1.4 Wie Sie das RSP Service-Plugin zurücksetzen....1380
25.16.1.5 Wie Sie eine PIN für die Aktivierung und Deaktivierung des RSP.servicelink-Plugin konfigurieren....1380
25.16.2 Remote-Zugang....1381
25.16.2.1 Wie Sie den Remote-Zugang über ISDN einschalten....1382
25.16.2.2 Wie Sie einen PC mit Microsoft Windows Vista für Remote-Zugang über ISDN konfigurieren....1382
25.16.2.3 Wie Sie einen PC mit Microsoft Windows 7 für Remote-Zugang über ISDN konfigurieren....1384
25.16.2.4 Wie Sie den Remote-Zugang über Internet-Zugang mit fester IP-Adresse einschalten....1385
25.16.2.5 Wie Sie den Remote-Zugang über Internet-Zugang ohne feste IP-Adresse einschalten....1386
25.16.2.6 Wie Sie den Remote-Zugang ausschalten....1387
25.16.3 Online-Benutzer....1387
25.16.3.1 Wie Sie Online-Benutzer starten....1388

26 Migration....1389
26.1 Software-Aktualisierung für OpenScape Business X Systeme....1390
26.1.1 Software-Aktualisierung von OpenScape Business X V2 auf OpenScape Business X V3....1391
26.1.1.1 SW-Aktualisierung von permanent lizenzierten Systemen mit CLS Connect....1392
26.1.1.2 SW-Aktualisierung von permanent lizenzierten Systemen ohne CLS Connect....1392
26.1.1.3 SW-Aktualisierung auf PayGo-lizenzierte Systeme....1392
26.2 Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3....1393
26.2.1 So aktualisieren Sie UC Business Booster Server V2 auf V3....1393
26.3 Hardware/Software-Migration von OpenScape Business X Systemen auf V3....1395
26.3.1 Migration von OpenScape Business X V2 zu OpenScape Business X V3....1396
26.3.1.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf V3 migrieren....1397
26.3.1.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf V3 migrieren....1398
26.3.1.3 Wie Sie PayGo-lizenzierte Systeme auf V3 migrieren....1399
26.4 OpenScape Business X V3 System von einem V2-Mainboard auf ein V3-Mainboard migrieren....1400
26.4.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf ein V3-Mainboard migrieren....1402
26.4.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf ein V3-Mainboard migrieren....1402
26.4.3 Wie Sie PayGo-lizenzierte Systeme auf ein V3-Mainboard migrieren....1404
26.5 Software-Aktualisierung von OpenScape Business S....1404
26.5.1 Software-Aktualisierung von OpenScape Business S V2 auf OpenScape Business S V3....1405
26.5.1.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf V3 aktualisieren....1406
26.5.1.2 Wie Sie PayGo-lizenzierte Systeme auf V3 aktualisieren....1407
26.5.2 Software-Aktualisierung von OpenScape Business S V2 auf OpenScape Business S V3....1407
26.6 OpenScape Business V2 Netzwerk-Migration/-Aktualisierung auf V3....1408
26.6.1 Szenario 1: Hardware-Migration von Master-Knoten, Software-Aktualisierung von Slave-Knoten....1410
26.6.1.1 Migration/Aktualisierung mit CLS Connect auf dem Master-Knoten....1410
26.6.1.2 Migration/Aktualisierung ohne CLS Connect auf dem Master-Knoten....1411
26.6.2 Szenario 2: Software-Aktualisierung aller Systeme im Netzwerk auf V3....1412
26.6.2.1 Software-Aktualisierung mit CLS Connect auf dem Master-Knoten....1412
26.6.2.2 Software-Aktualisierung ohne CLS Connect auf dem Master-Knoten....1413
26.6.3 Szenario 3a: Software-Aktualisierung aller Knoten....1414

26.6.4 Szenario 3b: Software-Aktualisierung auf dem Master-Knoten, Hardware-Migration auf den Slave-Knoten....1414
26.6.4.1 Migration/Aktualisierung mit CLS Connect auf dem Master-Knoten....1414
26.6.4.2 Migration/Aktualisierung ohne CLS Connect auf dem Master-Knoten....1415
26.7 Migration von HiPath 3000 auf OpenScape Business V3....1416
26.7.1 Migration von HiPath 33xx, 35xx, 3800 nach OpenScape Business X3/X5/X8 V3....1417
26.7.1.1 Wie Sie den KDS aus HiPath 3000 laden....1422
26.7.1.2 Wie Sie die HG1500 Einstellungen auslesen....1423
26.7.1.3 Wie Sie den HiPath 3000 KDS konvertieren....1423
26.7.1.4 Wie Sie die Hardware bei HiPath 3300/3500 austauschen....1424
26.7.1.5 Wie Sie die Hardware bei HiPath 3350/3550 austauschen....1425
26.7.1.6 Wie Sie die Hardware bei HiPath 3800 austauschen....1427
26.7.1.7 Wie Sie die Erstinstallation durchführen....1427
26.7.1.8 Wie Sie den konvertierten KDS in das neue System laden....1428
26.7.1.9 Wie Sie eine neue Lizenzdatei generieren....1429
26.7.1.10 Wie Sie die Lizenzdatei offline aktivieren....1430
26.7.1.11 Wie Sie Lizenzen zuordnen....1430
26.7.1.12 Wie Sie die LCR-Einträge zurücksetzen....1430
26.7.2 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit V3-Mainboard....1431
26.7.3 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit UC Booster Server....1432
26.7.3.1 Wie Sie ein OpenScape Office V3 HX Backup-Set konvertieren....1434
26.7.4 Migration von HiPath 3000 Netzwerk auf OpenScape Business Netzwerk....1435
26.7.5 Migration eines HiPath 3000 V9 Netzverbunds mit HiPath 5000 RSM....1437
26.7.6 Geänderte/gestrichene Leistungsmerkmale und Schnittstellen von HiPath 3000....1440
26.8 Migration innerhalb von OpenScape Business V3....1447
26.9 Migration von HW-Baugruppen....1448
26.9.1 Ersetzen von SLMO24N durch SLMU....1449
26.9.2 Ersetzen von SLM8N durch SLMU....1449
26.9.3 Ersetzen von SLCN durch SLMUC (SLMU + CMAe)....1449
26.10 Migration von OpenScape Business X1 V2 auf OpenScape Business X1W V3....1450
26.10.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf X1W V3 migrieren....1451
26.10.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf X1W V3 migrieren....1452

27 Ausbaugrenzen und Kapazitäten....1454
27.1 Maximalwerte für Teilnehmer....1454
27.2 Maximalwerte für Leitungen....1457
27.3 Maximalwerte der Ressourcen....1459
27.3.1 Details zur Verwendung von DSP-Kanälen....1461
27.3.2 Details zur Verwendung von RTP-Proxykanälen....1462
27.4 Maximalwerte für Leistungsmerkmale....1462
27.4.1 Anbindung an Service-Provider....1463
27.4.2 Teilnehmer....1463
27.4.3 UC Smart-Ausbaustufen....1463
27.4.4 Smart Voicemail Ausbaustufen....1467
27.4.5 UC Suite-Ausbaustufen....1469
27.4.6 Funktionen am Telefon....1477
27.4.7 Arbeiten im Team (Gruppen)....1480
27.4.8 Anruf-Routing....1484
27.4.9 Multimedia Contact Center....1486
27.4.10 Mobility Ausbaugrenzen....1486
27.4.11 Sicherheit....1488
27.4.12 Vernetzung von OpenScape Business....1489
27.4.13 Application Connectivity....1489
27.4.14 Gebührenabrechnung....1492

28 Experten-Modus **1493**
28.1 Darstellungskonventionen für Parameterbeschreibungen 1493
28.2 **Wartung** 1494
28.2.1 **Konfiguration** 1494
28.2.1.1 **Konfiguration > Wartemusik (MoH) > Laden zum Gateway** 1494
28.2.1.2 **Konfiguration > Ansagen > Auf Gateway laden** 1495
28.2.1.3 **Konfiguration > Port-Konfiguration** 1495
28.2.1.4 **Konfiguration > SmartVM** 1496
28.2.1.5 **Konfiguration > SmartVM > Mailbox-Operationen** 1496
28.2.1.6 **Konfiguration > SmartVM > Dateioperationen** 1497
28.2.1.7 **Konfiguration > Branding** 1499
28.2.1.8 **Konfiguration > IP-Gateway-Adresse** 1499
28.2.2 **Software-Image** 1500
28.2.2.1 **Software-Image > System-Software > Update via Internet** 1500
28.2.2.2 **Software-Image > System-Software > Update via File Upload** 1501
28.2.2.3 **Software-Image > System-Software > Update via USB-Stick** 1501
28.2.2.4 **Software-Image > Telefon-Images > Laden** 1502
28.2.2.5 **Software-Image > Telefon-Images > Verteilen** 1503
28.2.2.6 **Software-Image > Telefon-Images > Verteilen pro Endgerät** 1503
28.2.2.7 **Software-Image > Telefon-Logo-Images > Laden** 1503
28.2.2.8 **Software-Image > Telefon-Logo-Images > Verteilen** 1504
28.2.3 **Cordless** 1504
28.2.3.1 **Cordless > Basisstationen** 1504
28.2.4 **Port/Baugruppen Zustand** 1506
28.2.4.1 **Port/Baugruppen Zustand > Baugruppen Zustand** 1507
28.2.4.2 **Port / Baugruppen Zustand > Out of Service** 1507
28.2.5 **Traces** 1508
28.2.5.1 **Traces > Trace-Format-Konfiguration** 1508
28.2.5.2 **Traces > Trace-Ausgabe-Interfaces** 1509
28.2.5.3 **Traces > Trace-Protokoll** 1510
28.2.5.4 **Traces > Digitale Prüfschleife** 1510
28.2.5.5 **Traces > Kunden-Trace-Protokoll** 1511
28.2.5.6 **Traces > M5T-Trace-Komponenten** 1511
28.2.5.7 **Traces > Secure Trace** 1512
28.2.5.8 **Traces > Secure Trace > Secure Trace-Zertifikat** 1512
28.2.5.9 **Traces > Secure Trace > Secure Trace-Einstellungen** 1512
28.2.5.10 **Traces > H.323-Stack-Trace** 1513
28.2.5.11 **Traces > Call Supervision** 1514
28.2.5.12 **Traces > Lizenz-Komponente** 1516
28.2.5.13 **Traces > Trace-Profile** 1517
28.2.5.14 **Traces > Trace-Komponenten** 1517
28.2.5.15 **Traces > TCP Dump** 1518
28.2.5.16 **Traces > rpcap Dämon** 1519
28.2.5.17 **Traces > Kernel-Crash-Daten** 1519
28.2.5.18 **Traces > Medienserver-Trace** 1520
28.2.6 **Events** 1520
28.2.6.1 **Events > Event-Konfiguration** 1521
28.2.6.2 **Ereignisse > Event-Protokoll** 1521
28.2.6.3 **Events > E-Mail** 1521
28.2.6.4 **Events > Reaktionstabelle** 1522
28.2.6.5 **Events > Diagnosie Logs** 1523
28.2.6.6 **Events > Alarm-Signalisierung** 1523
28.2.7 **Restart / Reload** 1523
28.2.7.1 **Restart / Reload > Restart / Reload** 1524
28.2.8 **SNMP** 1525

28.2.8.1 **SNMP** > **Communities** 1525
28.2.8.2 **SNMP** > **Communities** > **Lesende Communities** 1525
28.2.8.3 **SNMP** > **Communities** > **Schreibende Communities** 1526
28.2.8.4 **SNMP** > **Communities** > **Trap Communities** 1526
28.2.8.5 **SNMP** > **Traps** 1526
28.2.9 **Admin-Protokoll**....1527
28.2.9.1 **Admin-Protokoll** > **Konfiguration** 1527
28.2.9.2 **Admin-Protokoll** > **Admin-Protokoll-Daten** 1527
28.2.10 **Aktionen**....1528
28.2.10.1 **Aktionen** > **Manuelle Aktionen** > **Diagnose-Protokolle** 1528
28.2.10.2 **Aktionen** > **Manuelle Aktionen** > **DLI-Wartung**....1530
28.2.10.3 **Aktionen** > **Automatische Aktionen** > **Garbage Collection** 1530
28.2.10.4 **Aktionen** > **Automatische Aktionen** > **DLS Notification** 1531
28.2.10.5 **Aktionen > Automatische Aktionen > SDHC-Integritätsprüfung**....1531
28.2.11 **Plattform-Diagnose**....1531
28.2.12 **Applikat.-Diagnose**....1532
28.2.12.1 **Applikat.-Diagnose** > **Entwickler-Einstellungen** > **Trace-Konsolen-Ausgabe** 1532
28.2.12.2 **Applikat.-Diagnose** > **Entwickler-Einstellungen** > **Übernahme des Write Tokens** 1532
28.2.12.3 **Applikat.-Diagnose** > **Mainboard** 1532
28.2.12.4 Applikat.-Diagnose > Entwickler-Einstellungen > SIP-Provider-Profile....1532
28.2.13 **IP-Diagnose**....1532
28.2.13.1 **IP-Diagnose** > **Mainboard** > **ARP-Protokoll** 1532
28.2.13.2 **IP-Diagnose** > **Mainboard** > **ICMP-Anforderung** > **Ping** 1533
28.2.13.3 **IP-Diagnose** > **Mainboard** > **ICMP-Anforderung** > **Traceroute** 1533
28.2.14 **Online-Benutzer**....1534
28.2.14.1 **Online-Benutzer** 1534
28.3 **Telefonie**....1534
28.3.1 **Grundeinstellungen**....1534
28.3.1.1 **Grundeinstellungen** > **System** > **System Flags**....1534
28.3.1.2 **Grundeinstellungen** > **System** > **Zeitarameter** 1543
28.3.1.3 **Grundeinstellungen** > **System** > **Display**....1548
28.3.1.4 **Grundeinstellungen** > **System** > **DISA** 1552
28.3.1.5 **Grundeinstellungen** > **System** > **Abwurf/Attendant/Hotline**....1553
28.3.1.6 **Grundeinstellungen** > **System** > **LDAP**....1556
28.3.1.7 **Grundeinstellungen** > **System** > **Texts** 1557
28.3.1.8 **Grundeinstellungen** > **System** > **Flexible Menüs** 1558
28.3.1.9 **Grundeinstellungen** > **System** > **Kurzwahlziele**....1558
28.3.1.10 **Grundeinstellungen** > **System** > **Service Codes**....1559
28.3.1.11 **Grundeinstellungen** > **System > HFA-Registrierungs-Passwort**....1559
28.3.1.12 **Grundeinstellungen** > **Gateway** 1560
28.3.1.13 **Grundeinstellungen** > **DynDNS** > **DynDNS Service** 1562
28.3.1.14 **Grundeinstellungen** > **DynDNS** > **Aktualisierungszeit der DNS-Namen** 1563
28.3.1.15 **Grundeinstellungen** > **Quality of Service** 1564
28.3.1.16 **Grundeinstellungen** > **Datum und Uhrzeit** > **Datum und Uhrzeit** 1565
28.3.1.17 **Grundeinstellungen** > **Datum und Uhrzeit** > **Zeitzonen-Einstellungen** 1565
28.3.1.18 **Grundeinstellungen** > **Datum und Uhrzeit** > **SNTP-Einstellungen** 1565
28.3.1.19 **Grundeinstellungen** > **Port-Verwaltung** 1566
28.3.1.20 **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe** 1567
28.3.1.21 **Grundeinstellungen** > **Gebühren** > **Gebühren Faktoren** 1569
28.3.1.22 **Grundeinstellungen** > **Gebühren** > **Gebühren Projekt Kennzahlen** 1570
28.3.1.23 **Grundeinstellungen** > **Wiedergabegerät für Sprachnachrichten/Ansagen** 1570
28.3.1.24 **Grundeinstellungen** > **Telefonparameter-Bereitstellung**....1571
28.3.1.25 **Grundeinstellungen** > **Power Management** 1574
28.3.1.26 Grundinstallation> Massendaten....1574
28.3.2 **Sicherheit**....1575
28.3.2.1 **Sicherheit** > **Anwendungsfirewall**....1575

28.3.2.2 **Sicherheit** > **Deployment- und Licensing-Client (DLSC)** 1577
28.3.2.3 **Sicherheit** > **Deployment- und Licensing-Client (DLSC)** > **DLSC Client-Zertifikat** 1577
28.3.2.4 **Sicherheit** > **Deployment- und Licensing-Client (DLSC)** > **DLSC CA -Zertifikat** 1579
28.3.2.5 **Sicherheit** > **Signaling- und Payload-Encryption** 1580
28.3.2.6 **Sicherheit** > **Signaling- und Payload-Encryption** > **SPE-Zertifikat** 1581
28.3.2.7 **Sicherheit** > **Signaling- und Payload-Encryption** > **SPE CA-Zertifikate** 1581
28.3.2.8 **Sicherheit** > **VPN** 1581
28.3.2.9 **Sicherheit** > **VPN** > **Lightweight CA** 1582
28.3.2.10 **Sicherheit** > **VPN** > **Zertifikatsverwaltung** 1583
28.3.2.11 **Sicherheit** > **VPN** > **Zertifikatsverwaltung** > **Trusted CA Zertifikate** > **Aktive Zertifikate** .1583
28.3.2.12 **Sicherheit** > **VPN** > **Zertifikatsverwaltung** > **Trusted CA Zertifikate** > **Konfigurierte Zertifikate** 1585
28.3.2.13 **Sicherheit** > **VPN** > **Peer-Zertifikate** 1585
28.3.2.14 **Sicherheit** > **VPN** > **Dienste** > **Aktive Dienste** 1586
28.3.2.15 **Sicherheit** > **VPN** > **Dienste** > **Konfigurierte Dienste** 1587
28.3.2.16 **Sicherheit** > **VPN** > **Tunnel** > **Aktive Tunnel** 1588
28.3.2.17 **Sicherheit** > **VPN** > **Tunnel** > **Konfigurierte Tunnel** 1590
28.3.2.18 **Sicherheit** > **VPN** > **Regeln** > **Aktive Regeln** 1594
28.3.2.19 **Sicherheit** > **VPN** > **Regeln** > **Konfigurierte Regeln** 1596
28.3.2.20 **Sicherheit** > **VPN** > **Public Key Infrastructure (PKI)** 1597
28.3.2.21 **Sicherheit** > **SSL** > **Zertifikatsgenerierung** 1598
28.3.2.22 **Sicherheit** > **SSL** > **Zertifikatsverwaltung** 1599
28.3.2.23 **Sicherheit** > **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate** 1599
28.3.2.24 **Sicherheit** > **Web Sicherheit** 1601
28.3.2.25 **Sicherheit** > **SQL Sicherheit** 1601
28.3.3 **Netzwerkschnittstellen** 1601
28.3.3.1 **Netzwerkschnittstellen** > **Mainboard** > **Host-Name** 1601
28.3.3.2 **Netzwerkschnittstellen** > **Hauptplatine** > **LAN 1 (WAN)** 1602
28.3.3.3 **Netzwerkschnittstellen** > **Mainboard** > **LAN 2** 1606
28.3.3.4 **Netzwerkschnittstellen** > **Mainboard** > **LAN 3 (Admin)** 1608
28.3.3.5 **Netzwerkschnittstellen** > **Mainboard** > **FTP-Server** 1608
28.3.3.6 **Netzwerkschnittstellen** > **Mainboard** > **DHCP Modus** 1609
28.3.3.7 **Netzwerkschnittstellen** > **Hauptplatine** > **DHCP-Modus** > **DHCP-Server** > **Globale Parameter** 1609
28.3.3.8 **Netzwerkschnittstellen** > **Hauptplatine** > **DHCP-Modus** > **DHCP-Server** > **IP-Adresspools** 1611
28.3.3.9 **Netzwerk-Schnittstellen** > **Hauptplatine** > **DHCP-Modus** > **DHCP-Server** > **Statische IP-Adressen** 1612
28.3.3.10 **Netzwerkschnittstellen** > **Hauptplatine** > **DHCP-Modus** > **DHCP Server** > **Letzte aktive Leasing** 1614
28.3.3.11 **Netzwerkschnittstellen** > **Mainboard** > **DHCP Modus** > **DHCP Server** > **Alle Leases** 1614
28.3.3.12 **Netzwerkschnittstellen** > **Application Board** > **Host-Name** 1615
28.3.3.13 **Netzwerkschnittstellen** > **Application Board** > **LAN 1** 1615
28.3.3.14 **Netzwerkschnittstellen** > **Application Board** > **LAN 2** 1616
28.3.4 **Routing** 1617
28.3.4.1 **Routing** > **IP-Routing** > **Mainboard** > **Statische Routen** 1617
28.3.4.2 **Routing** > **IP-Routing** > **Mainboard** > **Default Router** 1618
28.3.4.3 **Routing** > **IP-Routing** > **Mainboard** > **DNS-Server** 1618
28.3.4.4 **Routing** > **IP-Routing** > **Application Board** > **Statische Routen** 1618
28.3.4.5 **Routing** > **IP-Routing** > **Application Board** > **Default Router** 1619
28.3.4.6 **Routing** > **NAT** 1619
28.3.4.7 **Routing** > **PSTN** 1620
28.3.4.8 **Routing** > **PSTN** > **PPP-Protokoll** 1621
28.3.4.9 **Routing** > **PSTN** > **PSTN-Partner** 1621
28.3.5 **LCR** 1625
28.3.5.1 **LCR** > **LCR-Flags** 1625

28.3.5.2 **LCR** > **Berechtigungen** 1626
28.3.5.3 **LCR** > **Wahlplan** 1626
28.3.5.4 **LCR** > **Wegetabelle** 1627
28.3.5.5 **LCR** > **Wahlregel** 1628
28.3.5.6 **LCR** > **Multisite** 1630
28.3.6 **Sprachgateway** 1631
28.3.6.1 **Sprachgateway** > **SIP-Parameter** 1631
28.3.6.2 Sprachgateway > ITSP Loc-ID Einstellungen 1633
28.3.6.3 **Sprachgateway** > **Codec-Parameter** 1634
28.3.6.4 **Sprachgateway** > **Ziel-Codec-Parameter** 1636
28.3.6.5 **Voice Gateway** > **Internet-Telefonie-Dienstanbieter** 1637
28.3.6.6 **Sprachgateway** > **Networking** > **Knoten** 1649
28.3.6.7 **Sprachgateway** > **Networking** > **Routing** 1649
28.3.6.8 **Sprachgateway** > **SIPQ-Verbindung** 1649
28.3.6.9 **Sprach-Gateway** > **Nativer SIP-Server-Trunk** 1651
28.3.7 **Teilnehmer** 1656
28.3.7.1 **Teilnehmer** > **Teilnehmer** > **UP0 Teilnehmer** 1656
28.3.7.2 **Station** > **Station** > **IP-Clients** 1659
28.3.7.3 **Station** > **Station** > **Analog Stations** 1662
28.3.7.4 **Teilnehmer** > **Teilnehmer** > **ISDN-Teilnehmer** 1663
28.3.7.5 **Teilnehmer** > **Teilnehmer** > **DECT-Teilnehmer** > **SLC-Rufnummer** 1664
28.3.7.6 **Teilnehmer** > **Teilnehmer** > **DECT-Teilnehmer** > **DECT-Teilnehmer** 1665
28.3.7.7 **Teilnehmer** > **Teilnehmer** > **IVM/EVM Ports** > **EVM** 1667
28.3.7.8 **Teilnehmer** > **Teilnehmer** > **Virtuale Teilnehmer** 1668
28.3.7.9 **Teilnehmer** > **Teilnehmer** > **Teilnehmer-Parameter** 1669
28.3.7.10 **Teilnehmer** > **Teilnehmer** > **UC-Anwendungen** 1680
28.3.7.11 **Teilnehmer** > **Teilnehmer** > **Profile/Vorlagen** 1681
28.3.7.12 **Teilnehmer** > **Teilnehmer** > **Durchwahl Rufnummern** 1683
28.3.7.13 **Teilnehmer** > **Teilnehmer** > **Mobility Entry** 1683
28.3.7.14 **Station** > **Station** > **SfB-Benutzer** 1684
28.3.7.15 **Teilnehmer** > **Teilnehmer** > **Übersicht Teilnehmer** 1685
28.3.7.16 **Teilnehmer** > **Tastenprogrammierung** 1686
28.3.8 **Cordless** 1687
28.3.8.1 **Cordless** > **Systemweit** 1687
28.3.8.2 **Cordless** > **SLC** 1689
28.3.8.3 **Cordless** > **Multi-SLC** 1690
28.3.8.4 **Cordless** > **Basisstationen** 1691
28.3.9 **Kommende Rufe** 1691
28.3.9.1 **Eingehende Anrufe** > **Gruppen/Huntgruppen** 1691
28.3.9.2 **Kommende Rufe** > **Gruppen-Teilnehmer** 1695
28.3.9.3 **Kommende Rufe** > **Team/Top** 1697
28.3.9.4 **Kommende Rufe** > **Anrufübernahme** 1700
28.3.9.5 **Kommende Rufe** > **UCD** 1700
28.3.9.6 **Kommende Rufe** > **Rufweiterschaltungen** 1703
28.3.10 **Leitungen/Vernetzung** 1706
28.3.10.1 **Leitungen/Vernetzung** > **Leitungen** 1706
28.3.10.2 **Trunks/Routing** > **Trunkgruppe** 1709
28.3.10.3 **Leitungen/Vernetzung** > **QSIG-Leistungsmerkmale** 1717
28.3.10.4 **Leitungen/Routing** > **MSN zuweisen** 1718
28.3.10.5 **Leitungen/Vernetzung** > **ISDN-Parameter** 1718
28.3.11 **Berechtigungen (Classes of Service)** 1719
28.3.11.1 **Berechtigungen** > **Teilnehmer** 1719
28.3.11.2 **Berechtigungen** > **Tag: Berechtigungsgruppen** 1720
28.3.11.3 **Berechtigungen** > **Nacht: Berechtigungsgruppen** 1720
28.3.11.4 **Berechtigung** > **Erlaubnislisten** 1721
28.3.11.5 **Berechtigungen** > **Verbotslisten** 1722

28.3.11.6 **Berechtigungen > Blacklist** 1722
28.3.11.7 **Berechtigungen > Nachtschaltung** 1723
28.3.11.8 **Berechtigungen > VBZ Gruppenzuordnung** 1723
28.3.11.9 **Berechtigungen > CON Matrix** 1724
28.3.11.10 **Berechtigungen > Automatische Nachtschaltung** 1725
28.3.11.11 **Berechtigungen > Sondertage** 1725
28.3.12 **Hilfsausrüstung** 1726
28.3.12.1 **Hilfsausrüstung > Wartemusik** 1726
28.3.12.2 **Hilfsausrüstung > PhoneMail** 1727
28.3.12.3 **Hilfsausrüstung > Ansagen** 1727
28.3.12.4 **Hilfsausrüstung > Türöffner** 1729
28.3.12.5 **Hilfsausrüstung > SmartVM** 1730
28.3.13 **Payload** 1734
28.3.13.1 **Payload > Devices** 1734
28.3.13.2 **Payload > Media Stream Control (MSC)** 1734
28.3.13.3 **Payload > HW-Module** 1735
28.3.14 **Statistiken** 1738
28.3.14.1 **Statistik > Gateway-Statistik > Mainboard > Device-Statistik** 1738
28.3.14.2 **Statistiken > Gateway-Statistiken > Mainboard > MSC-Statistiken** 1739
28.3.14.3 **Statistiken > SNMP-Statistiken** 1739
28.3.14.4 **Statistiken > Telephonie Statistiken > System Texte** 1740
28.3.14.5 **Statistiken > Telephonie Statistiken > UCD Agenten** 1740
28.3.14.6 **Statistiken > Telephonie Statistiken > TZustand Leitung** 1740
28.3.14.7 **Statistiken > Telephonie Statistiken > Weiterleitung** 1741
28.3.14.8 **Statistiken > Telephonie Statistiken > Teilnehmer** 1741
28.4 **Applikationen** 1743
28.4.1 **Applikationsauswahl** 1743
28.4.1.1 **Applikationsauswahl** 1743
28.4.2 **Active Directory Integration Service** 1743
28.4.2.1 **Active Directory Integration Service** 1744
28.4.3 **UC Smart** 1745
28.4.3.1 **UC Smart > Grundeinstellungen** 1745
28.4.3.2 **UC Smart > Benutzerverwaltung** 1746
28.4.3.3 **UC Smart > -Status** 1747
28.4.4 **OpenScape Business, UC Suite** 1747
28.4.4.1 **OpenScape Business, UC Suite** 1747
28.4.4.2 **OpenScape Business, UC Suite > Benutzerverzeichnis** 1747
28.4.4.3 **OpenScape Business, UC Suite > Abteilungen** 1750
28.4.4.4 **OpenScape Business, UC Suite > Gruppen** 1751
28.4.4.5 **OpenScape Business UC Suite > Templates** 1752
28.4.4.6 **OpenScape Business UC Suite > Externes Verzeichnis** 1753
28.4.4.7 **OpenScape Business UC Suite > Externer Anbieter** 1754
28.4.4.8 **OpenScape Business UC Suite > Contact Center** 1755
28.4.4.9 **OpenScape Business UC Suite > Zeitpläne** 1764
28.4.4.10 **OpenScape Business UC Suite > Datei-Upload** 1765
28.4.4.11 **OpenScape Business UC Suite > Konferenzschaltung** 1767
28.4.4.12 **OpenScape Business UC Suite > Standort-Liste** 1767
28.4.4.13 **OpenScape Business UC Suite > Server** 1767
28.4.4.14 **OpenScape Business, UC Suite > Profile** 1774
28.4.4.15 **OpenScape Business, UC Suite > Faxkopfzeilen** 1776
28.4.5 **Web Services** 1777
28.4.5.1 **Web Services > Web Collaboration** 1777
28.4.6 **Open Directory Service** 1778
28.4.6.1 **Open Directory Service > Grundeinstellungen** 1778
28.4.6.2 **Open Directory Service > Data Sources > OpenScape Business-Benutzer** 1778
28.4.6.3 **Open Directory Service > Datenquellen > LXV3** 1779

28.4.6.4 **Open Directory Service** > **Datenquellen** > **LXV3** 1779
28.4.6.5 **Open Directory Service** > **Wartung** 1779
28.4.7 **Application Launcher** 1779
28.4.7.1 **Application Launcher** 1780
28.5 **Middleware** 1780
28.5.1 Ansage-Player 1780
28.5.2 Csta Message Dispatcher (CMD) 1780
28.5.3 Csta Service Provider (CSP) 1781
28.5.4 DSS-Server 1782
28.5.5 Media Extension Bridge (MEB) 1782

29 Anhang 1783
29.1 Unterstützte Standards 1783
29.2 Euro-ISDN-Leistungsmerkmale 1785
29.3 Verwendete Ports 1787
29.4 Projektierung der DSP-Kanäle für die Kommunikationssysteme OpenScape Business X3/X5/X8 1789

30 Glossar 1800
30.1 Glossar 1800

Index 1816

1 Versionsgeschichte von Änderungen

Die in der diesem Kapitel genannten Änderungen sind kumulativ.

Änderungen in V3R4 FR3

Betroffene Kapitel	Beschreibung der Änderung	Fehler Nr.	Datum
Trunks/RoutingTrunkgruppe auf Seite 1709	Korrektur für COLP (ITSP-Themen)	62	Okt. 2025
Assistenten - Cloud Services auf Seite 127 CloudLink Service auf Seite 1214 So konfigurieren Sie den Cloud Link-Dienst auf Seite 1214 So konfigurieren Sie die CloudLink Dämon-Webschnittstelle auf Seite 1215 So aktivieren/konfigurieren Sie den SIP-Connector für die Verbindung mit Workflow Studio auf Seite 1216 (neu) CloudLink-Pilotnummern auf Seite 1217 (neu) So konfigurieren Sie CloudLink-Pilotnummern auf Seite 1217 (neu)	Container-Unterstützung, SIP-Connector und CL-Pilotnummern aktivieren	62	Sept. 2025
Inventar auf Seite 1284	Neugestaltung der OCCe-Hardware	62	Sept. 2025

Änderungen in V3R4 FR2

Betroffene Kapitel	Beschreibung der Änderung	Fehler Nr.	Datum
Migration von OpenScape Business X V2 zu OpenScape Business X V3 auf Seite 1396	Hinweis bezüglich der nicht standardmäßigen DSP-IP-Adresse während der Migration hinzugefügt.	61	10. Sept. 2025
HilfsausrüstungAnsagen auf Seite 1727	Link zu „Konfiguration > Ankündigungen > In Gateway laden“ im WAVE-Dateiparameter hinzugefügt.	60	Sept. 2025
Heim-Mobilität auf Seite 987	Hinweis bezüglich Einschränkungen bei mehreren SIP/HFA-Geräten und NAT hinzugefügt.	56	Juli 2025
Open Directory Service auf Seite 1188	Hinweis bezüglich der Integration von Microsoft Excel in die ODS-Datenbank hinzugefügt.	56	Juli 2025
Eingehende AnrufeGruppen/ Huntgruppen auf Seite 1691	Hinweis zur Abhängigkeit von der Anrufweiterleitung (*1) an eine andere Hunt-Gruppe, Anrufwartegruppe und RNA-Gruppe hinzugefügt.	56	Juli 2025

Betroffene Kapitel	Beschreibung der Änderung	Fehler Nr.	Datum
Voraussetzungen für UC Suite PC-Clients auf Seite 544	Aktualisierungen für Betriebssysteme, Office-/ Outlook-Anwendungen, zusätzliche Software (z. B. Java/OpenJDK).	56	Juli 2025
Assistenten – Telefone / Abonnenten auf Seite 123 Struktur der Administratoren-Dokumentation auf Seite 69 Teilnehmer auf Seite 428 Mitel SIP DECT-Teilnehmer auf Seite 445 neu So konfigurieren Sie Mitel SIP-DECT-Teilnehmer über die Bereitstellung auf Seite 470 neu TeilnehmerTeilnehmerTeilnehmer-Parameter auf Seite 1669 So konfigurieren Sie SIP-Teilnehmer über den Expertenmodus auf Seite 472 neu	Aktualisierungen für die Bereitstellung von MITEL SIP-DECT	55	Mai/Juni 2025
Hilfsausrüstung auf Seite 1726 HilfsausrüstungAnsagen auf Seite 1727 HilfsausrüstungPhoneMail auf Seite 1727 So konfigurieren Sie die Ansagen (UC Suite & UC Booster) auf Seite 1248 So konfigurieren Sie die Ansagen (UC Smart) auf Seite 1249	Aktualisierungen für die Konfiguration von Ansagen	55	Mai/Juni 2025
Voice GatewayInternet-Telefonie-Dienstanbieter auf Seite 1637	Aktualisierungen für ITSP-Profile	55	Mai/Juni 2025

Änderungen in V3R4 FR1

Betroffene Kapitel	Beschreibung der Änderung
Teamschaltung / Team-Gruppe auf Seite 712 Basis-MULAP auf Seite 731	Überarbeiteter Absatz "Bestellung von Mulap-Mitgliedergeräten" für LAN/WAN mit UP.
Installation der Kommunikationssoftware auf Seite 227	Hinweis zur DHCP-Konfiguration von Yast oder WBM hinzugefügt.
WBM-Benutzerverwaltung auf Seite 118	Hinweis für die Protokollierung der Administratorrolle hinzugefügt.

Betroffene Kapitel	Beschreibung der Änderung
SIP-Stationen auf Seite 441 Gruppenruf auf Seite 691 Gruppennummer auf Seite 695	Updates in der Liste der Dienstcodes, die mit SIP-Geräten kompatibel sind.
Internetzugang auf Seite 168 Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port auf Seite 179 Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port auf Seite 245 Voice GatewayInternet-Telefonie-Dienstanbieter auf Seite 1637	Updates zu LAN/WAN und ITSP auf WAN.
So aktivieren und konfigurieren Sie den internen DHCP-Server auf Seite 147 So aktivieren Sie DHCP nur für Mitel/Unify Geräte auf Seite 149 Aktivieren und Konfigurieren des DHCP-Servers der Hardwareplattform auf Seite 359 NetzwerkschnittstellenHauptplatine DHCP-ModusDHCP-Server Globale Parameter auf Seite 1609 Netzwerkschnittstellen HauptplatineDHCP-Modus DHCP-ServerIP-Adresspools auf Seite 1611 Netzwerk-Schnittstellen HauptplatineDHCP-Modus DHCP-ServerStatische IP-Adressen auf Seite 1612	Aktualisierungen für die Subnetz-Behandlung von DHCP für Mitel/Unify-Geräte und Relais-Option.

Änderungen in V3R4

Betroffene Kapitel	Beschreibung der Änderung
Basis-MULAP auf Seite 731	SIP-Telefone wurden von einem der grundlegenden MULAP-Mitglieder entfernt.
Details zur Verwendung von DSP-Kanälen auf Seite 1461	Updates bezüglich Sicherheit und ITSP.
Open Directory Service Data Sources OpenScape Business-Benutzer auf Seite 1778	Updates bezüglich ODS Light.
Sprach-GatewayNativer SIP-Server-Trunk auf Seite 1651	Direkte Medien- und Nutzlastverschlüsselung für Unify Phone.
Unify Phone auf Seite 1206	myAgent zu UC-Clients von Drittanbietern mit Anrufsteuerung hinzugefügt.

Betroffene Kapitel	Beschreibung der Änderung
UC Software Modelle (Softswitch) auf Seite 107 UC Booster Hardware auf Seite 106 Wie Sie die Kommunikationssoftware installieren auf Seite 229 Voraussetzungen für die Ersteinrichtung auf Seite 222 Ersteinrichtung von OpenScape Business S auf Seite 222 Voraussetzungen für die Ersteinrichtung auf Seite 279 Ersteinrichtung OpenScape Business UC Booster auf Seite 277 Ersteinrichtung OpenScape Business UC Booster auf Seite 277 So aktualisieren Sie UC Business Booster Server V2 auf V3 auf Seite 1393	SLES 15-Unterstützung für OpenScape Business S und UC Booster Server.

Änderungen in V3R3 FR2 GA Update

Betroffene Kapitel	Beschreibung der Änderung
Desk Sharing auf Seite 971	Korrektur für den Hinweis zum Desk Sharing-Merkmal.
Verwendete Ports auf Seite 270	Konsolidierung und Korrektur der verwendeten Ports für CAR-Lebendigkeitsprüfungen.
Open Directory Service Data Sources OpenScape Business-Benutzer auf Seite 1778	Korrektur der Min- und Max-Werte für maximale interne und minimale externe Längen und Ausblenden von offenen Anrufen in der Journal-Schaltfläche.
Software-ImageSystem-Software Update via Internet auf Seite 1500	Fehlende Schaltfläche zum Bereinigen des Speichers vor dem Übertragen hinzugefügt.
Unify Phone auf Seite 1206 Wie fügen Sie bestehende Unify Phone-Benutzer hinzu auf Seite 1209	Informationen zu Unify Phone und Drittanwendungen hinzugefügt.
OpenScape Business, UC SuiteBenutzerverzeichnis auf Seite 1747 OpenScape Business UC Suite Server auf Seite 1767	Zwei Hinweise zu unterschiedlichen Benutzerpasswortlängen hinzugefügt und alle Benutzerpasswörter zurückgesetzt.
CloudLink Service auf Seite 1214 So konfigurieren Sie den Cloud Link-Dienst auf Seite 1214 So öffnen Sie die CloudLink Daemon-Webschnittstelle auf Seite 1215 So konfigurieren Sie die CloudLink Dämon-Webschnittstelle auf Seite 1215	Neue Kapitel für den CloudLink-Dienst hinzugefügt.

Änderungen in V3R3 FR2

Betroffene Kapitel	Beschreibung der Änderung
Sichern und Wiederherstellen auf Seite 1251	Hinweis zur Einschränkung bei der Unify Phone Cloud-Synchronisierung hinzugefügt.
-	Geänderte UI-Screenshots im gesamten Dokument.
Let's Encrypt-Dienst auf Seite 1212	BETA entfernt und neue Funktionalität für den Let's Encrypt-Dienst hinzugefügt.
Unterstützte Telefone auf Seite 108 Leistungsmerkmale auf Seite 519 Telefon-Logo ins System laden auf Seite 1241	Updates für die neuen unterstützten Geräte CP205T/ CP405T (TDM).

Änderungen in V3R3 FR1

Betroffene Kapitel	Beschreibung der Änderung
Unify Phone auf Seite 1206 Unify Phone-Konnektivität konfigurieren auf Seite 1207 Wie Sie Unify Phone-Benutzer erstellen auf Seite 1209 Wie fügen Sie bestehende Unify Phone-Benutzer hinzu auf Seite 1209 Unify Phone-Benutzerdetails bearbeiten auf Seite 1211	Aktualisierungen für den Verzeichnis- und Journalzugriff, den Bildschirm für das Nummerierungsschema und das Feld für die Amtskennziffer.
Assistenten - Cloud Services auf Seite 127 Let's Encrypt-Dienst auf Seite 1212	Assistent 'Cloud Services' und 'Lets encrypt'-Dienst hinzugefügt.
Open Directory Service auf Seite 1188	Der Abschnitt 'Open Directory Service und OpenScape Business-Hauptplatinen' wurde hinzugefügt.
Unify Phone-Benutzer verwalten auf Seite 1208 Wie Sie Unify Phone-Benutzer erstellen auf Seite 1209 Wie fügen Sie bestehende Unify Phone-Benutzer hinzu auf Seite 1209 Unify Phone-Benutzerdetails bearbeiten auf Seite 1211	Das Kapitel 'Wie Sie neue Unify Phone Benutzer erstellen' wurde hinzugefügt und die anderen Kapitel entsprechend aktualisiert.
Wie passen Sie eine alternative moderne Benutzeroberfläche für myPortal for Desktop an OpenScape Business UC Suite Skin-Einstellungen Wizards – UC Suite (nur mit UC Suite) auf Seite 126	Dateien und Erwähnungen für 'Skin-Einstellungen' entfernt.

Betroffene Kapitel	Beschreibung der Änderung
CSV-Datei vom lokalen Dateisystem in das externe Verzeichnis importieren auf Seite 572 Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen auf Seite 1196	Aktualisierungen in Bezug auf das Feld 'customer_id' für den Import und Export von Daten.
UC SmartGrundeinstellungenUC SmartGrundeinstellungen auf Seite 1745	Informationen über CloudService und andere fehlende Felder hinzugefügt.
Zeitgesteuerte Nachtschaltung konfigurieren auf Seite 777	Informationen zur Nachtmodus-Meldung auf der Landing Page des Admin-Portals hinzugefügt.
Voraussetzungen:myPortal to go auf Seite 958	Zusätzliche Unterstützung über 4G/5G-Datenverbindungen und Empfehlung von Datenflatrates.
Eingehende AnrufeGruppen/Huntgruppen auf Seite 1691	Informationen über die Umwandlung von Gruppentypen hinzugefügt.
Wie entfernen oder löschen Sie Unify Phone-Benutzer auf Seite 1211	Die Funktion zum Löschen oder Entfernen für Unify Phone-Benutzer bearbeitet.
Zeitplan hinzufügen auf Seite 925 Zeitplan ändern auf Seite 929	Es wurde ein Hinweis hinzugefügt, der die Eins-zu-Viel-Verknüpfung von Warteschlangen mit Zeitplänen erklärt.
Arbeiten im Team (Gruppen) auf Seite 689	Das Kapitel "17.1.3 Xpressions Compact" und seine Einträge aus dem Dokument entfernt. Update für reservierte Sammelanschlüsse.
Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP auf Seite 827	Einträge für Unify Phone und myPortal for Teams Anrufe hinzugefügt.
BerechtigungenTeilnehmer auf Seite 1719 Wie Sie die Berechtigungsgruppe für einen Sprachbox-Port ändern auf Seite 536	Hinweise zur Spracheinstellung von Dienstklassengruppen und EVM-Porttexten hinzugefügt.
Den Zeitplan Standard Schedule XYZ für das Beispiel-Contact-Center hinzufügen auf Seite 911 Den Zeitplan Standard Schedule Hotline für das Beispiel-Contact-Center hinzufügen auf Seite 916 Vorlagen (Templates) auf Seite 845 Zeitpläne auf Seite 837	Bild-Rebranding und der Ersatz für Contact Center. Auskommentiertes Bild für das Kapitel Zeitpläne wieder eingeführt.
Zeitpläne auf Seite 890	UCD (inkl. Contact Center) entfernt und eine Zeile bezüglich des CVV-Objekts Transfer to Queue hinzugefügt.

Änderungen in V3R3 X1R

Betroffene Kapitel	Beschreibung der Änderung
Gebührenabrechnung auf Seite 1492 Application Connectivity auf Seite 1489 Anruf-Routing auf Seite 1484 Anbindung an Service-Provider auf Seite 1463 Maximalwerte für Teilnehmer auf Seite 1454 Aufbau und Umweltbedingungen auf Seite 107 UC Hardware Modelle auf Seite 105 DECT-Teilnehmer auf Seite 444 Funktionen am Telefon auf Seite 1477 Maximalwerte für Leitungen auf Seite 1457 Maximalwerte der Ressourcen auf Seite 1459 Mobility Ausbaugrenzen auf Seite 1486 Multimedia Contact Center auf Seite 1486 Vernetzung von OpenScape Business auf Seite 1489 Sicherheit auf Seite 1488 Smart Voicemail Ausbaustufen auf Seite 1467 Teilnehmer auf Seite 1463 UC Smart-Ausbaustufen auf Seite 1463 Arbeiten im Team (Gruppen) auf Seite 1480	Updates für X1R

Änderungen in V3R3

Betroffene Kapitel	Beschreibung der Änderung
Migration auf Seite 1389	Hinweis zum Löschen von Unify-Telefonbenutzern hinzugefügt.
Updates auf Seite 1260 Lizenzierung auf Seite 297 Vernetzung von OpenScape Business auf Seite 1058	Informationen zur Netzwerk-Lizenzierung bei der Aktualisierung von Systemen hinzugefügt.
Neuflash auf Seite 219 Neuflash auf Seite 274	Zwei neue Kapitel über das Neuflash-Merkmal wurden hinzugefügt.
Lizenzierungsverfahren auf Seite 298 Verwendete Ports auf Seite 270 Aktivierung von CLS Connect auf Seite 313	Erwähnungen des veralteten Ports 7780 entfernt
Traces auf Seite 1322 Traces auf Seite 1508	Abschnitt für RtpProxy Trace gelöscht, da dieser Trace im WBM nicht mehr verfügbar ist

Betroffene Kapitel	Beschreibung der Änderung
Traces Medienserver-Trace auf Seite 1520 Wie Sie den Medienserver-Trace starten auf Seite 1344 Wie Sie den Medienserver-Trace anhalten auf Seite 1345	Neue Kapitel für Medienserver
OpenScape Business, UC SuiteBenutzerverzeichnis auf Seite 1747 OpenScape Business UC Suite Server auf Seite 1767	Updates des Datums- und Zeitformats
Wie entfernen oder löschen Sie Unify Phone-Benutzer auf Seite 1211	Updates über den Austausch von SDHC-Karten
myPortal for Teams im Überblick auf Seite 1204	myPortal for Teams: Unterstützung der Anrufsteuerung
GrundeinstellungenTelefonparameter-Bereitstellung auf Seite 1571	Updates für kanonische Wähleinstellungen
Migration auf Seite 1389	Zwei Hinweise zu bewährten Migrationsverfahren und Fehlerquellen hinzugefügt.
Teilnehmer lizenzieren (Standalone) auf Seite 319 User-orientierte Lizenzen auf Seite 303	Zwei Hinweise zur Zuweisung von Voicemail-Lizenzen hinzugefügt.
Software-ImageSystem-Software Update via File Upload auf Seite 1501 System über einen Datei-Upload aktualisieren auf Seite 1267	Informationen über das neue Kennzeichen für die Aktualisierung per Datei-Upload hinzugefügt.
Nachbearbeitung auf Seite 899 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" hinzufügen auf Seite 946	Informationen über Mehrfach-Umschlag und Gruppen hinzugefügt.
Wie Sie einen weiteren LAN-Anschluss als WAN-Schnittstelle aktivieren auf Seite 234 Wie wählen Sie den Ländercode und die Sprache für Trace-Protokolle aus auf Seite 233 Wie Sie das Sie das Anzeigelogo und den Produktnamen festlegen auf Seite 232	Der UI-Screenshot wurde ersetzt, um die Marke mit den Auswirkungen in den verlinkten Kapiteln anzuzeigen.

Betroffene Kapitel	Beschreibung der Änderung
Unify Phone-Konnektivität konfigurieren auf Seite 1207 Assistenten - Cloud Services auf Seite 127 Wie Sie den Internet-Zugang über einen Standard-ISP PPPoE konfigurieren auf Seite 381 Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP auf Seite 827 Systemlizenzen auf Seite 305 Maximalwerte für Teilnehmer auf Seite 1454 Vordefinierten ITSP konfigurieren auf Seite 182 Internet-Zugang über vorkonfigurierten ISP konfigurieren auf Seite 172 TeilnehmerTeilnehmerTeilnehmer-Parameter auf Seite 1669	Kapitel und Verweise auf das Produkt Circuit entfernt.

Änderungen in V3R2 FR1

Betroffene Kapitel	Beschreibung der Änderung
Konfiguration der Aufzeichnung von Konferenzen auf Seite 600 Aufzeichnung von Anrufen aktivieren oder deaktivieren auf Seite 592	Neues Kontrollkästchen, um die Aufzeichnung von Konferenzen zu aktivieren oder zu deaktivieren
Traces Kernel-Crash-Daten auf Seite 1519 Kernel Crash-Datendienst starten auf Seite 1343 Kernel Crash-Datendienst anhalten auf Seite 1344	Neuer Kernel Crash-Datendienst
Vorschläge für Lizenzkombinationen auf Seite 309	Hinzufügen von Informationen über die aktiven Lizenzen, die für die Nutzung der Funktionen von Contact Center und Company AutoAttendant erforderlich sind
TeilnehmerTeilnehmerTeilnehmer-Parameter auf Seite 1669	Hinweis darauf, dass das Feld **Rufnummer des vertrauenswürdigen externen Teilnehmers** obligatorisch ist
OpenScape Business UC Suite Server auf Seite 1767	Neue Option zum Löschen von Rückrufnachrichten, live aufgezeichneten Anrufen, Faxanrufen und mit Anrufen verknüpften E-Mails nach einer bestimmten Zeitspanne
Regel (CCV) als Backup-Datei herunterladen auf Seite 931 Heruntergeladene Regel (CCV) in einem Sicherungsdateiformat hochladen auf Seite 932	Neue Kapitel für das Herunterladen und Hochladen einer Regel (CCV)

Betroffene Kapitel	Beschreibung der Änderung
UC Suite auf Seite 540 Multimedia Contact Center auf Seite 873 Wartung auf Seite 1238 Experten-Modus auf Seite 1493	Aktualisierungen der Benutzeroberfläche in ganzen betroffenen Kapiteln
E-Mail-Versand konfigurieren auf Seite 205 OpenScape Business UC SuiteExterner Anbieter auf Seite 1754 OpenScape Business UC Suite Contact Center auf Seite 1755 Warteschlangen für das Beispiel-Contact-Center hinzufügen auf Seite 918 Warteschlange hinzufügen auf Seite 932 Warteschlange ändern auf Seite 936 OpenScape Business-System unter Verwendung von einfacher Authentifizierung mit Microsoft Office 365 verbinden auf Seite 629 OpenScape Business-System unter Verwendung von moderner Authentifizierung mit Microsoft Office 365 verbinden auf Seite 635	Support für OAuth 2.0-Authentifizierung
myReports auf Seite 877	myReports-Administratoren können nicht mehr das E-Mail-Konto konfigurieren, das für den Versand von Berichten per E-Mail verwendet werden soll
myPortal for Teams im Überblick auf Seite 1204	myPortal for Teams: Support für Wähltastatur und Favoriten
Voraussetzungen:myPortal to go auf Seite 958	Aktualisierte Voraussetzungen für den myPortal to go iOS-Client
Teilnehmerverwaltung auf Seite 865	Auf myAttendant wurde die Standardanzahl der Benutzertasten erhöht und kann geändert werden
Benutzer von UC Suite auf Seite 552 OpenScape Business, UC SuiteBenutzerverzeichnis auf Seite 1747	Aktualisierte Liste der unterstützten Dateiformate für das Hochladen eines Bildes

Betroffene Kapitel	Beschreibung der Änderung
Benutzerzugriff auf UC-Funktionen (UC Clients) auf Seite 98 Unterstützte Telefone auf Seite 108 Deployment Service (DLI und DLS) auf Seite 367 UC Smart Clients auf Seite 495 Voraussetzungen für myPortal @work auf Seite 497 Verzeichnisse für Systemtelefone konfigurieren auf Seite 516 Leistungsmerkmale auf Seite 519 Voraussetzungen für UC Suite PC-Clients auf Seite 544 Teamschaltung / Team-Gruppe auf Seite 712 OpenScape Business Attendant auf Seite 848 myAttendant auf Seite 863 Voraussetzungen für myAgent auf Seite 875 Telefon-Logo ins System laden auf Seite 1241 Automatisches Reflashing konfigurieren auf Seite 1271 Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 So aktualisieren Sie UC Business Booster Server V2 auf V3 auf Seite 1393 Hardware/Software-Migration von OpenScape Business X Systemen auf V3 auf Seite 1395 Software-Aktualisierung von OpenScape Business S auf Seite 1404 UC Smart-Ausbaustufen auf Seite 1463 UC Suite-Ausbaustufen auf Seite 1469 Application Connectivity auf Seite 1489	Neue unterstützte Telefone: • OpenScape Desk Phone CP 210 • OpenScape Desk Phone CP 710
Unterstützte Telefone auf Seite 108	Neue unterstützte Beistellgeräte: • OpenScape Key Module 410 • OpenScape Key Module 710
GrundeinstellungenSystem LDAP auf Seite 1556	Hinweis auf die Anzeige von LDAP-Quellen hinzugefügt.
DISA auf Seite 678	Hinweis zum Anruf von DISA-Nummern in OSBiz S und OSBiz X hinzugefügt.
OpenScape Business UC Suite Server auf Seite 1767	DB-Tabelleneintrag entfernt.
Open Directory Service auf Seite 1188	Externe Datenquellen wurden geändert und Informationen zum Feld 'Beschreibung' hinzugefügt.

Betroffene Kapitel	Beschreibung der Änderung
So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346	Text zu Problemen mit der UC Fax-Funktionalität hinzugefügt.
Migration von OpenScape Business X1 V2 auf OpenScape Business X1W V3 auf Seite 1450	Kapitel zur Migration von X1 V2 auf X1W V3 hinzugefügt.
Umschaltung von CLS Connect auf Seite 314	Einführung des Kapitels Umschalten von CLS connect.
So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346	Migration OCCLA eigenständig
Remote-Zugang auf Seite 1381 Übersicht über Funktionen und Codes auf Seite 684 IP-Adressen-Schema auf Seite 137 Wie Sie den Remote-Zugang über ISDN einschalten auf Seite 1382 Wie Sie einen PC mit Microsoft Windows Vista für Remote-Zugang über ISDN konfigurieren auf Seite 1382 Wie Sie einen PC mit Microsoft Windows 7 für Remote-Zugang über ISDN konfigurieren auf Seite 1384	Veraltete Fernzugriffsmethoden wurden geändert und die letzten drei Kapitel entfernt.
Migration von OpenScape Business X1 V2 auf OpenScape Business X1W V3 auf Seite 1450	Kapitel zur Migration von X1 V2 auf X1W V3 hinzugefügt.
Sprach-GatewayNativer SIP-Server-Trunk auf Seite 1651	Tabelleneinträge für Transport- und Mediensicherheit hinzugefügt.
OpenScape Business UC Suite Server auf Seite 1767	Text über den Neustart der UC-Anwendung hinzugefügt.
Umschaltung von CLS Connect auf Seite 314	Kapitel zum Umstellen von CLS Connect hinzugefügt.
OpenScape Business UC Suite Server auf Seite 1767	Text über den Neustart der UC-Anwendung hinzugefügt.
Sprach-GatewayNativer SIP-Server-Trunk auf Seite 1651	Tabelleneinträge für Transport- und Mediensicherheit hinzugefügt.
Remote-Zugang auf Seite 1381	Veraltete Fernzugriffsmethoden entfernt.
Umschaltung von CLS Connect auf Seite 314	Kapitel zum Umstellen von CLS Connect hinzugefügt.

Änderungen in V3R2

Betroffene Kapitel	Beschreibung der Änderung
Unterstützte Telefone auf Seite 108 Voraussetzungen für myPortal @work auf Seite 497 Leistungsmerkmale auf Seite 519 Voraussetzungen für UC Suite PC-Clients auf Seite 544 OpenScape Business Attendant auf Seite 848 myAttendant auf Seite 863 Voraussetzungen für myAgent auf Seite 875 Automatisches Reflashing konfigurieren auf Seite 1271 Bedeutung der Ergebnisse beim Test des Funkbereichs auf Seite 977	Neue unterstützte Telefone: • OpenScape Desk Phone CP 110 • OpenScape DECT Phone S6/SL6/R6
myPortal for Teams im Überblick auf Seite 1204	myPortal for Teams: Journal-Support
Vertriebliche Ausbaustufen auf Seite 102 Maximalwerte für Teilnehmer auf Seite 1454 UC Smart-Ausbaustufen auf Seite 1463 UC Suite-Ausbaustufen auf Seite 1469 Mobility Ausbaugrenzen auf Seite 1486 Application Connectivity auf Seite 1489	myPortal for Teams: Ausbaugrenzen und Kapazitäten
myPortal @work auf Seite 495	Anklopf-Szenarien mit myPortal @work werden unterstützt
Unify Phone auf Seite 1206 Unify Phone-Konnektivität konfigurieren auf Seite 1207 Unify Phone-Benutzer verwalten auf Seite 1208 Wie fügen Sie bestehende Unify Phone-Benutzer hinzu auf Seite 1209 Unify Phone-Benutzerdetails bearbeiten auf Seite 1211 Wie Sie alternative Nummern und Anruf-Routing für das Unify Phone-Interworking einrichten auf Seite 1212 GrundeinstellungenSystem System Flags auf Seite 1534	Neue/aktualisierte Kapitel für Unify Phone-Konnektivität

Betroffene Kapitel	Beschreibung der Änderung
Lizenzen auf Seite 300 Vorschläge für Lizenzkombinationen auf Seite 309 Benutzerlizenzen auf Seite 302 User-orientierte Lizenzen auf Seite 303 Systemlizenzen auf Seite 305 Lizenzzuordnung (Standalone) auf Seite 317 Teilnehmer lizenzieren (Standalone) auf Seite 319 Lizenzzuordnung (Netzverbund) auf Seite 328 Wie Sie Teilnehmer lizenzieren (Netzverbund) auf Seite 330	Neue Unify Phone-Lizenz
Details zur Verwendung von RTP-Proxykanälen auf Seite 1462	Hinzufügen von Informationen über die erforderlichen RTP-Proxy-Kanäle pro Unify Phone-Anruf
Anwesenheitsstatus (Präsenz) auf Seite 561	Hinweis zur Sichtbarkeit des Anwesenheitsstatus hinzugefügt.
Benutzer von UC Suite auf Seite 552	Hinweis auf Einschränkung beim Ändern des Benutzernamens hinzugefügt.
Lizenzierung auf Seite 297	Umbenennung von OCCLA und OCCL in V3-Hauptplatine bzw. V2-Hauptplatine, in den Kapiteln 8.11 bis 8.14

Änderungen in V3R1 FR2

Betroffene Kapitel	Beschreibung der Änderung
Voraussetzungen:myPortal to go auf Seite 958	myPortal to go: iOS CallKit-Support
RSP.servicelink auf Seite 1375	RSP-Anmeldedaten im Backup-Set speichern
OpenScape Business, UC SuiteGruppen auf Seite 1751 OpenScape Business, UC SuiteProfile auf Seite 1774	UC Suite Favoritengruppen
Trunks/RoutingTrunkgruppe auf Seite 1709 TeilnehmerTeilnehmerTeilnehmer-Parameter auf Seite 1669	Vertrauenswürdiger SBC
myPortal @work auf Seite 495	myPortal @work: Anrufübernahme-Support
myPortal for Teams im Überblick auf Seite 1204 myPortal for Teams konfigurieren auf Seite 1205 So laden Sie myPortal for Teams in den Teams-Speicher hoch auf Seite 1206	myPortal for Teams

Änderungen in V3R1 FR1

Betroffene Kapitel	Beschreibung der Änderung
Ausnahme in CCV hinzufügen auf Seite 844	Neuer CCV-Ausnahmetyp hinzugefügt

Betroffene Kapitel	Beschreibung der Änderung
OpenScape Business UC Suite Server auf Seite 1767	Parameter **Gesprächsverfolgung deaktivieren** hinzugefügt
OpenScape Business UC Suite Server auf Seite 1767	Parameter **Verzeichnis-Suchcache läuft ab in** hinzugefügt

Änderungen in V3R1

Betroffene Kapitel	Beschreibung der Änderung
• Unterstützte Telefone auf Seite 108 • Voraussetzungen für myPortal @work auf Seite 497 • Deployment Service (DLI und DLS) auf Seite 367 • Leistungsmerkmale auf Seite 519 • myAttendant auf Seite 863 • Voraussetzungen für myAgent auf Seite 875 • OpenScape Business Attendant auf Seite 848 • Automatisches Reflashing konfigurieren auf Seite 1271 • Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 • Hardware/Software-Migration von OpenScape Business X Systemen auf V3 auf Seite 1395 • Software-Aktualisierung von OpenScape Business S auf Seite 1404 • UC Smart-Ausbaustufen auf Seite 1463 • UC Suite-Ausbaustufen auf Seite 1469 • Application Connectivity auf Seite 1489	Neue unterstützte Telefone OpenScape Deskphone CP 700 und CP 700X
Unterstützte Telefone auf Seite 108	Neue unterstützte Telefone OpenScape WLAN Phone WL4/WL4 Plus
• Voice GatewayInternet-Telefonie-Dienstanbieter auf Seite 1637 • Sprach-GatewayNativer SIP-Server-Trunk auf Seite 1651 • StatistikenTelephonie Statistiken TZustand Leitung auf Seite 1740	ITSP-Verbesserungen
OpenScape Business UC Suite Externes Verzeichnis auf Seite 1753	Neue Schaltfläche **Alle entfernen**
OpenScape Business UC Suite Server auf Seite 1767	Neues Flag **Agentennamen bei Agentenzuweisung für Warteschlange in myAgent anzeigen** für die Anzeige von Benutzernamen zusammen mit deren Durchwahlnummern.
Anzeigen von Massendaten auf Seite 164	Massendaten sind auch im Menü der obersten Ebene der Setup-Assistenten verfügbar.
Grundinstallation> Massendaten auf Seite 1574	Zwei neue Spalten für **Mobile Rufnr** und **E-Mail-Adresse** hinzugefügt.
BerechtigungenAutomatische Nachtschaltung auf Seite 1725	Funktion **Kopierdienst** hinzugefügt.

Betroffene Kapitel	Beschreibung der Änderung
• Maximalwerte für Teilnehmer auf Seite 1454 • Maximalwerte für Leitungen auf Seite 1457 • Anbindung an Service-Provider auf Seite 1463 • UC Smart-Ausbaustufen auf Seite 1463 • Smart Voicemail Ausbaustufen auf Seite 1467 • UC Suite-Ausbaustufen auf Seite 1469 • Arbeiten im Team (Gruppen) auf Seite 1480 • Mobility Ausbaugrenzen auf Seite 1486 • Application Connectivity auf Seite 1489	Höchstwerte für neue Baugruppen aktualisiert.
• E-Mail-Versand konfigurieren auf Seite 205 • Wie Sie E-Mail-Einstellungen für Events ändern auf Seite 1350 • EventsE-Mail auf Seite 1521	Sicherheitsbeauftragten vor Ort für Notrufe benachrichtigen
• So aktualisieren Sie UC Business Booster Server V2 auf V3 auf Seite 1393 • Software-Aktualisierung von OpenScape Business S auf Seite 1404	Sicherheit - OpenSSL V1.1.1
Automatische Weiterleitung von Systemprotokolldateien auf Seite 1343	Linux Syslog-Dateien extern weiterleiten
Grundinstallation> Massendaten auf Seite 1574	UC-Mobiltelefonnummer wurde in der Konfiguration des Assistenten für Massendaten hinzugefügt
Diagnose-Traces für einen Fehlerfall erfassen auf Seite 218	Automatische Erfassung und Übertragung von Diagnosedaten

Änderungen in V3

Betroffene Kapitel	Beschreibung der Änderung
UC Software Modelle (Softswitch) auf Seite 107 UC Booster Hardware auf Seite 106 Wie Sie die Kommunikationssoftware installieren auf Seite 229 Voraussetzungen für die Ersteinrichtung auf Seite 222 Ersteinrichtung von OpenScape Business S auf Seite 222 Voraussetzungen für die Ersteinrichtung auf Seite 279 Ersteinrichtung OpenScape Business UC Booster auf Seite 277	Aktualisierung auf SLES 12 SP5.
Circuit So richten Sie die Circuit-Voicemail-Nummer ein So richten Sie alternative Nummer und Anruf-Routing für das Circuit-Interworking ein	Circuit verbesserte Kooperation.

Betroffene Kapitel	Beschreibung der Änderung
UC SmartBenutzerverwaltung auf Seite 1746 Migration innerhalb von OpenScape Business V3 auf Seite 1447 Vorschläge für Lizenzkombinationen auf Seite 309 User-orientierte Lizenzen auf Seite 303 Systemlizenzen auf Seite 305 Szenario 5: OpenScape Business BLF an einem OpenScape Business Einzelsystem auf Seite 861 Szenario 6: OpenScape Business BLF an einem OpenScape Business Netzverbund (BLF und Anwesenheitsstatus über WSI) auf Seite 863 OpenScape Business BLF auf Seite 851 OpenScape Business TAPI 120 auf Seite 1177 Grundeinstellungen für UC Smart auf Seite 491 myPortal @work auf Seite 495	UC Suite-Lizenzen für UC Smart Clients.
So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346	Blockieren von OptiPoint-Geräten auf V3 OCC Evolution.
So melden Sie sich bei der WBM an auf Seite 117	Externen WBM-Zugriff absichern.
So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346 So migrieren Sie den Master-Knoten eines vernetzten Systems von V2-Mainboard zu V3-Mainboard auf Seite 348 So migrieren Sie den Slave-Knoten eines vernetzten Systems von V2-Mainboard zu V3-Mainboard auf Seite 349 Migration von HiPath 3000 Systemen auf OSBiz V3 Software mit V3 Mainboard auf Seite 349 Aktualisierung von V2 auf V3 mit CLS Connect auf Seite 350 Aktualisierung von V2 auf V3 ohne CLS Connect auf Seite 350	OCC Evolution.
Telefon-Logo ins System laden auf Seite 1241	Unterstützung des Ladens von CP-Telefon-Logo mit WBM
Automatische Updates auf Seite 551 myPortal @work auf Seite 495 myPortal @work auf Seite 543	Aktualisierungen für myPortal @work

Änderungen in V2R7

Betroffene Kapitel	Beschreibung der Änderung
Wizards – Zentrale Telefonie Active Directory Integration Service Wie Sie die den Active Directory Service konfigurieren Active Directory Integration Service	Informationen zum Active Directory Integration Service wird hinzugefügt
Station > Station > Station-Parameter	Option zur Deaktivierung der PW-Steuerung gelöscht
Circuit	Anruf weiterschalten/verschieben, Konferenzrufe und Funktion zur Information Belegt in einem Anruf hinzugefügt
OpenScape Business UC Suite > Server	Flag Bearbeitung des Namens deaktivieren hinzugefügt
OpenScape Business, UC Suite > Profile	Abkürzungstastengruppe in UC Suite Profileinstellungen hinzugefügt
myPortal @work	Verfügbarkeit auf MacOS hinzugefügt
UC Software Modelle (Softswitch) UC Booster Hardware Migration eines HiPath 3000 Standalone-Systems mit OpenScape Office V3 HX Wie Sie die Kommunikationssoftware installieren Voraussetzungen für die Ersteinrichtung Ersteinrichtung von OpenScape Business S Voraussetzungen für die Ersteinrichtung Ersteinrichtung OpenScape Business UC Booster	Unterstützung von SLES 12 SP3 hinzugefügt
Voice Gateway > Internet-Telefonie-Dienstanbieter Voice Gateway > Native SIP-Server-Trunk	Wiki-Informationen hinzugefügt (ITSP)

Änderungen in V2R6FR2

Anmerkung: Dieses Dokument kann Beschreibungen für Funktionen enthalten, die sich möglicherweise noch im Beta-Stadium befinden. Weitere Informationen finden Sie in den Verkaufsinformationen und Freigabemitteilungen.

- Vorschläge für Lizenzkombinationen
  - Hinzugefügte Lizenzen für myPortal @work VoIP-Telefonie
- myPortal @work
  - Hinzugefügte VoIP-Informationen
- Voraussetzungen für myPortal @work
  - Hinzugefügte VoIP-Informationen

- Wartemusik
  - Verwendung von importierten MoH-Ansagen in UC Suite
- Wie Sie interne Wartemusik importieren
  - Verwendung von importierten MoH-Ansagen in UC Suite
- OpenScape Business UC Suite > Server
  - Konversation schließen nach dem Hinzufügen eines Flag

1.1 Versionsgeschichte von Verbesserungen/Fixes

Die in der diesem Kapitel genannten Änderungen sind kumulativ.

Änderungen in V3R4 FR2

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel	Fehler Nr.
PRB000086522	23. Okt. 2025	Abschnitt mit Richtlinien für die Erweiterung des Subnetzbereichs hinzugefügt.	Ersteinrichtung von OpenScape Business X auf Seite 133	63
PRB000086522	26. Aug. 2025	Erklärung zur gleichzeitigen Verbindung von zwei ITSPs über LAN und WAN hinzugefügt.	Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port auf Seite 179	59
PRB000081445	18. Aug. 2025	Anmerkungen zur automatischen Generierung von Medienkanälen hinzugefügt.	So konfigurieren Sie die UC Suite auf Seite 202 So konfigurieren Sie die UC Suite auf Seite 256	58
PRB000082631	15. Jan. 2025	Informationen zu IP-Clients > Geräteinformationen, Registerkarte „WBM“, Sortiermechanismus hinzugefügt.	StationStationIP-Clients auf Seite 1659	57

Änderungen in V3R4 FR1

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000082944	22. Apr. 2025	Hinweis hinzugefügt, dass die Benutzerdaten von Unify Phone nicht Teil der Exportdatei sind, hinzugefügt.	KonfigurationPort-Konfiguration auf Seite 1495

Änderungen in V3R4

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000080604	19 Feb. 2025	Der Satz über die Telefonnummer, die für ausgehende Anrufe verwendet werden soll, wenn keine DID-Nummer des Anrufers verfügbar ist, wurde geändert.	Vordefinierten ITSP konfigurieren auf Seite 182 Vordefinierten ITSP konfigurieren auf Seite 393
PRB000080170	15 Jan. 2025	Korrektur der Beschreibung des Tabelleneintrags des Anzeigenamen-Anzeigealgorithmus.	Grundeinstellungen System Display auf Seite 1548
PRB000077322	09 Dez. 2024	Korrektur der Maximalwerte für Stationen und TDM-Stationen für X1R/W.	Maximalwerte für Teilnehmer auf Seite 1454

Änderungen in V3R3 FR2 GA Update

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000079549	15 Sep 2024	Korrektur auf Schritt 5 der E-Mail-Benachrichtigungen.	So konfigurieren Sie E-Mail-Benachrichtigungen über Systemfehler auf Seite 1370
PRB000076788	13 Sep 2024	Hinweis zur Anwendungsfirewall hinzugefügt.	Sicherheit Anwendungsfirewall auf Seite 1575 Application Firewall auf Seite 1002 Überlebensfähigkeit auf Seite 1152
PRB000075233	18 Juli 2024	Korrekturen der Priorität von Zeitplänen und ihrer Ausnahmen.	Ausnahme in CCV hinzufügen auf Seite 844
PRB000077767	28 Aug 2024	Hinweis zur Anrufweiterleitung an die Voicemail-Box hinzugefügt.	Anwesenheitsstatus (Präsenz) auf Seite 561
PRB000076194	18 Juli 2024	Korrektur der Werte für verwendete Ports von CAR-Lebendigkeitsprüfungen	Verwendete Ports auf Seite 270

Änderungen in V3R3 FR2

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000076191	13. Juni 2024	Korrektur der Werte für X1 a/b-Ankündigungen und MEB-Kanäle für X1W /R	Maximalwerte für Leitungen auf Seite 1457 Maximalwerte der Ressourcen auf Seite 1459
PRB000076108	13. Juni 2024	Korrektur der CLS-Ports und neuer Abschnitt am Ende des Kapitels	Verwendete Ports auf Seite 270

Änderungen in V3R3 FR1

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000072445	1. April 2024	Die "Maximale lokale Nummernlänge" in den kanonischen Wähleinstellungen hinzugefügt	GrundeinstellungenTelefonparameter-Bereitstellung auf Seite 1571
PRB000074047	15. März 2024	Hinweis hinzugefügt, um zu erklären, wie das Kennzeichen "Daten vor dem Import entfernen" funktioniert.	CSV-Datei vom lokalen Dateisystem in das externe Verzeichnis importieren auf Seite 572
PRB000072007	1. April 2024	Ein neues Kapitel „Ändern des Wahlplans auf 4 Ziffern“ und zugehörige Informationen hinzugefügt.	Wie ändern Sie den Wahlplan auf 4 Ziffern auf Seite 235, Systemeinstellungen auf Seite 232
PRB000074908	08. April 2024	Die Benutzerkapazität für zeitgesteuerte Erinnerungen wurde hinzugefügt.	Weckeinrichtung und Termine auf Seite 684
PRB000073511	14. April 2024	Korrekturen und Behebung von Problemen mit jährlich wiederkehrenden Ausnahmen.	Zeitplan hinzufügen auf Seite 925 Ausnahme in CCV hinzufügen auf Seite 844

Änderungen in V3R3

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000068453	27. Juni 2023	Informationen zu Authenticated SMTP und OAuth 2.0 hinzugefügt.	E-Mail-Versand konfigurieren auf Seite 205
PRB000066465	17. Juli 2023	Informationen über den neuen Port in der Firewall für CLS Connect hinzugefügt.	Lizenzaktivierung (Standalone) auf Seite 314, Lizenzierungsverfahren auf Seite 298, Verwendete Ports auf Seite 270, Aktivierung von CLS Connect auf Seite 313
PRB000068453	17. Juli 2023	Unterstützte Bildformate aktualisiert.	OpenScape Business, UC SuiteBenutzerverzeichnis auf Seite 1747, Benutzer von UC Suite auf Seite 552
PRB000071258	18. Oktober 2023	Längenbegrenzungen für CSV-Daten hinzugefügt.	CSV-Datei vom lokalen Dateisystem in das externe Verzeichnis importieren auf Seite 572
PRB000061414	20. Oktober 2023	Neue Flagge hinzugefügt - Dedizierte statische Route verwenden.	Software-ImageSystem-Software Update via Internet auf Seite 1500
PRB000064083	26. Oktober 2023	Fehlende Werte für das Feld Authentifizierung für HFA-Geräte erzwingen hinzugefügt.	GrundeinstellungenSystem > HFA-Registrierungs-Passwort auf Seite 1559

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000071163	24. November 2023	Neue Kapitel und Informationen zur Handhabung von Zertifikaten hinzugefügt.	Einführung auf Seite 1043 (neu) Server-Zertifikat importieren (PEM) auf Seite 1048 (neu) Zertifikatshandling für Booster Server auf Seite 1051 (neu) Zertifikatsanforderungen (CSR) generieren auf Seite 1046 CA-Zertifikat generieren auf Seite 1045 Server-Zertifikat importieren (PKCS#12) auf Seite 1048 Zertifikatshandling auf Seite 1042
PRB000072442	04. Januar 2023	Hinweis zum DND-Verhalten in Teams hinzugefügt.	Teamschaltung / Team-Gruppe auf Seite 712
PRB000069431	05. Januar 2024	Informationen zu UC Suite, CLI-Routing und MS Teams hinzugefügt.	Zeitpläne auf Seite 837 Zeitpläne auf Seite 890
PRB000054882	02. Februar 2024	Info für fehlenden Abschnitt 'Switched Trunk Authorization' hinzugefügt.	GrundeinstellungenSystem Abwurf/ Attendant/Hotline auf Seite 1553
PRB000073109	22. Februar 2024	ITSP zu SIP-Leitungskanäle Zeile in Tabellen hinzugefügt.	Maximalwerte für Leitungen auf Seite 1457
PRB000073818	1. März 2024	Korrektur der Standardwerte für die Parameter Anzahl der Warteschlangenalarme, Warteschlangenalarmzeit, Zeitüberschreitung für verpasste Anrufe und Schwellenwert für abgebrochene Anrufe.	OpenScape Business UC Suite Contact Center auf Seite 1755

Änderungen in V3R2 FR1

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000066080	11. Mai 2023	Hinweis bezüglich des Camps zum Verhalten hinzugefügt.	Wie Sie sofortiges Anklopfen durch Vermittlungsplatz aktivieren oder deaktivieren auf Seite 674
PRB000067262	12. Mai 2023	Die Bereichswerte für den MOH-Verzögerungstimer wurden korrigiert.	GrundeinstellungenSystem ZeitarameterZeitparameter, Experten-ModusGrundeinstellungenSystem, Experten-Modus auf Seite 1543
PRB000065660	29. Juni 2023	Hinweis zum Hinzufügen und Entfernen von UC-Kontakten hinzugefügt.	Verzeichnisse auf Seite 515, Verzeichnisse auf Seite 566

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000067012	01. August 2023	Hinweis auf System-Kurzwahl und Gebührenbeschränkungsregeln hinzugefügt.	Kurzwahl zentral KWZ auf Seite 640
PRB000056655	05. September 2023	Hinweis auf die Aktualisierung der Anzeigeinformationen nach dem Weiterleiten eines Anrufs hinzugefügt.	Übergeben auf Seite 655

Änderungen in V3R2

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000052166	20. Juni 2022	Abschnitt für Auto DSP Trace gelöscht, da dieser Trace im WBM nicht mehr verfügbar ist	Traces auf Seite 1508
PRB000058845	01. Juli 2022	Aktualisierte Informationen über die SPE-Unterstützung in Netzwerken	Deployment Service (DLI und DLS) auf Seite 367
PRB000058415	22. August 2022	Der Abschnitt über nicht unterstützte Boards und Geräte wurde gestrichen und in die Service-Dokumentation verschoben.	Anhang auf Seite 1783
PRB000058021	22. August 2022	Aktualisierte Informationen über die zu ersetzenden Komponenten	Hardware/Software-Migration von OpenScape Business X Systemen auf V3 auf Seite 1395
PRB000061111	27. Oktober 2022	Hinweis auf das VoIP-Verhalten von myPortal@work hinzugefügt	UC Smart Clients auf Seite 495
PRB000062363	25. November 2022	Kapitel und Unterkapitel zur Migration von HW-Platinen hinzugefügt	Migration von HW-Baugruppen auf Seite 1448
PRB000063445	30. November 2022	Hinweis auf Backup-UCD-Gruppe unter Basis-Fallback-Lösung hinzugefügt	Rückfalllösung (Fallback-Lösung) auf Seite 901
RB000055773, PRB000055775	12. Januar 2023	Hinweis zum Hinzufügen einer neuen Datenquelle in ODS hinzugefügt.	Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen auf Seite 1196
PRB000061481	12. Januar 2023	Hinweis und Unterkapitel zum Löschen von Unify Phone-Benutzern hinzugefügt	Unify Phone auf Seite 1206
PRB000063445	12. Januar 2023	Hinweis unter Grundlegende Fallback-Lösung hinzugefügt	Rückfalllösung (Fallback-Lösung) auf Seite 901
PRB000062971	25. Januar 2023	Die im WBM nicht vorhandenen Ereignisse entfernt. Notiz hinzugefügt und Tabelle an den Inhalt angepasst.	SNMP (Simple Network Management Protocol) auf Seite 1303

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000065939	5. April 2023	Änderungen bei der Option 'myPortal-Einladungs-E-Mail deaktivieren'.	OpenScape Business UC Suite Server auf Seite 1767
PRB000065939	5. April 2023	Änderungen bei der Option 'myPortal-Einladungs-E-Mail deaktivieren'.	OpenScape Business UC Suite Server auf Seite 1767
PRB000067211	26. April 2023	Abschnitt über Migrationsbeschränkungen und Abhilfe hinzugefügt.	OpenScape Business X V3 System von einem V2-Mainboard auf ein V3-Mainboard migrieren auf Seite 1400

Änderungen in V3R1

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000052438	20. April 2021	Abschnitt für OCCLA und UC Suite/ Smart-Modus hinzugefügt	So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346
PRB000051654	14. Mai 2021	Neue Kapitel zur MS Office 365 Integration hinzugefügt	Überblick über Integration von Microsoft Office 365 auf Seite 628
PRB000051803	19. Mai 2021	Hinweis für Anklopf-Szenarien hinzugefügt	myPortal @work auf Seite 495
PRB000052202	02. Sept. 2021	Zusätzliche Informationen über Internetanrufe	Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP auf Seite 827

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000054381	03. Sept. 2021	myPortal Smart-Einträge entfernt	• UC-Funktionen (Überblick) auf Seite 91 • Vertriebliche Ausbaustufen auf Seite 102 • Unterstützte Sprachen auf Seite 109 • Tastenprogrammierung auf Seite 451 • UC Smart auf Seite 490 • UC Smart Clients auf Seite 495 • Anwesenheitsstatus (Präsenz) auf Seite 514 • Vernetzung von OpenScape Business X und OpenScape 4000 auf Seite 1130 • Geänderte/gestrichene Leistungsmerkmale und Schnittstellen von HiPath 3000 auf Seite 1440 • Benutzerzugriff auf UC-Funktionen (UC Clients) auf Seite 98 • Teilnehmer lizenzieren (Standalone) auf Seite 319 • myPortal @work auf Seite 495 • myPortal to go auf Seite 956 • Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390
PRB000054046	06. Sept. 2021	Hinweis zu Geräten hinzugefügt	Teamschaltung / Team-Gruppe auf Seite 712Chef/Sekretär / Top-Gruppe auf Seite 716
PRB000053988	06. Sept. 2021	Hinweis zur Gruppennamensuche in myPortal @work hinzugefügt	Leistungsmerkmale auf Seite 519

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000054258	10. Sept. 2021	Kapitel zur Konfiguration von DECT-Telefonen aktualisiert	Wie Sie die DECT-Systemkennung eingeben und weitere Cordless-Parameter (systemweite Daten) konfigurieren auf Seite 979 Wie Sie Cordless-Basisstationen konfigurieren auf Seite 980 Wie Sie DECT-Telefone erstmalig konfigurieren auf Seite 981 Wie Sie ein DECT-Telefon (OpenStage/Gigaset-Mobilteil) an Cordless anmelden auf Seite 982 Wie Sie weitere DECT-Telefone hinzufügen auf Seite 983 Wie Sie DECT-Telefone löschen auf Seite 984 Wie Sie die Multi-SLC-Parameter konfigurieren auf Seite 984 Wie Sie die Daten zu den Basisstationen abfragen auf Seite 985 Wie Sie den Hinweiston der Message Waiting Indication (MWI) für DECT-Telefone aktivieren auf Seite 985 Wie Sie den Anmeldestatus der DECT-Telefone abfragen auf Seite 986
PRB000051960, PRB000052019	11. Okt. 2021	Hinweis zum myPortal@work-Benutzerkonto hinzugefügt, das im UC Suite-Modus gesperrt ist	Benutzerkonfiguration für myPortal@work auf Seite 499
PRB000053691	18. Okt. 2021	Tabelle über die Durchführung der LDAP-Suche aktualisiert	GrundeinstellungenSystem LDAP auf Seite 1556
PRB000054934	12 Nov. 2021	Information über die Anzahl der Gespräche, die im Client angezeigt werden, hinzugefügt	myPortal @work auf Seite 495
PRB000054816	03. Februar 2022	Hinweis zum CallMe-Dienst hinzugefügt	CallMe-Dienst auf Seite 564
PRB000054995/ PRB000055780	18. Februar 2022	Hinweis für ODBC zu ODBC Bridge Server hinzugefügt	ODBC-ODBC Bridge Server konfigurieren auf Seite 1194
PRB000055651	28. Februar 2022	Informationen über den Abschluss des Registrierungsprozesses für DECT-Telefone hinzugefügt	Wie Sie ein DECT-Telefon (OpenStage/Gigaset-Mobilteil) an Cordless anmelden auf Seite 982
PRB000056047	15. März 2022	Hinweis für RSP hinzugefügt	RSP.servicelink auf Seite 1375

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000055842	30. März 2022	Informationen über die unterstützten Dateiformate und die Größenbegrenzung für das Hochladen von Bildern hinzugefügt	Benutzer von UC Suite auf Seite 552 OpenScape Business, UC SuiteBenutzerverzeichnis auf Seite 1747

Änderungen in V3

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
NA16738104	19. Aug. 2020	Hinweis zur Eingabe von Vorname und Nachname in die Felder im externen Verzeichnis hinzugefügt	Externes Verzeichnis auf Seite 571
NA16759874	13. Nov. 2020	Info über Unterstützung des Vollduplex-Modus mit OCCLA hinzugefügt	So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346 Power Management auf Seite 1300NetzwerkschnittstellenMainboard LAN 2 auf Seite 1606NetzwerkschnittstellenMainboard LAN 3 (Admin) auf Seite 1608NetzwerkschnittstellenApplication BoardLAN 1 auf Seite 1615NetzwerkschnittstellenApplication BoardLAN 2 auf Seite 1616NetzwerkschnittstellenHauptplatine LAN 1 (WAN) auf Seite 1602
PRB000050351	12. Nov. 2020	Hinweis zu CP0-Telefonen korrigiert	Wie Sie eine PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X konfigurieren auf Seite 1277
PRB000050248	12. Nov. 2020	Einträge für CAR in der Tabelle hinzugefügt	Verwendete Ports auf Seite 270
NA16756853/ PRB000049732	10. Dez. 2020	Hinweis zum Neustart des Booster Servers bei Konfigurationsänderungen bei der E-Mail-Weiterleitung hinzugefügt.	E-Mail-Versand konfigurieren auf Seite 623
PRB000050722	15. Dez. 2020	Informationen zur Aktivierung der Nummernkonvertierung für Kurzwahlnummern über LDAP hinzugefügt.	Regeln und Konventionen auf Seite 522
PRB000051401	09. Feb. 2021	Hinweis zu Firewall-Einstellungen in Gerät@Home hinzugefügt.	Konfiguration für Systemgerät@Home auf Seite 991
PRB000050983	11. Feb. 2021	Hinweis zur Anzahl der Circuit-Teilnehmer pro System hinzugefügt.	Maximalwerte für Teilnehmer auf Seite 1454

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000051647	11. Feb. 2021	Informationen für die Anrufweiterleitung nach Deflect Call / Single Step Transfer sowie für die Ermittlung des Ziels über Rufzielliste bei Flags für Deflect Call / Single Step Transfer hinzugefügt.	GrundeinstellungenSystem System Flags auf Seite 1534
PRB000051165	19. Feb. 2021	Hinweis mit Gerätetyp korrigiert.	Chef-MULAP auf Seite 734
PRB000050983	15. Feb. 2021	Hinweis auf nicht unterstützte Funktion hinzugefügt	SIP-Stationen auf Seite 441

Änderungen in V2R7

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
NA16740815	11. Aug. 2020	Fußnote zur maximalen Anzahl gleichzeitiger Anrufe in MOH hinzugefügt	Maximalwerte der Ressourcen auf Seite 1459
NA16653104	2. Juni 2020	Aktualisierung der Dokumentation in Bezug auf verwendete Ports	Verwendete Ports auf Seite 270
NA16692823	30. April 2020	Option zur Verwendung von FQDN auch im WAN-Feld von myPortal @work hinzugefügt.	Voraussetzungen für myPortal @work auf Seite 497
NA16652178	8. April 2020	Hinweis zum Öffnen von Port 8101 in einem Proxy für den korrekten Betrieb von `CommunicationsServer.exe` hinzugefügt.	Wie Sie eine Silent Deinstallation durchführen auf Seite 550 Wie Sie eine Silent Installation durchführen auf Seite 549
NA16582432	6. April 2020	Informationen zum Aktivieren von **Call Supervision** hinzugefügt.	Call Supervison auf Seite 657

2 Einführung und wichtige Hinweise

In der Einführung erhalten Sie einen Überblick über die Struktur dieser Dokumentation. Die Einführung soll Ihnen helfen, Informationen zu Themen schneller zu finden. Bevor Sie mit der Montage und Inbetriebnahme des Kommunikationssystems beginnen, beachten Sie unbedingt die Sicherheitshinweise und Warnungen und die wichtigen Hinweise.

Tipp: Die Sicherheitshinweise und Warnungen informieren Sie über die zu beachtenden Sicherheits- und Warnhinweise. Die wichtigen Hinweise enthalten Angaben über das Verhalten in Notfällen, die Normen und Richtlinien bezüglich der Installation und die Funkstöreigenschaften des Kommunikationssystems. Darüber hinaus erhalten Sie Informationen zur sachgemäßen Entsorgung und zum sachgemäßen Recycling.

2.1 Über diese Dokumentation

Diese Dokumentation beschreibt die Administration von OpenScape Business™.

Enthalten Sie die Hardwaremodelle OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 und OpenScape Business X8 sowie das Softwaremodell OpenScape Business S (Softswitch). Die UC-Lösung UC Smart ist auf allen OpenScape Business Modellen integriert. Die UC-Lösung UC Suite wird für die Hardwaremodelle mit der optionalen UC Booster Card oder dem UC Booster Server geboten; beim Softswitch kann zwischen UC Smart oder UC Suite gewählt werden.

Anmerkung: Die Hardwaremodelle OpenScape Business X1/X3/X5/X8 (kurz OpenScape Business X) und der Softswitch OpenScape Business S werden in dieser Dokumentation auch als Kommunikationssysteme bezeichnet.

UC Suite bezeichnet die erweiterten Unified-Communications-Funktionen inkl. Multimedia Contact Center.

Die Informationen in dieser Dokumentation enthalten allgemeine Beschreibungen der technischen Möglichkeiten, welche im Einzelfall nicht immer vorliegen müssen. Die gewünschten Leistungsmerkmale sind im Einzelfall bei Vertragsabschluss festzulegen.

Wenn eine Funktion nicht wie beschrieben verfügbar ist, dann kann dies folgende Ursachen haben:

- Das Kommunikationssystem verfügt nicht über dieses Leistungsmerkmal.
- Die benötigte Lizenz ist nicht vorhanden oder aktiviert.

2.1.1 Dokumentationen und Zielgruppen

Die Dokumentationen zu OpenScape Business richten sich an unterschiedliche Zielgruppen.

Vertrieb und Projektplanung

Die folgenden Dokumentationen richten sich an Vertrieb und Projektplanung.

- Leistungsmerkmalbeschreibung

  Diese Dokumentation beschreibt sämtliche Leistungsmerkmale. Dieses Dokument ist ein Auszug aus der Administratordokumentation.

Installation und Service

Die folgenden Dokumentationen richten sich an Servicetechniker.

- OpenScape Business X1/X1W, Installationsanleitung

  Diese Dokumentation beschreibt die Montage der Hardware und die Erstinstallation von OpenScape Business X1.
- OpenScape Business X3/X5/X8, Installationsanleitung

  Diese Dokumentation beschreibt die Montage der Hardware und die Erstinstallation von OpenScape Business X3/X5/X8.
- OpenScape Business S, Installationsanleitung

  Diese Dokumentation beschreibt die Erstinstallation des Softswitchs OpenScape Business S.
- OpenScape Business X1/X1W, Service-Dokumentation

  Diese Dokumentation beschreibt die Hardware von OpenScape Business X1.
- OpenScape Business X3/X5/X8, Servicedokumentation

  Diese Dokumentation beschreibt die Hardware von OpenScape Business X3/X5/X8.
- OpenScape Business X1R, Service- und Installationsanleitung, Service-Dokumentation

  Dieses Dokument beschreibt die Installation der Hardware, die Erstinstallation und den Service von OpenScape Business X1R.

Administration

Die folgenden Dokumentationen richten sich an Administratoren.

- Administratordokumentation

  Diese Dokumentation beschreibt die Konfiguration der Leistungsmerkmale, die über den OpenScape Business Assistant (WBM) eingerichtet werden. Die Administratordokumentation ist im System als Online-Hilfe verfügbar.
- Konfiguration für Kundenadministratoren, Administratordokumentation

  Diese Dokumentation beschreibt die Konfiguration der Leistungsmerkmale, die über den OpenScape Business Assistant (WBM) mit dem Administratorprofil **Basic** eingerichtet werden können.
- Manager E, Administratordokumentation

  Diese Dokumentation beschreibt die Konfiguration der Leistungsmerkmale, die über den Manager E eingerichtet werden.

UC Clients / Telefon User Interfaces (TUI)

Die folgenden Dokumentationen richten sich an UC Benutzer.

- myPortal for Desktop, Bedienungsanleitung

  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des UC Clients myPortal for Desktop.
- myPortal for Outlook, Bedienungsanleitung

  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des UC Clients myPortal for Outlook.
- myPortal@work, Benutzerhandbuch

  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des UC Clients myPortal @work.
- Fax Printer, Bedienungsanleitung

  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung von Fax Printer.
- myPortal to go, Bedienungsanleitung

  Diese Dokumentation beschreibt die Konfiguration und Bedienung des mobilen UC Clients myPortal to go für Smartphones und Tablet-PC.
- myAgent, Bedienungsanleitung

  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Contact Center Clients myAgent.
- myReports, Bedienungsanleitung

  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Contact Center Clients myReports.
- myAttendant, Bedienungsanleitung

  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Vermittlungsplatzes myAttendant.
- OpenScape Business Attendant, Bedienungsanleitung

  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Vermittlungsplatzes OpenScape Business Attendant.
- UC Smart Telefon User Interface (TUI), Kurzbedienungsanleitung

  Diese Dokumentation beschreibt das Sprachbox-Telefonmenü der UC-Lösung UC Smart.
- UC Suite Telefon User Interface (TUI), Kurzbedienungsanleitung

  Diese Dokumentation beschreibt das Sprachbox-Telefonmenü der UC-Lösung UC Suite.

2.1.2 Struktur der Administratoren-Dokumentation

Dieser Abschnitt zeigt Ihnen, wie der Inhalt der Administratoren-Dokumentation aufgebaut ist. Die Hardware wird in der Service-Dokumentation beschrieben.

Abschnitt	Inhalte
Einleitung und wichtige Hinweise	Übersicht über den Aufbau dieser Dokumentation und wichtige Informationen/ Sicherheitshinweise, die bei Installation und Betrieb zu beachten sind
Systemübersicht	Übersicht über das Kommunikationssystem für den schnellen Start

Abschnitt	Inhalte
Administrationskonzept	Übersicht über Administrationsprogramme und Benutzerrollen im WBM
Erstinstallation von OpenScape Business X	Integration von OpenScape Business X3/X5/X8 in das Kunden-LAN und Grundkonfiguration über Assistenten
Erstinstallation von OpenScape Business S	Integration von OpenScape Business S in das Kunden-LAN und Grundkonfiguration über Assistenten
Erstinstallation des OpenScape Business UC Booster	Integration von OpenScape UC Business Booster in das Kunden-LAN und Grundkonfiguration über Assistenten
Lizenzierung	Lizenzierungsverfahren und Lizenzen
Integration in das interne Datennetz (LAN)	LAN/WAN-Schnittstelle, Namensauflösung, Datenrouting, DLI und DLS
Verbindung zum Service-Provider	Internetzugang, IP-Telefonie, Trunk-Zugang
Teilnehmer	Wahl-Plan, IP-Teilnehmer, UP0-Teilnehmer; DECT-Teilnehmer, Mitel SIP-DECT-Teilnehmer, ISDN- und Analog-Teilnehmer, virtuelle Teilnehmer, Benutzer von UC-Klienten, Benutzerprofile
UC Smart	Klienten und Funktionen der Unified-Communications-Lösung UC Smart, einschließlich Smart Voicemail. Anwesenheitsstatus, Verzeichnisse und Journal, Konferenzen, Teamfunktionen, Voicemails
UC Suite	Klienten und Funktionen der Unified -Kommunikationslösung UC Suite: Anwesenheitsstatus und CallMe, Verzeichnisse und Journal, Konferenzen und Web-Kollaboration, Sprach- und Faxnachrichten, Instant Messaging
Funktionen am Telefon	Anrufen, Rufsignalisierung, Rufnummernanzeige, Funktionen während des Gesprächs, Optimierung der Kommunikation
Arbeiten im Team (Gruppen)	Anrufübernahmegruppe, Gruppenruf, Sammelanschluss, Team/Top, MULAP, UCD
Anruf-Routing	Dienstklassen, Gebührenbeschränkung, Mandanten-System, LCR, Notrufe
Vermittlungsplätze	AutoVermittlung, OpenStage-Vermittlung, PC-basierte Vermittlungsplätze, Abhörplatz
Multimedia Contact Center	Klienten und Funktionen des Contact Centers: Agenten, Warteschlangen und Zeitpläne, VIP-Service, Fallback, Berichte

Abschnitt	Inhalte
Mobility	myPortal zum Mitnehmen, Mobility Entry, Ein-Rufnummern-Dienst, Dualmodus-Telefonie, IP-Mobilität, Schnurlos/DECT
Sicherheit	Firewall, SPE, VPN, Zertifikate
Netzwerk OpenScape Business	Netzwerkplan, Netzwerkszenarien, zentraler Abhörplatz, Überlebensfähigkeit
Hilfsausrüstung	Ansagegeräte, Türsprechanlagen und Türöffner, Aktoren und Sensoren
Anwendungsanbindung	CSTA, TAPI, Anwendungsstarter
Protokollierung	Gesprächsdatenerfassung, Gesprächsgebühren und Gesprächsdauer, Kostenkontrolle
Wartung	Sichern und Wiederherstellen, Aktualisierung, Neustart, Neuladen, Herunterfahren, Zurücksetzen auf Werkseinstellungen, Inventarisierung, Aktionen, Remote Services
Migration	Aktualisierung von HiPath 3000 auf OpenScape Business
Konfiguration-Grenzen und -Kapazitäten	Maximalwerte für die Konfiguration-Grenzen und -Kapazitäten der verschiedenen Kommunikationssysteme
Expertenmodus	Referenzbeschreibung der Fenster/Masken im Expertenmodus
Anhang	Liste der unterstützten Standards, der Euro-ISDN-Leistungsmerkmale und der verwendeten IP-Protokolle und Portnummern
Glossar	Kurzbeschreibungen häufig verwendeter Begriffe

2.1.3 Arten von Themen

Die Arten von Themen umfassen Konzepte und Tasks:

Art des Themas	Beschreibung
Konzept	Erklärt das "Was" und gibt einen Überblick über Zusammenhänge sowie Hintergrundinformationen z.B. zu Leistungsmerkmalen.

Art des Themas	Beschreibung
Task (Handlungsanweisung)	Beschreibt das "Wie" für aufgabenorientierte Anwendungsfälle Schritt für Schritt das und setzt Kenntnis der zugehörigen Konzepte voraus. Tasks sind erkennbar an der Überschrift **Wie Sie ...**.

2.1.4 Darstellungskonventionen

Diese Dokumentation verwendet unterschiedliche Mittel zur Darstellung verschiedener Arten von Informationen.

Art der Information	Darstellung	Beispiel
Elemente der Benutzeroberfläche	Fett	Klicken Sie auf **OK**.
Menüfolge	>	**Datei** > **Beenden**
Besondere Hervorhebung	Fett	Name **darf nicht gelöscht werden**
Querverweistext	Kursiv	Weitere Informationen finden Sie im Themenbereich *Netzwerk*.
Ausgabe	Schriftart mit fester Laufweite, z. B. Courier	`Befehl nicht gefunden.`
Eingabe	Schriftart mit fester Laufweite, z. B. Courier	`LOCAL` als Dateiname eingeben
Tastaturkombination	Schriftart mit fester Laufweite, z. B. Courier	`<Strg>+<Alt>+<Esc>`

2.2 Sicherheits- und Warnhinweise

Sicherheits- und Warnhinweise kennzeichnen Situationen, die Tod, schwere Verletzungen, Sachschäden und/oder Datenverlust zur Folge haben können.

Arbeiten an Kommunikationssystemen und Geräten dürfen **nur** von qualifizierten Personen durchgeführt werden.

Im Kontext dieser Sicherheits- und Warnhinweise sind qualifizierte Personen definiert als Personen, die autorisiert sind, Systeme, Geräte und Leitungen gemäß den geltenden Sicherheitsvorgehensweisen und -standards in Betrieb zu nehmen, zu erden und zu beschriften.

Lesen und beachten Sie unbedingt die nachfolgenden Sicherheits- und Warnhinweise, bevor Sie mit der Montage und Inbetriebnahme des Kommunikationssystems beginnen.

Lesen Sie darüber hinaus alle Sicherheits- und Warnhinweise auf dem Kommunikationssystem und den Geräten sorgfältig durch, und befolgen Sie diese.

Informieren Sie sich auch über die Notrufnummern.

Arten von Sicherheits- und Warnhinweisen

In dieser Dokumentation werden folgende Abstufungen der Sicherheits- und Warnhinweise verwendet:

GEFAHR: Kennzeichnet unmittelbar gefährliche Situation, die Tod oder schwere Verletzungen zur Folge haben wird.

Achtung: Kennzeichnet allgemein gefährliche Situation, die Tod oder schwere Verletzungen zur Folge haben kann.

ACHTUNG: Kennzeichnet gefährliche Situation, die Verletzungen zur Folge haben kann.

Anmerkung: Kennzeichnet Situationen, die Sachschäden und/ oder Datenverlust zur Folge haben können.

Weitere Symbole zur näheren Bestimmung der Gefahrenquelle

Das folgende Symbol wird in der Regel nicht in der vorliegenden Dokumentation verwendet, sondern kann auf Geräten oder Verpackungen abgebildet sein.

EGB Elektrostatisch gefährdete Bauelemente

Zugehörige Konzepte

Wichtige Hinweise auf Seite 81

2.2.1 Warnhinweise: Gefahr

Warnhinweise des Typs Gefahr kennzeichnen eine unmittelbar gefährliche Situation, die Tod oder schwere Verletzungen zur Folge haben wird.

GEFAHR: Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Beachten Sie: Spannungen über 30 V AC (Wechselstrom) oder 60 V DC (Gleichstrom) sind gefährlich!
- Arbeiten am Niederspannungsnetz (<1000 V AC) dürfen nur mit entsprechender Qualifizierung oder durch einen qualifizierten

Elektrotechniker durchgeführt werden und müssen den nationalen/ lokalen Bestimmungen für elektrische Anschlüsse entsprechen.

2.2.2 Warnhinweise: Warnung

Warnhinweise des Typs Warnung kennzeichnen eine allgemein gefährliche Situation, die Tod oder schwere Verletzungen zur Folge haben kann.

Achtung: Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Schutzerden Sie die Kommunikationssysteme OpenScape Business X3R, X3W, X5R und X5W durch einen separaten Schutzleiter. Verbinden Sie Ihr Kommunikationssystem vor Inbetriebnahme und Anschluss der Telefone und Leitungen ordnungsgemäß mit dem Schutzleiter.
- Schutzerden Sie jede Systembox des Kommunikationssystems OpenScape Business X8 durch einen separaten Schutzleiter. Verbinden Sie Ihr Kommunikationssystem vor Inbetriebnahme und Anschluss der Telefone und Leitungen ordnungsgemäß mit dem Schutzleiter.
- Benutzen Sie Systeme, Geräte und Betriebsmittel nur im einwandfreien Zustand. Die Inbetriebnahme von Geräten mit äußeren Beschädigungen ist verboten.
- Erneuern Sie beschädigte Sicherheitseinrichtungen (Abdeckungen, Aufkleber und Schutzleitungen) sofort.
- Wechseln Sie das Netzkabel sofort aus, wenn es Beschädigungen aufweist.
- Nehmen Sie die Kommunikationssysteme und Server nur über Steckdosen mit angeschlossenem Schutzkontakt in Betrieb.
- Während eines Gewitters sollten Sie Leitungen weder anschließen noch entfernen und Baugruppen weder einbauen noch entfernen.
- Trennen Sie sämtliche Versorgungsstromkreise, wenn die Stromversorgung eines Kommunikationssystems für bestimmte Arbeiten nicht erforderlich ist (zum Beispiel bei Änderungen der Verkabelung). Ziehen Sie sämtliche Netzstecker des Kommunikationssystems und vergewissern Sie sich, dass das Kommunikationssystem nicht von einer zusätzlichen Spannungsquelle (zum Beispiel eine unterbrechungsfreie Stromversorgung) versorgt wird.

  Prüfen Sie vor Beginn jeder Arbeit, ob das Kommunikationssystem spannungsfrei ist. Halten Sie es nie für selbstverständlich, dass mit Ausschalten einer Sicherung oder eines Hauptschalters alle Stromkreise auch zuverlässig unterbrochen sind.
- Rechnen Sie mit Ableitstrom aus dem Telekommunikationsnetz. Trennen Sie alle Telekommunikationsleitungen vom Kommunikationssystem, bevor der vorgeschriebene Schutzleiter vom System getrennt wird.
- Führen Sie Messungen an spannungsführenden Teilen sowie Wartungsarbeiten an Baugruppen und Abdeckungen nur mit

der allergrößten Vorsicht aus, solange die Stromversorgung eingeschaltet ist.

Metallisch beschichtete Oberflächen (zum Beispiel Spiegel) sind stromleitend, bei Berührung besteht die Gefahr eines elektrischen Schlages oder eines Kurzschlusses.

2.2.3 Warnungen: Vorsicht

Warnhinweise des Typs Vorsicht kennzeichnen eine gefährliche Situation, die Verletzungen zur Folge habe kann.

ACHTUNG: Explosionsgefahr bei unsachgemäßem Austausch von Akkus und Batterien

- Verwenden Sie ausschließlich die zugelassenen Akkus.
- Ersetzen Sie die Lithium-Batterie nur durch identische oder vom Hersteller empfohlene Typen.

ACHTUNG: Brandgefahr

- Verwenden Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer.
- Hinterlegen Sie keine Unterlagen oder ähnliche brennbare Gegenstände in einem Kommunikationssystem.

ACHTUNG: Allgemeine Verletzungs- bzw. Unfallgefahr am Arbeitsplatz

- Installieren Sie nach Test- und Wartungsarbeiten alle Sicherheitseinrichtungen wieder am richtigen Platz und schließen Sie die Deckel und Gehäuse wieder.
- Verlegen Sie Leitungen so, dass sie keine Unfallquelle (Stolpergefahr) bilden und nicht beschädigt werden.
- Stellen Sie sicher, dass bei Arbeiten an einem geöffneten Kommunikationssystem oder Server dieses nie unbeaufsichtigt bleibt.
- Verwenden Sie geeignete Hilfsmittel, um schwere Gegenstände oder Lasten zu heben.
- Prüfen Sie Ihr Werkzeug regelmäßig. Benutzen Sie nur intaktes Werkzeug.
- Tragen Sie bei Arbeiten an den Anlagen keine lose Kleidung und binden Sie längeres Haar immer zurück.
- Tragen Sie keinen Schmuck, metallene Uhrbänder oder zum Beispiel Metallbeschläge und Nieten an Kleidungsstücken.
- Tragen Sie bei entsprechenden Arbeiten immer den erforderlichen Augenschutz.
- Tragen Sie überall dort einen Schutzhelm, wo herabfallende Gegenstände Sie gefährden können.
- Sorgen Sie für gute Beleuchtung am Arbeitsplatz und achten Sie auf Ordnung.

2.2.4 Warnhinweise: Hinweis

Warnhinweise des Typs Hinweis kennzeichnen Situationen, die Sachschäden und/oder Datenverlust zur Folge haben können.

Beachten Sie die folgenden Hinweise, um Sachbeschädigungen und/oder Datenverlust zu vermeiden:

- Prüfen Sie vor der Inbetriebnahme, ob die Nennspannung der Netzspannungsversorgung mit der Nennspannung des Kommunikationssystems oder Servers übereinstimmt (Typenschild).
- Befolgen Sie folgende EGB-Maßnahmen zum Schutz der elektrostatisch gefährdeten Bauelemente:
  - Legen Sie vor allen Arbeiten an Baugruppen und Modulen das Erdungsarmband ordnungsgemäß an.
  - Legen Sie Baugruppen und Module immer auf einer geerdeten, leitfähigen Unterlage ab.
  - Transportieren und versenden Sie Komponenten des Kommunikationssystems (zum Beispiel Baugruppen) nur in geeigneten Verpackungen.
- Verwenden Sie ausschließlich Originalzubehör. Bei Nichtbeachtung können Beschädigungen am Kommunikationssystem auftreten oder Sicherheits- und EMV-Bestimmungen verletzt werden.
- Bei einer plötzlichen Temperaturänderung kann die Luftfeuchtigkeit kondensieren. Wird ein Kommunikationssystem oder Server beispielsweise aus kalter Umgebung in warme Räume gebracht, kann Feuchtigkeit kondensieren. Warten Sie, bis die Temperatur ausgeglichen ist und das Kommunikationssystem oder der Server absolut trocken ist, bevor Sie es in Betrieb nehmen.
- Schließen Sie alle Leitungen nur an den vorgegebenen Anschlusspunkten an.
- Wenn keine Notstromversorgung verfügbar ist oder bei Stromausfall nicht auf analoge Notfalltelefone umgeschaltet werden kann, lassen sich bei einem Ausfall der Stromversorgung keine Notfallanrufe mehr über das Kommunikationssystem tätigen.
- Prüfen Sie vor Beginn einer Wandmontage, ob die Wand eine ausreichende Tragfähigkeit hat. Verwenden Sie immer geeignete Installations- und Befestigungsmittel, um Kommunikationssysteme und Geräte sicher zu montieren.
- Lassen Sie es nicht zu, dass in unmittelbarer Nähe des Kommunikationssystems leicht entflammbare Materialien gelagert werden.

2.2.5 Länderspezifische Sicherheitshinweise

Hier erhalten Sie Informationen über die zu beachtenden Sicherheitshinweise für Montage, Inbetriebnahme und Betrieb des Kommunikationssystems in bestimmten Ländern.

2.2.5.1 Sicherheitshinweise für Australien

Bei der Montage, der Inbetriebnahme und dem Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S

sowie des OpenScape Business UC Booster Servers (Application Server) in Australien sind folgende Sicherheitshinweise unbedingt zu beachten:

- Die Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie der OpenScape Business UC Booster Server (Application Server) dürfen nur von autorisiertem Fachpersonal installiert und gewartet werden.
- OpenScape Business Wandsysteme müssen in der Nähe einer Wandsteckdose installiert werden, über die das jeweilige Kommunikationssystem mit Spannung versorgt wird. Die Wandsteckdose muss frei zugänglich sein. Es ist unbedingt sicherzustellen, dass der Erdkontakt der Wandsteckdose intakt ist.
- Die Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie der OpenScape Business UC Booster Server (Application Server) müssen grundsätzlich so konfiguriert werden, dass Notrufnummern (zum Beispiel 000) jederzeit gewählt werden können.
- Bei einem Ausfall der Netzspannungsversorgung können keine Notfallanrufe über das Kommunikationssystem getätigt werden, wenn keine Notstromversorgung verfügbar ist oder bei einem Spannungsausfall nicht auf analoge Notfalltelefone umgeschaltet werden kann (Amtsleitungsumschaltung).
- Wartemusik- und Paging-Geräte müssen über eine von der Australian Communications Authority ACA zugelassene Line Isolation Unit an das Kommunikationssystem angeschlossen werden.

2.2.5.2 Sicherheitshinweise für Brasilien

Bei der Montage, der Inbetriebnahme und dem Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) in Brasilien sind folgende Sicherheitshinweise unbedingt zu beachten:

- Die Verwendung der Steckdosenleiste mit Überspannungsschutz mit der Sachnummer C39334-Z7052-C33 ist zwingend vorgeschrieben. Der Netzspannungsanschluss der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) muss über die Steckdosenleiste mit Überspannungsschutz geführt werden.
- Die Verwendung von abgeschirmten Ethernet-Kabeln für die LAN-/WAN-Schnittstellen/Anschlüsse der Mainboards OCCL, OCCM und OCCMR und der UC Booster Card OCAB (Application Board) ist zwingend vorgeschrieben.

2.2.5.3 Sicherheitshinweise für USA

Bei der Montage, der Inbetriebnahme und dem Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) in den USA sind folgende Sicherheitshinweise unbedingt zu beachten:

- Netzunterbrechungen und T1-Ausfall

  Bei einer Vernetzung von Kommunikationssystemen über T1 (1,544 MBit/s) muss die Telekommunikationsgesellschaft (Federal

Communications Commission FCC) darüber informiert werden, wenn ein Kommunikationssystem aus dem Netz entfernt wird.

Falls eines der in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify Software and Solutions GmbH & Co. KG den Betrieb des öffentlichen Telekommunikationsnetzes stört, ist die Telekommunikationsgesellschaft berechtigt, den Amtszugang vorübergehend zu sperren. Im allgemeinen wird die Telekommunikationsgesellschaft Sie vorab darüber informieren. Falls dies nicht möglich ist, erfolgt die Meldung zum frühsten möglichen Termin. In diesem Zusammenhang werden Sie gleichzeitig darüber informiert, dass Sie eine Beschwerde bei der Telekommunikationsgesellschaft einreichen können.

- Modifikation von Telekommunikationseinrichtungen

  Die Telekommunikationsgesellschaft ist befugt, die eigenen Einrichtungen, Geräte, Betriebsabläufe und Prozesse bei Bedarf anzupassen. Derartige Modifikationen können gegebenenfalls den Betrieb Ihrer Kommunikationssysteme beeinträchtigen. Im allgemeinen werden Sie vorab benachrichtigt, damit Sie eine Unterbrechung des Telekommunikationsbetriebs vermeiden können.
- Geräte für die Sprachwiedergabe

  Geräte für die Sprachwiedergabe, wie zum Beispiel Wartemusik- und Sprachaufzeichnungsgeräte müssen von der Unify Software and Solutions GmbH & Co. KG freigegeben und gemäß den Richtlinien und Bestimmungen der FCC-Vorschriften Teil 68, Unterabschnitt C registriert sein.

  Nicht freigegebene Geräte für die Sprachwiedergabe dürfen nur über Schutzschaltungen angeschlossen werden, die von der Unify Software and Solutions GmbH & Co. KG freigegeben und gemäß den Richtlinien und Bestimmungen der FCC-Vorschriften Teil 68, Unterabschnitt C registriert wurden.
- Ringer Equivalence Number REN

  Der Anschlusswert (Ringer Equivalence Number REN) bestimmt, wie viele Geräte gleichzeitig an eine Telefonleitung angeschlossen werden und einen Ruf signalisieren können, wenn die betreffende Rufnummer angewählt wird. In den meisten, jedoch nicht in allen Bereichen, dürfen maximal fünf Geräte an eine Leitung angeschlossen werden (REN = 5). Wenden Sie sich gegebenenfalls an Ihre lokale Telekommunikationsgesellschaft, um festzustellen, wie viele RENs in Ihrem Rufbereich unterstützt werden.
- Neue Ortsnetz- und Amtskennzahlen

  Die Leitweglenkung (Least Cost Routing LCR) ist so zu konfigurieren, dass Änderungen von Ortsnetz- und Amtskennzahlen automatisch erkannt und berücksichtigt werden können. Ansonsten können nach Kennzahländerungen diese nicht für Anrufe genutzt werden.
- Kompatibilität mit Hörhilfen

  Notfalltelefone und öffentliche Telefone (zum Beispiel Telefone in Eingangshallen, Krankenhauszimmern, Aufzügen und Hotelzimmern) müssen mit Handapparaten ausgestattet sein, die den Einsatz magnetisch gekoppelter Hörhilfen gewährleisten. Bei Bedarf müssen für hörgeschädigte Personen, die sich nicht in öffentlichen Bereichen aufhalten, geeignete Handapparate bereitgestellt werden.

  Alle nach dem 16. August 1989 hergestellten digitalen Telefone der Unify Software and Solutions GmbH & Co. KG sind kompatibel mit Hörhilfen

und erfüllen die Anforderungen gemäß den FCC-Vorschriften, Teil 68, Abschnitt 68.316/68.317.

- Programmierte Wählfunktionen

  Wenn Sie Notrufnummern programmieren oder über ein Produkt der Unify Software and Solutions GmbH & Co. KG mit programmierten Wählfunktionen eine Testverbindung zu einer Notrufnummer herstellen, müssen Sie die Verbindung halten und dem Einsatzleiter kurz den Grund Ihres Anrufs erklären, bevor Sie auflegen. Diese Maßnahmen sollten zu verkehrsarmen Zeiten durchgeführt werden, beispielsweise am frühen Morgen oder am späten Abend.

- Anschaltung von außenliegenden Nebenstellen

  Kunden, die die Anschaltung von außenliegenden Nebenstellen (Off-Premises Station OPS) wünschen, müssen die Telekommunikationsgesellschaft darüber informieren, für welche OPS-Klasse die betreffenden Geräte registriert sind und welcher Verbindungstyp gewünscht wird.

- Überwachung der Rufannahme bei Durchwahl

  Kunden, die eines der in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify Software and Solutions GmbH & Co. KG ohne ordnungsgemäße Rufannahme-Überwachung betreiben, verstoßen gegen Teil 68 der FCC-Vorschriften.

  Die in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify Software and Solutions GmbH & Co. KG unterstützen ordnungsgemäße Rückmeldungen an das öffentliche Telekommunikationsnetz, wenn Durchwahlanrufe

  – von dem gerufenen Teilnehmer angenommen werden.
  – von einer Vermittlungsperson angenommen werden.
  – an eine kundenseitig verwaltete Ansage weitergeleitet werden.

  Ferner unterstützen die in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify Software and Solutions GmbH & Co. KG ordnungsgemäße Rückmeldungen für Durchwahlanrufe, die an das öffentliche Telekommunikationsnetz weitergeleitet werden. Zulässige Ausnahmen:

  – Ein Anruf wird nicht angenommen.
  – Es wird besetzt signalisiert.
  – Es wird gassenbesetzt (Reorder Tone) signalisiert.

- Voraussetzungen für den gleichberechtigten Zugriff

  Für Bereiche mit erhöhtem Verkehrsaufkommen (zum Beispiel Hotels, Krankenhäuser, Flughäfen, Schulen) müssen den Teilnehmern gleichberechtigte Zugangscodes für die gewünschten Provider zur Verfügung gestellt werden. Die aktuellen Codes für den gleichberechtigten Zugang (Carrier Access Codes CAC) lauten 10xxx und 101xxxx, sowie 800/888 und 950, wobei xxx oder xxxx für den jeweilige Provider-Code steht.

  Um eine Verbindung über einen bestimmten Provider herzustellen, muss der Teilnehmer vor der Rufnummer des gewünschten Gesprächspartners zunächst einen Provider-spezifischen Zugangscode eingeben. Der

gleichberechtigte Zugang ist auch über die Codes 800/888 oder 950 des gewünschten Providers möglich.

Über gleichberechtigte Zugangscodes unterstützen die in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify Software and Solutions GmbH & Co. KG den Zugang zu Interstate Providern.

Modifikationen dieser Funktionalität stellen eine Verletzung des Telephone Operator Consumer Services Improvement Act von 1990 sowie Teil 68 der FCC-Vorschriften dar.

2.2.5.4 Sicherheitshinweise für Kanada

GEFAHR: Elektrischer Schlag durch Berühren spannungsführender Leitungen

Arbeiten am Niederspannungsnetz (<1000 V AC) dürfen nur mit entsprechender Qualifizierung oder durch einen qualifizierten Elektrotechniker durchgeführt werden und müssen den nationalen/ lokalen Bestimmungen für elektrische Anschlüsse entsprechen.

Bei der Montage, der Inbetriebnahme und dem Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) in Kanada sind folgende Sicherheitshinweise unbedingt zu beachten:

- Ringer Equivalence Number REN

  Der Anschlusswert (Ringer Equivalence Number REN) bestimmt, wie viele Geräte gleichzeitig an eine Telefonleitung angeschlossen werden können. Der Schnittstellenabschluss kann eine beliebige Gerätekombination umfassen, vorausgesetzt, die REN-Anzahl aller Geräte ist kleiner oder gleich fünf.
- Einschränkungen für den Anschluss von Geräten

  Die Kennzeichnung durch „Innovation, Science and Economic Development Canada (ISED)“ weist zertifizierte Geräte aus. Diese Zertifizierung besagt, dass die Geräte bestimmte Anforderungen im Hinblick auf den Schutz, den Betrieb und die Sicherheit von Telekommunikationsnetzen erfüllen. Die Anforderungen sind in den Terminal Equipment Technical Requirements dokumentiert. „Innovation, Science and Economic Development Canada (ISED)“ gibt keine Zusicherungen, dass zertifizierte Geräte jederzeit zur Kundenzufriedenheit funktionieren.

  Vor Installation der in dieser Dokumentation beschriebenen Geräten und Komponenten sollte der Benutzer sicherstellen, dass eine Anschaltung an Einrichtungen der lokalen Telekommunikationsgesellschaft gestattet ist. Außerdem ist bei Installation der Kommunikationssysteme und Server darauf zu achten, dass ein geeignetes Anschlussverfahren gewählt wird. Der Kunde sollte darauf hingewiesen werden, dass auch bei Einhaltung aller genannten Vorgaben in bestimmten Situationen Leistungseinbußen auftreten können.

  Reparaturen an zertifizierten Geräten sollten von einem Servicetechniker des Herstellers oder Lieferanten koordiniert werden. Benutzerseitig durchgeführte Reparaturen oder Modifikationen an den in dieser Dokumentation beschriebenen Geräten und Komponenten oder Gerätefehlfunktionen können die Telekommunikationsgesellschaft dazu

berechtigen, den Benutzer aufzufordern, die betreffenden Geräte zu deinstallieren.

Zur eigenen Sicherheit sollte der Benutzer sicherstellen, dass die elektrischen Erdungsverbindungen von Stromversorgung, Telefonleitungen und metallischem Wasserleitungssystem (sofern vorhanden) miteinander verbunden sind. Insbesondere in ländlichen Gebieten kann diese Vorsichtsmaßnahme besonders wichtig sein.

2.3 Wichtige Hinweise

Die wichtigen Hinweise informieren Sie über das Verhalten in Notfällen, die sachgemäße Entsorgung und das sachgemäße Recycling und den bestimmungsgemäßen Gebrauch und die Betriebsbedingungen der Kommunikationssysteme und Server. Darüber hinaus erhalten Sie Angaben über die Normen und Richtlinien bezüglich der Installation, die Funkstöreigenschaften der Kommunikationssysteme und über Datenschutz und Datensicherheit.

Zugehörige Konzepte

Sicherheits- und Warnhinweise auf Seite 72

2.3.1 Verhalten in Notfällen

Hier erhalten Sie Informationen über die Maßnahmen, die bei einem Notfall zu ergreifen sind.

Vorgehensweise bei Unfällen

Erste Hilfe Maßnahmen

Notruf

Meldung von Unfällen

- Gehen Sie bei Unfällen stets überlegt und mit Ruhe vor.
- Schalten Sie immer zuerst die Stromversorgung aus, bevor Sie ein Unfallopfer berühren.
- Falls Sie die Stromversorgung auf Anhieb nicht ausschalten können, berühren Sie das Opfer nur mit nicht leitenden Materialien (z.B. Besenstiel aus Holz), und versuchen Sie als erstes, es von der Stromquelle zu isolieren.
- Die Grundsätze der ersten Hilfe bei Stromschlägen müssen Ihnen vertraut sein. Dringend notwendig in solchen Notfällen sind Grundkenntnisse der verschiedenen Wiederbelebungsmaßnahmen für den Fall eines Atem- oder Herzstillstands sowie die ersten Maßnahmen bei Verbrennungen.
- Führen Sie bei Atemstillstand sofort eine Atemspende (Mund-zu-Mund oder Mund-zu-Nase) durch.
- Falls Sie über eine entsprechende Ausbildung verfügen, führen Sie bei Herzstillstand sofort eine Herzdruckmassage durch.

Rufen Sie unverzüglich einen Krankenwagen oder den Notarzt. Geben Sie den Notruf in folgender Reihenfolge durch:

- Wo geschah was?
- Was geschah?
- Wie viele Verletzte?
- Welche Art von Verletzungen?
- Warten auf Rückfragen.

- Melden Sie umgehend alle Unfälle, “Beinahe-Unfälle" und potentielle Gefahrenquellen an Ihren Vorgesetzten.
- Melden Sie jeden elektrischen Stromschlag, auch wenn er nur schwach war.

2.3.2 Bestimmungsgemäßer Gebrauch

Die Kommunikationssysteme und Server dürfen nur für die in dieser Dokumentation beschriebenen Einsatzmöglichkeiten und nur in Verbindung mit den von Unify GmbH & Co. KG empfohlenen und zugelassenen Zusatzgeräten und -komponenten verwendet werden.

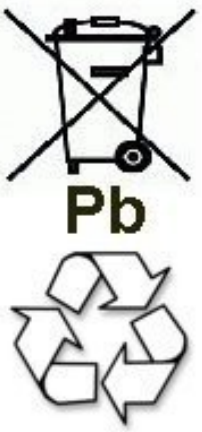
Der bestimmungsgemäße Gebrauch der Kommunikationssysteme und Server setzt sachgemäßen Transport, sachgemäße Lagerung, Montage und Inbetriebnahme sowie sorgfältige Bedienung und Instandhaltung voraus.

Anmerkung: Reinigen Sie das Gehäuse von Kommunikationssystem und Server nur mit einem weichen, leicht feuchten Tuch. Benutzen Sie keine scharfen Reiniger oder Scheuerschwämme.

2.3.3 Sachgemäße Entsorgung und Recycling

Beachten Sie die Informationen über die sachgemäße Entsorgung und das sachgemäße Recycling von Elektro- und Elektronikgeräten und von Altbatterien und Akkus.

Alle Elektro- und Elektronikgeräte sind getrennt vom allgemeinen Hausmüll über dafür staatlich vorgesehene Stellen zu entsorgen. Die sachgemäße Entsorgung und die getrennte Sammlung von Altgeräten dient der Vorbeugung von potentiellen Umwelt- und Gesundheitsschäden. Sie sind eine Voraussetzung für die Wiederverwendung und das Recycling gebrauchter Elektro- und Elektronikgeräte. Ausführliche Informationen zur Entsorgung Ihrer Altgeräte erhalten Sie bei Ihrer Kommune, Ihrem Müllentsorgungsdienst, dem Fachhändler bei dem Sie das Produkt erworben haben oder Ihrem Vertriebsansprechpartner. Diese Aussagen sind nur gültig für Geräte, die in den Ländern der Europäischen Union installiert und verkauft werden und die der Europäischen Richtlinie 2012/ 19/EU unterliegen. In Ländern außerhalb der Europäischen Union können davon abweichende Bestimmungen für die Entsorgung von Elektro- und Elektronikgeräten gelten.



Altbatterien oder Akkus mit diesem Zeichen sind verwertbares Wirtschaftsgut und müssen dem Recyclingprozess zugeführt werden. Altbatterien oder Akkus, die nicht dem Recyclingprozess zugeführt werden, sind unter Beachtung aller Vorschriften als Sondermüll zu entsorgen.

2.3.4 Normen und Richtlinien bezüglich der Installation

Beachten Sie die Informationen, welche Vorgaben beim Anschluss der Kommunikationssysteme und Server an den Versorgungsstromkreis und bei der geschirmten Verkabelung für LAN- und WAN-Anschlüsse einzuhalten sind.

2.3.4.1 Anschluss von OpenScape Office X an den Versorgungsstromkreis

Die Kommunikationssysteme OpenScape Business X sind zum Anschluss an TN-S-Energieversorgungssysteme freigegeben. Ebenfalls erlaubt ist der Anschluss an ein TN-C-S-Energieversorgungssystem, bei dem der PEN-Leiter in jeweils einen Schutz- und Neutralleiter aufgeteilt ist. TN-S und TN-C-S gemäß Definition der Norm IEC 60364-1 und IEC60364-5-51

Sind Arbeiten am Niederspannungsnetz erforderlich, müssen diese von einem qualifizierten Elektrotechniker durchgeführt werden. Diese

Installationstätigkeiten zum Anschluss der Kommunikationssysteme müssen unter Beachtung der IEC 60364-1 und der IEC 60364-4-41 oder entsprechender gesetzlicher Normen bzw. nationaler Vorschriften erfolgen.

2.3.4.2 Anschließen von OpenScape Business S und OpenScape Business UC Booster Server an den Stromversorgungskreis

Angaben zum Anschluss von OpenScape Business S und OpenScape Business UC Booster Server (Application Server) an den Versorgungsstromkreis entnehmen Sie bitte den Herstellerunterlagen des Server-PCs und der weiteren Komponenten.

Sind Arbeiten am Niederspannungsnetz erforderlich, müssen diese von einem qualifizierten Elektrotechniker durchgeführt werden. Diese Installationstätigkeiten zum Anschluss von OpenScape Business S und OpenScape Business UC Booster Server müssen unter Beachtung der IEC 60364-1 und der IEC 60364-4-41 oder entsprechender gesetzlicher Normen bzw. nationaler Vorschriften (zum Beispiel in den USA und in Kanada) erfolgen.

2.3.4.3 Geschirmte Verkabelung für LAN- und WAN-Anschlüsse von OpenScape Business X

Die Einhaltung der CE-Anforderungen bezüglich elektromagnetischer Verträglichkeit der Kommunikationssysteme OpenScape Business X und deren LAN- und WAN-Anschlüsse setzt folgende Bedingung voraus:

- Der Betrieb der Kommunikationssysteme ist nur mit geschirmter Anschlussverkabelung erlaubt. Das bedeutet zwischen den geschirmten LAN- und WAN-Anschlussbuchsen der Kommunikationssysteme und dem Anschluss an die Gebäudeinstallation oder dem Anschluss an externe aktive Komponenten ist ein geschirmtes Kategorie-5-Kabel (CAT.5-Kabel) mit einer Länge von mindestens 3 m zu verwenden. An dem der Gebäudeinstallation oder der externen aktiven Komponente zugewandten Kabelende ist der Kabelschirm zu erden (Verbindung zum Gebäudepotentialausgleich).
- Bei kürzeren Verbindungen mit einer externen aktiven Komponente (LAN-Switch oder ähnliches) ist ebenfalls ein geschirmtes Kategorie-5-Kabel (CAT.5-Kabel) zu verwenden. Jedoch muss die aktive Komponente einen entsprechend geschirmten LAN-Anschluss aufweisen, dessen Schirmanschluss geerdet ist (Verbindung zum Gebäudepotentialausgleich).
- Die Schirmeigenschaften der Verkabelungskomponenten sollen die Anforderungen der Europäischen Norm EN 50173-1[*)] „Anwendungsneutrale Kommunikationskabelanlagen“ (und der dort genannten Verweise) mindestens erfüllen.[***)]
- Gebäudeinstallationen, die mit durchgängig geschirmter symmetrischer Kupfer-Verkabelung gemäß den Klasse D-Anforderungen[**)] der EN 50173-1 ausgestattet sind, erfüllen die oben genannten Bedingung.[***)]

[*)] Die europäische Norm EN 50173-1 ist aus dem globalen Standard ISO/IEC 11801 abgeleitet.

[**)] Klasse D wird unter anderem erreicht, wenn Komponenten (Kabel, Anschlussdosen, Anschlusskabel, etc.) der Kategorie 5 (CAT.5) installiert sind.

2.3.4.4 Brandschutzanforderungen

Brandschutzanforderungen sind in den Bauordnungen länderspezifisch geregelt. Die jeweils gültigen Vorschriften sind zu beachten.

Um die gesetzlich geforderten Brandschutz- und EMV-Anforderungen zu gewährleisten, dürfen die Kommunikationssysteme OpenScape Business X nur geschlossen betrieben werden. Ein Öffnen ist nur kurzzeitig zu Montage- und Wartungszwecken gestattet.

Die OpenScape-Business-Systemkabel entsprechen bezüglich des Brennverhaltens den Anforderungen des internationalen Standards IEC 60332-1. Die folgenden Standards enthalten gleichwertige Anforderungen bezüglich des Brennverhaltens von Kabeln.

IEC 60332-1 Hinweis: IEC 60332-1 entspricht der Prüfart UL VW-1	EN 60332-1-1 und EN 60332-2-1	DIN EN 60332-1-1 (VDE 0482-332-1-1) und DIN EN 60332-2-1 (VDE 0482-332-2-1)

Ob der Standard IEC 60332-1 den jeweiligen Bauordnungen und eventuell darüber hinausreichenden Vorschriften genügt, ist durch den verantwortlichen Bereich in Projektierung und Service zu prüfen.

2.3.4.5 Blitzschutzanforderungen

Der Schutz der Kommunikationssysteme gegen energiereiche Überspannungen erfordert eine niederohmige Erdanbindung gemäß den Angaben in der *OpenScape Business Installationsanleitung*.

Anmerkung: Nach der Schutzerdung eines Kommunikationssystems ist die niederohmige Erdanbindung des Systems über den Schutzleiter des Netzspannungsversorgungskreises und die niederohmige Anbindung des zusätzlichen, permanent angeschlossenen Schutzerdungsleiters zur Potentialausgleichsschiene des Gebäudes zu prüfen.

Anmerkung:

Brandgefahr durch Überspannung

Telekommunikationsleitungen über 500 m Länge oder Telekommunikationsleitungen, die das Gebäude verlassen

***) Im nordamerikanischen Markt ist überwiegend UTP-Verkabelung (US-Norm EIA/TIA 568 A) installiert, daher gilt dort für die LAN- und WAN-Anschlüsse der Kommunikationssysteme: Der Betrieb der Systeme ist nur mit geschirmter Anschlussverkabelung erlaubt. Das bedeutet zwischen den geschirmten LAN- und WAN-Anschlussbuchsen der Kommunikationssysteme und dem Anschluss an die Gebäudeinstallation oder dem Anschluss an externe aktive Komponenten ist ein geschirmtes Kategorie-5-Kabel (CAT.5-Kabel) mit einer Länge von mindestens 3 m zu verwenden. An dem der Gebäudeinstallation oder der externen aktiven Komponente zugewandten Kabelende ist der Kabelschirm zu erden (Verbindung zum Gebäudepotentialausgleich).

müssen über einen zusätzlichen externen Blitzschutz geführt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den fachgerechten Einbau von ÜSAGs (Überspannungsableiter, gasgefüllt) im Hauptverteiler, im Patch-Panel oder am Eintrittspunkt der Leitung in das Gebäude gewährleistet. Dazu muss ein ÜSAG mit 230 V Nennspannung von jeder zu schützenden Ader gegen Erde geschaltet werden.

Ohne diesen zusätzlichen Primärschutz kann es bei einer Blitzbeeinflussung zu einer Zerstörung von Baugruppen kommen. Dies kann zum Ausfall des gesamten Kommunikationssystems und zur Überhitzung von Bauelementen führen (Brandgefahr).

2.3.4.6 Kennzeichnungen für OpenScape Business X

Die Konformität des Gerätes zu der EU-Richtlinie 1999/5/EG wird durch das CE-Kennzeichen bestätigt.

2.3.5 Hinweise zu Störaussendung und Funkstörung von OpenScape Business X

Die Kommunikationssysteme OpenScape Business X sind Einrichtungen der Klasse B gemäß EN 55032.

2.3.6 Datenschutz und Datensicherheit

Beachten Sie die Informationen zur Gewährleistung des Datenschutzes und der Datensicherheit.

Bei den in dieser Dokumentation beschriebenen Kommunikationssystemen und Servern werden unter anderem personenbezogene Daten verarbeitet und genutzt, zum Beispiel bei der Gebührenerfassung, den Displayanzeigen, der Kundendatenerfassung.

In Deutschland gelten für die Verarbeitung und Nutzung solcher personenbezogenen Daten unter anderem die Bestimmungen des Bundesdatenschutzgesetzes (BDSG). Für andere Länder beachten Sie bitte die jeweiligen entsprechenden Landesgesetze.

Datenschutz hat die Aufgabe, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Ferner hat Datenschutz die Aufgabe, durch den Schutz der Daten vor Missbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen.

Tipp: Der Kunde ist dafür verantwortlich, dass Kommunikationssysteme und Server in Übereinstimmung mit dem jeweils gültigen Datenschutz-, Arbeits- und Arbeitsschutzrecht installiert, betrieben und gewartet werden.

Mitarbeiter der Unify Software and Solutions GmbH & Co. KG sind durch die Arbeitsordnung zur Wahrung von Geschäfts- und Datengeheimnissen verpflichtet.

Um die gesetzlichen Bestimmungen beim Service – ob beim “Service vor Ort" oder bei “Remote Services" – konsequent einzuhalten, sollten Sie folgende Regeln unbedingt befolgen. Sie wahren damit nicht nur die Interessen Ihrer und unserer Kunden, sondern vermeiden dadurch auch persönliche Konsequenzen.

Tragen Sie durch problembewusstes Handeln mit zur Gewährleistung des Datenschutzes und der Datensicherheit bei:

- Achten Sie darauf, dass nur berechtigte Personen Zugriff auf Kundendaten haben.
- Nutzen Sie alle Möglichkeiten der Passwortvergabe konsequent aus; geben Sie keinem Unberechtigten Kenntnis der Passwörter, zum Beispiel per Notizzettel.
- Achten Sie mit darauf, dass kein Unberechtigter in irgendeiner Weise Kundendaten verarbeiten (speichern, verändern, übermitteln, sperren, löschen) oder nutzen kann.
- Verhindern Sie, dass Unbefugte Zugriff auf Datenträger haben, zum Beispiel auf Sicherungs-CDs-/DVDs oder Protokollausdrucke. Das gilt sowohl für den Serviceeinsatz, als auch für Lagerung und Transport.
- Sorgen Sie dafür, dass nicht mehr benötigte Datenträger vollständig vernichtet werden. Vergewissern Sie sich, dass keine Papiere allgemein zugänglich zurückbleiben.
- Arbeiten Sie mit Ihren Ansprechpartnern beim Kunden zusammen: Das schafft Vertrauen und entlastet Sie selbst.

2.3.7 Technische Vorschriften und Konformität von OpenScape Business X

Hier erhalten Sie Informationen über die Erfüllung festgelegter Forderungen (Konformität) durch die Kommunikationssysteme OpenScape Business X.

2.3.7.1 CE-Konformität

Die CE-Zertifizierung beruht auf: 2014/35/EU - Niederspannungsrichtlinie (LVD); (Amtsblatt der EU L96 vom 29.03.2014, S. 357-374) 2014/30/EU - Richtlinie über die elektromagnetische Verträglichkeit (EMV); (Amtsblatt der EU L96 vom 29.03.2014, S. 79-106) 2011/65/EU - Richtlinie zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe (RoHS); (Amtsblatt der EU L174 vom 01.07.2011, S. 88-110)

	Normenreferenz
Safety	EN 62368-1
Electromagnetic Compatibility EMC	EN55032 (EMC Emission) EN55024 (EMC Immunity Residential)

2.3.7.2 Konformität mit US- und kanadischen Normen

	Normenreferenz
Safety USA and Canada	CSA/UL 62368-1
EMC Emission Canada	ICES-003 Issue 6 Class B
EMC Emission USA	FCC 47 CFR Part 15 Subpart B Class B

FCC-Registrierungsnummer und Anschlusswert

Auf der Gehäuserückseite der Kommunikationssysteme befindet sich ein Aufkleber mit der FCC-Registrierungsnummer, dem Anschlusswert (Ringer Equivalence Number REN) sowie weiteren Informationen. Diese Informationen können auf Anforderung an die Telekommunikationsgesellschaft weitergegeben werden.

2.3.7.3 Konformität mit internationalen Normen

	Normenreferenz
Safety	IEC 60950-1 und IEC 62368-1
EMC Emission	CISPR 32

2.3.8 Betriebsbedingungen

Beachten Sie die klimatischen und mechanischen Bedingungen für den Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server).

2.3.8.1 Betriebsbedingungen OpenScape Business X

Angegeben sind die klimatischen und mechanischen Bedingungen für den Betrieb der Kommunikationssysteme OpenScape Business X.

Klimatische Betriebsbedingungen

Grenzbetriebsbereich:

- Raumtemperatur: + 5 bis + 40 °C (41 bis 104 °F)

- absolute Luftfeuchte: 1 bis 25 g H_2O/m^3
- Relative Luftfeuchte: 5 bis 80%

Die Entlüftung der Kommunikationssysteme erfolgt durch Konvektion. Zwangsentlüftung ist bei OpenScape Business X5W erforderlich, wenn mehr als 32 a/b-Schnittstellen vorhanden sind.

Anmerkung: Schäden durch lokale Temperaturerhöhungen

Vermeiden Sie direkte Sonneneinstrahlung oder Wärmeeinwirkung durch Heizkörper auf die Kommunikationssysteme.

Anmerkung: Schäden durch Kondensation von Luftfeuchtigkeit

Vermeiden Sie unter allen Umständen vor und während des Betriebs die Kondensation von Luftfeuchtigkeit auf oder in den Kommunikationssystemen.

Ein Kommunikationssystem muss absolut trocken sein, bevor Sie es in Betrieb nehmen.

Mechanische Betriebsbedingungen

Die Kommunikationssysteme sind grundsätzlich für stationären Einsatz entwickelt worden.

2.3.8.2 Betriebsbedingungen OpenScape Business S und OpenScape Business UC Booster Server

Angaben zu den klimatischen und mechanischen Bedingungen für den Betrieb von OpenScape Business S und OpenScape Business UC Booster Server (Application Server) entnehmen Sie bitte den Herstellerunterlagen der Server-PCs und der weiteren Komponenten.

3 Systemübersicht

OpenScape Business bietet kleinen und mittleren Unternehmen die Antwort auf deren individuelle und vielseitige Kommunikationsanforderungen, vereint in einer flexiblen und skalierbaren Lösung. Die OpenScape Business Lösungsarchitektur ermöglicht den Einsatz unabhängig von der vorhandenen Telefonie-Infrastruktur, egal ob klassische Telefonie, IP oder DECT. Von leistungsstarker Telefonie bis zur umfassenden Unified Communications (UC) Komplettlösung liefert OpenScape Business immer die richtige Lösung.

Flexibel, skalierbar und leistungsstark

OpenScape Business führt das Beste aus HiPath 3000 und OpenScape Office in einer neuen Lösungsplattform zusammen.

3.1 Highlights

OpenScape Business ist die All-In-One-Lösung für kleine und mittlere Unternehmen und bietet folgende Highlights.

Highlights

- Integrierte Sprachdienste, Präsenzmanagement (Anwesenheitsstatus), Drag&Drop-Konferenz, visuelle Voicemail (Sprachboxen), AutoAttendant, Multimedia Contact Center, IM (Instant Messaging, Sofortnachrichten), Mobility, Verzeichniszugriff mit Datenbank-Anbindung, Fax, Integration in Geschäftsprozesse und vieles mehr
- individuell auf den Arbeitsplatz und die Arbeitsweise abgestimmte UC-Clients
- Oberflächen-Integration von OpenScape Web Collaboration
- für Kunden mit einem Standort oder als netzweite Lösung mit mehreren Standorten
- OpenScape Business bietet eine einheitliche Lösungsarchitektur.
- In Abhängigkeit von der vorhandenen Infrastruktur sind verschiedene OpenScape Business Modelle für unterschiedliche Ausbaugrößen verfügbar. Alternativ besteht die Möglichkeit die OpenScape Business Software auf einem Standard-Server zu betreiben (Softswitch) - selbstverständlich auch in voll virtualisierten Umgebungen.
- Die UC-Lösung UC Smart ist bereits auf dem Mainboard vorgeleistet. Die additive UC-Lösung UC Suite unterstützt eine größere Anzahl von UC Benutzern und bietet einen erweiterten UC-Leistungsumfang. Dafür ist eine UC Booster Card oder ein UC Booster Server notwendig.
- für die vielseitigen und heterogenen Anforderungen sind alle Kommunikationsschnittstellen bereits vorhanden: IP, digital, analog und DECT sowie alle gängigen Amtschnittstellen für die Sprachkommunikation

3.2 Unified Communications

Unified Communications (UC) ist eine Technologie zur Verbesserung der Kommunikation in Unternehmen und integriert verschiedene Kommunikationsmedien in einer einheitlichen Anwendungsumgebung. Unified Communications vereinfacht die Geschäftsprozesse im Unternehmen durch ein durchgängiges Präsenzmanagement (z.B. werden Anrufe automatisch zum

Mobiltelefon umgeleitet, wenn sie außer Haus sind). Auch die Bereitstellung von Einwahlkonferenzen, persönlicher Voicemail (Sprachbox), persönlicher Faxbox, Instant Messaging (IM), Einsatz des Mobiltelefons als Nebenstelle des Kommunikationssystems, Contact Center, Video und Web Collaboration sind in dieser einheitlichen Lösung vereint.

Mit dem flexiblen Unified-Communication-Ansatz der OpenScape Business werden, je nach Anforderung an den Arbeitsplatz und der vorhandenen Infrastruktur, verschiedene UC-Lösungen angeboten. Bei der UC-Lösung wählen Sie zwischen UC Smart und UC Suite (UC Smart und UC Suite können nicht parallel genutzt werden).

Die bereits in OpenScape Business integrierte UC-Smart-Lösung kann jederzeit über eine Upgrade-Lizenz auf die erweiterte UC-Suite-Lösung migriert werden. Je nach Anzahl der UC-Teilnehmer muss dann OpenScape Business nur noch durch die interne Baugruppe "UC Booster Card" oder mit den externen Linux-Server "UC Booster Server" erweitert werden. Als reiner Softswitch steht die OpenScape Business S als Server-Lösung mit wahlweise UC Smart oder UC Suite zur Verfügung.

3.2.1 UC-Funktionen (Überblick)

Abhängig von der gewählten UC-Lösung (UC Smart oder UC Suite) stehen Ihnen unterschiedliche UC-Funktionen zur Verfügung.

Die folgenden Tabellen sollen Ihnen helfen, die für Sie geeignete UC-Lösung auszuwählen. Detaillierte funktionale Einschränkungen finden Sie in den entsprechenden Kapiteln (UC Smart, UC Suite, Attendants) der Leistungsmerkmalbeschreibung bzw. Administratordokumentation.

UC-Funktion	**UC Smart**	**UC Suite**			**Bemerkungen**
	myPortal to go	**myPortal for Desktop/ Outlook**	**myPortal @work**	**myPortal to go**	
Anwesenheitsstatus					
Anwesenheitsstatus (Präsenz-Management)	x	x	x	x	
Änderung des Anwesenheitsstatus über Client	x	x	x	x	
Änderung des Anwesenheitsstatus über TUI	-	x	-	-	

UC-Funktion	UC Smart	UC Suite			Bemerkungen
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Statusbezogene Anrufumleitung	x	x	x	über myPortal definierte Ziele	Bei UC Smart kann eine beliebige Nummer als Ziel ausgewählt werden. Bei UC Suite kann nur eine Nummer aus der Vorauswahl ausgewählt werden
Statusanzeige in Favoriten	x	x	x	x	
Statusanzeige in Verzeichnissen	x	x	x	x	
Statusanzeige im Journal	-	x	-	-	
CallMe aktivieren	-	x	x	x	
Kalender-Integration (Outlook)	-	x	-	-	
Kalenderintegration (iCal) (nur mit myPortal for Desktop)	-	x	-	-	
Favoriten					
Anzeige des Anrufstatus	x	x	x	x	
Anlegen von Gruppen	x	x	-	-	
Kompakte Anzeige der Favoriten	-	x	-	-	
Verzeichnisse					
Persönliches Verzeichnis	x	x	x	x	
Internes Verzeichnis	x	x	x	x	
Externes Verzeichnis	-	x	x	x	
Suche in den Verzeichnissen	x	x	x	x	
Zugriff auf im System definierte Kurzwahlziele (KWZ)	x	-	x	x	
Import / Verwalten persönlicher Kontakte (CSV/XML)	-	x	-	-	
Zugriff auf Outlook-Kontakte	-	x	-	-	
Import von persönlichen Kontakten (Mac OS) (myPortal for Desktop)	-	x	-	-	
Integration externer Verzeichnisserver über LDAP	-	x	-	-	

UC-Funktion	UC Smart	UC Suite			Bemerkungen
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Journal					
Alle Anrufe	x	x	-	x	
Offene Anrufe	-	x	-	-	
Entgangene Anrufe	x	x	-	x	
Angenommene Anrufe	x	x	-	x	
Geplante Anrufe	-	x	-	-	
Voicemail	x	x	-	x	
Fax-Journal	-	x	-	-	
Gespräche					
Chat	-	-	-	-	
Journal	-	-	x	-	
Voicemail	-	-	x	-	
Anrufe					
Manuelle Wahl	x	x	x	x	
Desktop-Wahl (Click to Call)	-	x	-	-	
Umleiten	x	x	x	x	
Anruf halten	x	x	x	x	
Aufzeichnen von Anrufen (Voice Recording)	-	x	-	-	
E-Mail senden	x	x	x	x	
SMS senden	x	-	-	x	
Chat starten	-	x	-	-	
Popups	-	x	-	-	
Konferenzen					
AdHoc-Konferenz	x	x	x	x	
Geplante Konferenzen	-	x	-	-	
Permanente und offene Konferenzen (Drag&Drop-Konferenz)	-	x	-	-	
Web Collaboration-Einbindung	-	x			
Sprach- und Faxnachrichten					
Sprachbox (Visuelle Voicemail)	x	x	x	x	VoiceMail-Funktionalität für Teilnehmer (IP, TDM)

UC-Funktion	UC Smart	UC Suite			Bemerkungen
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Abhören über Telefon	x	x	x	x	
Abhören über PC-Soundkarte	-	x	-	-	
Wie Sie eine Sprachnachricht als E-Mail senden	x	x	-	-	
Fax	-	x	-	-	
Instant Messaging					
Instant Messaging (Chat)	-	x	-	-	

1 myPortal to go ermöglicht auch den Zugriff auf die lokalen Smartphone-Kontakte.

Contact Center

UC-Funktion	UC Smart	UC Suite		Bemerkungen
		myAgent	myReports	
Agenten, Warteschlangen und Zeitpläne	-	x	-	
Fax und E-Mail	-	x	-	
vordefinierte Reports/ Berichtsvorlagen	-	x	x	
Zeitgesteuertes Erstellen von Reports/ Berichten	-	-	x	

Optional ist die Anschaltung von OpenScape Contact Center möglich.

Attendants (Vermittlungsplätze)

UC-Funktion	UC Smart	UC Suite	Bemerkungen
	Business Attendant	myAttendant	
Anzeige wartender Anrufe mit Anrufart,# Name und Rufnummer	x	x	
Anzeige des Verbindungsstatus	x	x	
Schnelle Vermittlung von Anrufen	x	x	
Kurzwahl über Belegtfelder/ Benutzerschaltflächen. Individuelle Konfiguration der Belegtfelder/ Benutzerschaltflächen mit Rufnummer oder Name	x	x	

UC-Funktion	UC Smart	UC Suite	Bemerkungen
	Business Attendant	**myAttendant**	
Anwesenheitsstatus anderer Teilnehmern sehen	x	x	Bei OpenStage Business Attendant wird für Präsenz UC Booster Card/Server oder Business S benötigt
Anwesenheitsstatus von anderen Teilnehmern ändern	x	x	
Persönliches Verzeichnis	-	x	
Internes Verzeichnis	x	x	
Externes Verzeichnis	x	x	
Outlook-Kontakte	x	x	
LDAP-Zugang	x	x	
Journal	-	x	
AdHoc-Konferenz	x	x	
Geplante, permanente und offene Konferenzen (Drag&Drop-Konferenz)	-	x	
Nachrichtencenter	-	x	Im Nachrichten-Center werden Sprach-, Fax- und Sofortnachrichten, sowie SMS und E-Mails protokolliert und verwaltet
Zugriff auf Sprach- und Faxnachrichten von anderen Teilnehmern	-	x	Muss vom jeweiligen Teilnehmer freigeschaltet werden
Instant Messaging (Chat)	-	x	
Nachtschaltung	x	x	

Der empfohlene Attendant Client für UC Suite ist myAttendant. OpenScape Business Attendant kann aber auch beim Einsatz von UC Suite verwendet werden.

Voicemail & Company AutoAttendant

UC-Funktion	UC Smart	UC Suite	Bemerkung
UC Smart Voicemail & Company AutoAttendant Basisfunktionalität	x	-	
UC Suite Voicemail & Company AutoAttendant Basisfunktionalität	-	x	UC Booster Card/Server oder Business S benötigt
UC-Funktionen			
Grafische Bedienung der Voicemail für Teilnehmer (Web-Interface bzw. Client-Oberfläche)	x	x	

UC-Funktion	UC Smart	UC Suite	Bemerkung
Voicemail-Ansagen für Präsenzfunktion	x	x	Unterschiedliche Ansagen je eingestellter UC Präsenz
Persönliche Regeln für Begrüßungen pro Mailbox	-	x	Teilnehmer legt detaillierte Regeln für die Auswahl seiner persönlichen Ansagen fest
Voicemail to E-Mail	x	x	Voicemail wird als Wave-Datei an E-Mail angehängt
AutoAttendant-Funktionen			
Vermittlungs-Mailboxen (Basic AutoAttendants)	100	20	
Company AutoAttendant	x	x	Zentraler Vermittlungsplatz und zentrale Voicemail mit alternativen Ansagen je Nebenstelle
Ansagen vor Melden / Parallel-Signalisierung	x	x	Ansage zum Anrufer während der Teilnehmer angerufen wird bei UC Suite ist das nur in Verbindung mit dem Contact Center möglich
Einwahlziele für 4 Tagesabschnitte / Kalender für AutoAttendant	x	x	Automatische Vermittlung unterschiedlich zu verschiedenen Tageszeiten Kalender-Funktion bei UC Smart über die automatische Nachtschaltung möglich
Kalender zentral für Mailbox	x	x	Ansagen und Rufbehandlung für firmenweite Termine z. B. Feiertage, Betriebsferien etc.
Profile individuell für Mailbox und pers. AutoAttendant	-	x	Präsenzabhängige Rufbehandlung individuell je Teilnehmer einstellbar
Zeitpläne	Tag-Nachschaltung	Zeitplan mit Regeln (Call Control Vector CCV)	
Vorlagen (Templates)	1 AutoAttendant standardmäßig eingerichtet	5 anpassbare Vorlagen	
grafischer Regel-Editor (CCV-Editor)	-	x	

UC-Funktion	UC Smart	UC Suite	Bemerkung
Verkettung von Mailboxen / Multi Step AutoAttendant	x	-	Das Gespräch wird von einer verketteten Mailbox auf die nächste weitergeleitet und dabei wird immer die jeweilige Ansage abgespielt
Nach Name wählen	-	x	
Nebenstellenwahl	x	x	
Voicemail-Funktionen			
Individuelle Begrüßungen pro Mailbox	4	10	Verschiedene Ansagen speichern und einstellen
Weiterleiten von Sprachnachrichten	-	x	Nachricht an andere Teilnehmer/Mailboxen weiterleiten
Rückruf aus der Voicebox	x	x	Rückruf zum Anrufer der Nachricht aktivierbar
Benachrichtigungsruf	-	x	Wenn eine Nachricht vorliegt erfolgt ein Ruf zu einem externen Ziel, z. B. Handy
Vertreterfunktion	-	x	Weiterleitung des Anrufers an Vertreter mit persönlicher Ansage
Anruferbasierte Voicemail / CLI-Routing	-	x	Behandlung von Rufnummer abhängig, z. B. Begrüßung in Anruferssprache
Zentrale Gruppen-Mailbox	x	x	Mit Ansagen für Abteilungen/Gruppen
Mitschneiden / Live Recording	-	x	Mitschneiden von Gesprächen mit Sicherheitsfunktionen In OpenScape Business S, in dem eine Live-Aufzeichnung von UC verwendet wird, wird G.729A nicht berücksichtigt.
Nachrichten speichern	-	x	Teilnehmer können einzelne Voicemail-Nachrichten für sich abspeichern
Automatisches Löschen von Nachrichten	x	x	Nach Zeit werden Nachrichten gelöscht, um Speicher frei zu machen
Mailbox-Sprachwechsel teilnehmerindividuell	-	x	Auswahl der autom. Ansagen in individueller Sprache

Zugehörige Konzepte

UC Smart auf Seite 490

3.2.2 Benutzerzugriff auf UC-Funktionen (UC Clients)

Der Zugriff der UC-Funktionen erfolgt über UC Clients. Auf Anwesenheitsstatus (UC Suite) und Sprachbox (UC Smart und UC Suite) kann auch über TUI (Telefonie User Interface) zugegriffen werden.

UC Clients werden für die gängigen Betriebssysteme angeboten. Bitte beachten Sie hierzu auch die Voraussetzungen der Clients in den jeweiligen Freigabemitteilungen.

Communication Clients (Desktop und Groupware Clients)

Client	Empfohlen für		Beschreibung
	UC Smart	UC Suite	
myPortal @work	x	x	UC-Desktop-Client für Microsoft Windows und Mac OS X
myPortal for Desktop	-	x	Erweiterter UC-Desktop-Client für Microsoft Windows und Apple Mac
myPortal for Outlook	-	x	UC-Groupware-Client für Microsoft Outlook-Integration
OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA (in der Telefon-Software integrierter Client)	x	x	Präsenz-Steuerung und Zugriff auf das Telefonbuch bei UC Suite und UC Smart

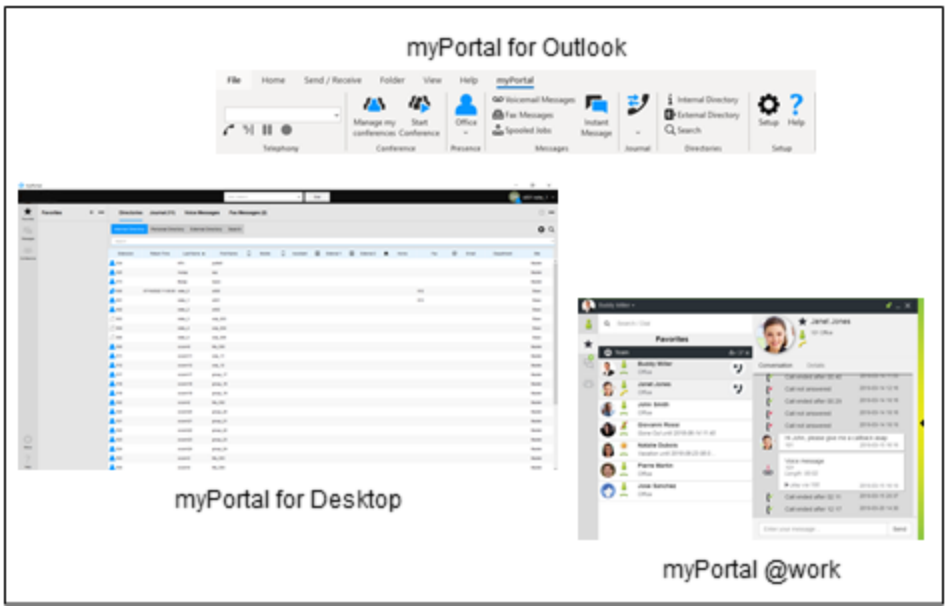


Abbildung 1: myPortal for Desktop, myPortal for Outlook und myPortal @work

Mobility Clients

Client	Empfohlen für		Beschreibung
	UC Smart	UC Suite	
myPortal to go	x	x	Mobile App für Smartphones und Tablet-PC myPortal to go ist mit leicht unterschiedlichem Funktionsumfang für UC Smart und UC Suite verfügbar

Abbildung 2: myPortal to go

Contact Center Clients

Client	Empfohlen für		Beschreibung
	UC Smart	UC Suite	
myAgent	-	x	Contact Center Client
myReports	-	x	Reports/ Auswertungsoberfläche für Contact Center myReports kann unabhängig vom Contact Center auch für Systemstatistiken eingesetzt werden

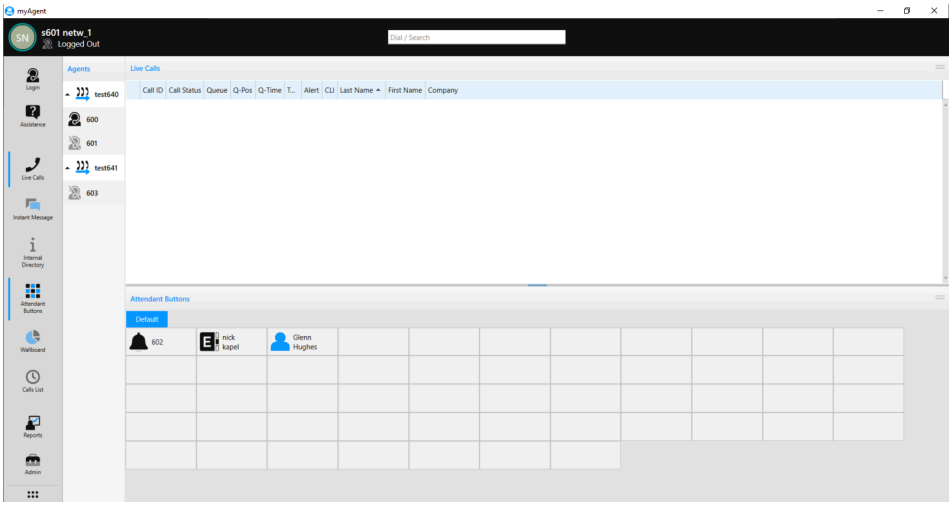


Abbildung 3: myAgent

Attendants/Vermittlungsplätze

Client	Empfohlen für		Beschreibung
	UC Smart	UC Suite	
OpenScape Business Attendant	x	-	UC-Vermittlungsplatz inklusive Präsenz
myAttendant	-	x	Erweiterter UC-Vermittlungsplatz für UC Suite

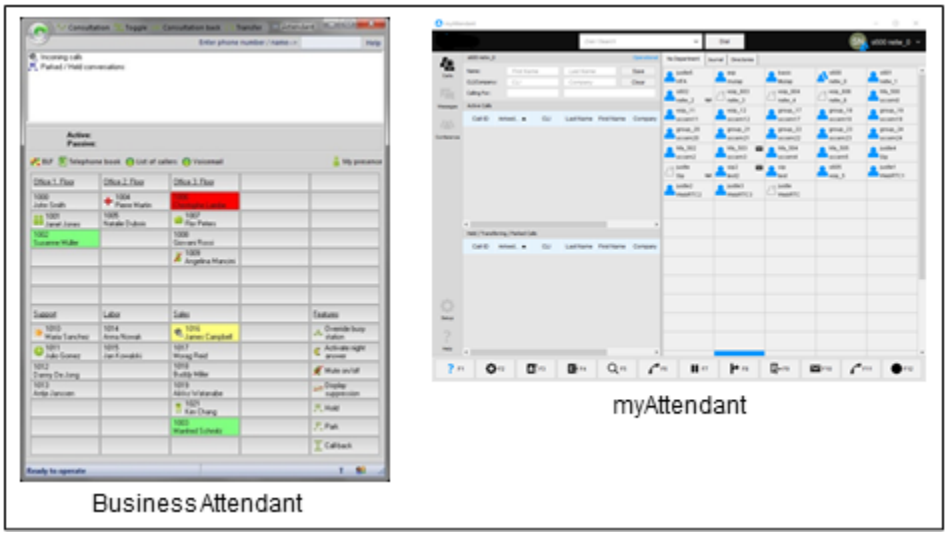


Abbildung 4: myAttendant

3.2.3 Integration in Geschäftsanwendungen

OpenScape Business kann in bestehende IT-Infrastrukturen und Geschäftsanwendungen integriert werden.

Applikationen

- Application Launcher für eine aktive Interaktion mit CRM/ERP-Applikationen
- Accounting Software für Gebührenauswertungen

Integrierte Services

- Directory Services für Informationen zu Anrufern und der Suche in internen und externen Verzeichnissen
- Präsenz-Management und IM (Instant Messaging) zu sozialen Netzwerken (Social Media Networks)
- Web Services für Interaktionen mit Web-basierten Applikationen auf z.B. Mobiletelefonen und Tablet-PC

CTI-Middleware

- First- and Third-party TAPI Service Provider für die Anrufsteuerung aus CTI- oder CRM/ERP-Applikationen

Schnittstellen und Protokolle

- CSTA für die Überwachung und Steuerung unterschiedlichster Applikationen
- SIP für die Verbindung zu SIP-Trunking basierten Applikationen
- LDAP für die Verbindung zu externen Verzeichnissen oder von externen LDAP-Clients
- HTTP und HTTPS für den Zugriff auf UC-Funktionen des integrierten Web-Servers
- TCP/IP als Basisprotokoll für alle Ethernet-Verbindungen
- SQL Konnektor für die Anschaltung von SQL-Datenbanken (Microsoft SQL Server, PostgreSQL, Sybase SQL Server)
- LDAP Konnektor für externe LDAP-Server wie z.B. Active Directory

3.3 OpenScape Business Modelle

Für die Nutzung der Telefonie und UC-Funktionen werden unterschiedliche Modelle angeboten. Sie können zwischen Hardwaremodellen und reinen Softwaremodellen wählen, die auf Standard Servern oder in einer virtuellen Umgebung mit VMware vSphere betrieben werden.

Die UC-Funktionalität für UC Smart ist bereits in OpenScape Business integriert. UC Suite benötigt zusätzlich entweder die intern steckbare Baugruppe "UC Booster Card" oder den externen Linux-Server "UC Booster Server". Der Softswitch OpenScape Business S unterstützt wahlweise UC Smart oder UC Suite.

3.3.1 Vertriebliche Ausbaustufen

Die OpenScape Business Modelle haben unterschiedliche Ausbaustufen.

	X1	X3R/X3W	X5R/X5W	X8	S
Anbindung an Service-Provider					
ITSP-Kanäle (SIP-Provider)	30	60	60	60	180
Max. Anzahl aktiver SIP-Provider	8	8	8	8	8
ISDN S_0 (BRI)	4	20	52	128	-
	via Mainboard	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	SW-Limit, d.h. unabhängig von der Anzahl der STDM3-Baugruppen	
ISDN S_{2M} (PRI)	-	30	30	120	-
			1* TS2	3 * DIUT3	
Max. Anzahl Leitungskanäle (ITSP, SIP-Q, Native SIP, TDM Leitungen, MEB)	250	250	250	250	250
Teilnehmer					
ISDN	4	20	52	128	-

	X1	X3R/X3W	X5R/X5W	X8	S
	via Mainboard	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	8* STMD3	
Analog	4	20	52/68	384	-
	via Mainboard	X3R: 2* SLAV8R X3W: 1* SLAV16	X5R: 6* SLAV8R X5W: 4* SLAV16	16* SLMA	
Digital ($U_{P0/E}$)	8	24	56	384	-
	via Mainboard	2* SLU8(R)	6* SLU8(R)	16* SLMO2	
IP-Teilnehmer	20[1]	500	500	500	2000 (max. 500 SIP-Teilnehmer)
Cordless/DECT(CMI)	16	32	32/64	250	-
	1-7 Basisstationen via Mainboard	1-7 Basisstationen via Mainboard + 8-15 über SLUN	1-7 Basisstationen via Mainboard + 8-15 über SLUN	4* SLMUC	
Max. Anzahl Teilnehmer	30[1]	500	500	500	2000
Unified Communications (UC Smart)					
UC Smart VoiceMail (Smart VM)	30	500/320[2]	500/320[2]	500/320[2]	1500
Max. Anzahl gleichzeitig aktiver UC Smart Clients (Summe aus myPortal to go, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF und WSI-Clients von Drittanbietern)	30	250/50[2]	250/50[2]	250/50[2]	250
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	250
	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten
Max. Anzahl der mobilen Teilnehmer	30	250/50[2]	250/50[2]	250/50[2]	250
Anzahl Mobility Entry User	30	150	150	150	250
myPortal to go	30	250/50[2]	250/50[2]	250/50[2]	250
myPortal for Teams	-	-	-	-	250
Max. Anzahl Kanäle für UC-Konferenzen	30	30	30	30	60
Unified Communications (UC Suite)					
UC Suite VoiceMail	-	500	500	500	1500

	X1	X3R/X3W	X5R/X5W	X8	S
Max. Anzahl gleichzeitig aktiver UC Suite Clients (Summe aus myPortal for Desktop, myPortal for Outlook, myAttendant, myAgent)	-	500/150[3]	500/150[3]	500/150[3]	1500
Max. Anzahl weiterer gleichzeitig aktiver Cllents (Summe aus myPortal to go, myPortal for Teams, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF und 3rd Party WSI Clients)	-	-	-	-	500
myPortal for Desktop	-	500/150[3]	500/150[3]	500/150[3]	1500
myPortal for Outlook	-	500/150[3]	500/150[3]	500/150[3]	1500
myAttendant	-	20	20	20	20
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	500
	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten
myAgent	-	192 einrichtbar / 64 parallel aktiv	192 einrichtbar / 64 parallel aktiv	192 einrichtbar / 64 parallel aktiv	192 einrichtbar / 64 parallel aktiv
Max. Anzahl der mobilen Teilnehmer	-	250/150[3]	250/150[3]	250/150[3]	250
Anzahl Mobility Entry User	-	150	150	150	250
myPortal to go	-	250/100[3]	250/100[3]	250/100[3]	250
myPortal for Teams	-	-	-	-	250
myReports	-	1	1	1	1
Max. Anzahl gleichzeitiger Fax Kanäle	-	8	8	8	8
Max. Anzahl Fax User	-	500/150[3]	500/150[3]	500/150[3]	1500
Max. Anzahl Kanäle für UC-Konferenzen	-	20	20	20	60
Unified Communications (CRM, Datenbankanbindung)					
Application Launcher	30 einrichtbar/ 30 parallel aktiv	500 einrichtbar/ 50 parallel aktiv	500 einrichtbar/ 50 parallel aktiv	500 einrichtbar/ 50 parallel aktiv	500

	X1	X3R/X3W	X5R/X5W	X8	S
TAPI 120/170 User (über CSTA, UC Booster Server/Card notwendig)	-	500/150[3]	500/150[3]	500/150[3]	1500
TAPI 120 User (im UC Smart Modus via Mainboard ohne CSTA)	30	30	30	30	-
Directory Service Connector (UC Booster Card/Server notwendig)	-	4	4	4	4

Für eine detaillierte Beschreibung der Ausbaustufen/Ausbaugzenzen siehe auch Ausbaugrenzen und Kapazitäten .

OpenScape Business UC-Vernetzung

OpenScape Business bietet weitreichende UC-Vernetzungsmöglichkeiten:

- Umfassende Voice- und UC-Vernetzung zwischen den verschiedenen OpenScape Business X (bei UC-Vernetzung UC Booster Card/Server notwendig) und OpenScape Business S
- mit mehreren Gebäuden auf dem Firmengelände
- mit verteilten Standorten
- zentrale Administration inkl. Lizenzen (HiPath 5000 RSM nicht mehr notwendig)
- Voice-Vernetzung mit OpenScape Enterprise in Vorbereitung

Bei Voice-Vernetzung werden Vernetzungen mit bis zu 32 Knoten unterstützt. Bei UC-Vernetzung werden Vernetzungen mit maximal 8 Knoten und bis zu 1000 Teilnehmern unterstützt (1500 Teilnehmer bei OpenScape Business S). Darüber hinaus sind projektspezifische Freigaben möglich.

Für eine detaillierte Beschreibung der Vernetzungsszenarien siehe Ausbaugrenzen und Kapazitäten .

3.3.2 UC Hardware Modelle

Die Kommunikationssysteme OpenScape Business X bieten ein hohes Maß an Flexibilität hinsichtlich Leistungsumfang und Konstruktion. Je nach OpenScape Business X Modell werden bis zu 500 Teilnehmer für IP, Digital (ISDN), Analog (a/b) und Cordless (DECT) sowie die Anbindung ans öffentliche Netz über ITSP (SIP), ISDN (BRI und PRI), CAS und Analog und onboard-IP (auf dem Mainboard vorgeleistet) unterstützt.

- OpenScape Business X1W

  Kommunikationssystem im Wandgehäuse, das an einer Wand montiert werden muss.

[1] Max. Summe aus IP und Deskshare User = 20 (Begrenzung über Konfiguration) - max. Summe aus IP, Deskshare, analogen und digitalen Teilnehmern = 30 (Begrenzung über Lizenzen)

[2] 1. Wert: Maximaler Ausbau mit UC Booster Server / 2. Wert: Maximaler Ausbau mit UC Booster Card

[3] 1. Wert: Maximaler Ausbau mit UC Booster Server / 2. Wert: Maximaler Ausbau mit UC Booster Card

- OpenScape Business X1R

  Kommunikationssystem im 19”-Rackgehäuse, das in einen 19”-Schrank montiert, frei aufgestellt (Tischbetrieb) oder an einer Wand montiert werden kann.
- OpenScape Business X3W

  Kommunikationssystem im Wandgehäuse, das an einer Wand montiert werden muss.
- OpenScape Business X3R

  Kommunikationssystem im 19”-Rackgehäuse, das in einen 19”-Schrank montiert, frei aufgestellt (Tischbetrieb) oder an einer Wand montiert werden kann.
- OpenScape Business X5 W

  Kommunikationssystem im Wandgehäuse, das an einer Wand montiert werden muss.
- OpenScape Business X5R

  Kommunikationssystem im 19”-Rackgehäuse, das in einen 19”-Schrank montiert, frei aufgestellt (Tischbetrieb) oder an einer Wand montiert werden kann.
- OpenScape Business X8

  Modulares Kommunikationssystem, das als Einboxsystem (Basisbox) oder als Zweiboxsystem (Basisbox + Erweiterungsbox) eingesetzt werden kann. Das Kommunikationssystem kann frei aufgestellt oder in einen 19"-Schrank montiert werden.

Abbildung 5: Hardware-Plattformen

3.3.3 UC Booster Hardware

UC Booster Hardware für OpenScape Business X.

- OpenScape Business UC Booster Card

  Platine für OpenScape Business X, wenn die UC Suite als UC-Lösung mit bis zu 150 UC-Benutzern verwendet werden soll.

- OpenScape Business UC Booster Server

  Externer UC Booster Server (Linux) für OpenScape Business X, wenn die UC Suite als UC-Lösung mit bis zu 500 UC-Benutzern verwendet werden soll.

  SLES 12 SP5 64-Bit oder SLES 15 SP6 64-Bit wird auf dem UC Booster Server verwendet. Der UC Booster Server kann auch in einer virtuellen Umgebung mit VMware vSphere ausgeführt werden.

  Bei Verwendung vom UC Booster Server ist die UC Booster Card nicht erforderlich.
- OpenScape Business Voice Channel Booster Card

  Zwei optionale Module zur Erweiterung von OpenScape Business X um zusätzliche DSP-Kanäle (z.B. für simultane Sprachverbindungen mit IP/TDM-Übergängen).

  Acht DSP-Kanäle sind auf der Hauptplatine vorhanden. Die Sprachkanal-Booster-Karte OCCB/1 stellt weitere 48 DSP-Kanäle und die Sprachkanal-Booster-Karte OCCB/3 stellt bis zu 128 DSP-Kanäle zur Verfügung.

3.3.4 UC Software Modelle (Softswitch)

Serverbasierte All-in-One-UC-Softwarelösung, die bis zu 1000 IP-Stationen mit Verbindungen zum öffentlichen Netzwerk über ITSP (SIP) unterstützt.

Unabhängig von der verwendeten Plattform kann OpenScape Business S auf einem Linux-Server installiert werden. Als Betriebssysteme werden SLES 12 SP5 64-Bit oder SLES 15 SP6 64-Bit verwendet. OpenScape Business S kann auch in einer virtuellen Umgebung mit VMware vSphere ausgeführt werden. Werden TDM-Schnittstellen für den Anschluss an TDM-Telefone oder TDM-Trunks benötigt, können OpenScape Business X-Systeme als Gateway verwendet werden.

3.3.5 Aufbau und Umweltbedingungen

	X1	X1R	X3W	X3R	X5W	X5R	X8
Aufbau	Wandsystem	Rack	Wandsystem	Rack	Wandsystem	Rack	Standardsyste (auch Einbau i Rack möglich
Abmessungen (HxBxT in mm)	470x370x80	450x460x130	450x460x130	89x440x380 (2U)	450x460x200	155x440x380 (3,5U)	490x440x430
Gewicht	ca. 2,8 kg	ca. 6 kg	ca. 6 kg	ca. 6 kg	ca. 8 kg	ca. 8 kg	ca. 34 kg (vol bestückt)
Gehäusefarbe	Weiß	Schwarz	Weiß	Grün/Dunkelgrau	Weiß	Grün/Dunkelgrau	Grün/Dunkelgra
Stromversorgung	Die Modelle sind standardmäßig für den Netzbetrieb ausgelegt • Nenneingangsspannung (AC): 100 bis 240 V • Nennfrequenz: 50/60 Hz • Batteriestrom (DC): -48 V						

	X1	X1R	X3W	X3R	X5W	X5R	X8
Leistungsaufnahme	Abhängig von der Hardware-Plattform und dem Ausbau						
Umweltbedingungen	• Betriebsbedingungen: +5 bis +40 °C (41 bis 104 °F) • Feuchtigkeit: 5 bis 85%						

3.3.6 Unterstützte Telefone

OpenScape Business X ermöglicht Telefonieren über IP/HFA (HiPath Feature Access), SIP, TDM, a/b, Cordless/DECT und WLAN. An OpenScape Business S können IP/HFA-, SIP- und WLAN-Telefone angeschlossen werden.

OpenStage-Telefone (IP/HFA, SIP und T))	• OpenStage 5/10/15/20/30/40/60/80
OpenScape Desk Phone (IP/HFA, SIP und T)	• OpenScape Desk Phone IP 35G/55G/35G Eco • OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA und SIP 200/400/205/405 TDM • OpenScape Desk Phone CP 110/210/410/710 HFA und SIP
Beistellgeräte	• OpenStageKey Module nur für OpenStage 15/40/60 • OpenStage BLF 40 (Besetztlampenfeld), nur für OpenStage 40 und OpenStage 30 T • OpenScape Key Module 400/600, nur für CP 400/600/600E/700/700X • OpenScape Key Module 410/710, nur für CP 710
OpenScape Business Cordless	• OpenStage M3 • OpenScape DECT-Telefon S6/SL6/R6
PC-Clients (HFA, SIP)	• OpenScape Personal Edition (bei SIP inkl. Video)
SIP-Telefone (UC Suite) / AP-Adapter	• SIP-Telefone mit RFC 3725-Unterstützung • Mediatrix 4102S (zum Anschluss von 2 analogen Telefonen oder Faxgeräten)
WLAN-Telefone	• OpenStage WL3 professional • OpenScape WLAN-Telefon WL4/WL4 Plus
Analog- und ISDN-Telefone	• Analoge (a/b) Telefone • Digitale (S_0) ISDN-Telefone

Ältere Geräte (z. B. optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 und optiPoint WL2 SIP) werden unterstützt. Optiset E-Geräte können nicht betrieben werden.

Funktionen und Konfiguration der SIP-Telefone

OpenScape Business bietet für OpenStage HFA Telefone einen umfangreichen Funktionsumfang für die Sprachkommunikation. Viele Funktionen sind auch für Standard-SIP-Telefone möglich.

Eine Übersicht der mit OpenStage SIP-Telefonen unterstützen Leistungsmerkmale und weitere Hinweise finden Sie im Unify Wiki unter dem Link

`http://wiki.unify.com/wiki/Features_and_Configuration_of_SIP_Devices`

Für die Steuerung von Sprachverbindungen für SIP Telefone über CTI (3PCC) wird bei OpenScape Business X3/X5/X8 eine UC Booster Card oder ein UC Booster Server benötigt.

Die Steuerung von Sprachverbindungen für SIP Telefone über UC Smart Clients wird für OpenScape Business X3/X5 Rack mit UC Booster Card unterstützt.

Mit Hilfe der DLI-Funktionen können die OpenScape Desk Phone (SIP) Telefone zentral administriert und mit Software versorgt werden.

Zugehörige Konzepte

CSTA auf Seite 1171

3.4 Weiterführende Informationen

Weiterführende Informationen finden Sie im Internet und Extranet.
Für Einschränkungen und letzte Änderungen beachten Sie auch die Freigabemitteilungen.

3.4.1 Unterstützte Sprachen

Für die unterschiedlichen Softwarekomponenten (Clients und WBM) und Dokumentation/Online-Hilfe stehen verschiedene Sprachen zur Verfügung.

Die folgenden Sprachen werden im Rahmen der Ländereinführungen bereitgestellt.

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
UC Smart Clients										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
myPortal @work (Benutzerhandbuch)	X	X	X	X	X	X	X	-	-	-
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	–	X	–	X
TUI (Kurzbedienungsanleitung)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Attendant / BLF (Client)	X	X	–	–	–	X	–	–	–	–
OpenScape Business Attendant / BLF (Bedienungsanleitung)	X	X	–	–	–	X	–	–	–	–
UC Suite Clients										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (Benutzerhandbuch)	X	X	X	X	X	X	X	-	-	-
myPortal for Desktop (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Desktop (Bedienungsanleitung/ Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myPortal for Outlook (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Outlook (Bedienungsanleitung/ Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myAttendant (Client)	X	X	X	X	X	X	X	X	X	X
myAttendant (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myAgent (Client)	X	X	X	X	X	X	X	X	X	X
myAgent (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myReports (Client)	X	X	–	X	X	X	X	–	–	–
myReports (Bedienungsanleitung/Online-Hilfe)	X	X	–	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	X	X	X	X
TUI (Kurzbedienungsanleitung)	X	X	–	–	–	–	–	–	–	–
Administration										

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
OpenScape Business Assistant (WBM)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Assistant (Administratordokumentation/Online-Hilfe)	X	X (kein nl)	–	–	–	–	–	–	–	–
Manager E	X	X	X	X	X	X	X	–	–	–
Manager E (Administratordokumentation/ Online/Hilfe)	X	X	–	–	X	–	–	–	–	–

Zusätzlich wird die UC Smart TUI auch in den Sprachen Belgisch (flämisch) und Slowenisch angeboten.

Tipp: Ein russisches bzw. chinesisches Windows-Betriebssystem ist Voraussetzung, um die russische bzw. chinesische Bedienoberfläche nutzen zu können.

Bei den in der Tabelle verwendeten Abkürzungen handelt es sich um folgende Sprachcodes (ISO 639-1):

- de = Deutsch
- en = Englisch
- cs = Tschechisch
- da = Dänisch
- es = Spanisch
- fi = Finnisch
- fr = Französisch
- hr = Kroatisch
- hu = Ungarisch
- it = Italienisch
- nl = Niederländisch
- no = Norwegisch
- pl = Polnisch
- pt = Portugiesisch
- ru = Russisch
- sv = Schwedisch
- tr = Türkisch
- zh = Chinesisch

3.4.2 Internet-Links

Weitere Informationen und ggf. aktuellere Informationen finden Sie auf der Unify Homepage, in unserem Experten-Wiki und im Unify Partnerportal.

Internet-Links

- Unify Homepage:

  http://www.unify.com
- Experten-Wiki für Telefone, Kommunikationssysteme und UC:

  http://wiki.unify.com
- Partnerportal (Registrierung erforderlich):

  https://www.unify.com/de/partners/partner-portal.aspx

  oder

  https://www.unify.com/en/partners/partner-portal.aspx

4 Administrationskonzept

Die Administration des Kommunikationssystems erfolgt mit dem OpenScape Business Assistant.

4.1 OpenScape Business Assistant (WBM)

Der OpenScape Business Assistant ist webbasiert und wird daher auch Web Based Management (WBM) genannt.

Der Umfang der angebotenen Administrationsaufgaben ist abhängig vom verwendeten Addministratorprofil.

Zu jeder Seite des WBM steht eine Online-Hilfe zur Verfügung.

4.1.1 Voraussetzungen für das WBM

Um das WBM nutzen zu können, benötigt der Administrations-PC geeignete Software.

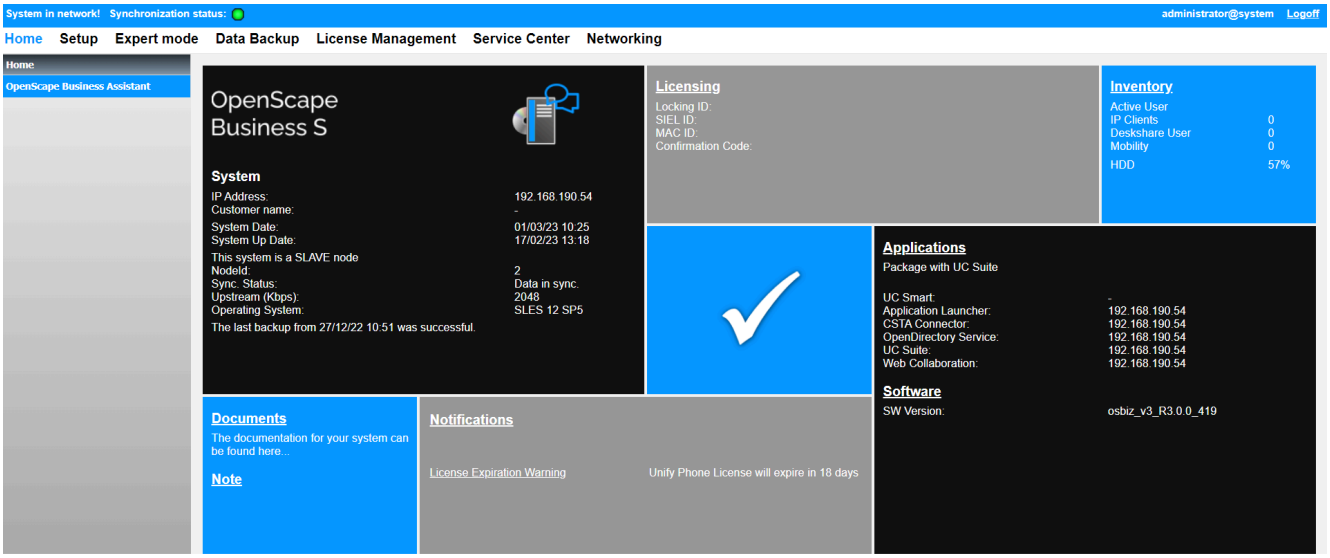
Unterstützte Webbrowser:

- Microsoft Internet Explorer 10 oder neuer
- Microsoft Edge
- Mozilla Firefox 18 oder neuer
- Google Chrome

4.1.2 Startseite des WBM

Auf der Startseite des WBM werden wichtige Systeminformationen angezeigt, die in verschiedene Bereiche (Kacheln) aufgeteilt sind. Zusätzlich gibt sie Hinweise und informiert über Systemfehler, Ereignisse und Aktionen.

Die angezeigten Systeminformationen sind vom verwendeten Administratorprofil abhängig. Die unterstrichenen Überschriften in den einzelnen Bereichen sind anklickbar und verweisen auf das zugehörige Thema im WBM.



Die folgenden Informationen werden angezeigt:

- Bereich: **Status** (Mitte)
  - Weißes Häkchen auf blauem Hintergrund: das Kommunikationssystem ist voll funktionsfähig - rot hinterlegte Meldungen in den anderen Feldern weisen auf Aktionen hin, die durchgeführt werden sollten.
  - Weißes Ausrufezeichen auf rotem Hintergrund: das Kommunikationssystem ist nicht voll funktionsfähig und erfordert den Eingriff des Administrators - rot hinterlegte Meldungen in den anderen Feldern weisen auf Systemfehler oder Ereignisse hin, die behoben werden müssen.
- Bereich: **System**
  - Produkt
  - IP-Adresse des Kommunikationssystems
  - Datum und Uhrzeit aktuell
  - Datum und Uhrzeit des letzten Neustarts des Systems
  - Hinweise beim Betrieb in einem Netzverbund (System ist Master oder Slave, Anzeige der Knoten-ID)
  - Synchronisationsstatus
  - Upstream-Bandbreite in Kbit/s
  - SDHC-Integritätsstatus
  - Hinweise für Sichern und Wiederherstellen
  - Status der Booster-Karte
- Bereich: **Dokumente**
  - Link zur Dokumentation
- Bereich: **Benachrichtigungen**
  - Verschiedene Benachrichtigungen über das System
- Bereich: **Hinweis**
  - Zeigt die von einem Administrator zuletzt eingegebenen Informationen an. Durch Klicken auf die unterstrichene Überschrift wird ein Textfenster

geöffnet, in dem alle Informationen angezeigt und weitere Informationen eingegeben werden können.

Daten des Notizfelds sind nicht im Backup-Set des Systems enthalten. Daher werden diese Daten beim Wiederherstellen eines Backup-Sets nicht wiederhergestellt.

- Bereich: **Lizenzierung**
  - Locking-ID für die Lizenzierung
  - SIEL-ID für die Lizenzierung
  - Hinweis auf den Lizenzierungsstatus, der angibt, ob das System sich im Lizenzmodus "Permanent" oder "Pay As You Go" (PAYG) befindet.
- Bereich: **Inventory**
  - Typ und Anzahl der aktiven Teilnehmer
  - Anzahl der aktivierten ITSPs und Link zum ITSP-Status-Dialog im Service-Center der aktiven Teilnehmer
- Bereich: **Applikationen** und Software

  Applikationen:
  - Verwendetes Applikationspaket (UC Smart oder UC Suite) und dessen Komponenten inkl. der IP-Adressen der verwendeten Server.
  - Gibt an, ob eine UC Booster Card gesteckt ist.

  Software:
  - Version der installierten Software des Kommunikationssystems
  - Gibt an, ob eine UC Booster Card gesteckt ist. Ist sie zusätzlich über eine IP-Adresse erreichbar, wird die Version der installierten UC Booster Card-Software angezeigt.

    UC Booster Card und Kommunikationssystem sollten immer auf dem gleichen Softwarestand sein.
  - Ablaufdatum des 3-jährigen Software-Supports.

    Nach dem Ablaufdatum erscheint die Meldung "Die Software-Support-Lizenz ist abgelaufen. Bitte aktualisieren Sie Ihre Software-Support-Lizenz".
  - Hinweis auf neue Softwareversion

4.1.3 Einführung in das WBM

Das WBM ist die webbasierte Anwendung für die Administration des Systems.

Sprache der Benutzeroberfläche

Sie können beim Anmelden eine der folgenden Sprachen wählen:

- Deutsch
- Englisch
- Französisch
- Italienisch
- Niederländisch (Online-Hilfe nur Englisch verfügbar)
- Portugiesisch
- Spanisch

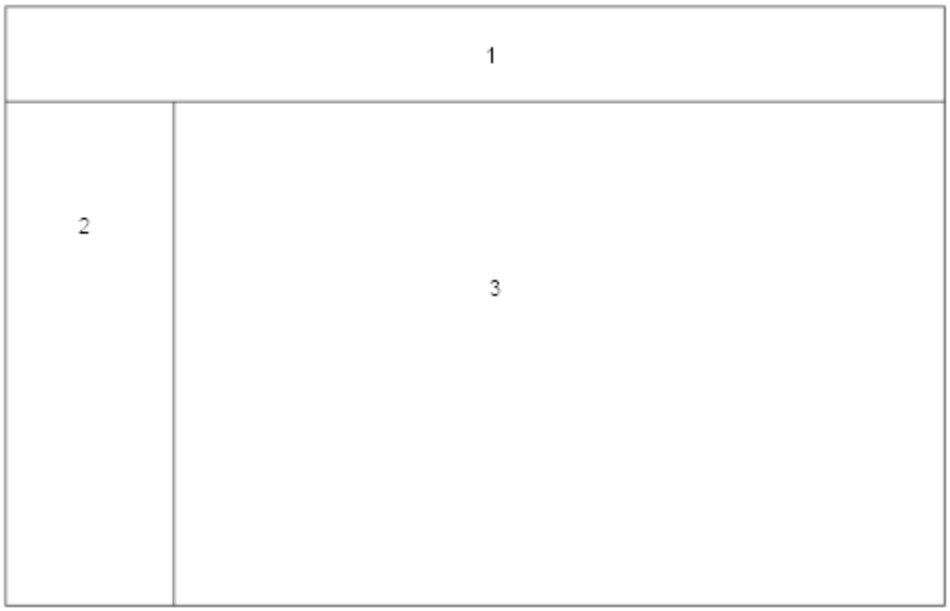
Rangfolge der beschriebenen Benutzeroberflächen

Sämtliche Tasks, die in einem Wizard durchgeführt werden können, sind nur für den entsprechenden Wizard beschrieben.

Weitere Tasks, die im Experten-Modus durchgeführt werden können, sind nur für den Experten-Modus beschrieben.

Nur die übrigen Tasks sind für Manager E beschrieben.

Elemente der Benutzeroberfläche



- Navigationsleiste (1)

  Die Navigation ist die primäre Navigationshilfe und zeigt immer die gleichen Links zu den Hauptaufgabenbereichen, d. h. **Startseite**, **Administratoren**, **Setup**, **Expertenmodus**, **Datensicherung**, **Lizenzmanagement**, **Service Center** sowie den aktuellen Benutzernamen und den Link **Logout** . Nach Anklicken eines Aufgaben-Centers öffnet sich im Navigationsbereich der zugehörige Navigationsbaum und im Arbeitsbereich die Startseite des Aufgaben-Centers.
- Navigationsbereich (2)

  Der Navigationsbereich ist die Sekundärnavigation und enthält den Navigationsbaum mit den Menüpunkten des gewählten Aufgaben-Centers. Im Navigationsbaum erscheint an oberster Stelle der Name des gewählten Aufgaben-Centers. Darunter befinden sich auf- und zuklappbare Menügruppen und Menüpunkte. Die Menügruppen enthalten situationsabhängig unterschiedliche Menüpunkte. Nach Anklicken eines Menüpunktes wird die zugehörige Seite im Arbeitsbereich dargestellt.
- Arbeitsbereich (3)

  Im Arbeitsbereich führen Sie die Administrationsaufgaben im Detail durch. Der Arbeitsbereich öffnet sich in der Regel in einem eigenen Fenster. Anzahl und Auswahl der angezeigten Informationen und Aktionen hängen ab vom gewählten Menüpunkt im Navigationsbaum. Im Experten-Modus wird im Arbeitsbereich links der Menübaum angezeigt.

Navigation im Menübaum

Der Menübaum dient zur Navigation im Experten-Modus des WBM. Der Menübaum enthält Ordner (z. B. **Wartung**) mit weiteren Elementen (z. B. **Neustart/Neuladen**).

Sie navigieren im Menübaum durch Klick auf den Ordner (wechselweise auf- und zuklappen).

Automatisches Abmelden nach Zeit

Nach 30 Minuten ohne Aktion werden Sie automatisch abgemeldet. Für weitere Aktionen mit dem WBM müssen Sie sich erneut anmelden. Laden Sie nach einer Pause zur Sicherheit die Seite neu, bevor Sie Änderungen durchführen, damit diese nicht wegen automatischem Abmelden verloren gehen.

4.1.3.1 So melden Sie sich bei der WBM an

Voraussetzungen

Sie müssen Zugriff auf Ihre Benutzeranmeldeinformationen (Benutzername und Passwort) haben. Wenn nicht, erhalten Sie diese von Ihrem Administrator.

TLS 1.2 ist in den Einstellungen Ihres Webbrowsers aktiviert.

Schritt für Schritt

1) Öffnen Sie die Anmeldeseite in Ihrem Webbrowser, indem Sie folgende Adresse eingeben: `https://<IP-Adresse des Kommunikationssystems>`. Die Standard-IP-Adresse ist 192.168.1.2.
2) Klicken Sie oben rechts auf den Sprachcode und wählen Sie aus dem Menü die Sprache aus, in der die Benutzeroberfläche des WBM angezeigt werden soll. Die Login-Seite wird in der ausgewählten Sprache angezeigt.
3) Geben Sie im ersten Feld unter **Login** den Benutzernamen ein. "@system" wird beim Verlassen des Feldes automatisch hinzugefügt.
4) Geben Sie Ihr Passwort in das zweite Feld unter **Login**ein. Beachten Sie die Verwendung von Groß- und Kleinschreibung und den Status der **Num-Taste**. Das Passwort wird mit Sternchen (*) angezeigt.
5) Klicken Sie auf **Login**.

Wenn Sie ungültige Anmeldeinformationen eingeben, wird nach dem dritten fehlgeschlagenen Anmeldeversuch eine Meldung angezeigt, die Sie darüber informiert, dass das Konto für 5 Minuten gesperrt ist. Sie können versuchen, sich nach diesem Zeitraum erneut anzumelden.

Bei jedem weiteren fehlgeschlagenen Anmeldeversuch wird dieser Zeitraum verdoppelt und erreicht im achten fehlgeschlagenen Versuch 160 Minuten. Für jeden fehlgeschlagenen Versuch beträgt die Sperrzeit des Kontos 160 Minuten.

4.1.3.2 Wie Sie sich vom WBM abmelden

Prozedur

- Klicken Sie oben rechts auf **Abmelden**.

4.1.4 WBM-Benutzerverwaltung

Sie können bis zu 16-Administratoren für WBM (webbasierte Verwaltung) konfigurieren und verwalten. Jedem Administrator wird ein Profil zugewiesen, das den Umfang seiner Berechtigung angibt. Sie können auch das Passwort eines Manager E-Administrators ändern.

Die Benutzer von WBM werden auch als Administratoren bezeichnet.

Der Standardadministrator ist `administrator@system` mit dem Standardpasswort `administrator` und hat das Profil **Erweitert**. Dieses Passwort muss bei der ersten Anmeldung geändert werden. Das Passwort für einen Administrator muss aus mindestens 8 Zeichen und maximal 128 Zeichen bestehen, von denen mindestens ein Zeichen eine Ziffer sein muss. Außerdem sollten für ein sicheres Passwort mindestens ein Großbuchstaben, ein Kleinbuchstaben und ein Sonderzeichen im Passwort enthalten sein.

Anmerkung: Der administrative Zugriff (einschließlich Administrator-Benutzerrolle) wird in der Nachrichtenprotokolldatei/syslog protokolliert. Sie kann über das Menü **Diagnose** > **Trace** aufgerufen werden.

Profile

Der WBM unterstützt vier Profile mit unterschiedlichen Dienstklassen (Berechtigungen) für Administratoren mit unterschiedlichen technischen Kenntnissen und Aufgaben.

Um zu verhindern, dass sich kein böswilliger Benutzer über ISDN anmelden und bei der erstmaligen Anmeldung das Standardpasswort ändern könnte, ist es für den Benutzer obligatorisch, das Passwort über Manager E als Installationsschritt zu ändern.

Anmerkung: Ein Passwort, das aus 5 Zeichen (****) besteht, wird aus Sicherheitsgründen vom System nicht akzeptiert.

Tabelle 1: Profildienstklassen

Profil	Berechtigung
Basic Grundkenntnisse in der Konfiguration des Systems	Systeminformationen auf der Startseite
	Assistent zur **Schlüsselprogrammierung**
	Assistent für **Telefonbuch / Kurzwahl**
	Assistent für **Anrufdetailaufzeichnung**
	Assistent für **Wartemusik / Ankündigungen**
	Assistent für **Stationsname und Freigabe**
	Zugang zu **Administratoren** (nur um ihre eigenen Passwörter zu ändern)
	Zugang zu **Lizenzverwaltung** > **Lizenzinformationen**
	Zugang zu **Service Center** > **Dokumente**
	Zugang zu **Service Center** > **Software**

Profil	Berechtigung
Verbessert Gute Kenntnisse in der Konfiguration des Systems	Wie für das **Basisprofil**, plus: Zugang zu allen Assistenten (außer den Assistenten **Grundinstallation**, **UC Suite** und **UC Smart**) **Anmerkung:** Der Zugriff auf alle Assistenten wird in OpenScape Business S-Systemen nicht unterstützt. Zugang zu **Administratoren** (nur um ihre eigenen Passwörter zu ändern) Zugang zu **Sichern und Wiederherstellen** Zugang zu **Lizenzverwaltung** (ohne Registrierung, Lizenzaktivierung und Einstellungen) Zugang zu **Service Center** > **Inventar** Zugang zu **Service Center** > **Neustart / Nachladen** (ohne Nachladen) Zugang zu **Service Center** > **Diagnose** > **Status** Zugang zu **Service Center** > **Diagnose** > **Event Viewer**
Erweitert Geschulte Benutzer	Wie für das **erweiterte** Profil, plus: Zugang zu allen Assistenten Zugang zu **Administratoren** (nur um ihre eigenen Passwörter zu ändern) Zugang zur vollständigen **Lizenzverwaltung** Zugang zum vollständigen **Service Center** Zugang zu **Vernetzung**
Experte Geschulte Diensttechniker	Wie für das **Erweiterte** Profil, plus: Zugang zu **Administratoren** (vollständig) Zugang zum **Expertenmodus**

Tabelle 2: Profilverwaltung

Profil	Wartung
Basic Grundkenntnisse in der Konfiguration des Systems	Kann eigenes Passwort ändern. Sieht keine anderen konfigurierten Administratoren außer sich selbst.
Verbessert Gute Kenntnisse in der Konfiguration des Systems	Kann eigenes Passwort ändern. Sieht keine anderen konfigurierten Administratoren außer sich selbst.

Profil	Wartung
Erweitert Geschulte Benutzer	Kann eigenes Passwort ändern. Sieht keine anderen konfigurierten Administratoren außer sich selbst.
Experte Geschulte Diensttechniker	Kann das eigene Passwort sowie die Benutzernamen und Passwörter anderer Administratoren ändern. Sieht alle konfigurierten Administratoren. Kann Administratoren hinzufügen, bearbeiten und entfernen.

Anmerkung: Solange kein Administrator mit dem **Expertenprofil** existiert, können Administratoren mit dem Profil **Erweitert** weitere Administratoren hinzufügen, bearbeiten und entfernen. Sobald ein Administrator mit dem **Expertenprofil** existiert, können nur Administratoren mit dem **Expertenprofil** weitere Administratoren hinzufügen, bearbeiten und entfernen.

Administratorverwaltung im Internet

Die direkte Verwaltung von Administratoren ist nur im WBM des Masterknotens möglich. Das **Administratormenü** wird auf Slave-Knoten nicht angezeigt. Alle Administrator-Konfigurationen werden an die Slave-Knoten übertragen. Es ist jedoch möglich, den WBM des Master-Knotens aus dem WBM des Slave-Knotens über die Knotenansicht aufzurufen. Das **Administrator-Menü** wird hier angezeigt und Administratoren können nur angezeigt werden.

Anmerkung: Das Hinzufügen/Bearbeiten/Löschen der Benutzer ist nicht über den Slave-Modus WBM-Zugriff möglich (sondern nur über Master-Modus WBM-Zugriff).

Manager E Passwortadministration

Ein Administrator kann das Passwort der vorhandenen Benutzer ändern (aber keine neue Benutzerrolle erstellen), die über Manager E auf das eingebettete System zugreifen können.

Der Benutzer wird aufgefordert, Passwörter nur für die vorhandenen Benutzer zu ändern und kann die Benutzergruppe nicht ändern. Optionen wie Erstellt, Zuletzt verwendet sind nicht sichtbar. Dies ist eine Sicherheitsfunktion und stellt daher nicht den gesamten Administrationsbildschirm des Manager E zur Verfügung.

4.1.4.1 Wie Sie einen Administrator hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet. (Solange noch kein Administrator mit Profil **Expert** existiert.)

Sie sind am WBM mit dem Profil **Expert** angemeldet. (Sofern bereits ein Administrator mit Profil **Expert** existiert.)

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.
2) Klicken Sie auf **Hinzufügen...**.
3) Geben Sie folgende Daten ein: **Login-Name**, **Vorname**, **Nachname**, **Passwort**, **Passwort wiederholen**.
4) Wählen Sie in der Aufklappliste **Benutzerrolle** das gewünschte Benutzerprofil.
5) Klicken Sie auf **OK & Weiter**.

4.1.4.2 Wie Sie einen Administrator bearbeiten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.
2) Aktivieren Sie in der **Administratoren-Liste** das Kontrollkästchen des gewünschten Administrators.
3) Klicken Sie auf **Bearbeiten**.
4) Passen Sie die Daten an (Login-Name, Vorname und Nachname, Passwort und Benutzerrolle).
5) Klicken Sie auf **OK & Weiter**.

4.1.4.3 Wie Sie das eigene Administratorpasswort ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.
2) Geben Sie im Feld **Passwort** und im Feld **Passwort wiederholen** jeweils das neue Passwort ein.

   Anmerkung: Ein Passwort, das aus 5 Sternen (*****) besteht, wird aus Sicherheitsgründen vom System nicht akzeptiert.

3) Klicken Sie auf **OK & Weiter**.

Zugehörige Konzepte

Sofortiges Sichern auf Seite 1256

4.1.4.4 Wie Sie einen Administrator löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.
2) Aktivieren Sie in der **Administratoren-Liste** das Kontrollkästchen des betreffenden Administrators.
3) Klicken Sie auf **Löschen...**.

4.1.4.5 So ändern Sie ein Manager E Administrator-Kennwort

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.
2) Klicken Sie auf Manager E **AdministratorsList**.
3) Bearbeiten Sie die Daten (Benutzerkonten, Neues Kennwort, Kennwort bestätigen) nach Bedarf.
4) Klicken Sie auf **Speichern**.

Anmerkung: Das Kennwort muss aus mindestens 5 Zahlen bestehen. Die Verwendung von Buchstaben oder anderen Zeichen ist nicht erlaubt. Außerdem können alte Kennwörter nicht wiederverwendet werden.

4.1.5 Wizards

Kundenadministrator (Profil Basic) steht ein ausgewählter Teil der Wizards zur Verfügung. Für einen Kundenadministrator (Profil **Basic**) steht ein ausgewählter Teil der Wizards zur Verfügung, für einen Administrator mit Fachkenntnissen oder einen geschulten Servicetechniker (Profil **Advanced**) hingegen sämtliche Wizards.

Die zur Verfügung stehenden Wizards hängen von der Systemkonfiguration ab (UC Smart oder UC Suite). Wizards können aus mehreren aufeinanderfolgenden Seiten bestehen. OK & Weiter speichert durchgeführte Änderungen und wechselt zur nächsten Seite des Wizards. Mit OK & Weiter gespeicherte Änderungen können nicht verworfen werden. Sofern keine Änderungen gespeichert wurden, beendet **Abbrechen** den Wizard. Das Anklicken des Symbols **X** in der rechten oberen Ecke des Wizard-Fensters beendet den Wizard und behält zuvor mit OK & Weiter gespeicherte Änderungen bei.

4.1.5.1 Wizards – Grundinstallation

Wizards unter **Grundinstallation** unterstützen die einfache Grundinstallation.

Folgende Wizards sind unter **Grundinstallation** verfügbar:

- **Erstinstallation**

  Einmalige Nutzung bei Ersteinrichtung. Länderintialisierung, System IP-Adresse und DHCP-Server.
- **Basisinstallation**

  Grundeinrichtung des Systems mit Teilnehmerdaten, Amtsleitungen, Netzwerkparameter, Internet.
- **Lizenzierung**

  Lizenzen online aktivieren über den Lizenzserver.
- **Vernetzung-Konfiguration**

  Einrichtung des Systems als Teil einer Vernetzung.
- **Power Management**

  Einrichtung und Aktivierung des Power Managements.

4.1.5.2 Wizards – Netzwerk / Internet

Wizards unter **Netzwerk / Internet** unterstützen die einfache Konfiguration des Netzwerks und des Internet-Zugangs.

Folgende Wizards sind unter **Netzwerk / Internet** verfügbar:

- **Netzwerk-Konfiguration**

  Einrichtung von DHCP, IP-Routing und DNS-Server.
- **Internet-Konfiguration**

  Zugangsparameter der Internet-Providerdaten z.B. User-Account und Passwort.
- **VPN-Konfiguration**

  Anbindung von Arbeitsplätzen über das Internet.

4.1.5.3 Assistenten – Telefone / Abonnenten

Die Assistenten unter **Telefone / Abonnenten** unterstützen die einfache Konfiguration von Telefonen und Abonnenten.

Die folgenden Assistenten sind unter **Telefone / Abonnenten**verfügbar:

- **IP-Geräte**

  Einrichten von systemspezifischen IP- und SIP-Telefonen, FAX-Rufnummern sowie IP/Analog-Adaptern.
- **UP0-Geräte**

  Einrichten von UP0-Telefonen, FAX-Rufnummern.
- **DECT-Telefone**

  Einrichten von DECT-Telefonen, FAX-Rufnummern.

- **Mitel SIP DECT**

  Konfiguration von Mitel SIP DECT RFP-Geräten.
- **ISDN-Geräte**

  Unversorgte ISDN-Anschlüsse für ISDN-Karten / Modems und S0-Teilnehmer.
- **Analoge Endgeräte**

  Analoge DTMF- und CLIP-fähige Anschlüsse für Fax und Telefon.
- **Tastenprogrammierung**

  Namens- und Funktionstastenprogrammierung für systemspezifische IP-Geräte und UP0-Telefone.

4.1.5.4 Wizards – Zentrale Telefonie

Wizards unter **Zentrale Telefonie** unterstützen die einfache Konfiguration zentraler Telefonie-Leistungsmerkmale.

Folgende Wizards sind unter **Zentrale Telefonie** verfügbar:

- **Amtsleitung ISDN / Analog / ITSP**

  Mehrgeräteanschluss (MSN) und Anlagenrufnummer für ISDN-Anschlüsse, sowie Zuweisung von analogen Amts- und ITSP Leitungen.
- **Internet-Telefonie**

  Zugangsparameter des Internet-Telefonie Service Provider (ITSP) z.B. Benutzerkonto, Passwort, SIP-Rufnummer.
- **Telefonbuch/Kurzwahl**

  Einrichtung von zentralen Kurzwahlzielen für das Systeminterne Telefonbuch.
- **Gesprächsdatenerfassung**

  Einrichtung von Verbindungsparameter der Gesprächsdatenerfassung für Gebührenapplikationen.
- **Wartemusik / Ansagen**

  Einspielen von neuen Melodien und Ansagen für die Wartemusik und Ansage vor dem Melden.
- **Türsprechstelle (Türöffner)**

  Einrichtung von Rufzuordnung und Zugriffsberechtigung der Türsprechstelle am analogen Teilnehmeranschluss.
- **SmartVM**

  Einrichtung der UC Smart Sprachbox (SmartVM).
- **Blacklist für eingehende Anrufe**

  Sie können eine Liste mit Nummern erstellen, um unerwünschte Anrufer dauerhaft zu blockieren.
- **Active Directory Integration Service**

  Active Directory einrichten

4.1.5.5 Wizards – User-Telefonie

Wizards unter **User-Telefonie** unterstützen die einfache Konfiguration von Leistungsmerkmalen der User-Telefonie.

Folgende Wizards sind unter **User-Telefonie** verfügbar:

- **Berechtigung**

  Einrichtung von Berechtigungsgruppen mit externen Rufnummern, die dem Teilnehmer zugeordnet werden können, z.B. Notruf, erlaubte Rufnummern, verbotene Rufnummern sowie Zuordnung der Berechtigung zur Nachtschaltung.
- **Teilnehmername und Freischaltung**

  Ändern von Teilnehmer- und Gruppennamen sowie Rücksetzen des Codeschlosses für einzelne Teilnehmer.
- **Gruppenruf / Sammelanschluss**

  Einrichtung von kommenden Anrufen für Teilnehmergruppen (parallele, lineare oder zyklischen Rufreihenfolge).
- **Anrufumleitung**

  Einrichtung von zentraler systemweiter Teilnehmerrufzuordnung sowie Weiterschaltung nach Zeit und bei Besetzt.
- **Anrufübernahme**

  Einrichtung von Teilnehmern zu einer Gruppe mit der Möglichkeit der gegenseitigen Rufannahme.
- **Teamschaltung**

  Einrichtung von Teilnehmern, die bei kommenden Gesprächen parallel zum Hauptteilnehmer gerufen werden und bei gehender Verbindung dessen Rufnummer verwenden können.
- **Mobiltelefon Integration**

  Einrichtung einer Verknüpfung zwischen einem Mobiltelefon und einem internen Teilnehmer mit dem Ziel der Erreichbarkeit kommend und gehend unter einer Rufnummer (One Number Service).
- **Chef / Sekretär**

  Einrichtung einer Verknüpfung zwischen einem oder mehreren Chef-Telefonen sowie einem oder mehreren Sekretärinnen-Telefon(en) mit dem Ziel der vereinfachten Gesprächsübergabe und Rufumschaltung.
- **UCD**

  Einrichtung einer automatischen intelligenter Anrufverteilung auf eine Gruppe mit ausgewählten Teilnehmer.
- **Vermittlungsplatz**

  Einrichtung von Teilnehmern als Vermittlungsplatzrufnummer sowie des Verhaltens bei Besetzt, Falsch-Wahl und Nicht-Melden.
- **Teilnehmer-Profile**

  Teilnehmer einem Profil zuordnen und Profil-Daten importieren/exportieren.

4.1.5.6 Wizards – Sicherheit

Wizards unter **Sicherheit** unterstützen die einfache Konfiguration der Firewall.

Folgende Wizards sind unter **Sicherheit** verfügbar:

- **Firewall**

  Einrichtung von Portfreigabe zur Einschränkung des Internetverkehrs.

4.1.5.7 Wizards – UC Smart (nur mit UC Smart)

Wizards unter **UC Smart** unterstützen die Einrichtung der UC Lösung UC Smart.

Folgende Wizards sind unter **UC Smart** verfügbar:

- **UC Smart**

  Grundeinrichtung und Benutzerkonfiguration für UC Smart.

4.1.5.8 Wizards – UC Suite (nur mit UC Suite)

Wizards unter **UC Suite** unterstützen die Einrichtung der UC Lösung UC Suite.

Folgende Wizards sind unter **UC Suite** verfügbar:

- **Benutzerverzeichnis**

  Konfiguration der Benutzer.
- **Abteilungen**

  Konfiguration von Abteilungen.
- **Gruppen**

  Konfiguration von Voicemail- und Fax-Gruppen.
- **Vorlagen (Templates)**

  Konfiguration von SMS-Templates.
- **Externes Verzeichnis**

  Manuelles Hinzufügen einzelner Kontakte zum externen Verzeichnis.
- **Externer Anbieter**

  Eingabe der Zugangsdaten des Exchange- oder LDAP-Servers.
- **Contact Center**

  Konfiguration des Contact Centers.
- **Zeitpläne**

  Konfiguration der Zeitpläne.
- **Datei-Upload**

  Hochladen von Audiodateien für Ansagen und Wartemusik.
- **Konferenzschaltung**

  Konfiguration von Konferenzschaltungen.
- **Profile**

  Erstellen von Benutzer-Profilen.
- **Faxkopfzeilen**

  Konfiguration von Faxkopfzeilen.

4.1.5.9 Assistenten – Globales Verzeichnis

Die Assistenten unter **Globales Verzeichnis** unterstützen das Importieren und Bearbeiten von Verzeichniskontakten.

Folgende Assistenten sind unter **Globales Verzeichnis** verfügbar:

- **Kontakte importieren**

  Der Assistent führt Sie durch den Import von Kontaktdaten aus CSV in das globale Verzeichnis.
- **Kontakte bearbeiten**

  Sie können manuelle Einträge im globalen Verzeichnis hinzufügen oder bearbeiten.

4.1.5.10 Assistenten - Cloud Services

Die Assistenten unter **Cloud Services** unterstützen die in der Cloud unterstützten Funktionalität.

Die folgenden Assistenten sind unter **Cloud Services**verfügbar:

- **Microsoft Teams Client-Plugin**

  Konfigurieren Sie das myPortal for Teams-Client-Plugin und laden Sie es herunter.
- **Unify Phone Konnektivität**

  Konfiguration der Grundeinstellungen für Unify Phone.
- **Unify Phone-Benutzerinstanz**

  Konfigurieren der Unify Phone-Benutzerinstanz
- **Let's Encrypt-Dienst**

  Konfigurieren Sie den Let's Encrypt-Dienst
- **CloudLink Service**

  Konfigurieren Sie den CloudLink Service
- **CloudLink-Pilotnummern**

  Pilotnummern für CloudLink konfigurieren

4.1.6 Service-Center

Das **Service-Center** des WBM bietet verschiedene Wartungsfunktionen, startet den Software-Update und stellt Dokumentation und Software zur Verfügung.

4.1.6.1 Service Center – Dokumente

Die Option **Dokumente** stellt Dokumentationen, CSV-Vorlagen und Links zu weiterführenden Informationen zur Verfügung. Die Dokumentationen können in allen unterstützten Sprachen als PDF aufgerufen werden.

Je nach Systemkonfiguration sind folgende Inhalte verfügbar:

Inhalt	UC Smart	UC Suite
Administratordokumentation (PDF)	-	x
Benutzerdokumentation (PDF)	-	x
Links (Wiki)	x	x
Templates (CSV-Templates) für den Import von Daten für • Teilnehmer • Kurzwahl zentral KWZ • Externes Verzeichnis	x	x
EULA	x	x

Zugehörige Konzepte

Accounting-Tools auf Seite 1237

4.1.6.2 Service Center – Software

Die Option **Software** stellt die Software für die UC Clients, USB-Treiber und Tools zur Verfügung.

Folgende Inhalte sind verfügbar:

Inhalt	UC Smar	UC Suite
Installationsdateien für die Software der UC Clients	x	x
USB-Treiber	x	x
Tools	x	x
Links für den direkten Zugriff auf die Installationsdateien	-	x

4.1.6.3 Service Center – Inventory > System

System gibt einen Überblick über grundlegende Konfigurationsdaten des Systems.

4.1.6.4 Service Center – Inventory > Rufnummern

Rufnummern stellt eine Liste aller zugeordneten Rufnummern zur Verfügung.

4.1.6.5 Service Center – Inventory > Netzwerkübersicht

Netzwerkübersicht bietet eine Liste mit Informationen über die aktuell im Netzwerk befindlichen Systeme.

4.1.6.6 Service-Center – Software-Update

Software-Update überprüft, ob ein SW-Update auf dem Webserver verfügbar ist und führt die Aktualisierung durch.

4.1.6.7 Service-Center – Email-Weiterleitung

Email-Weiterleitung ermöglicht den Versand von E-Mails mit Systemmeldungen von UC Suite an den Administrator und den Versand von E-Mails mit angehängten Sprach- oder Faxnachrichten an Teilnehmer.

4.1.6.8 Service-Center – Remote-Zugang

Remote-Zugang ermöglicht die Konfiguration des Zugangs für die ortsunabhängige Administration des Systems.

4.1.6.9 Service-Center – Restart / Reload

Restart/Reload ermöglicht einen Neustart des Systems, wahlweise mit Zurücksetzen auf Werkseinstellungen.

4.1.6.10 Service-Center – Diagnose > Status

Status bietet Statusinformationen über Netzwerk, Teilnehmer, Verbindungsaufbau, ITSP und VPN.

Siehe auch Inventory-Management .

4.1.6.11 Service-Center – Diagnose > Event Viewer

Event Viewer protokolliert Systemereignisse.

Siehe auch Traces .

4.1.6.12 Service-Center – Diagnose > Trace

Trace bietet Möglichkeiten zur Fehlerprotokollierung.

Siehe auch Traces .

4.1.6.13 Service-Center – Diagnose > Service-Protokoll

Im Service-Protokoll werden verschiedene Systemdaten in Form von HiPath 3000-Ereignissen protokolliert.

Sie müssen sich im WBM-Ansichtsmodus befinden, um die Datei zu aktualisieren oder herunterzuladen.

4.1.7 Experten-Modus

Der Experten-Modus stellt geschulten Servicetechnikern (Profil **Experten**) Menüs mit Funktionen für die Konfiguration und Wartung des Systems zur Verfügung.

Ausführliche Informationen finden Sie in Kapitel Experten-Modus.

4.1.8 Online-Hilfe

Die integrierte Online-Hilfe beschreibt wichtige Konzepte und Handlungsanweisungen. Zu jeder geöffneten WBM-Seite wird kontextsensitiv das zugehörige Hilfe-Thema aufgerufen.

Navigation

Die Schaltflächen in der Online-Hilfe bieten folgende Funktionen:

- **Inhalt**

  gibt einen Überblick über die Struktur
- **Index**

  bietet direkten Zugang zu einem Thema über Stichworte
- **Suche**

  bietet eine Volltextsuche zum gezielten Auffinden relevanter Themen

4.1.8.1 Wie Sie die Online-Hilfe kontextsensitiv aufrufen

Voraussetzungen

Sie sind am WBM angemeldet.

Prozedur

- Klicken Sie im geöffneten WBM-Fenster entweder auf das Fragezeichensymbol rechts oben oder auf die Hilfe-Schaltfläche links unten.

4.2 Manager E

Manager E ist ein Servicetool mit integrierter Hilfe unter Windows für Tasks, die nicht im WBM durchführbar sind.

Der Manager E kann verwendet werden für die OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 und OpenScape Business X8. Die OpenScape Business S ist nicht mit dem Manager E administrierbar.

Es ist ratsam, Konfigurationsänderungen nur dann über Manager E vorzunehmen, wenn Sie nicht über WBM vorgenommen werden können, wie beispielsweise die Dämpfung, Klingelimpuls, Tonfrequenz usw. Änderungen,

die über Manager E vorgenommen werden, müssen über den Deltamodus abgesendet werden.

Manager E ist für geschultes Servicepersonal bestimmt und beinhaltet folgende Funktionsblöcke:

- Generierung (auch Offline-Generierung)
- Kundendatenabzug und -sicherung
- Serviceaufträge wie z.B. Neustart von Baugruppen
- Rücksetzen von aktivierten Leistungsmerkmalen
- Erstellung und Ausdruck von:
  - Tastenbeschriftungen für optiPoint 500
  - Kundendatenlisten
  - Hauptverteilerbelegungen
- Eigene Nutzer- und Passwortverwaltung für den Service
- Konvertierungsroutine für Kundendatenspeicher

Der Systemzugang über Manager E erfolgt mit einem eigenen Benutzernamen und Passwort. Um kleinere Änderungen schnell durchzuführen steht der Online-Mode zur Verfügung. Die Funktionalität des Online-Mode entspricht der Bedienoberfäche von Assistant T.

Folgende Leistungsmerkmale sind nicht mehr über Manager E administrierbar:

- Lizenzierung
- Netzwerk
  - SNMP-Partner
  - PSTN-Partner
  - Routing
  - Mapping
  - Gatekeeper
  - Durchw. H.323
  - IP-Ports
- Wartung
  - Error History
  - Event-Protokoll
  - Tracereinstellungen
  - Error Reaction Table
  - V.24 Status
  - DMA
- Traces

Arbeitsweise mit dem Kundendatenspeicher (KDS)

Die grundsätzliche Arbeitsweise läuft in folgenden Schritten ab:

- KDS vom System in Manager E laden
- Änderungen in Manager E durchführen
- KDS von Manager E in das System sichern

4.2.1 Wie Sie den KDS in den Manager E laden

Führen Sie die folgenden Schritte durch um anschließend Konfigurationsaufgaben in Manager E durchzuführen.

Schritt für Schritt

1) Starten Sie Manager E am Admin-PC.
2) Geben Sie **Benutzername** für Manager E ein.
3) Geben Sie das **Kennwort** für Manager E ein.
4) Klicken Sie auf **Datei** > **Übertragen**.
5) Klicken Sie auf die Registerkarte **Kommunikation**.
6) Aktivieren Sie im Bereich **Zugang** die entsprechende Option, je nach Verbindungsart des Admin-PC zum System.
7) Aktivieren Sie die Option **KDS lesen/schreiben**.
8) Klicken Sie auf **Anlage -> PC**.
9) Klicken Sie auf **OK**. Der KDS wird vom System zu Manager E übertragen.
10) Klicken Sie nach erfolgreicher Übertragung auf **OK**.
11) Klicken Sie auf **Schließen**.

4.2.2 Wie Sie den KDS in das System zurücksichern

Führen Sie die folgenden Schritte durch um im Manager E durchgeführte Konfigurationen in das System zurück zu sichern.

Schritt für Schritt

1) Klicken Sie auf **Datei** > **Übertragen**.
2) Klicken Sie auf die Registerkarte **Kommunikation**.
3) Aktivieren Sie im Bereich **Zugang** die entsprechende Option, je nach Verbindungsart des Admin-PC zum System.
4) Aktivieren Sie die Option **KDS lesen/schreiben**.
5) Klicken Sie auf **PC -> Anlage**.
6) Klicken Sie auf **OK**. Der KDS wird von Manager E zum Sytem übertragen.
7) Klicken Sie nach erfolgreicher Übertragung auf **OK**.
8) Klicken Sie auf **Schließen**.

5 Ersteinrichtung von OpenScape Business X

Dieses Kapitel beschreibt die Ersteinrichtung von OpenScape Business X1/X3/X5/X8. Das Kommunikationssystem und seine Komponenten werden in eine bestehende Infrastruktur integriert, die aus einem Kunden-LAN und einem TDM-Telefonnetz besteht. Der Internetzugang und die Amtsverbindung werden eingerichtet und die angeschlossenen Sprechstellen konfiguriert.

Die Ersteinrichtung von OpenScape Business X1/X3/X5/X8 (d. h. des Kommunikationssystems) erfolgt mit dem Verwaltungsprogramm OpenScape Business Assistant (webbasierte Verwaltung, auch WBM genannt).

Hier wird die Standard-Ersteinrichtung häufig verwendeter Komponenten beschrieben. Die konkreten Installationsschritte hängen vom Kommunikationssystem und den beteiligten Komponenten (z. B. der UC Booster Card) ab. Während der Ersteinrichtung müssen Sie möglicherweise an einigen Stellen zwischen mehreren Optionen wählen oder sogar einige Konfigurationen vollständig überspringen. Es ist auch möglich, dass die hier beschriebenen Installationsschritte in Ihrem Kommunikationssystem nicht angezeigt werden.

Die detaillierten Konfigurationen von Funktionen, die nicht in der Standard-Ersteinrichtung enthalten sind, werden in den folgenden Kapiteln beschrieben.

Voraussetzung für die Ersteinrichtung ist die Erstellung eines IP-Adress-Schemas und eines Rufnummernplans.

Die wichtigsten Installationsschritte sind die folgenden:

- IP-Adressen und DHCP-Einstellungen
- Länder- und Zeiteinstellungen
- Systemrufnummern und Vernetzung
- ISDN-Konfiguration
- Internet-Zugang
- Internet-Telefonie
- Teilnehmerkonfiguration
- Lizenzierung
- Systemhärtung
- Datensicherung

Richtlinien zur Erweiterung des Subnetzbereichs, um mögliche Fehlkonfigurationen zu vermeiden

Zu den wichtigen Überlegungen, die Sie berücksichtigen sollten, bevor Sie solche Änderungen vornehmen, gehören:

Stellen Sie sicher, dass sich bestimmte Netzwerke nicht mit anderen Systemnetzwerken überschneiden. Insbesondere:

- DSP-Netzwerk
- LAN1 (WAN)-Netzwerk
- LAN2-Netzwerk
- LAN3 (Admin)-Netzwerk

Darüber hinaus müssen Sie sicherstellen, dass keine Konflikte mit der Standard-Gateway-IP-Adresse bestehen. Wenn eine Booster-Karte verwendet wird, muss sich die LAN2-Schnittstelle des Systems im selben Subnetz wie die LAN2-Schnittstelle der Booster-Karte befinden.

5.1 Voraussetzungen für die Erstinstallation

Die Erfüllung der Voraussetzungen für die Erstinstallation gewährleistet den Betrieb des Kommunikationssystems.

Allgemein

Abhängig von der verwendeten Hardware (Baugruppen, Telefone usw.) und der vorhandenen Infrastruktur gelten folgende allgemeine Voraussetzungen:

- Die Infrastruktur (LAN, TDM-Telefonienetz) ist vorhanden und nutzbar.
- Die Hardware ist korrekt montiert und angeschlossen.
- Für die Intergration des Mainboards und der UC Booster Card ins Kunden-LAN wird jeweils eine LAN-Schnittstelle benötigt.
- Das Kommunikationssystem ist noch nicht ans LAN angeschlossen.
- Wird die UC Booster Card verwendet, sollte es vor der Erstinstallation gesteckt werden.
- Ein Internet-Zugang bei einem Internet-Service-Provider ist vorhanden.
- Für die Nutzung eines ISDN-Amtszugangs ist ein ISDN-S_0- oder ein ISDN-Primärmultiplexanschluss nötig.
- Für die Nutzung eines CAS-Amtszugangs ist ein CAS-Amtsanschluss nötig.
- Für die Nutzung eines analogen Amtszugangs ist ein analoger Amtsanschluss nötig.
- Ein IP-Adressen-Schema ist vorhanden und bekannt (siehe IP-Adressen-Schema).
- Ein Rufnummernplan ist vorhanden und bekannt (siehe Rufnummernplan).

Admin-PC

Für den Administrations-PC (Admin-PC), mit dem die Erstinstallation und die spätere Administration des Kommunikationssystems durchgeführt wird, sind folgende Voraussetzungen nötig:

- Netzwerkschnittstelle:

  Der Admin-PC benötigt eine freie LAN-Schnittstelle.
- Betriebssystem:

  Für eine evtl. Konfiguration des Kommunikationssystems mit dem Manager E ist ein Windows-Betriebssystem (ab Windows XP) Voraussetzung.

  Die Konfiguration mit dem WBM ist browserbasiert und somit betriebssystemunabhängig.
- Webbrowser:

  Es werden die nachfolgenden Webbrowser unterstützt:

  – Microsoft Internet Explorer ab Version 10
  – Microsoft Edge
  – Mozilla Firefox ab Version 17.
  – Google Chrome

  Falls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Erstinbetriebnahme begonnen werden kann.

- Java:

  Es muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein. Ist eine ältere Version installiert, muss auf die aktuellste Version aktualisiert werden, bevor mit der Erstinbetriebnahme begonnen werden kann.

5.2 Komponenten

Die Komponenten des Installationsbeispiels sind im Folgenden beschrieben und skizziert.

Das Installationsbeispiel umfasst folgende Komponenten:

- OpenScape Business X

  Das Kommunikationssystem wird über die LAN-Schnittstelle in das vorhandene Kunden-LAN eingebunden
- Admin-PC

  Der Admin-PC wird ebenfalls über eine LAN-Schnittstelle mit dem Kommunikationssystem verbunden.
- IP-Teilnehmer (IP-Clients)

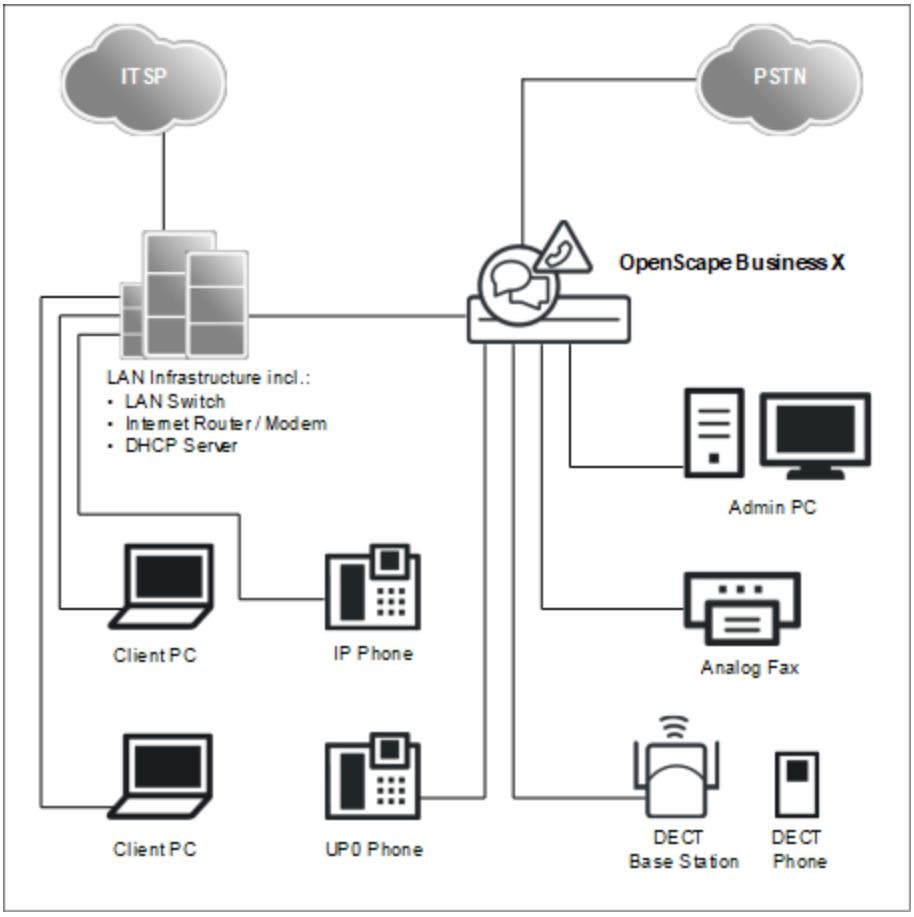
  Die IP-Teilnehmer (IP-Systemtelefone, Client-PCs, WLAN Access Points, ...) sind über einen oder mehrere Switches im LAN integriert.
- UP0-Teilnehmer

  Die UP0-Teilnehmer (z.B. TDM-Systemtelefon OpenStage 60T) sind direkt am Kommunikationssystem angeschlossen.
- Analoge Teilnehmer

  Die analogen Teilnehmer (z.B. analoges FAX) sind direkt am Kommunikationssystem angeschlossen.
- DECT-Teilnehmer

  Die DECT-Teilnehmer sind über eine Basisstation am Kommunikationssystem angemeldet.

Die IP-Clients erhalten ihre IP-Adressen dynamisch von einem internen oder externen DHCP-Server (z.B. Internet-Router).



5.3 Rufnummernplan

Ein Rufnummernplan ist eine Liste aller im Kommunikationssystem verfügbaren Rufnummern. Er beinhaltet u.a. interne Rufnummern, Durchwahlrufnummern und Gruppenrufnummern.

Standard-Rufnummernplan

Die internen Rufnummern sind mit Standardwerten vorbelegt. Diese Werte können bei Bedarf an die eigenen Belange angepasst werden (individueller Rufnummernplan).

Auszug aus dem Standard-Rufnummernplan:

Art der Rufnummern	**X1**	X3/X5/X8
Interne Teilnehmer-Rufnummern	11-30	100-742
Teilnehmer-Durchwahlnummern	11-30	100-742
Leitungsrufnummern	700-703	ab 7801

Art der Rufnummern	**X1**	X3/X5/X8
Richtungskennzahlen (Externkennzahlen): Rtg. 1 (Amt ISDN, analog) Rtg. 8 (UC Suite) Rtg. 12-15 (Amt ITSP) Rtg. 16 (Vernetzung)	0 = Welt / 9 = USA - Nicht vorbelegt Nicht vorbelegt	0 = Welt / 9 = USA 851 855-858 859
Rufnummer für den Remote-Zugang	Nicht vorbelegt	Nicht vorbelegt
Rufnummer für Sprachnachrichten UC Smart UC Suite	351 -	351 Nicht vorbelegt

Individueller Rufnummernplan

Ein individueller Rufnummernplan kann während der Basiskonfiguration über eine XML-Datei importiert werden.

Die XML-Datei enthält mehrere Register. Das Register "Kunde" enthält zusätzlich zu den Namen und den Rufnummern der Teilnehmer weitere Teilnehmerdaten, wie z.B. die Teilnehmer-Typen und die E-Mail-Adressen der Teilnehmer.

Ein Beispiel einer XML-Datei mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**. Die dort abgelegte XML-Datei können Sie auch als Vorlage für Ihre Daten verwenden. Sie kann z.B. mit Microsoft Excel bearbeitet werden.

5.4 IP-Adressen-Schema

Ein IP-Adressen-Schema ist eine Festlegung, wie die IP-Adressen im Kunden-LAN vergeben sind. Es beinhaltet die IP-Adressen von PCs, Servern, Internet-Routern, IP-Telefonen usw.

Für eine bessere Übersicht bei der Zuordnung von IP-Adressen sollte ein IP-Adressen-Schema erstellt werden.

Beispiel eines IP-Adressen-Schemas mit dem IP-Adressband `192.168.1." - x`:

IP-Adressbereich	**Clients**
192.168.1.1 bis **192.168.1.19**	Clients mit fester IP-Adresse:
192.168.1.1	Internet-Router (Gateway)
192.168.1.2	Kommunikationssystem
192.168.1.3	Application Board (optional)
192.168.1.10	E-Mail-Server

IP-Adressbereich	Clients
192.168.1.50 bis **192.168.1.254**	Client-PCs & IP-Telefone, zugleich IP-Adressband des DHCP-Servers, Zuweisung der IP-Adressen an die Clients erfolgt dynamisch

Folgende IP-Adressbereiche sind intern reserviert und dürfen nicht belegt sein:

ausgeschlossene IP-Adressbereiche	Beschreibung
10.0.0.1; 10.0.0.2	Reserviert für Lizenzserver
10.186.237.65; 10.186.237.66	Reserviert für Remote ISDN (überholt)
192.168.3.2	Interne IP-Adresse des Kommunikationssystems
192.168.2.1	IP-Adresse der LAN3-Schnittstelle (Admin-Port)

Diese Liste finden Sie auch im WBM unter **Service-Center** > **Diagnose** > **Status** > **Übersicht IP-Adressen**.

Erweiterung der Netzmaske bei Verwendung des voreingestellten Netzsegments

Sowohl die interne IP-Adresse des Kommunikationssystems als auch die IP-Adresse der LAN3-Schnittstelle (Admin-Port) dürfen nicht im gleichen Netzsegment liegen wie die IP-Adresse der Kommunikationssystems.

Voreingestellte Netzsegment-Konfiguration:

- 192.168.1.2: IP-Adresse des Kommunikationssystems
- 255.255.255.0: Netzmaske
- 192.168.3.2: Interne IP-Adresse des Kommunikationssystems
- 192.168.2.1: IP-Adresse der LAN3-Schnittstelle (Admin-Port)

Wird die Netzmaske bei Verwendung des voreingestellten Netzsegments von 255.255.255.0 auf z.B. 255.255.0.0 erweitert, müssen die o.g. IP-Adressen geändert werden:

Beispiel einer geänderten Konfiguration:

- 192.168.1.2: IP-Adresse des Kommunikationssystems
- 255.255.**0**.0: Netzmaske
- 192.**169**.3.2: Interne IP-Adresse des Kommunikationssystems

  Änderbar über **Experten-Modus** > **Telefonie** > **Payload** > **HW-Module** > **DSP-Einstellungen ändern**
- 192.**170**.2.1: IP-Adresse der LAN3-Schnittstelle (Admin-Port)

  Änderbar über **Experten-Modus** > **Telefonie** > **Netzwerkschnittstellen** > **Mainboard** > **LAN 3 (Admin)**

5.5 Erstinbetriebnahme

Die Erstinbetriebnahme umfasst den Start des Kommunikationssystems, den Anschluss und die Konfiguration des Admin-PCs und das erstmalige Starten des Administrationsprogramms OpenScape Business Assistant (WBM).

Die Erstinbetriebnahme des Kommunikationssystems muss durchgeführt werden, bevor das Kommunikationssystem in das interne LAN integriert wird. Es kann zu Problemen kommen, wenn die vorkonfigurierte IP-Adresse des Kommunikationssystems schon im internen LAN vorhanden ist und/oder bereits ein DHCP-Server genutzt wird. Für diese Fälle muss zuerst die IP-Adresse des Kommunikationssystems umkonfiguriert werden und/oder der DHCP-Server des Kommunikationssystems deaktiviert werden. Erst dann kann das Kommunikationssystems ins interne LAN integriert werden.

Anmerkung: Vor der Erstinbetriebnahme sind die Hinweise zum Datenschutz und zur Datensicherheit zu beachten.

GEFAHR: Das Einschalten von OpenScape Business X8 darf erst erfolgen, wenn die Rückseite aller Systemboxen mit den dafür vorgesehenen Anschluss- und Blind-Panels verschlossen ist.

GEFAHR: Das Einschalten von OpenScape Business X3R/X5R darf nur mit geschlossener Gehäusefront erfolgen. Nicht mit Baugruppen bestückte Steckplätze sind immer mit Leerblenden (C39165-A7027-B115) zu verschließen.

GEFAHR: Das Einschalten von OpenScape Business X1W/X3W/X5W darf nur bei geschlossenem Gehäuse erfolgen.

Anschluss des Admin-PCs

Um das Kommunikationssystem zu konfigurieren, wird der Admin-PC direkt an die LAN-Schnittstelle "LAN" des Kommunikationssystems angeschlossen und so konfiguriert, dass er seine IP-Adresse vom internen DHCP-Server des Kommunikationssystems bezieht. Nach erfolgreicher Installation kann der Admin-PC ohne weitere Konfigurationsänderungen ins interne LAN integriert werden.

5.5.1 Wie Sie das Kommunikationssystem starten

Voraussetzungen

Die Montage der Hardware wurde ordnungsgemäß durchgeführt (siehe *OpenScape Business Installationsanleitung*).

Die Speicherkarte (mit der System-Software) ist gesteckt.

Das Kommunikationssystem ist noch nicht in das Kunden-LAN integriert.

Schritt für Schritt

Verbinden Sie das Kommunikationssystem mit dem Stromnetz.

Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Achten Sie darauf, dass das Kommunikationssystem (und bei OpenScape Business X8 jede Systembox) durch einen separaten Schutzleiter geerdet ist (siehe *OpenScape Business Installationsanleitung*).

Das Kommunikationssystem wird jetzt hochgefahren. Dabei leuchten die LEDs des Systems in unterschiedlichen Farben und Sequenzen (Details siehe *OpenScape Business Installationsanleitung*). Während des Hochfahrens darf das Kommunikationssystem nicht vom Stromnetz getrennt werden.

Nach Abschluss des Hochfahrens blinkt die LED "Run" des Mainboards grün im 1Hz-Takt (0,5s an / 0,5s aus).

5.5.2 Wie Sie den Admin-PC mit dem Kommunikationssystem verbinden

Voraussetzungen

Das Kommunikationssystem ist betriebsbereit.

Schritt für Schritt

1) Starten Sie den Admin-PC.
2) Kontrollieren Sie, ob dem PC eine dynamische IP-Adresse zugewiesen werden kann. Falls nicht, müssen Sie den Admin-PC umkonfigurieren. Dafür benötigen Sie Administratorrechte.

   Anmerkung: Die hier beschriebenen IP-Einstellungen gelten für Windows 7. Ausführliche Informationen zur Einrichtung bei anderen Windows-Betriebssystemen entnehmen Sie bitte der jeweiligen Betriebssystemanleitung.

   a) Wählen Sie **Start** > **Systemsteuerung** und doppelklicken Sie auf **Netzwerk und Internet** und anschließend auf **Netzwerk- und Freigabecenter**.
   b) Klicken Sie bei dem entsprechenden aktiven Netzwerk auf **LAN-Verbindung** und anschließend auf **Eigenschaften**.
   c) Markieren Sie in der Registerkarte **Netzwerk** mit der linken Maustaste den Eintrag **Internetprotokoll Version 4 (TCP/IPv4)** und klicken Sie auf **Eigenschaften**.
   d) Klicken Sie auf die Registerkarte **Allgemein** und kontrollieren Sie, ob das Optionsfeld **IP-Adresse automatisch beziehen** aktiviert ist. Falls nicht, aktivieren Sie es.
   e) Schließen Sie alle geöffneten Fenster mit **OK**.
3) Verbinden Sie über ein LAN-Kabel die soeben konfigurierte LAN-Schnittstelle des Admin-PC mit der LAN-Schnittstelle "LAN" des

Kommunikationssystems. Über diese Schnittstelle wird dem Admin-PC eine dynamische IP-Adresse zugewiesen.

Anmerkung: Sie können den Admin-PC auch an die LAN-Schnittstelle "Admin" anschließen, dann müssen Sie allerdings dem Admin-PC eine feste IP-Adresse aus dem Bereich 192.168.2.xxx (z.B. 192.168.2.40) und die Netzmaske 255.255.255.0 vergeben. Das Kommunikationssystem hat über die LAN-Schnittstelle "Admin" die IP-Adresse 192.168.2.1 - wichtig für WBM-Zugang!

5.5.3 Wie Sie das WBM starten

Voraussetzungen

Das Kommunikationssystem ist betriebsbereit. Die LED "Run" des Mainboards blinkt grün im 1Hz-Takt (0,5s an / 0,5s aus).

Admin-PC und Kommunikationssystem können über LAN miteinander kommunizieren.

Schritt für Schritt

1) Starten Sie auf dem Admin-PC den Webbrowser und rufen Sie die Anmeldeseite von OpenScape Business Assistant (WBM) unter folgender Adresse auf:

`https://192.168.1.2`

Anmerkung: Lässt sich das WBM nicht starten, prüfen Sie die LAN-Verbindung und wiederholen Sie den Aufruf. Lässt es sich noch immer nicht starten, prüfen Sie, ob die IP-Adresse durch Ihre PC-interne Firewall geblockt wird. Genauere Informationen finden Sie in der Dokumentation Ihrer Firewall.

2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).

a) Schließen Sie den Webbrowser.

b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.

c) Erlauben Sie die Benutzerkontensteuerung.

d) Rufen Sie die Anmeldeseite von OpenScape Business Assistant (WBM) unter folgender Adresse auf:

`https://192.168.1.2`

e) Klicken Sie auf **Laden dieser Website fortsetzen**.

f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.

g) Klicken Sie auf **Zertifikate anzeigen**.

h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).

i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.

j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.

k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.

l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.

m) Schließen Sie den Webbrowser.

n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie die Anmeldeseite von OpenScape Business Assistant (WBM) unter folgender Adresse auf:

`https://192.168.1.2`

3) Klicken Sie oben rechts auf das Sprachkürzel und wählen Sie aus dem Menü die Sprache aus, in der die Oberfläche des WBM angezeigt werden soll. Die Anmeldeseite wird in der ausgewählten Sprache angezeigt.

4) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

Anmerkung: Wenn Sie nach Eingabe von `administrator` in das Feld **Passwort** wechseln, wird `@system` automatisch ergänzt.

---

5) Geben Sie im zweiten Feld unter **Login** das Standard-Passwort `administrator` für den Zugang als Administrator ein.

6) Klicken Sie auf **Login**.

7) Folgende Schritte sind nur einmalig beim ersten Anmelden am WBM nötig:

a) Geben Sie im Feld **Passwort** nochmal das Standard-Passwort `administrator` ein.

b) Geben Sie in den Feldern **Neues Passwort** und **Neues Passwort bestätigen** ein neues Passwort ein, um das System gegen Missbrauch zu schützen. Berücksichtigen Sie Groß-/Kleinschreibung und den

Zustand der Tasten `Num` und `CapsLock` (Feststelltaste). Das Passwort erscheint verdeckt durch Sternchen (*).

Anmerkung: Das Passwort muss mindestens 8 Zeichen lang sein und eine Ziffer enthalten. Bitte merken Sie sich Ihr neues Passwort genau.

---

c) Klicken Sie auf **Login**.
d) Wählen Sie das aktuelle Datum aus und tragen Sie die Uhrzeit korrekt ein.
e) Klicken Sie auf **OK & Weiter**. Sie werden automatisch vom WBM abgemeldet.
f) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

Anmerkung: Wenn Sie nach Eingabe von `administrator` in das Feld **Passwort** wechseln, wird `@system` automatisch ergänzt.

---

g) Geben Sie im zweiten Feld unter **Login** Ihr neu definiertes Passwort für den Zugang als Administrator ein.
h) Klicken Sie auf **Login**. Es erscheint die Startseite des WBM.

Nächste Schritte

Erstinstallation starten.

5.6 Integration ins Kunden-LAN

Die Integration ins Kunden-LAN wird mit dem Wizard **Erstinstallation** des WBM durchgeführt. Dabei werden die grundlegenden Einstellungen für die Einbindung des Kommunikationssystems in das bestehende LAN festgelegt.

5.6.1 Wie Sie den Wizard Erstinstallation starten

Voraussetzungen

Das WBM ist gestartet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.

Anmerkung: Wenn bei niedrigen Bildschirmauflösungen der Arbeitsbereich aufgrund der Größe des Browserfensters nicht komplett angezeigt werden kann, so erscheinen horizontale oder vertikale Rollbalken an den Rändern, mit denen der angezeigte Ausschnitt verschoben werden kann.

Nächste Schritte

Führen Sie die Erstinstallation wie nachstehend beschrieben Schritt für Schritt durch. Felder, die hier nicht beschrieben werden, sind passend für den Standardfall vorbelegt und müssen nur geändert werden, wenn sie nicht zu Ihren Netzwerkdaten passen. Die ausführlichen Informationen finden Sie in der Administratordokumentation bei der Beschreibung der einzelnen Wizards.

5.6.2 Systemeinstellungen

Im Fenster **Systemeinstellungen** konfigurieren Sie die Systemeinstellungen des Kommunikationssystems.

Gehen Sie folgendermaßen vor:

1) Display-Logo und Produktbezeichnung festlegen

Sie können einen Display-Text festlegen, das im Display der Systemtelefone angezeigt wird. Zusätzlich können Sie die Produktbezeichnung auswählen.

2) IP-Adressen festlegen (falls nötig)

Dem Kommunikationssystem ist standardmäßig eine IP-Adresse und eine Subnetzmaske zugewiesen. Eventuell müssen Sie IP-Adresse und/oder Subnetzmaske an Ihren eigenen IP-Adressbereich anpassen.

Zusätzlich können Sie die IP-Adresse Ihres Default-Routers angeben, z.B. die IP-Adresse des Internet-Routers.

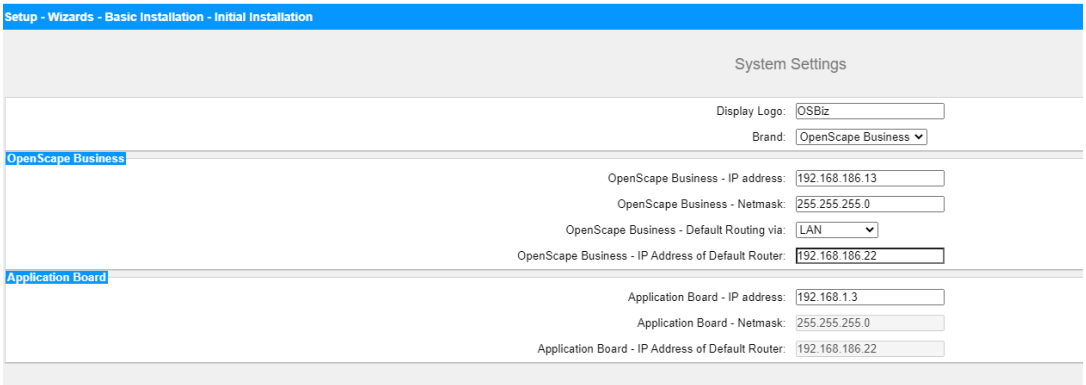
Das Application Board (UC Booster Card) benötigt ebenfalls eine IP-Adresse. Sie können unabhängig davon, ob es montiert ist oder nicht, eine IP-Adresse aus Ihrem IP-Adressbereich vergeben.

Soll die Netzmaske erweitert werden, z.B. von 255.255.**255**.0 auf 255.255.**0**.0, müssen sowohl die interne IP-Adresse des Kommunikationssystems als auch die IP-Adresse der LAN3-Schnittstelle (Admin-Port) geändert werden, da diese nicht im gleichen Netzsegment liegen dürfen wie die IP-Adresse des Kommunikationssystems (siehe auch IP-Adressen-Schema).

5.6.2.1 Wie Sie das Display-Logo und die Produktbezeichnung festlegen

Voraussetzungen

Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) Geben Sie im Feld **Display-Logo** einen Text Ihrer Wahl ein (z.B. OpenScape Biz). Der Text kann bis zu 16 Zeichen lang sein. Vermeiden Sie Umlaute und Sonderzeichen.
2) Wählen Sie in der Aufklappliste **Produkt** die Produktbezeichnung aus.

Nächste Schritte

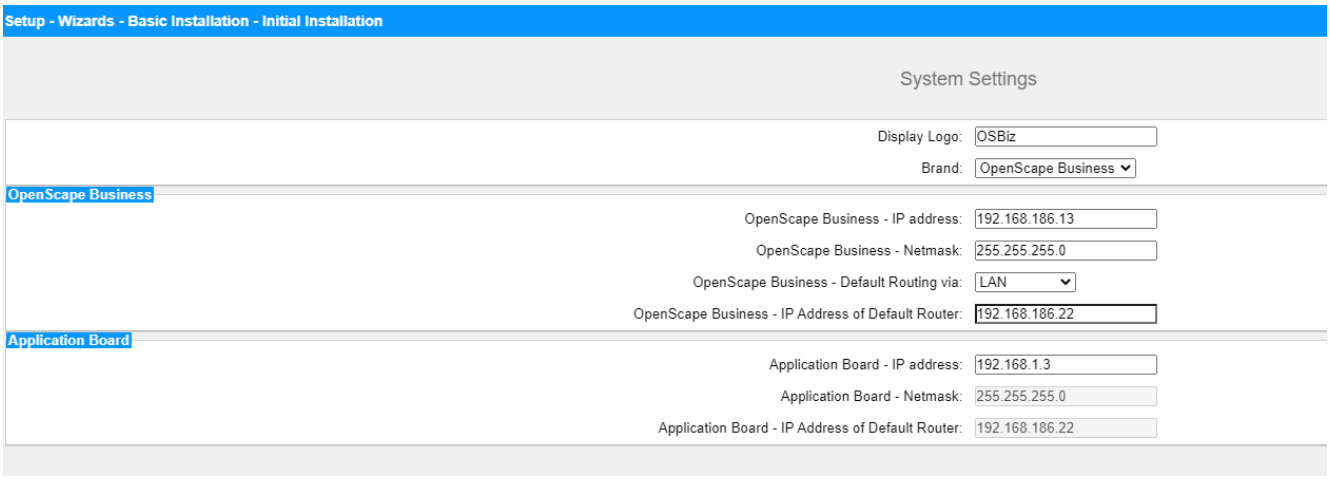
IP-Adressen ändern (falls nötig) oder DHCP konfigurieren.

5.6.2.2 Wie Sie die IP-Adressen festlegen (optional)

Voraussetzungen

Ihnen ist der IP-Adressbereich Ihres internen Netzes bekannt.

Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) IP-Adresse des Kommunikationssystems festlegen:
   a) Geben Sie im Feld **OpenScape Business - IP-Adresse** eine IP-Adresse ein, die im IP-Adressbereich Ihres internen Netzwerkes liegt (z. B. internes Netzwerk: `192.168.1.x`, OpenScape Business: `192.168.1.2`.

      Anmerkung: Die IP-Adresse für OpenScape Business darf keinem weiteren Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt.

   b) Geben Sie im Feld **OpenScape Business - Netzmaske** die Netzmaske Ihres internen Netzwerkes an (z. B. `255.255.255.0`).
2) IP-Adresse des Default-Routers festlegen:
   a) Wählen Sie im Feld **OpenScape Business - Default Routing über** den Eintrag **LAN** aus.
   b) Geben Sie im Feld **OpenScape Business - IP-Adresse des Default-Routers** die IP-Adresse Ihres Default-Routers an (z. B. internes

Netzwerk: `192.168.1.x`, Internet-Router als Default-Router: `192.168.1.1`).

3) IP-Adresse der UC Booster Card festlegen (nötig, wenn gesteckt):
4) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

DHCP konfigurieren.

5.6.2.3 So legen Sie Richtungsnamen fest

Voraussetzungen

Sie befinden sich im Fenster **Systemeinstellungen**.

Das System befindet sich im DTAG-Modus.

Schritt für Schritt

1) Aktivieren Sie das Kontrollkästchen **Automatische RSP.servicelink-Registrierung**:

   Das Feld **Gerätename** kann bearbeitet werden.
2) Legen Sie **Gerätename** fest.

   Wenn Sie die automatische RSP.servicelink-Registrierung auswählen, versucht das System alle 10 Minuten, sich automatisch zu registrieren und mit dem angegebenen Gerätenamen eine Verbindung zum RSP-Server herzustellen.
3) Klicken Sie auf **OK & Weiter.**

Nächste Schritte

DHCP konfigurieren.

5.6.3 DHCP-Einstellungen

Im Fenster **DHCP globale Einstellungen** aktivieren und konfigurieren oder deaktivieren Sie den internen DHCP-Server des Kommunikationssystems.

Ein DHCP-Server weist den IP-Teilnehmern (IP-Systemtelefone, PCs, usw.) automatisch eine IP-Adresse zu und versorgt sie mit netzwerkspezifischen Daten, wie z.B. der IP-Adresse des Standard-Gateways (Internet-Router).

Als DHCP-Server kann ein externer DHCP-Server genutzt werden (z.B. der DHCP-Server des Internet-Routers) oder der interne DHCP-Server, der im Kommunikationssystem integriert ist.

Für die automatische Softwareaktualisierung der IP-Systemtelefone kann der im Kommunikationssystem integrierte DLI oder ein externer DLS-Server verwendet werden (Deployment Service (DLS und DLI)). Dem DHCP-Server muss die IP-Adresse des integrierten DLI oder des externen DLS-Servers bekannt sein.

Sie haben folgende Möglichkeiten:

- Internen DHCP-Server aktivieren und konfigurieren

  Wird der interne DHCP-Server des Kommunikationssystems verwendet, muss ein externer DHCP-Server (z.B. der DHCP-Server des Internet-Routers) deaktiviert werden. Eventuell müssen die Einstellungen des internen DHCP-Servers an das Kunden-LAN angepasst werden. Wird der interne DHCP-Server und der interne DLI genutzt, werden die Systemtelefone automatisch aktualisiert. Wird ein externer DLS-Server genutzt, muss seine IP-Adresse im internen DHCP-Server über den Experten-Modus eingetragen werden (Deployment Service (DLS und DLI)).
- Internen DHCP-Server deaktivieren

  Wird ein externer DHCP-Server genutzt, muss der interne DHCP-Server des Kommunikationssystems deaktiviert werden. Damit die IP-Systemtelefone automatisch mit der aktuellsten Telefonsoftware versorgt werden, müssen im externen DHCP-Server die netzwerkspezifischen Daten eingegeben werden, wie z.B. die IP-Adresse des internen DLI oder des externen DLS-Servers.

Anmerkung: Nicht alle externen DHCP-Server unterstützen die Eingabe von netzwerkspezifischen Daten! In diesem Fall müssen die Daten an allen IP-Systemtelefonen manuell eingeben werden.

5.6.3.1 So deaktivieren Sie den internen DHCP-Server

Voraussetzungen

Im internen Netzwerk ist ein externer DHCP-Server (z.B. der DHCP-Server des Internetrouters) aktiviert.

Sie befinden sich im Fenster **Globale DHCP-Einstellungen**.

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **DHCP-Server aktivieren**.
2) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

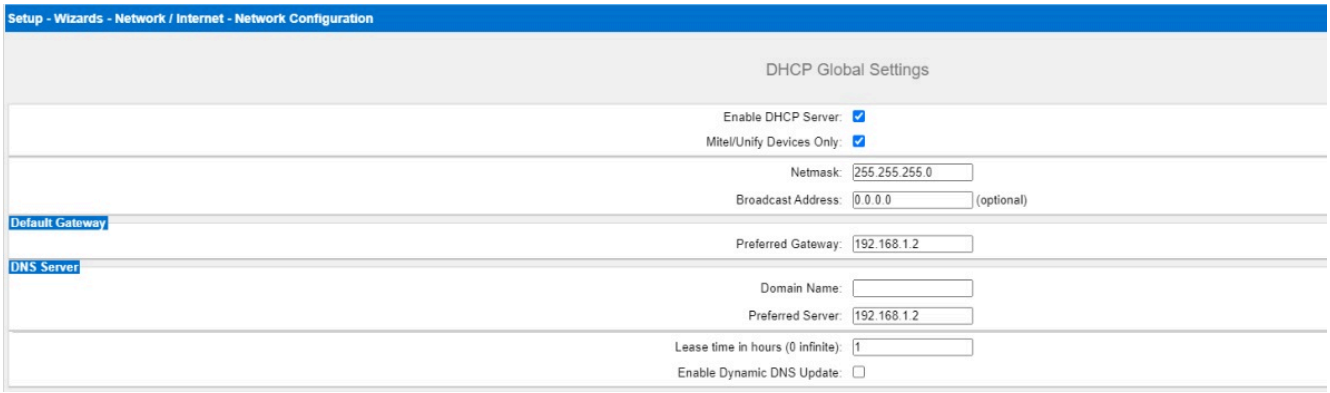
Land- und Zeiteinstellungen konfigurieren.

5.6.3.2 So aktivieren und konfigurieren Sie den internen DHCP-Server

Voraussetzungen

Der externe DHCP-Server (z. B. der DHCP-Server des Internetrouters) wurde im internen Netzwerk deaktiviert.

Sie befinden sich im Fenster **Globale DHCP-Einstellungen**.



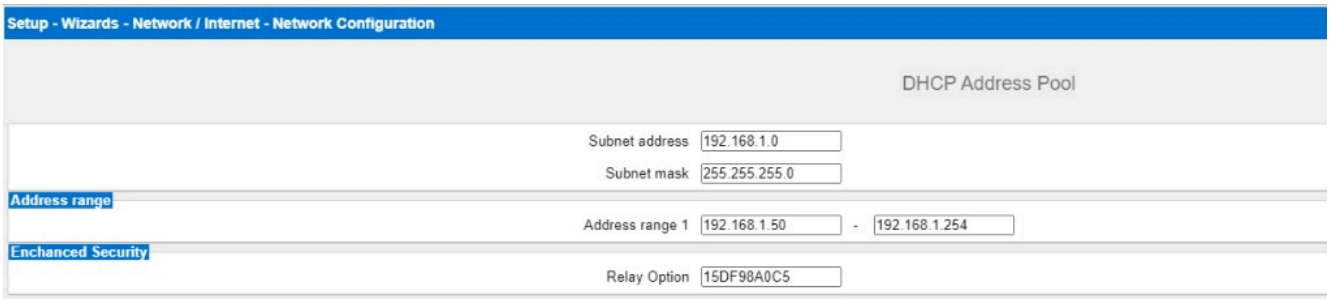
Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **DHCP-Server aktivieren** aktiviert.
2) Aktivieren Sie bei Bedarf das Kontrollkästchen **Nur Mitel-/Unify-Geräte** checkbox.

   Anmerkung: Diese Option ist nur für V3-Hauptplatinen verfügbar.

   ---

3) Gehen Sie zum Feld **Netmaske** und passen Sie die Subnetzmaske an Ihren IP-Adressbereich an (z. B. `255.255.255.0`).
4) Geben Sie im Feld **Bevorzugtes Gateway** die IP-Adresse des Internetrouters ein (z. B. `192.168.1.1`).
5) Geben Sie im Feld **Bevorzugter Server** die IP-Adresse des DNS-Servers ein (z.B. die IP-Adresse des Internet-Routers `192.168.1.1` ein.
6) Klicken Sie auf **OK & Weiter**. Das **DHCP-Adresspool** erscheint.



7) Geben Sie die Werte für **Subnetzadresse**, **Netzmaske** und **Adressbereich 1** an, um den IP-Adressbereich zu definieren, der vom internen DHCP-Server verwaltet werden soll.

   Wenn das interne Netzwerk statische IP-Adressen verwendet (z.B. für einen Drucker-Server), muss der IP-Adressbereich (DHCP-Adresspool)

ausgewählt werden, damit die festen IP-Adressen nicht in diesen Bereich einbezogen werden.

Beispiel:

Internetrouter: `192.168.1.1`

OpenScape Business: `192.168.1.2`

UC Booster Card: `192.168.1.3`

Subnetzadresse: `192.168.1.0`

Subnetzmaske: `255.255.255.0`

Drucker-Server: `192.168.1.10`

DHCP-Adresspool: `192.168.1.50` zu `192.168.1.254`

8) Geben Sie bei Bedarf den Wert des Feldes **Relay-Option** ein.

Anmerkung: Diese Option ist nur für V3-Hauptplatinen verfügbar.

---

9) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

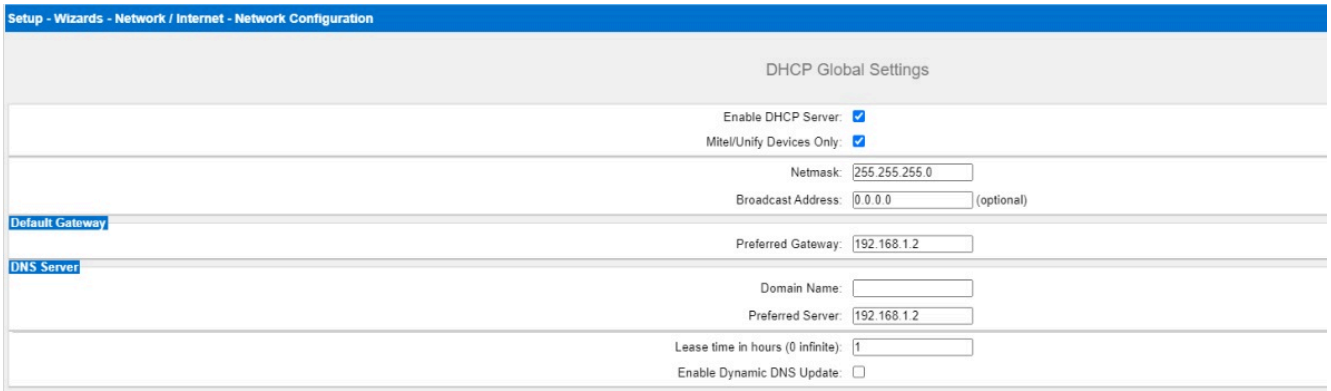
Land- und Zeiteinstellungen konfigurieren.

5.6.3.3 So aktivieren Sie DHCP nur für Mitel/Unify Geräte

Mit dieser Option kann der Systemadministrator den OpenScape Business DHCP-Dienst ausschließlich für Mitel- und Unify-Geräte aktivieren.

Voraussetzungen

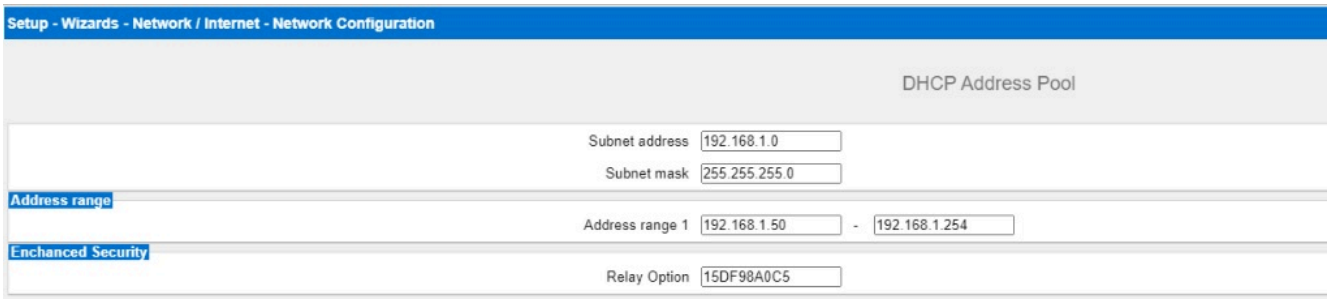
Sie befinden sich im Fenster **Globale DHCP-Einstellungen**.



Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **DHCP-Server aktivieren** aktiviert.
2) Klicken Sie, um das Kontrollkästchen **Nur Mitel-/Unify-Geräte** zu aktivieren. Weitere Informationen zu dieser Option finden Sie unter DHCP-Server > Globale Parameter.

3) Gehen Sie zum Feld **Netmaske** und passen Sie die Subnetzmaske an Ihren IP-Adressbereich an (z. B. `255.255.255.0`).
4) Geben Sie im Feld **Bevorzugtes Gateway** die IP-Adresse des Internetrouters ein (z. B. `192.168.1.1`).
5) Geben Sie im Feld **Bevorzugter Server** die IP-Adresse des DNS-Servers ein (z.B. die IP-Adresse des Internet-Routers `192.168.1.1` ein.
6) Klicken Sie auf **OK & Weiter**. Das **DHCP-Adresspool** erscheint.



7) Geben Sie die Werte für **Subnetzadresse**, **Subnetzmaske** und **Adressbereich 1** an, um den IP-Adressbereich zu definieren, der vom internen DHCP-Server verwaltet werden soll.

   Wenn das interne Netzwerk statische IP-Adressen verwendet (z.B. für einen Drucker-Server), muss der IP-Adressbereich (DHCP-Adresspool) ausgewählt werden, damit die festen IP-Adressen nicht in diesen Bereich einbezogen werden.

   Beispiel:

   Internetrouter: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Subnetzadresse: `192.168.1.0`

   Subnetzmaske: `255.255.255.0`

   Drucker-Server: `192.168.1.10`

   DHCP-Adresspool: `192.168.1.50` zu `192.168.1.254`
8) Geben Sie den Wert des Feldes **Relais-Option** an.
9) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

Land- und Zeiteinstellungen konfigurieren.

5.6.4 Länder- und Zeiteinstellungen

Im Fenster **Basiskonfiguration** wählen Sie Ihr Land und die Sprache für die Event-Logs aus und stellen Datum und Uhrzeit ein. Wenn Sie die integrierte Cordless-Lösung nutzen, geben Sie hier die systemweite DECT-Systemkennung ein.

Gehen Sie folgendermaßen vor:

1) Länderkennzeichen und Sprache für Event-Logs auswählen

   Für eine korrekte Länderinitialisierung müssen Sie das Land auswählen, in dem das Kommunikationssystem betrieben wird. Zusätzlich können Sie die Sprache auswählen, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) abgespeichert werden.

2) DECT-Systemkennung eingeben (nur bei integrierter Cordless-Lösung)

   Wenn Sie die integrierte Cordless-Lösung nutzen, geben Sie hier die systemweite DECT-Systemkennung ein.

3) Datum und Uhrzeit einstellen

   - Wie Sie das Datum und die Uhrzeit manuell einstellen

     Kommunikationssystem und Teilnehmer (IP-Telefone, TDM-Telefone, Client-PCs) sollten über eine einheitliche Zeitbasis (Datum und Uhrzeit) verfügen. Ist für die Zeitsynchronisation kein SNTP-Server bekannt, können Sie Datum und Uhrzeit auch manuell eingeben.

     Anmerkung: Datum und Uhrzeit werden auch aktualisiert, wenn eine Verbindung über eine ISDN-Amtsleitung aufgebaut wird.

   - Wie Sie das Datum und die Uhrzeit von einem SNTP-Server beziehen

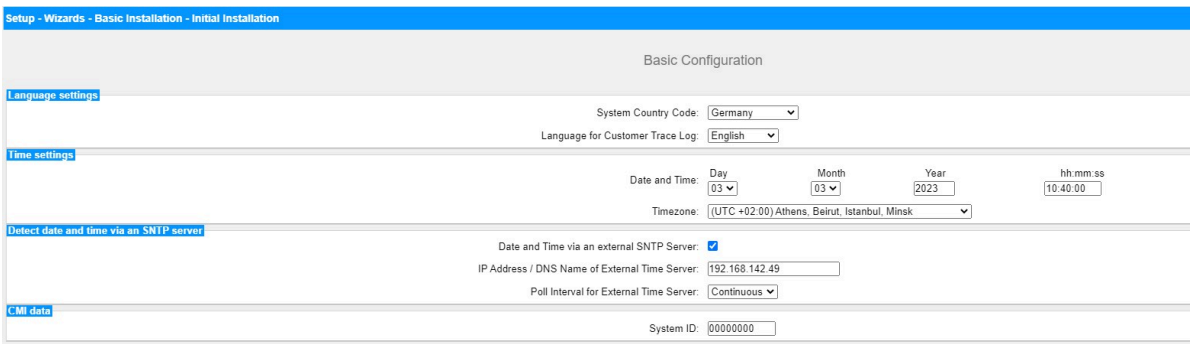
     Kommunikationssystem und IP-Teilnehmer (IP-Telefone, Client-PCs) sollten über eine einheitliche Zeitbasis (Datum und Uhrzeit) verfügen. Diese Zeitbasis kann von einem SNTP-Server zur Verfügung gestellt werden. Der SNTP-Server kann sich im internen Netz oder im Internet befinden.

Die IP-Telefone erhalten Datum & Uhrzeit automatisch vom Kommunikationssystem. Die Client-PCs, auf denen die UC-Clients laufen, müssen so eingestellt sein, dass sie zeitsynchron mit dem Kommunikationssystem sind (siehe Anleitung des Betriebssystems der Client-PCs).

5.6.4.1 Wie Sie das Länderkennzeichen und die Sprache für Event-Logs auswählen

Voraussetzungen

Sie befinden sich im Fenster **Basiskonfiguration**.



Schritt für Schritt

1) Wählen Sie in der Aufklappliste **System-Länderkennzeichen** das Land aus, in dem das Kommunikationssystem betrieben wird.
2) Wählen Sie im Feld **Sprache für Kunden-Eventlog** die Sprache aus, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) ausgegeben werden sollen.

Nächste Schritte

DECT-Systemkennung eingeben (nur bei integrierter Cordless-Lösung)

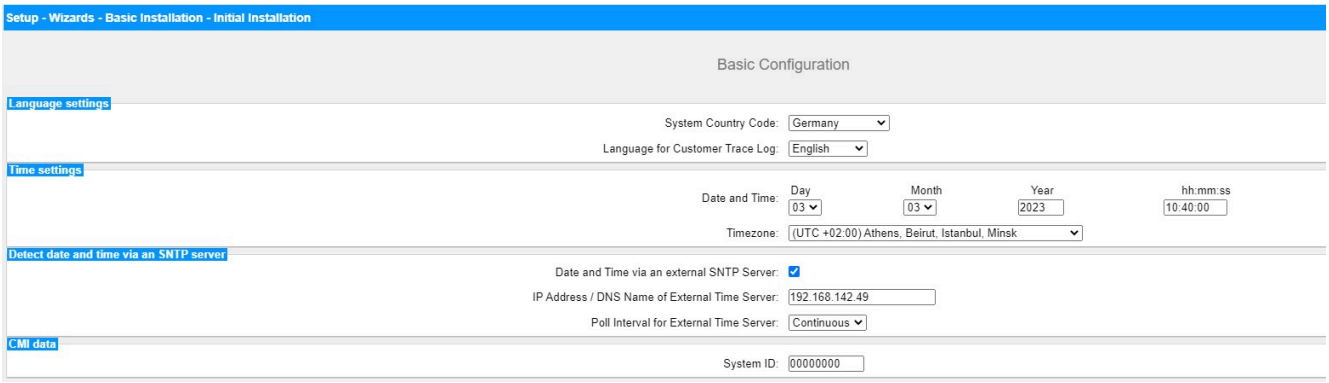
oder

Datum und Uhrzeit manuell einstellen oder Datum und Uhrzeit von einem SNTP-Server beziehen.

5.6.4.2 Wie Sie die DECT-Systemkennung eingeben

Voraussetzungen

Sie befinden sich im Fenster **Basiskonfiguration**.



Schritt für Schritt

Geben Sie im Bereich **CMI-Daten** unter **Systemkennung** die 8-stellige, hexadezimale DECT-Systemkennung ein, die Sie beim Erwerb Ihrer integrierten Cordless-Lösung erhalten haben.

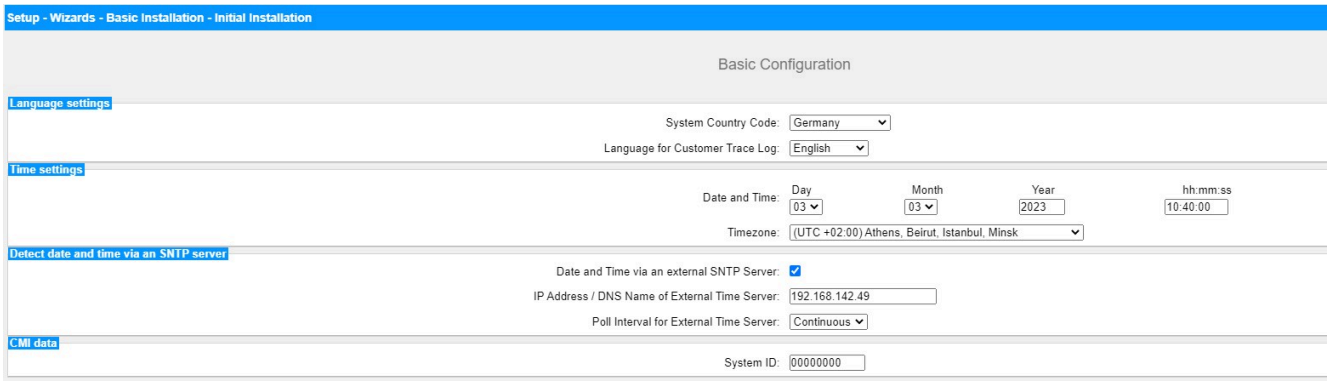
Nächste Schritte

Datum und Uhrzeit manuell einstellen oder Datum und Uhrzeit von einem SNTP-Server beziehen.

5.6.4.3 Wie Sie das Datum und die Uhrzeit manuell einstellen

Voraussetzungen

Sie befinden sich im Fenster **Basiskonfiguration**.



Schritt für Schritt

1) Geben Sie die aktuellen Werte für **Datum und Uhrzeit** ein.
2) Wählen Sie im Feld **Zeitzone** die gewünschte Zeitzone aus.
3) Klicken Sie auf **OK & Weiter**.

Anmerkung: Wird die Zeitzoneneinstellung geändert, dann wird das System im letzten Schritt des Ersteinrichtungsassistenten **neu gestartet**.

Wenn die Zeitzoneneinstellung nicht geändert wird, wird das System nicht neu gestartet.

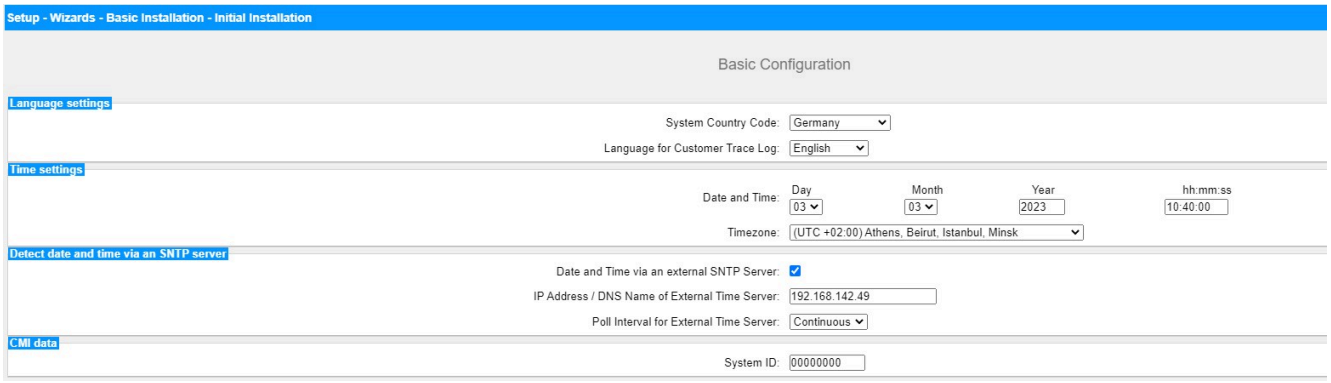
Nächste Schritte

UC-Lösung festlegen.

5.6.4.4 Wie Sie das Datum und die Uhrzeit von einem SNTP-Server beziehen

Voraussetzungen

Sie befinden sich im Fenster **Basiskonfiguration**.



Schritt für Schritt

1) Aktivieren Sie das Kontrollkästchen **Datum und Uhrzeit über externen SNTP Server**.

2) Geben Sie im Feld **IP-Adresse / DNS-Name des externen Zeitservers** die IP-Adresse oder den DNS-Namen des SNTP-Servers ein (z. B. `0.de.pool.ntp.org`).
3) Wählen Sie aus der Aufklappliste **Pollzeit für externen Zeitserver** aus, nach wie vielen Stunden Datum und Uhrzeit vom SNTP-Server synchronisiert werden sollen (empfohlen: `4 h`).
4) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

UC-Lösung festlegen.

5.6.5 UC-Lösung

Im Fenster **Applikationsauswahl ändern** legen Sie fest, welche UC-Lösung Sie nutzen.

Sie haben folgende Möglichkeiten:

- **Paket mit UC Smart**

  Die UC-Lösung UC Smart ist auf dem OpenScape Business X Mainboard intergiert.
- **Paket mit UC Suite**

  Die UC-Lösung UC Suite ist auf der zusätzlich intern steckbaren Baugruppe "UC Booster Card" intergiert.
- **Paket mit UC Suite auf OSBiz UC Booster-Server**

  Die UC-Lösung UC Smart ist auf dem externen Linux-Server "OpenScape Business UC Booster Server" intergiert.
- **Paket mit UC Suite auf OSBiz UC Booster-Server**

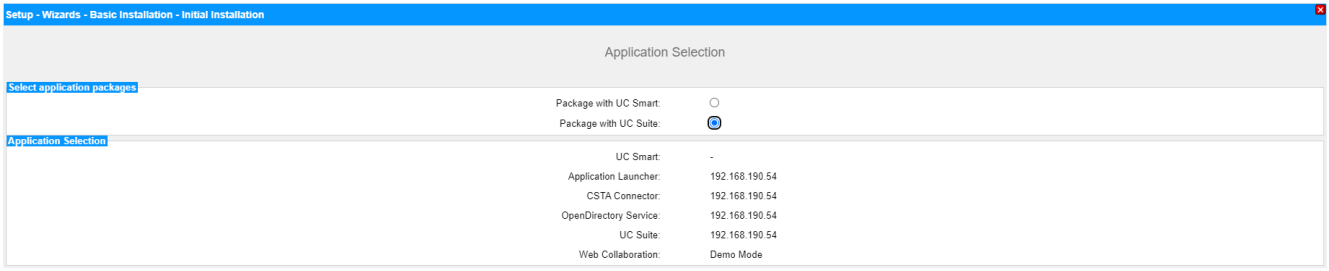
  Die UC-Lösung UC Suite ist auf dem externen Linux-Server "OpenScape Business UC Booster Server" intergiert.

5.6.5.1 Wie Sie die UC-Lösung festlegen

Voraussetzungen

Sie haben Lizenzen erworben entweder für die UC-Lösung UC Smart oder für die UC-Lösung UC Suite.

Sie befinden sich im Fenster **Applikationsauswahl**.



Schritt für Schritt

1) Wenn Sie die UC-Lösung UC Smart ohne UC Booster Server nutzen, klicken Sie auf **Paket mit UC Smart**.
2) Wenn Sie die UC-Lösung UC Smart mit UC Booster Server nutzen, klicken Sie auf **Paket mit UC Smart auf OSBiz UC Booster-Server**. Geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers „OpenScape Business UC Booster Server“ an.
3) Wenn Sie die UC-Lösung UC Suite mit UC Booster Card nutzen, klicken Sie auf **Paket mit UC Suite**.
4) Wenn Sie die UC-Lösung UC Suite mit UC Booster Server nutzen, klicken Sie auf **Paket mit UC Suite auf OSBiz UC Booster-Server**. Geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers „OpenScape Business UC Booster Server“ an.
5) Klicken Sie auf **OK & Weiter**.
6) Der Wizard **Erstinstallation** ist abgeschlossen. Klicken Sie auf **Fertig**.
7) Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

Anmerkung: Wurden IP-Adressen oder Einstellungen des DHCP-Servers geändert, führt das Kommunikationssystem einen Neustart durch. Dies kann einige Minuten dauern.

Nächste Schritte

Kommunikationssystem ans Kunden-LAN anschließen.

5.6.6 Anschluss des Kommunikationssystems ans Kunden-LAN

Nach erfolgreicher Erstinstallation wird das Kommunikationssystem an das bestehende Kunden-LAN angeschlossen.

5.6.6.1 Wie Sie das Kommunikationssystem ans Kunden-LAN anschließen

Voraussetzungen

Das Kommunikationssystem ist betriebsbereit.

Schritt für Schritt

1) Entfernen Sie das LAN-Kabel des Admin-PC aus der mittleren LAN-Schnittstelle "LAN" und integrieren Sie den Admin-PC in das Kunden-LAN, indem Sie ihn z.B. an einen Switch anschließen.
2) Schließen Sie ein LAN-Kabel an die mittlere LAN-Schnittstelle "LAN" des Kommunikationssystems an.
3) Integrieren Sie das Kommunikationssystem über dieses LAN-Kabel in das Kunden-LAN, indem Sie es z.B. an einen Switch anschließen.
4) Ist eine UC Booster Card (Application Board) gesteckt, schließen Sie ein weiteres LAN-Kabel an die LAN-Schnittstelle "LAN2" der UC Booster Card an (rechte/untere der beiden LAN-Schnittstellen) und integrieren Sie die UC

Booster Card über dieses LAN-Kabel in das Kunden-LAN, indem Sie es z.B. an einen Switch anschließen.

Nächste Schritte

Basiskonfiguration starten.

5.7 Basiskonfiguration

Die Basiskonfiguration wird mit dem Wizard **Basisinstallation** des WBM durchgeführt. Dabei werden die wichtigsten Einstellungen für den Betrieb des Kommunikationssystems festgelegt.

Der Wizard Basisinstallation beinhaltet einen Progress Indicator, der den aktuellen Schritt sowie die darauf folgenden Schritte anzeigt.

5.7.1 Wie Sie den Wizard Basisinstallation starten

Voraussetzungen

Der Wizard **Erstinstallation** ist durchlaufen.

Das Kommunikationssystem ist ins Kunden-LAN integriert.

Das Kommunikationssystem ist betriebsbereit. Die LED "Run" des Mainboards blinkt grün im 1Hz-Takt (0,5s an / 0,5s aus).

Schritt für Schritt

1) Rufen Sie auf dem Admin-PC in Ihrem Webbrowser die Anmeldeseite des WBM unter folgender Adresse auf:

   `https://<IP-Adresse von OpenScape Business>`

   Die Standard-IP-Adresse von OpenScape Business ist `192.168.1.2`, also z.B. `https://192.168.1.2`
2) Geben Sie im Feld **Benutzername** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.
3) Geben Sie im Feld **Passwort** das von Ihnen während der Erstinbetriebnahme definierte Passwort ein.
4) Klicken Sie auf **Anmelden**.
5) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
6) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

Nächste Schritte

Führen Sie die Basisinstallation wie nachstehend beschrieben Schritt für Schritt durch. Felder, die hier nicht beschrieben werden, sind passend für den Standardfall vorbelegt und müssen nur geändert werden, wenn sie nicht zu Ihren Netzwerkdaten passen. Die ausführlichen Informationen finden Sie in der Administratordokumentation bei der Beschreibung der einzelnen Wizards.

5.7.2 Systemrufnummern und Vernetzung

Im Fenster **Übersicht** geben Sie die Systemrufnummern ein (Anlagenrufnummer, Länder- und Ortsvorwahl, Internationales Präfix) und legen fest, ob OpenScape Business mit anderen OpenScape Business-Systemen vernetzt werden soll.

Gehen Sie folgendermaßen vor:

1) Systemrufnummern eingeben

- Systemrufnummern für Anlagenanschluss eingeben

  Hier geben Sie die Anlagenrufnummer für Ihren Anlagenanschluss ein sowie die Länder- und Ortsvorwahl.

  Die Eingabe der Ländervorwahl ist für Internet-Telefonie und Konferenz-Server-Funktionalitäten zwingend erforderlich.

  Das internationale Präfix ist abhängig von der zuvor gewählten Länderkennzahl vorbelegt.
- Systemrufnummern für Mehrgeräteanschluss eingeben

  Hier geben Sie Länder- und Ortsvorwahl für Ihren Mehrgeräteanschluss ein.

  Die Eingabe der Ländervorwahl ist für Internet-Telefonie und für MeetMee-Konferenzen zwingend erforderlich.

  Das internationale Präfix ist abhängig von der zuvor gewählten Länderkennzahl vorbelegt.

2) Vernetzung aktivieren oder deaktivieren

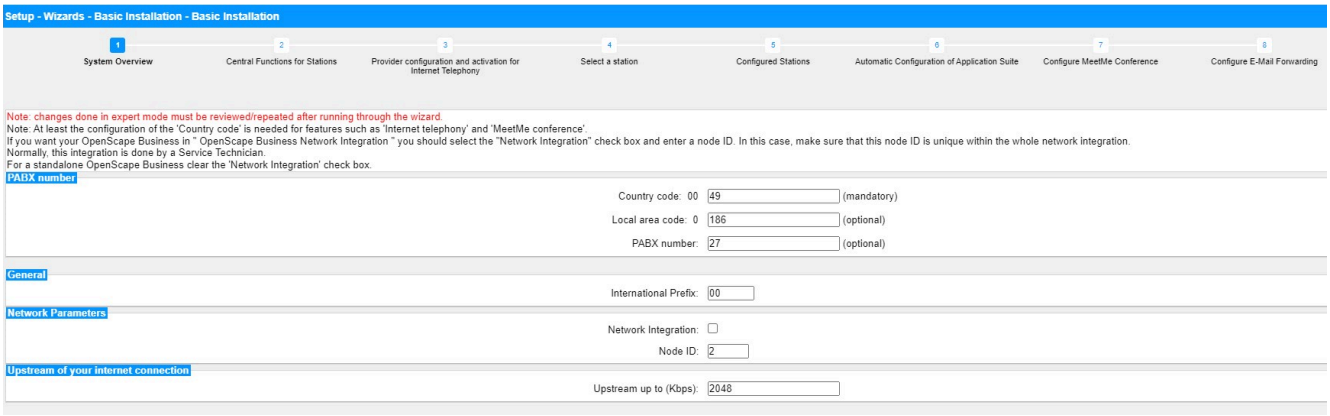
Soll OpenScape Business mit anderen OpenScape Business vernetzt werden, muss die Vernetzung aktiviert und OpenScape Business eine Knoten-ID zugewiesen werden. Jede OpenScape Business muss im Netzverbund eine eindeutige Knoten-ID besitzen.

5.7.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben

Voraussetzungen

Sie haben einen Anlagenanschluss.

Sie befinden sich im Fenster **Systemüberblick** des Assistenten **Basisinstallation**.



Schritt für Schritt

1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.
2) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. `89` für München.
3) Geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z. B. `7007` (Ihre Anschlussnummer).
4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

   Bei Telefonaten ins Ausland werden der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. bei einem Telefonat von Deutschland nach USA die "00-1-..." und bei einem Telefonat von USA nach Deutschland die "011-49-...".

Nächste Schritte

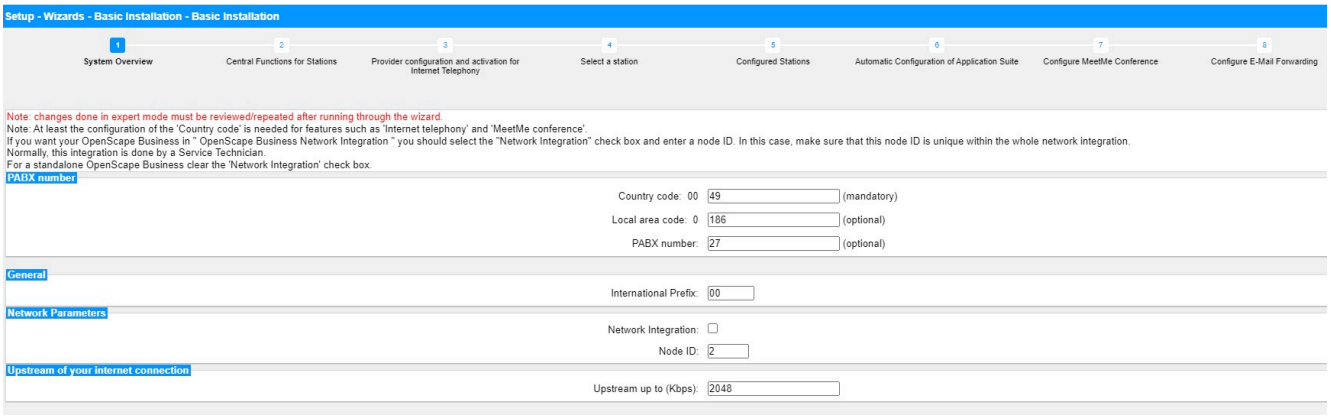
Vernetzung aktivieren oder deaktivieren

5.7.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben

Voraussetzungen

Sie haben einen Mehrgeräteanschluss.

Sie befinden sich im Fenster **Systemüberblick** des Assistenten **Basisinstallation**.



Schritt für Schritt

1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.
2) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. `89` für München.
3) Lassen Sie das Feld **Anlagenrufnummer** leer.
4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

   Bei Telefonaten ins Ausland werden der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. bei einem Telefonat von Deutschland nach USA die "00-1-..." und bei einem Telefonat von USA nach Deutschland die "011-49-...".

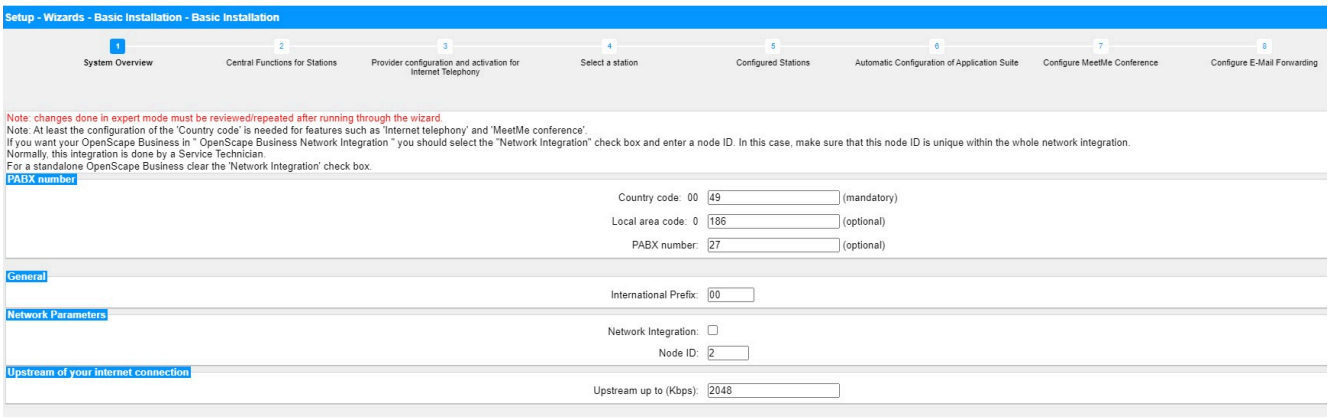
Nächste Schritte

Vernetzung aktivieren oder deaktivieren

5.7.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren

Voraussetzungen

Sie befinden sich im Fenster **Systemüberblick** des Assistenten **Basisinstallation**.



Schritt für Schritt

1) Wenn das Kommunikationssystem mit anderen Kommunikationssystemen vernetzt werden soll:
   a) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
   b) Vergeben Sie im Feld **Knoten-ID** für das Kommunikationssystem eine im Netzverbund eindeutige Knoten-ID (Ziffern von `1` bis `100` möglich).
2) Wenn das Kommunikationssystem nicht mit anderen Kommunikationssystemen vernetzt werden soll, lassen Sie das Kontrollkästchen **Netzwerk-Integration** deaktiviert.

Nächste Schritte

Konfigurieren Sie den Upstream Ihrer Internetverbindung.

5.7.3 Teilnehmerdaten

Im Fenster **Zentrale Teilnehmer-Funktionen** können Sie bei Bedarf anstelle des vordefinierten Standardrufnummernplans Ihren individuellen Rufnummernplan konfigurieren und weitere Teilnehmerdaten importieren. Im Netzverbund muss der Standard-Rufnummernplan an den Rufnummernplan des Netzverbunds angepasst werden.

Der Standardrufnummernplan enthält vordefinierte Rufnummern für verschiedene Teilnehmertypen (IP-Telefone, analoge Telefone, ...) und für spezielle Funktionen (Internet-Telefonie, Sprachbox, AutoAttendant, ...).

Die Teilnehmerdaten enthalten u.a. die internen Rufnummern, die Durchwahlnummern und die Namen der Teilnehmer. Über eine XML-Datei im UTF-8-Format können diese Daten und weitere Teilnehmerdaten während der Basiskonfiguration in das Kommunikationssystem importiert werden.

Anmerkung:

Eine XML-Vorlage mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**. In diese Vorlage können Sie z.B. mit Microsoft Excel Ihre Daten eintragen.

Sie haben folgende Möglichkeiten:

- **Teilnehmerdaten ohne Netzverbund konfigurieren**

  Gehen Sie folgendermaßen vor:

  1) Teilnehmerdaten anzeigen

  Sie können sich alle vorkonfigurierten Rufnummern und Teilnehmerdaten anzeigen lassen.

  2) Alle Rufnummern löschen (optional)

  Verwenden Sie einen individuellen Rufnummernplan, müssen Sie alle vorkonfigurierten Rufnummern löschen.

  3) Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen (optional)

  Verwenden Sie einen individuellen Rufnummernplan, können Sie die vorkonfigurierten Rufnummern an den eigenen Rufnummernplan anpassen.

  Anmerkung:

  Geht der Benutzer die Option **Vorkonfigurierte Rufnummern ändern** durch, muss eine bereits in UC Suite vorhandene, benutzerdefinierte Konfiguration geändert oder wiederholt werden (z.B. Pilot-Warteschlangen)

  ---

  4) Teilnehmerdaten über XML-Datei importieren (optional)

  Ihre individuellen Rufnummern inkl. zusätzlicher Teilnehmerdaten können Sie bequem über eine XML-Datei während der Basiskonfiguration importieren.

- **Teilnehmerdaten mit Netzverbund konfigurieren**

  Gehen Sie folgendermaßen vor:

  1) Alle Rufnummern löschen

  Falls im Netzverbund die UC Suite zum Einsatz kommt, ist ein geschlossener Rufnummernplan erforderlich, d.h. alle Rufnummern im Netzverbund müssen eindeutig sein. Daher müssen die vorkonfigurierten Rufnummern gelöscht und an den Netzverbund angepasste Rufnummern verwendet werden.

  2) Teilnehmerdaten über XML-Datei importieren

  Die an den Netzverbund angepassten Rufnummern sind inkl. zusätzlicher Teilnehmerdaten bequem über eine XML-Datei während der Basiskonfiguration zu importieren. Diese Datei kann alle Teilnehmer des Netzverbundes enthalten. Beim Import werden nur die Rufnummern und Teilnehmerdaten übernommen, die der zuvor angegebenen Knoten-ID des Kommunikationssystems zugeordnet sind.

Zugehörige Tasks

Anzeigen von Massendaten auf Seite 164
Wie Sie die LCR-Einträge zurücksetzen auf Seite 1430

Zugehörige Verweise

LCR > LCR-Flags auf Seite 1625

5.7.3.1 Wie Sie die Teilnehmerdaten anzeigen

Voraussetzungen

Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen**.
2) Klicken Sie auf **Funktion ausführen**. Es wird eine Teilnehmerliste mit den vorkonfigurierten Rufnummern (Standardrufnummernplan) angezeigt.
3) Klicken Sie auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
4) Wenn Sie keine Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

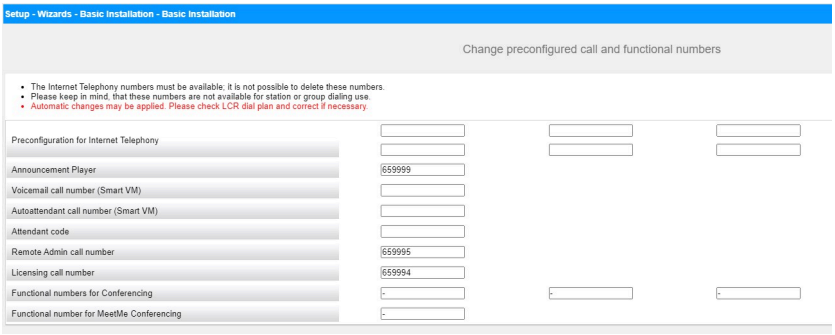
5.7.3.2 Wie Sie alle Rufnummern löschen

Voraussetzungen

Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Alle Rufnummern löschen**.
2) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen**.
3) Klicken Sie auf **Funktion ausführen**. Alle vorbelegten Rufnummern, außer **Wiedergabegerät für Ansagen, Remote-Admin Rufnummer** und **Licensing Rufnummer** werden gelöscht. Anschließend erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



4) Passen Sie die Kennzahlen und speziellen Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
5) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

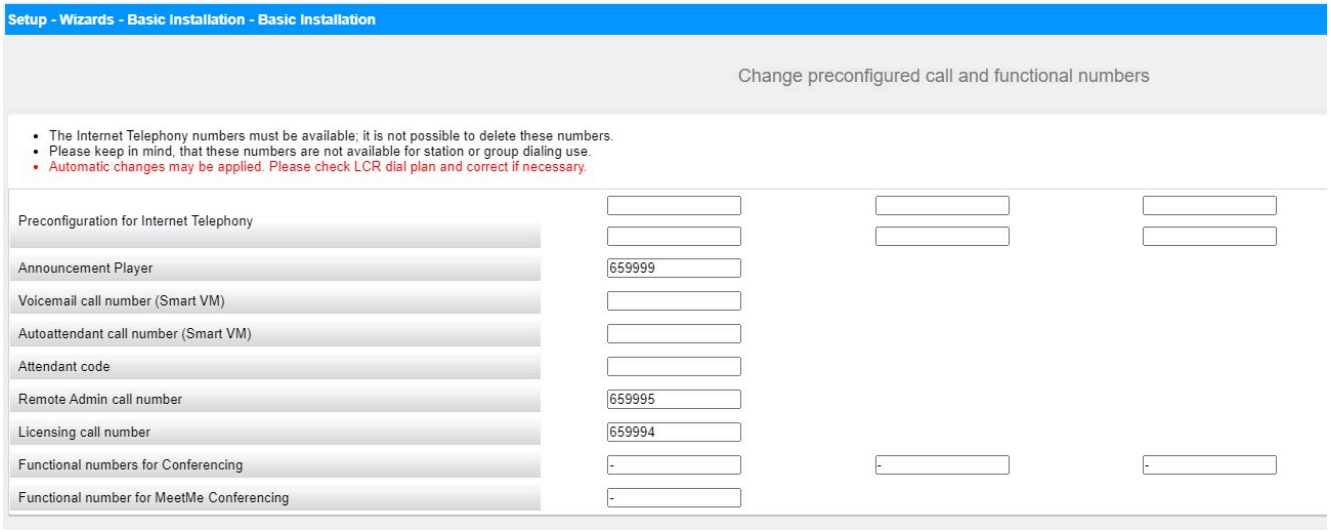
5.7.3.3 Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen

Voraussetzungen

Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Vorkonfigurierte Rufnummern ändern**.
2) Klicken Sie auf **Funktion ausführen**. Es erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



3) Passen Sie die vorkonfigurierten Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
4) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

5.7.3.4 Teilnehmerdaten über eine XML-Datei importieren

Voraussetzungen

Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.

Eine XML-Datei im UTF-8-Format mit den eingetragenen Daten liegt vor. Eine XML-Vorlage finden Sie unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **CSV/XML-Datei mit Teilnehmerdaten importieren**.
2) Klicken Sie auf **Funktion ausführen**.
3) Wählen Sie mit **Durchsuchen** die erstellte XML-Datei aus und klicken Sie auf **Öffnen**.
4) Klicken Sie anschließend auf **OK**. Die Teilnehmerdaten werden importiert.
5) Klicken Sie auf **OK & Weiter**.

5.7.3.5 Anzeigen von Massendaten

Voraussetzungen

- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.
- Sie haben auch Zugriff auf den **Massendaten**-Assistent über **Einrichtung** > **Assistenten**.

Schritt für Schritt

1) Aktivieren Sie die Schaltfläche **Massendaten-Assistent**.

2) Klicken Sie auf **Funktion ausführen**.

3) Im Fenster **Massendaten-Assistent** können Sie die Einträge durch Klicken auf **Validieren** validieren. Es gibt zwei Arten der Validierung: den Front-End-Konsistenz Check und den Back-End-Konsistenz Check.
Ein grünes Validierungsfeld zeigt nur die Aktionen an, die kürzlich validiert wurden. Die Validierung der Daten wird nicht gespeichert. Wenn die Werte geändert werden, muss der Benutzer die Daten erneut validieren.

4) Während des Backend-Konsistenz-Checks und nach erfolgreicher Validierung der Daten ist keine Bearbeitung im Fenster **Massendaten-Assistent** möglich. Nach der erfolgreichen Validierung ist **OK&Weiter** im Bearbeitungsbeschränkungsmodus verfügbar. Wenn der Benutzer auf **Zurück** klickt, wird der Bearbeitungsmodus verfügbar, während **OK&Weiter** ausgeblendet wird. Schlägt die Validierung fehl, bleibt der Bearbeitungsmodus aktiv und **OK&Weiter** bleibt ausgeblendet.

> **Anmerkung:** Der Benutzer kann auf **Zurück** klicken, um die Daten erneut zu bearbeiten, und das Fenster kehrt wieder in den Bearbeitungsmodus zurück. Der Bearbeitungsbeschränkungsmodus stellt sicher, dass der Benutzer nicht auf „OK&Weiter“ klicken und Änderungen übermitteln kann, die nicht validiert sind.

5) Klicken Sie nach der erfolgreichen Konfiguration von **Massendaten-Assistent** auf **Fertigstellen**. Auf der Seite „Fertigstellen“ wird eine Zusammenfassung mit allen Änderungen angezeigt.

Felder, die nicht bearbeitet werden können, sind bereits mit den relevanten Werten aus der Datenbank versehen. Als Folge davon wirkt sich die Funktion „Kopieren/Einfügen“ nicht auf die Daten aus.

Das Feld „Typ“ ist ein auswählbares Dropdown-Menü mit Bearbeitungsfunktion. Die einzigen zulässigen Optionen sind „No Port“, „System Client“, „SIP Client“, „Deskshare User“ und unter Umständen ein vordefinierter Wert, der auf der zugehörigen Baugruppe basiert. Wenn der Benutzer versucht, etwas anderes einzugeben, wird seine Eingabe verworfen, und das Dropdown-Menü wird nicht ausgeblendet, um eine ordnungsgemäße Eingabe zu gewährleisten.

Eine andere Einschränkung besteht darin, dass einige Ports nicht änderbar sind (z. B. ist für Ports, die zu einer analogen Karte gehören, der Typ nicht änderbar und „Analoger Teilnehmer“ bleiben). Es gelten alle Einschränkungen, wenn der Benutzer versucht, Text in die Spalte „Typ“ zu kopieren. Wenn der Benutzer versucht, irrelevante Daten einzufügen, ohne

die obigen Regeln zu verletzen, kann „Kopieren und Einfügen“ überhaupt nicht ausgeführt werden.

„Kopieren und Einfügen“ kann sowohl auf die gesamte Tabelle als auch auf bestimmte Teile angewendet werden.

Anmerkung: Wenn Sie zwei aufeinanderfolgende Zellen mit einem numerischen Wert auswählen und die Felder nach unten ziehen, werden die folgenden Spalten nicht mit aufsteigenden Zahlen versehen, sondern mit einer Kopie der Werte aus den ausgewählten Zellen.

Zugehörige Konzepte

Teilnehmerdaten auf Seite 160

5.7.4 ISDN-Konfiguration

Im Fenster **ISDN-Konfiguration** legen Sie fest, ob ISDN-Teilnehmer angeschlossen werden sollen und ob der Amtsanschluss über ISDN erfolgen soll. Der ISDN-Amtsanschluss kann als ISDN-Anlagenanschluss und/oder ISDN-Mehrgeräteanschluss eingerichtet werden. Je nach Kommunikationssystem und evtl. verwendeter Baugruppe stehen dafür unterschiedlich viele S_0-Schnittstellen zur Verfügung.

Sie haben folgende Möglichkeiten:

- ISDN-Konfiguration aktivieren:

  1) ISDN-Anlagenanschluss konfigurieren

  Sie können einen ISDN-Amtsanschluss als Anlagenanschluss mit Durchwahlnummern einrichten.

  2) ISDN-Mehrgeräteanschluss konfigurieren

  Sie können einen ISDN-Amtsanschluss als Mehrgeräteanschluss mit MSN einrichten.

  3) Anschluss von ISDN-Teilnehmern konfigurieren (optional)

  Eine oder mehrere S_0-Schnittstellen können als interne S_0-Anschlüsse konfiguriert werden, um ISDN-Teilnehmer (ISDN-Telefon oder ISDN-Fax) daran anzuschließen. Für jeden ISDN-Teilnehmer benötigen Sie eine Teilnehmer-Lizenz.
- ISDN-Konfiguration deaktivieren

  Wenn Sie keinen ISDN-Amtsanschluss haben, müssen Sie die ISDN-Konfiguration deaktivieren. Alle S_0-Schnittstellen werden automatisch als interne S_0-Anschlüsse konfiguriert.

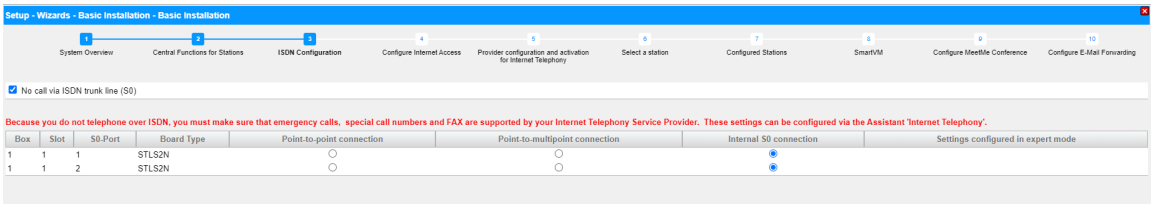
Weitere Möglichkeiten für einen Amtsanschluss

Anstelle des ISDN-Amtsanschlusses können Sie auch einen analogen Amtsanschluss oder einen Amtsanschluss über einen Internet-Telefonie-Service-Provider (ITSP, SIP-Provider) einrichten. Die Konfiguration des analogen Amtsanschlusses ist erst nach Abschluss der Basisinstallation möglich.

5.7.4.1 Wie Sie den Anschluss von ISDN-Teilnehmern konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **ISDN Konfiguration** des Assistenten **Basisinstallation**.



Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)** deaktiviert.
2) Aktivieren Sie bei der gewünschten S_0-Schnittstelle das Optionsfeld **interner S0-Anschluss**.

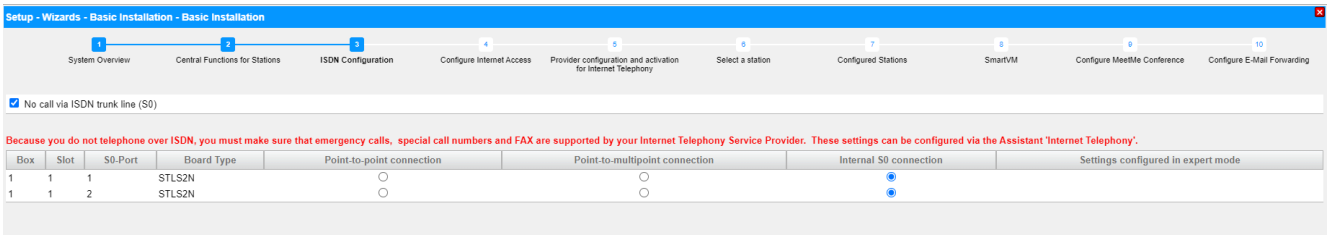
Nächste Schritte

ISDN-Anlagenanschluss konfigurieren und/oder ISDN-Mehrgeräteanschluss konfigurieren.

5.7.4.2 Wie Sie den ISDN-Anlagenanschluss konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **ISDN Konfiguration** des Assistenten **Basisinstallation**.



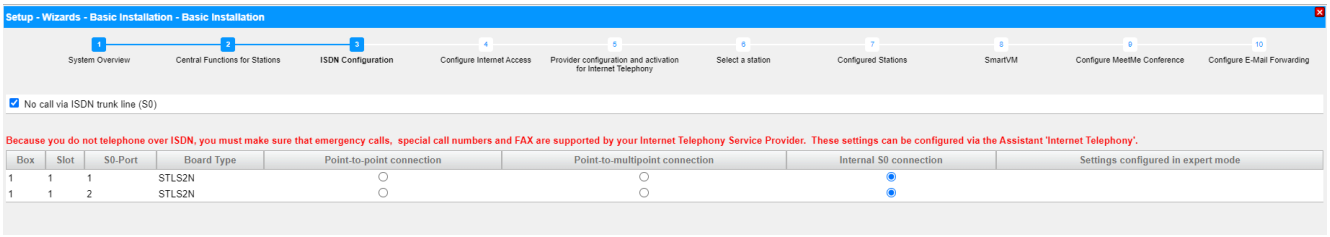
Schritt für Schritt

1) Um den ISDN-Amtsanschluss einzurichten, lassen Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)** deaktiviert.
2) Aktivieren Sie bei dem gewünschten S_0-Anschluss das Optionsfeld **Anlagenanschluss**.
3) Klicken Sie auf **OK & Weiter**.

5.7.4.3 Wie Sie den ISDN-Mehrgeräteanschluss konfigurieren

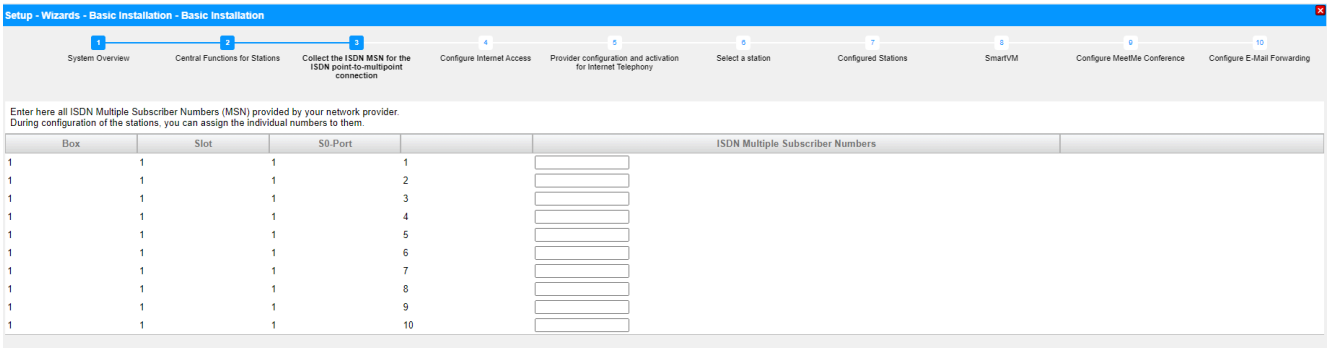
Voraussetzungen

Sie befinden sich im Fenster **ISDN Konfiguration** des Assistenten **Basisinstallation**.



Schritt für Schritt

1) Um den ISDN-Amtsanschluss einzurichten, lassen Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)** deaktiviert.
2) Aktivieren Sie bei dem gewünschten S**0**-Anschluss das Optionsfeld **Mehrgeräteanschluss**.
3) Klicken Sie auf **OK & Weiter**.



4) Geben Sie in der Spalte **ISDN-Mehrfachrufnummern** alle Rufnummern (MSN) ein, die Ihnen Ihr Netzanbieter bereitgestellt hat. Pro S_0-Anschluss können Sie bis zu 10 MSN eingeben. Die Anzahl der S_0-Anschlüsse ist abhängig vom Kommunikationssystem und von der evtl. verwendeten Baugruppe.
5) Klicken Sie auf **OK & Weiter**.

5.7.4.4 Wie Sie die ISDN-Konfiguration deaktivieren

Voraussetzungen

Sie befinden sich im Fenster **ISDN Konfiguration** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Aktivieren Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)**.

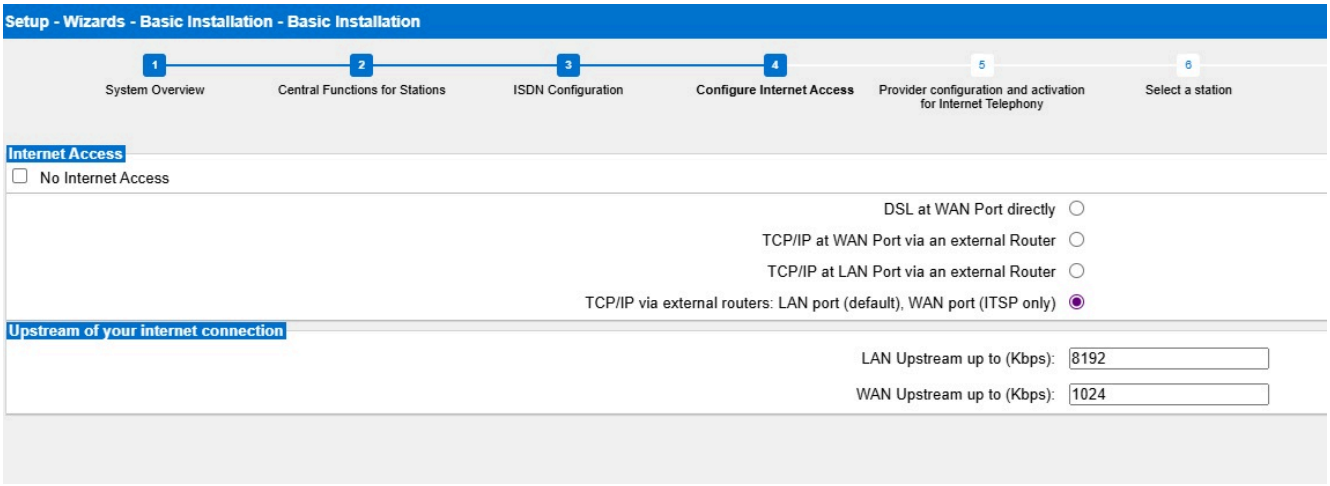
Anmerkung: Gespräche können auch über einen Internet-Telefonie-Service-Provider geführt werden, siehe Internet-Telefonie.

---

2) Klicken Sie auf **OK & Weiter**.

5.7.5 Internetzugang

Das Fenster **Internetzugang konfigurieren** kann zum Konfigurieren des Internetzugriffs verwendet werden.



Die Konfiguration des Internetzugangs im WBM hängt davon ab, ob die Internetverbindung bereits in einem externen Router eingerichtet wurde oder ob sie über ein Internetmodem erfolgt und somit im WBM eingerichtet werden muss.

Es kann nur eine der hier aufgeführten Optionen ausgewählt werden.

- Internetzugang über ein Internetmodem (**DSL direkt am WAN-Port**)

  Sie möchten das Kommunikationssystem direkt an einem Internetmodem betreiben (DSL, Kabel, UMTS,...). OpenScape Business hat den Internet Router integriert. Geben Sie die Zugangsdaten des Internet Service

Providers (ISP) direkt in das Kommunikationssystem ein und verwenden Sie den WAN-Port des Kommunikationssystems.

Sie haben folgende Möglichkeiten:

– **Internetzugang über einen vorkonfigurierten ISP**
– **Internet-Zugang über Standard-ISP PPPoE**
– **Internetzugang über den Standard ISP PPTP**

Wenn Ihr ISP nicht unter den vorkonfigurierten ISPs aufgeführt ist, verwenden Sie den Standard-ISP PPPoE oder PPTP.

- Internetzugang über einen externen Internetrouter

  Sie möchten das Kommunikationssystem an einem externen Internetrouter betreiben. Der Internet Service Provider ist bereits im Internetrouter konfiguriert.

  Sie haben folgende Möglichkeiten:

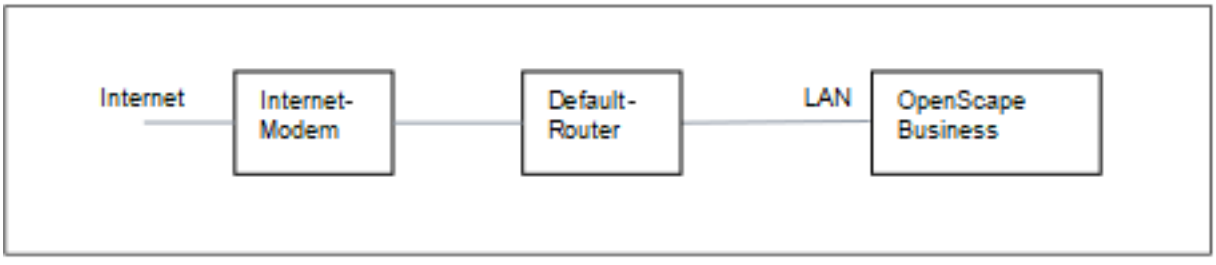
  – **Internetzugang über einen externen Internetrouter am WAN-Port**

    (**TCP/IP am WAN Port über einen externen Router**)

Dazu verwenden Sie den WAN-Port des Kommunikationssystems. OpenScape Business kennt entweder den Internet-Router oder arbeitet als DHCP-Client. Diese Option kann verwendet werden, wenn sich der Internet-Router in einem anderen Netzwerksegment befindet und über einen eigenen DHCP-Server verfügt.

  – **Internetzugang über einen externen Internetrouter am LAN-Port**

    (**TCP/IP am LAN Port über einen externen Router**)

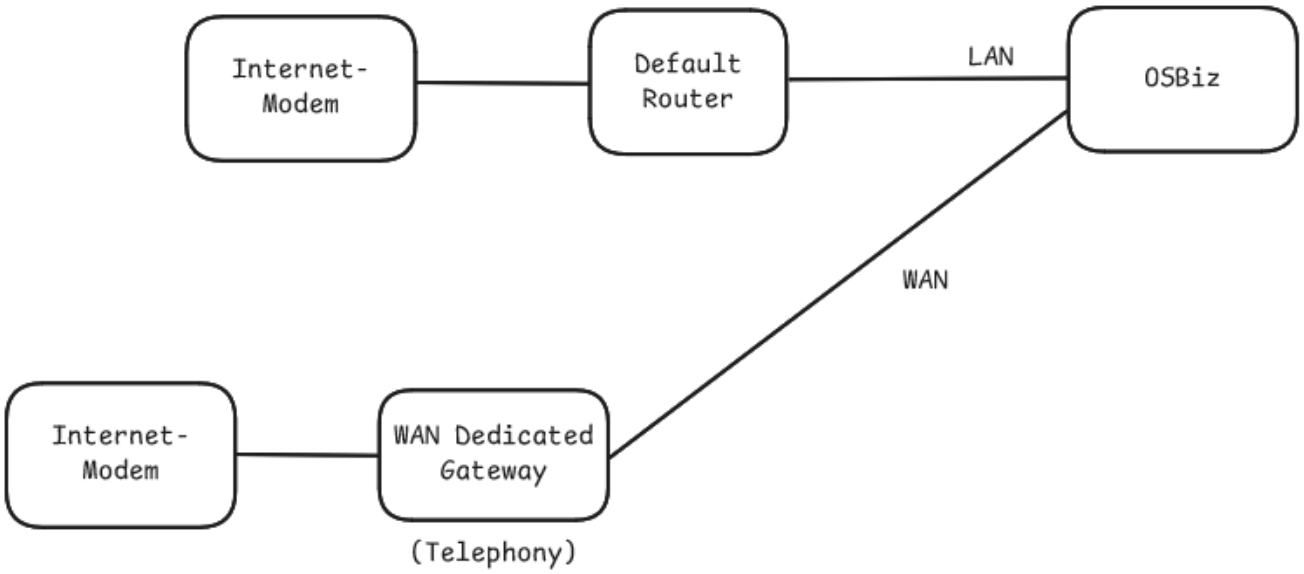


Dazu verwenden Sie den LAN-Port des Kommunikationssystems. OpenScape Business kennt nur den Standard-Router und nicht die

zugrunde liegende Infrastruktur. Um die Verbindung zum Internetrouter zu aktivieren, muss die IP-Adresse des Standard-Routers und die des DNS-Servers dem Kommunikationssystem bekannt gegeben werden.

– **Internetzugang über einen externen Internetrouter am LAN-Port**

(**TCP/IP am LAN/WAN-Port über einen externen Router mit WAN-Port für ITSP**)



Dazu verwenden Sie den LAN-Port des Kommunikationssystems, während der WAN-Port dem ITSP gewidmet ist. OpenScape Business kennt nur den Standard-Router und nicht die zugrunde liegende Infrastruktur. Um die Verbindung zum Internetrouter zu aktivieren, muss die IP-Adresse des Standard-Routers und die des DNS-Servers dem Kommunikationssystem bekannt gegeben werden.

- Internetzugang deaktivieren (Standardeinstellung)

  Sie möchten das Internet nicht verwenden.

5.7.5.1 Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren

Voraussetzungen

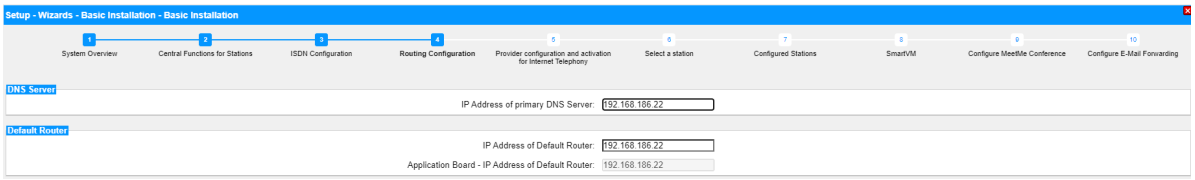
Das Kommunikationssystem muss über die LAN-Schnittstelle "LAN" mit dem Kunden-LAN verbunden sein. Die Verbindung darf nicht über den WAN-Anschluss erfolgen, da dieser deaktiviert wird.

Sie befinden sich im Fenster **Konfiguration des Internetzugangs** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **TCP/IP am LAN Port über einen externen Router**, geben Sie die Upload-Geschwindigkeit Ihrer Internetverbindung in das Feld **Upstream bis Kbit/s** ein und klicken Sie auf **OK&Weiter**.



3) Geben Sie im Feld **IP-Adresse des bevorzugten DNS-Servers** die IP-Adresse des lokalen DNS-Servers (z. B. Internet-Router) oder des Internet-DNS-Servers (z. B. für Internet-Telefonie) ein.
4) Geben Sie im Feld **IP-Adresse des Default Routers** die IP-Adresse des externen Internet-Routers ein.
5) Klicken Sie auf **OK & Weiter**.

5.7.5.2 Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren

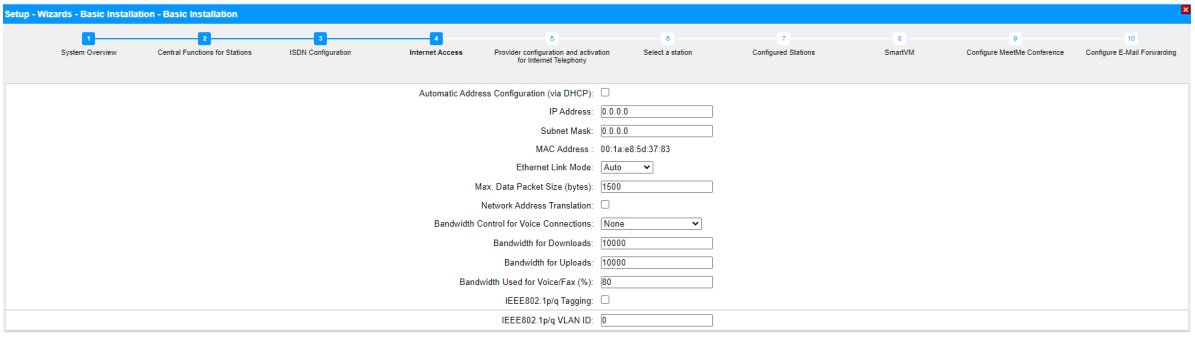
Voraussetzungen

Das Kommunikationssystem muss über die LAN-Schnittstelle "WAN" mit dem LAN-Segment des Kunden-LAN verbunden sein, indem sich der Internet-Router befindet.

Sie befinden sich im Fenster **Konfiguration des Internetzugangs** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
2) Aktivieren Sie das Optionsfeld **TCP/IP am WAN Port über einen externen Router** und klicken Sie auf **OK & Weiter**.



3) Wenn für die WAN-Schnittstelle die netzwerkspezifischen Daten von einem bereits aktiven DHCP-Server bezogen werden sollen:
   a) Aktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.
   b) Aktivieren Sie das Kontrollkästchen **IP-Adresse des Default Routers übernehmen**, wenn diese IP-Adresse verwendet werden soll.
   c) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des DNS-Servers übernehmen**.
   d) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des SNTP-Servers übernehmen**.
4) Wenn der WAN-Schnittstelle eine feste IP-Adresse zugeordnet werden soll:
   a) Deaktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.
   b) Geben Sie die gewünschte **IP-Adresse** und **Netzmaske** der WAN-Schnittstelle ein.
5) Aktivieren Sie das Kontrollkästchen **Netzwerkaddressübersetzung (NAT)**.
6) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Bei einer hohen Download-Bandbreite und zugleich niedrigen Upload-Bandbreite sollte die Bandbreitensteuerung nur für den Upload aktiviert werden, damit nicht unnötig viel Download-Bandbreite für die Sprachübertragung reserviert wird.
7) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download und Upload ein, die Ihnen Ihr Internet-Service-Provider zur Verfügung stellt.
8) Klicken Sie auf **OK & Weiter**.

5.7.5.3 Internet-Zugang über vorkonfigurierten ISP konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Konfiguration des Internetzugangs** des Assistenten **Basisinstallation**.

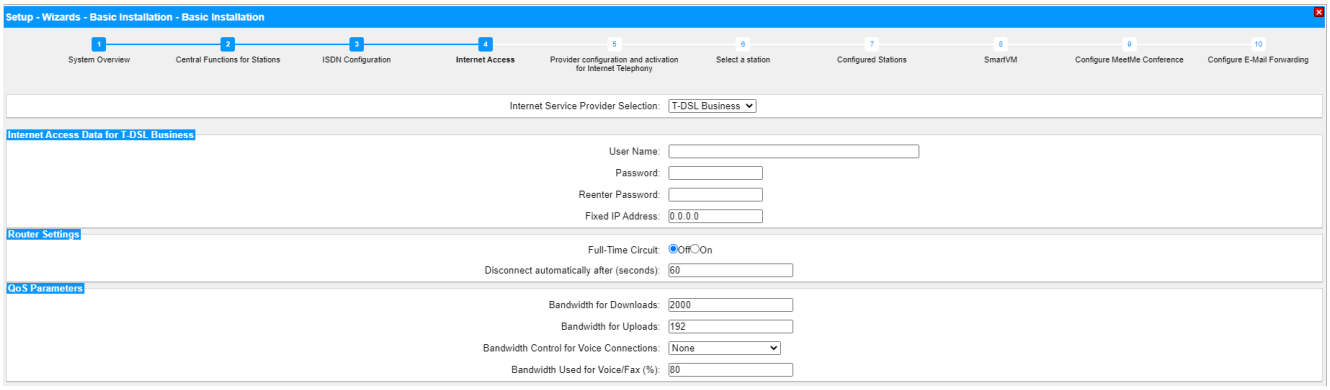
Die Internet-Zugangsdaten Ihres ISP sind verfügbar (z. B. Benutzerkennung, Passwort, Bandbreite für Upload und Download).

Optional: Die Daten für ein DynDNS-Konto stehen Ihnen zur Verfügung (Name, Passwort, Hostname, Domainname des DynDNS-Anbieters)

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **DSL direkt am WAN-Port der Hauptplatine** und klicken Sie auf **OK & Weiter**.



3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** Ihren ISP aus.

4) Geben Sie im Bereich **Internet-Zugangsdaten für...** die Zugangsdaten ein, die Sie von ihrem ISP bekommen haben. Die Felder in diesem Bereich sind providerabhängig. Achten Sie bei der Eingabe der Daten auf korrekte Groß- und Kleinschreibung.

5) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:

- Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z.B. 01:30). Zu dieser Zeit sollten keine Daten mit dem Internet ausgetauscht werden (z.B. Software-Downloads oder Internet-Telefonie).
- Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).

6) Stellen Sie im Bereich **QoS-Parameter** die folgenden Werte ein:

a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)**in Prozent an, wie viel Bandbreite für Sprach- und Faxverbindungen als Prozentwert reserviert werden soll (Standardwert: 80%).

7) Klicken Sie auf **OK& Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

8) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.

a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).

b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den

gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.
d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z.B. myhost.dyndns.org.
e) Testen Sie den DynDNS-Account mit **Verbindung testen**.
f) Klicken Sie nach erfolgreichem Test auf **OK**.
g) Klicken Sie auf **OK& Weiter**.

9) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

10) Klicken Sie auf **OK& Weiter**.

5.7.5.4 Internet-Zugang über Standard-ISP PPPoE konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Konfiguration des Internetzugangs** des Assistenten **Basisinstallation**.

Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feldname	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmode	Authentifizierungsmodus für die PPP-Verbindung über PAP: **PAP-Client**, **PAP-Host** oder **Nicht verwendet**.	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmode	Authentifizierungsmodus für PPP-Verbindung über CHAP: **CHAP-Client**, **CHAP-Host**, **CHAP-Client und -Host** oder **Nicht verwendet**.	

Feldname	Beschreibung	Wert vom ISP
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

Optional: Die Daten für ein DynDNS-Konto stehen Ihnen zur Verfügung (Name, Passwort, Hostname, Domainname des DynDNS-Anbieters)

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
2) Aktivieren Sie das Optionsfeld **DSL am WAN-Port direkt** und klicken Sie auf **OK & Weiter**.
3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPPoE** aus.
4) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.
5) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:
   - Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z.B. 01:30). Zu dieser Zeit sollten keine Daten mit dem Internet ausgetauscht werden (z.B. Software-Downloads oder Internet-Telefonie).
   - Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).
6) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.
   - Authentifizierung durch den ISP erforderlich: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Der gebräuchliche Standard ist der Authentifizierungsmode **CHAP-Client**.
   - Keine Authentifizierung durch den ISP erforderlich: Stellen Sie sicher, dass das Kontrollkästchen PPP-Authentifizierung deaktiviert ist.
7) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

8) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:
   a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.
   b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)**in Prozent an, wie viel Bandbreite für Sprach- und Faxverbindungen als Prozentwert reserviert werden soll (Standardwert: 80%).
9) Klicken Sie auf **OK& Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.
10) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.
   a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).
   b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

      `http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
   c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.
   d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z.B. myhost.dyndns.org.
   e) Testen Sie den DynDNS-Account mit **Verbindung testen**.
   f) Klicken Sie nach erfolgreichem Test auf **OK**.
   g) Klicken Sie auf **OK& Weiter**.
11) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.
12) Klicken Sie auf **OK& Weiter**.

5.7.5.5 Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Konfiguration des Internetzugangs** des Assistenten **Basisinstallation**.

Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feldname	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		

Feldname	Beschreibung	Wert vom ISP
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
PPTP-Parameter		
Lokale IP-Adresse der Kontrollverbindung	IP-Adresse, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 10.0.0.140.	
Partner-IP-Adresse der Kontrollverbindung	IP-Adresse des ISP-Servers für die PPTP-Verbindung. Der voreingestellte Wert lautet 10.0.0.138.	
Partner-Netzmaske für die Kontrollverbindung	Netzmaske, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 255.255.255.248.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über PAP: **PAP-Client**, **PAP-Host** oder **nicht benutzt**.	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über CHAP: **CHAP-Client**, **CHAP-Host**, **CHAP-Client und -Host** oder **nicht benutzt**.	
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

Optional: Die Daten für einen DynDNS-Account liegen Ihnen vor (Name, Passwort, Hostname, Domänenname des DynDNS-Providers)

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.

3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPTP** aus.

4) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.

5) Geben Sie in dem Bereich **PPTP-Parameter** die Werte ein, die Sie von Ihrem ISP bekommen haben.

6) Wenn Sie als Tarifmodell einen Zeittarif haben, aktivieren Sie das Kontrollkästchen **Short-Hold-Modus**. Geben Sie im Feld **Short-Hold-Zeit (s)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z.B. 60 Sekunden).

7) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.

   - Authentifizierung wird vom ISP gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Treffen Sie die PAP- und CHAP-Einstellungen, wie Sie sie von Ihrem ISP zugeteilt bekommen haben.
   - Authentifizierung wird vom ISP nicht gefordert: Stellen Sie sicher, dass das Kontrollkästchen PPP-Authentifizierung deaktiviert ist.

8) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

9) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:

   a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

   b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

10) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

11) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.

   a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).

   b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL**

die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

`http://www.anydns.info/update.php?user=<Benutzername>&password=<Kennwort>&host=<Domäne>&ip=<IP-Adresse>`

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.

d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z.B. myhost.dyndns.org.

e) Testen Sie den DynDNS-Account mit **Verbindung testen**.

f) Klicken Sie nach erfolgreichem Test auf **OK**.

g) Klicken Sie auf **OK & Weiter**.

12) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

13) Klicken Sie auf **OK & Weiter**.

5.7.5.6 Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port

Voraussetzungen

Sie befinden sich im Fenster **Konfiguration des Internetzugangs** des Assistenten **Basisinstallation**.

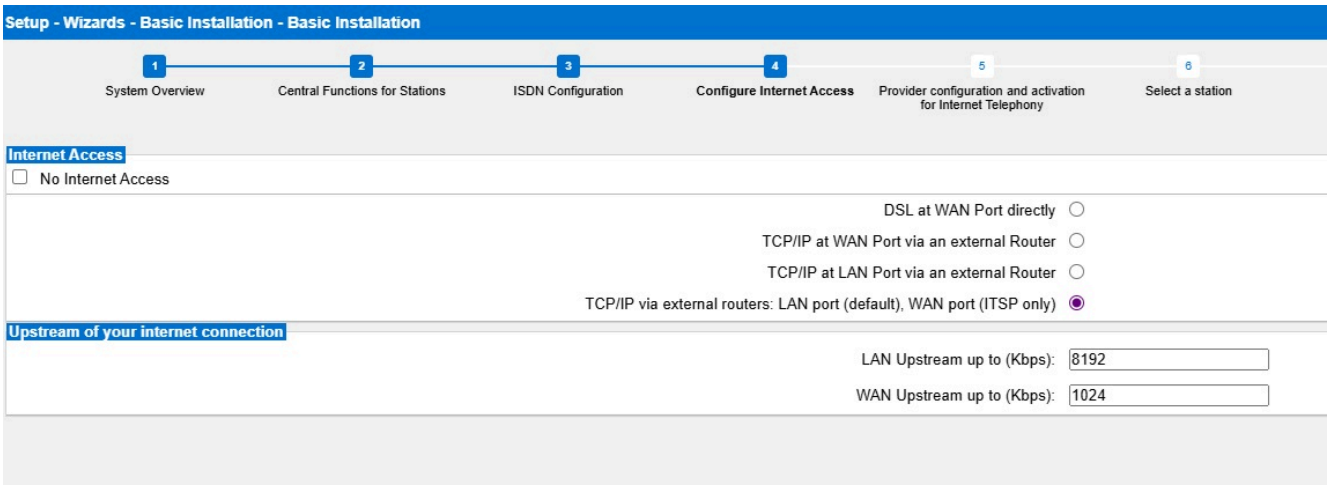
Diese Funktion ist nur für ITSPs verfügbar, die keine Verwendung von STUN in den Anbietereinstellungen erfordern.

Es ist nicht möglich, zwei identische ITSPs (mit demselben Registrar/Proxy) gleichzeitig über LAN und WAN zu verbinden.

Schritt für Schritt

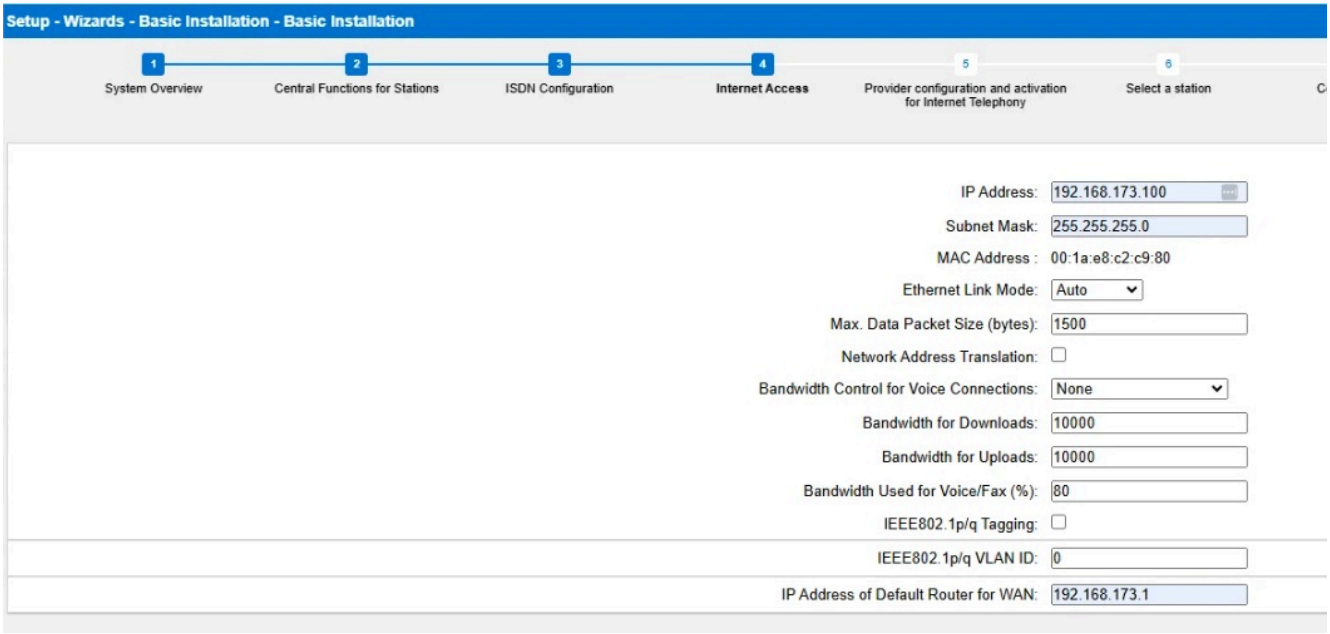
1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **TCP/IP über externe Router: LAN-Port (Standard), WAN-Port nur ITSP**.



3) Konfigurieren Sie den maximalen Upstream-Kbit/s-Wert für jede Schnittstelle unter **LAN-Upstream bis zu (Kbps)** und **WAN-Upstream bis zu (Kbit/s)**.

4) Klicken Sie auf **OK & Weiter**.
5) Geben Sie die WAN-Port-IP-Konfiguration und zusätzlich die IP-Adresse des Standard-Routers für den WAN-Port ein.



6) Klicken Sie auf **OK & Weiter**.

5.7.5.7 Wie Sie den Internet-Zugang deaktivieren

Voraussetzungen

Sie befinden sich im Fenster **Konfiguration des Internetzugangs** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **Kein Internet-Zugang** aktiviert.
2) Klicken Sie auf **OK & Weiter**.

5.7.6 Internet-Telefonie

Im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** konfigurieren Sie die Internet-Telefonie. Sie können vorkonfigurierte oder neue Internet-Telefonie-Service-Provider (ITSP) konfigurieren. Für jeden ITSP können Sie einen oder mehrere Accounts konfigurieren. Es können bis zu 8 ITSP gleichzeitig aktiv sein.

Sie haben folgende Möglichkeiten:

- **Vordefinierten ITSP konfigurieren**

  Sie können vordefinierte ITSP-Vorlagen verwenden. Dazu werden in diese Vorlage die eigenen Zugangsdaten und Rufnummern eingetragen und diese anschließend aktiviert.

- **Neuen ITSP konfigurieren**

  Sie können auch neue ITSP hinzufügen und aktivieren.

  Einen neuen ITSP zu konfigurieren ist nur in seltenen Fällen nötig und sehr aufwändig. Deshalb wird diese Möglichkeit nicht in der Erstinstallation beschrieben. Genauere Informationen finden Sie im Kapitel Konfiguration eines ITSP.
- **Internet-Telefonie deaktivieren**

  Sie können die Internet-Telefonie deaktivieren.

Anmerkung:

Einrichtebeispiele finden Sie im Internet im **Unify Experts Wiki** unter *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Zuordnung der ITSP-Rufnummern

- Bei einem **Internet-Telefonie-Teilnehmeranschluss** stellt der ITSP Einzelrufnummern zur Verfügung, z.B. 70005555, 70005556, ... Diese Einzelrufnummern werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.
- Bei einem **Internet-Telefonie-Anlagenanschluss** stellt der ITSP ein Rufnummernband (Rufnummernbereich) zur Verfügung, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Bereich werden dann manuell als interne Rufnummern der Teilnehmer vergeben.

Die beiden Anschlussarten können kombiniert werden.

Alternativ können für beide Anschlussarten die ITSP-Rufnummern bei der Teilnehmer-Konfiguration als Durchwahlrufnummern der Teilnehmer eingetragen werden.

Interne Rufnummer	Name	Durchwahl
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Somit ergeben sich die ITSP-Rufnummern aus der eingerichteten Anlagenrufnummer (z.B. Länderkennzahl 49) und den eingetragenen Durchwahlnummern im Langformat. Das hat Vorteile bei der Wahlbewertung und dem Call-Management, auch in einem Netzverbund. So ist der ITSP-Anschluss z. B. durchwahlfähig zu einem anderen Knoten.

Ein weiterer Amtsanschluss über ISDN ist in diesem Fall nur eingeschränkt möglich (sinnvoll z.B. für Notrufe).

5.7.6.1 Vordefinierten ITSP konfigurieren

Voraussetzungen

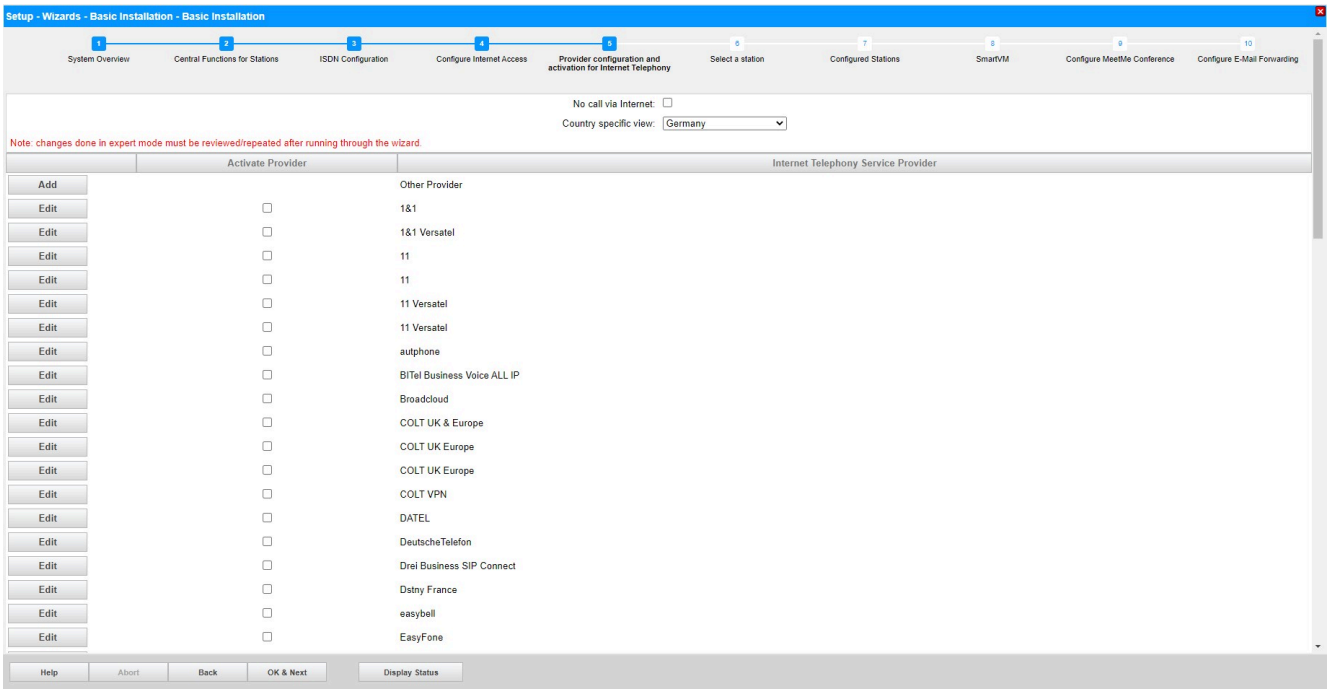
Sie befinden sich im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** des Assistenten für die **Grundinstallation**.

Die Verbindung zum Internet ist betriebsbereit.

Die Internet-Telefonie-Zugangsdaten Ihres ITSP liegen Ihnen vor (z. B. Benutzerkennung, Passwort, Internet-Telefonie-Rufnummern).

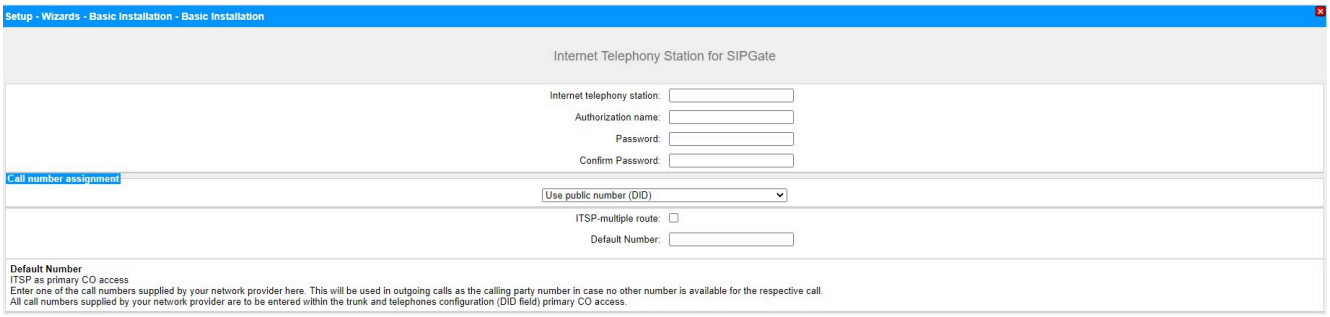
Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt. Die Liste enthält die für das gewählte Land vordefinierten ITSP und die eventuell bereits angelegten ITSP.



2) Wenn Sie das voreingestellte Land ändern möchten, wählen Sie aus der Aufklappliste **Länderspezifische Ansicht** das gewünschte Land aus. Es werden die für das gewählte Land möglichen ITSP angezeigt.
3) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie 8 ITSP aktivieren. Klicken Sie anschließend auf **OK**.
4) Klicken Sie in der Zeile des entsprechenden ITSP auf **Bearbeiten**, um einen vordefinierten ITSP zu konfigurieren.
5) Aktivieren Sie das Kontrollkästchen **Provider aktivieren**.
6) Klicken Sie auf **OK & Weiter**.

7) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.



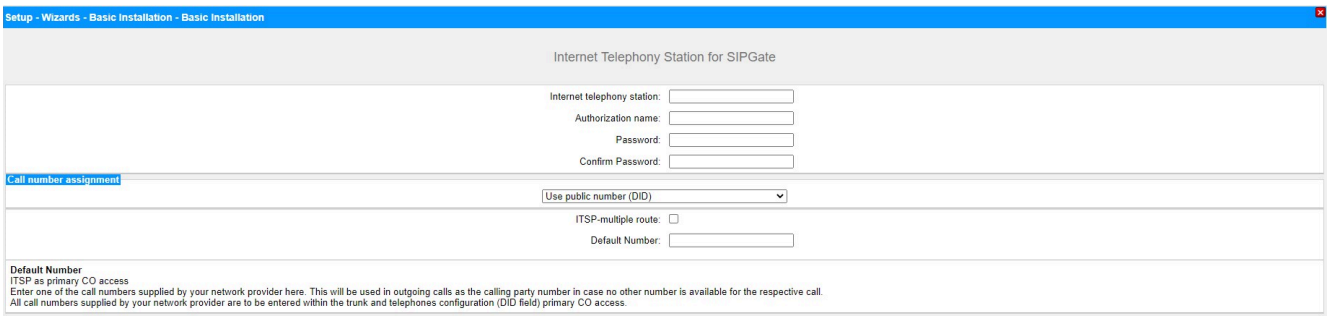
8) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: SIP-Benutzer, SIP-ID usw.

9) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen Autorisierungsnamen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

10) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, dass Sie vom ITSP erhalten haben. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: Kennwort, SIP-Kennwort usw.

11) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

Öffentliche Rufnummer (DuWa): die Internet-Telefonie-Rufnummern Ihres Internet-Telefonie-Teilnehmeranschlusses oder Internet-Telefonie-Anlagenanschlusses werden nicht hier bei der ITSP-Konfiguration, sondern bei der Teilnehmer-Konfiguration in den Feldern **DuWa** eingetragen.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.

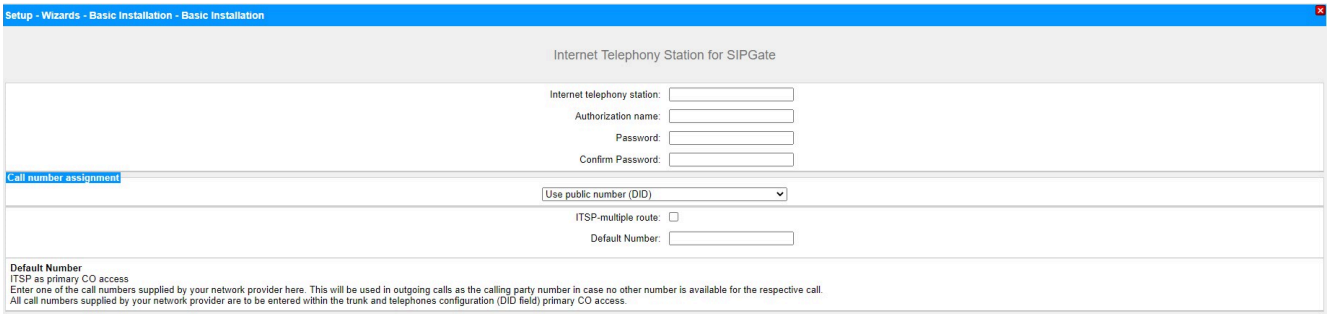
b) Unter **Standardnummer**, geben Sie die Telefonnummer, die für ausgehende Anrufe verwendet werden soll, wenn keine DID-Nummer des Anrufers verfügbar ist, ein.

c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern).

12) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

Interne Nummer (Rufnr.) verwenden / Einzeleinträge: Sie haben einen Internet-Telefonie-Teilnehmeranschluss und als Internet-Telefonie-Rufnummern Einzelrufnummern erhalten (z. B. 70005555, 70005556,...).

Diese Einzelrufnummern ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



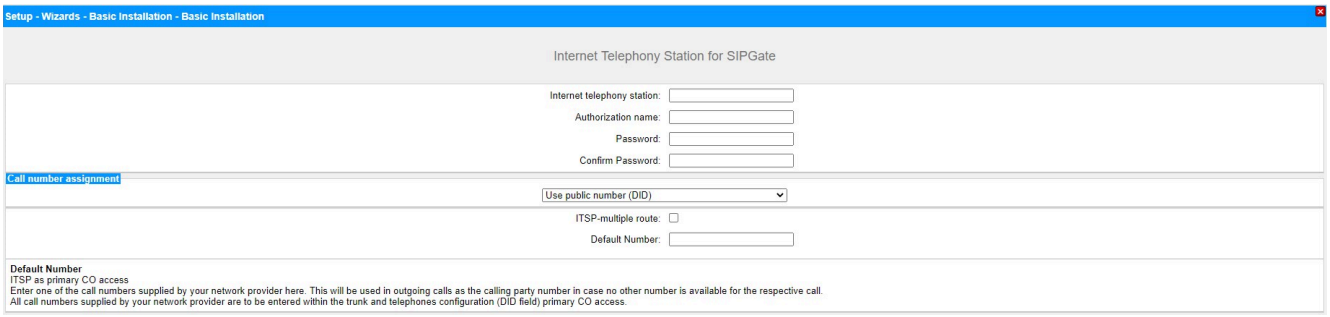
a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.

b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP mitgeteilten Internet-Telefonie-Teilnehmerrufnummern ein und klicken Sie auf **Hinzufügen**.

c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).

13) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:

Interne Nummer (Rufnr.) verwenden / Bereichseintrag: Sie besitzen einen Internet-Telefonie-Anlagenanschluss und haben als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z.B. (+49) 89 7007-100 bis (+49) 89 7007-147. Sie weisen dann die Rufnummern aus dem Rufnummernbereich den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.

b) Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.

c) Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.

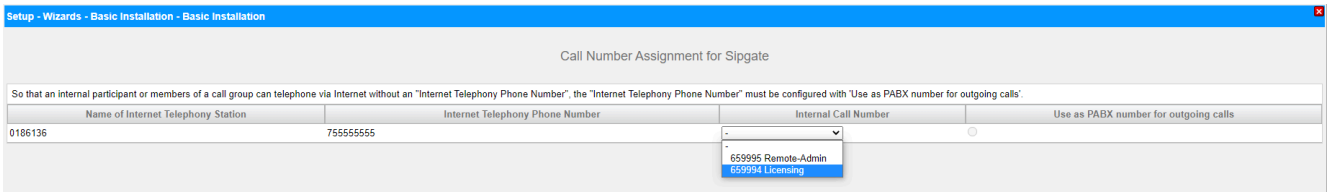
14) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie weitere Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern einrichten möchten, wiederholen Sie die Schritte 7 bis 14.

16) Klicken Sie auf **OK & Weiter**. Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.

17) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.

Dieser Schritt entfällt, wenn Sie für die Zuordnung der Internet-Telefonie-Rufnummern die Möglichkeit 1 gewählt haben. Die Zuordnung treffen Sie in diesem Fall bei der Teilnehmer-Konfiguration im Feld **DuWa**.



a) Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.

b) Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.

18) Klicken Sie auf **OK & Weiter**. Hier sehen Sie nochmals die Liste der vordefinierten und neu hinzugefügten ITSP. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit **Restart ITSP** können Sie sich bei Verbindungsproblemen bei bereits aktivierten ITSP neu registrieren

19) Klicken Sie auf **OK & Weiter**.

20) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!

Anmerkung: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig zu führenden Internet-Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

Weitere Informationen über die Anzahl der gleichzeitigen Internetanrufe finden Sie unter Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP auf Seite 827.

---

21) Klicken Sie auf **OK & Weiter**.

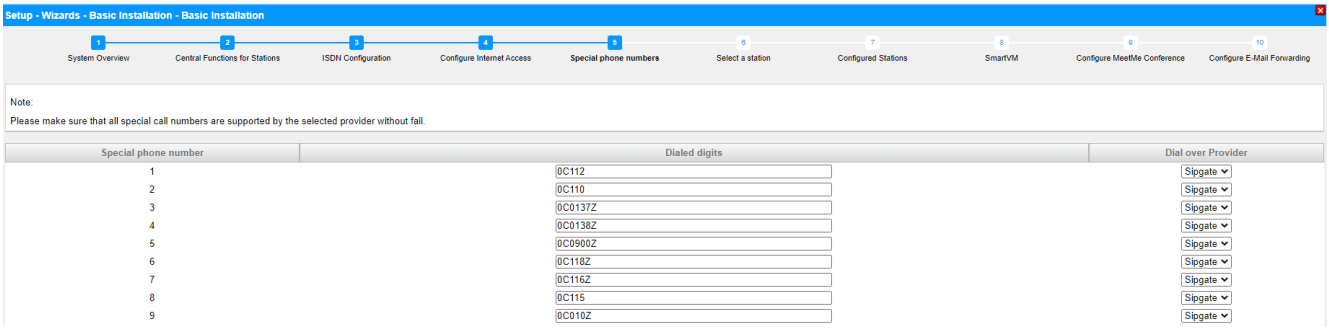
22) Falls Sie bei der Einrichtung Ihres Internet-Zugangs die Dauerverbindung noch nicht aktiviert haben, können Sie das hier nachholen. Ohne Dauerverbindung können Sie keine Anrufe über das Internet empfangen. Ist die Dauerverbindung bereits eingerichtet, erscheinen die unter a) bis c) beschriebenen Felder nicht.

a) Aktivieren Sie unter **Dauerverbindung** das Optionsfeld **An**.

b) Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).

c) Klicken Sie auf **OK & Weiter**.

23) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.



Folgende Rufnummerneinträge sind gültig:

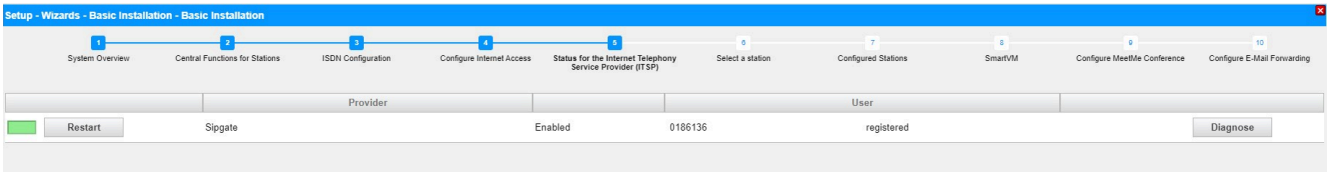
- 0 bis 9: Zulässige Ziffern
- -: Feldtrennzeichen
- X: beliebige Ziffer von 0 bis 9
- N: beliebige Ziffer von 2 bis 9
- Z: Eine oder mehrere Ziffern folgen bis Wahlende
- C: Simulierter Wählton (kann max. dreimal eingetragen werden)

24) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

Anmerkung: Stellen Sie sicher, dass Notrufnummern immer gewählt werden können. Falls Notrufnummern über einen Internet-Telefonie-Service-Provider gewählt werden sollen, muss der ITSP dies unterstützen.

---

25) Klicken Sie auf **OK & Weiter**. Der Status Ihres ITSP wird angezeigt.



Grün markiert sind ITSP, die eingerichtet und an denen Sie bereits registriert sind.

Orange markiert sind ITSP, die eingerichtet und an denen Sie noch nicht registriert sind.

26) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

5.7.6.2 Wie Sie Internet-Telefonie deaktivieren

Voraussetzungen

Sie befinden sich im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** des Assistenten für die **Grundinstallation**.

Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **Keine Telefonie über Internet** aktiviert.

2) Klicken Sie zweimal auf **OK & Weiter**.

5.7.7 Teilnehmer

In den Fenstern **Teilnehmer auswählen - ...** konfigurieren Sie die an dem Kommunikationssystem angeschlossenen Teilnehmer.

Gehen Sie folgendermaßen vor:

1) ISDN-Teilnehmer konfigurieren

   ISDN-Teilnehmer sind z.B. ISDN-Telefone oder ISDN-Faxgeräte. ISDN-Teilnehmer können Sie nur konfigurieren, wenn Sie eine S_0-Schnittstelle als internen S_0-Anschluss konfiguriert haben.

2) Analoge Teilnehmer konfigurieren

   Analoge Teilnehmer sind z.B. analoge Telefone oder analoge Faxgeräte.

3) UP0-Teilnehmer konfigurieren

   UP0-Teilnehmer sind Systemtelefone wie OpenStage 60 T.

4) DECT-Teilnehmer konfigurieren

   DECT-Teilnehmer sind Cordless/DECT-Telefone. DECT-Teilnehmer können Sie nur konfigurieren, wenn eine oder mehrere Cordless-Basisstationen angeschlossen und die DECT-Telefone dort angemeldet sind. Die Konfiguration wird mit dem Manager E durchgeführt. Genauere Informationen zur Konfiguration von Cordless siehe Konfiguration der integrierten Cordless-Lösung

5) IP- und SIP-Teilnehmer konfigurieren

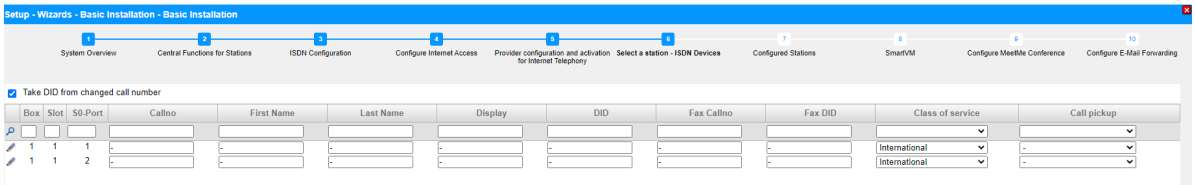
   IP-Teilnehmer und SIP-Teilnehmer sind z.B. LAN-Telefone oder WLAN-Telefone.

5.7.7.1 ISDN-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - ISDN-Endgeräte** im Assistenten für die **Grundinstallation**.

Die S_0-Anschlüsse, an denen die ISDN-Telefone angeschlossen sind, müssen als interner S_0-Anschluss eingerichtet sein.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:
   - Nur bei Anlagenanschluss:

     Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
   - Nur bei Mehrgeräteanschluss:

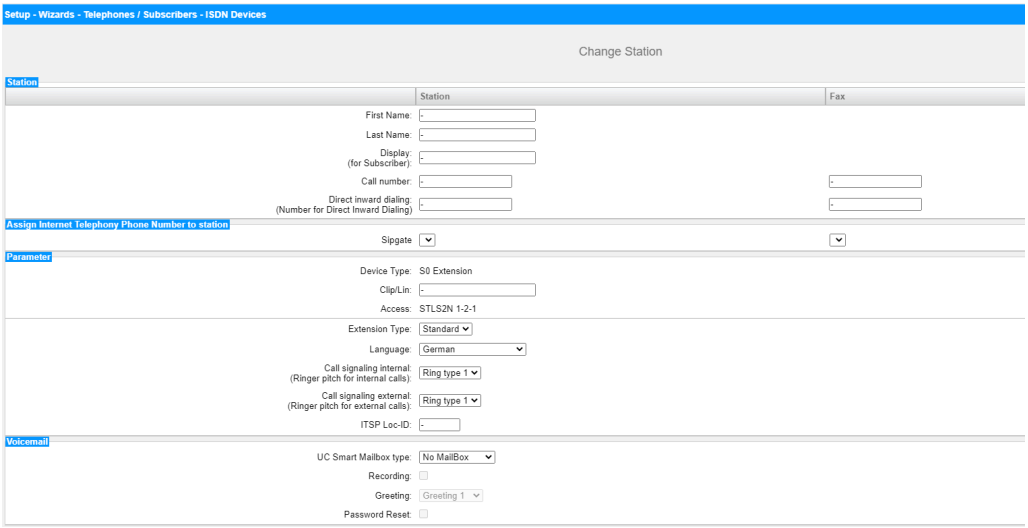
     Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
   - Bei Anlagenanschluss und Mehrgeräteanschluss:

     Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.
2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.
3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

   Anmerkung: Der Name kann aus bis zu 16 Zeichen bestehen, darf aber keine Umlaute oder Sonderzeichen enthalten.
4) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:
   a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
   b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.
6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten ISDN-Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des ISDN-Endgeräts aus.

d) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er

von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Klicken Sie auf **OK & Weiter**.

h) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

i) Klicken Sie auf **OK & Weiter**.

8) Wenn Sie weitere ISDN-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.

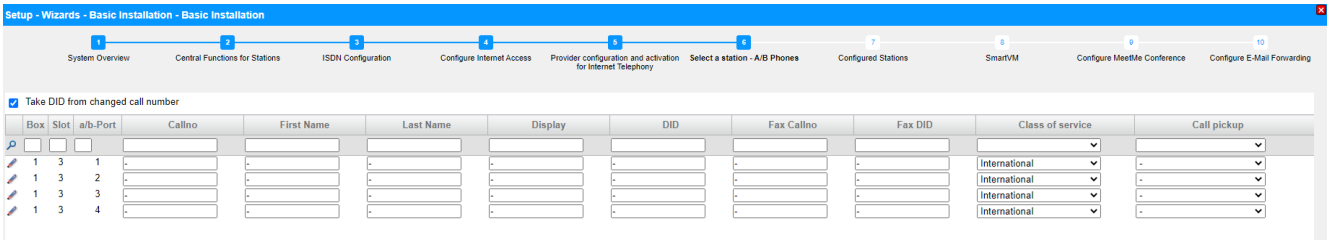
9) Klicken Sie auf **OK & Weiter**.

5.7.7.2 Analoge Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - A/B-Endgeräte** im Assistenten für die **Grundinstallation**.

Ein Mainboard oder eine Baugruppe mit analogen Schnittstellen ist vorhanden.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- Nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- Nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- Bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte

Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

Anmerkung: Der Name kann aus bis zu 16 Zeichen bestehen, darf aber keine Umlaute oder Sonderzeichen enthalten.

---

4) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

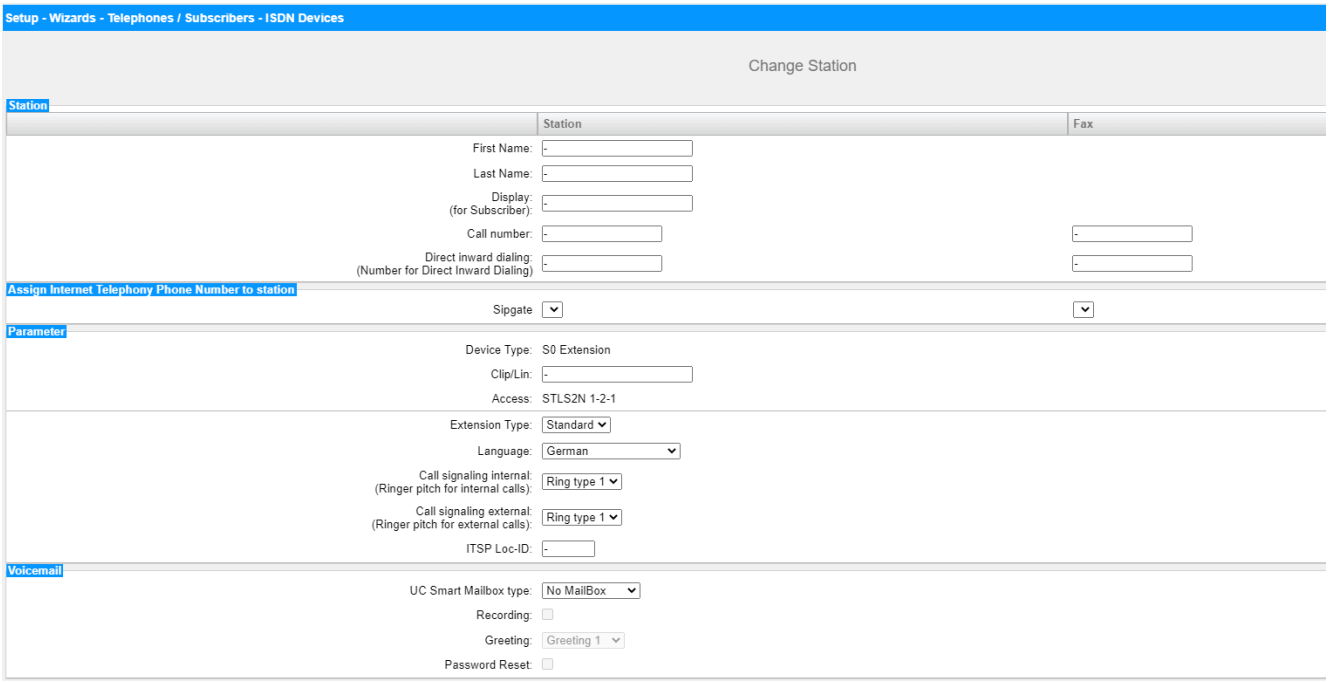
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten analogen Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des analogen Endgeräts (z. B. Fax) aus.

d) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer

anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Klicken Sie auf **OK & Weiter**.

h) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

i) Klicken Sie auf **OK & Weiter**.

8) Wenn Sie einen weiteren analogen Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.

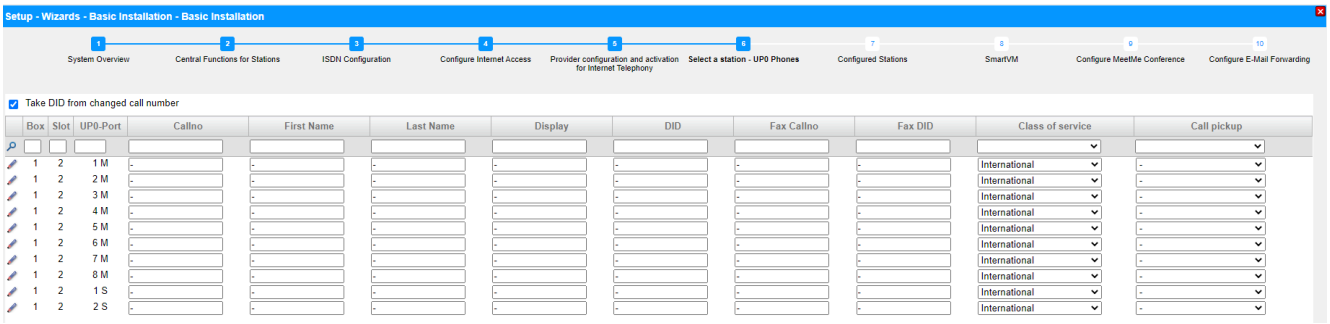
9) Klicken Sie auf **OK & Weiter**.

5.7.7.3 UP0-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - UP0-Endgeräte** im Assistenten für die **Grundinstallation**.

Ein Mainboard oder eine Baugruppe mit UP0-Schnittstellen ist vorhanden.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- Nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- Nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- Bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie

über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.
3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

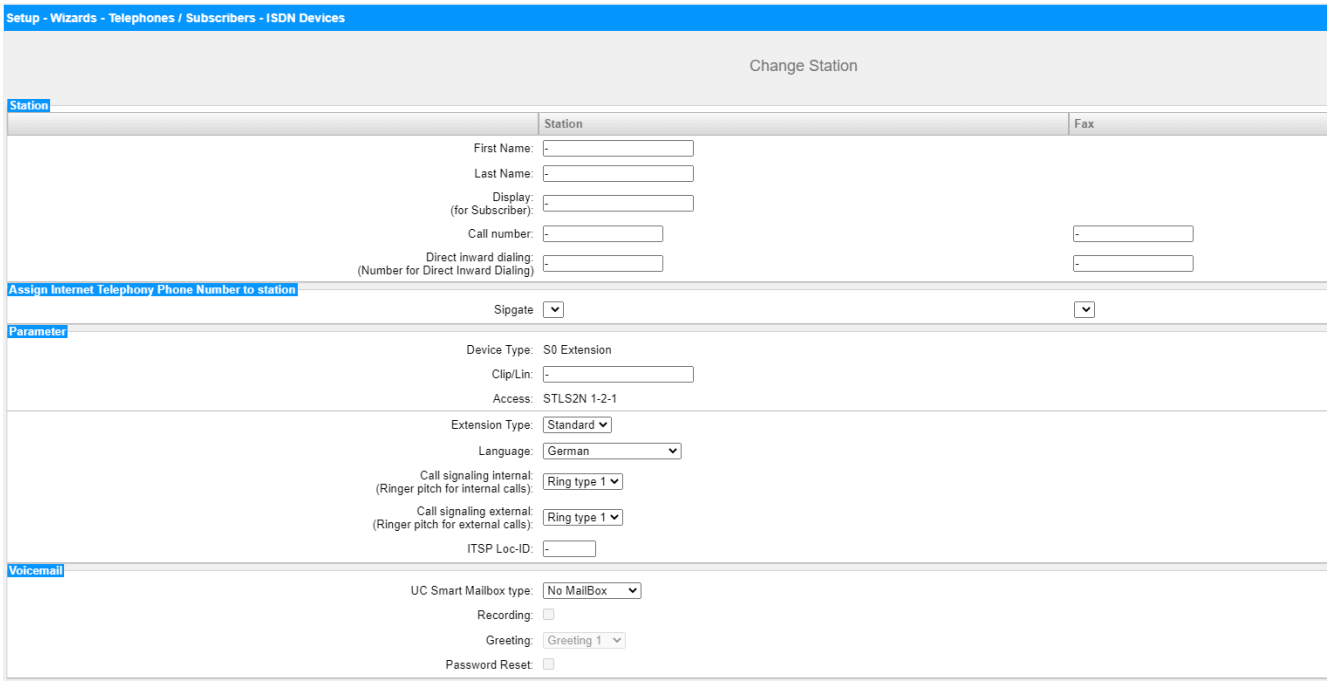
Anmerkung: Der Name kann aus bis zu 16 Zeichen bestehen, darf aber keine Umlaute oder Sonderzeichen enthalten.

---

4) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:
   a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
   b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.
6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des TDM-Endgeräts aus.

d) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für TDM-Endgeräte ist diese Einstellung ohne Bedeutung.

e) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie

nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

h) Klicken Sie auf **OK & Weiter**.

i) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

j) Klicken Sie auf **OK & Weiter**.

8) Wenn Sie einen weiteren UP0-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.

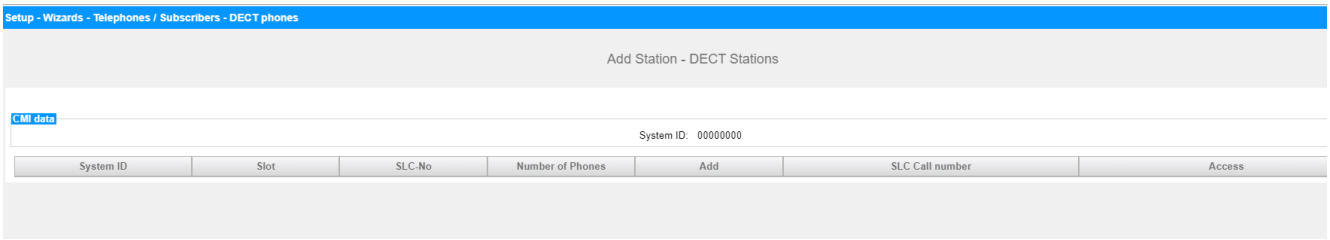
9) Klicken Sie auf **OK & Weiter**.

5.7.7.4 Wie Sie DECT-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - DECT-Endgeräte** im Assistenten für die **Grundinstallation**.

Für die Konfiguration von DECT-Teilnehmern muss eine Basisstation angeschlossen und die DECT-Telefone dort angemeldet sein. Ist dies nicht der Fall, überspringen Sie dieses Fenster. Sie können die DECT-Teilnehmer auch später noch konfigurieren (siehe Konfiguration der Teilnehmer).



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- Nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- Nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- Bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

4) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

Anmerkung: Der Name kann aus bis zu 16 Zeichen bestehen, darf aber keine Umlaute oder Sonderzeichen enthalten.

---

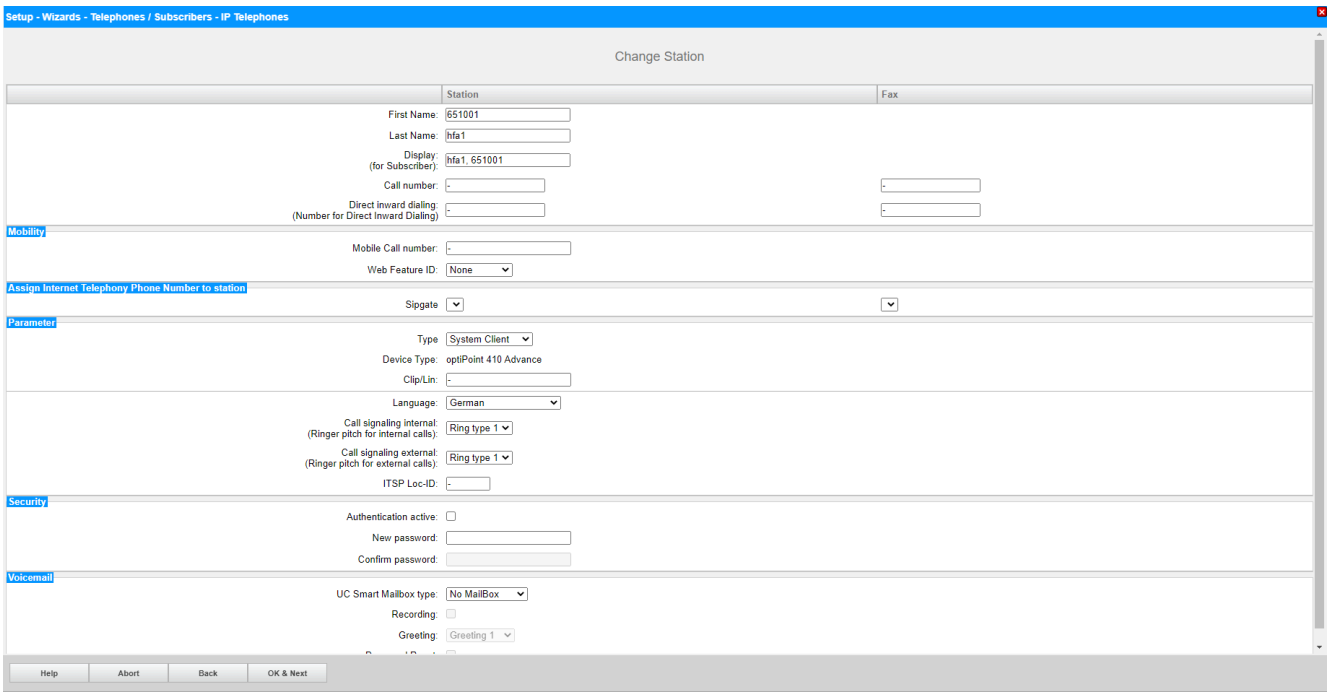
5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

7) Falls Sie den DECT-Telefoncode (PIN) ändern wollen, geben Sie in der Zeile des gewünschten Teilnehmers unter **Mobilcode** den neuen Code ein. Der DECT-Teilnehmer muss sich mit diesem Code neu an der Basisstation anmelden.

8) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des Schnurlos-Endgeräts aus.

d) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für Schnurlos-Endgeräte ist diese Einstellung ohne Bedeutung.

e) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie

nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

h) Klicken Sie auf **OK & Weiter**.

i) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

j) Klicken Sie auf **OK & Weiter**.

9) Wenn Sie einen weiteren Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 8.

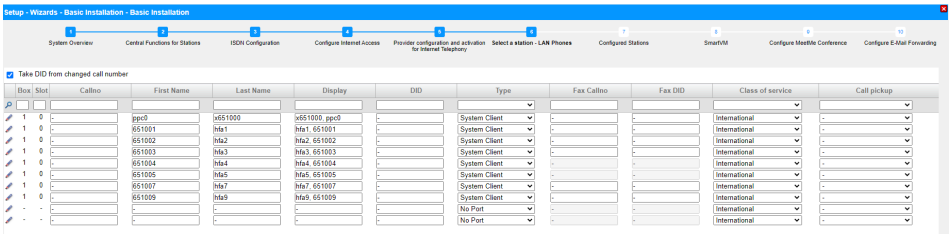
10) Klicken Sie auf **OK & Weiter**.

5.7.7.5 Wie Sie IP- und SIP-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - LAN-Telefone** im Assistenten für die **Grundinstallation**.

Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless LAN-Netzwerk.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- Nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- Nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- Bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` ein.

Anmerkung: Der Name kann aus bis zu 16 Zeichen bestehen, sollte aber keine Umlaute oder Sonderzeichen enthalten. Der Name wird wie hier angegeben bei den UC Clients als Nachname eingetragen, kann dort aber nachbearbeitet werden.

---

4) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ des IP-Teilnehmers aus (z. B. "System Client" oder "SIP Client").

5) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

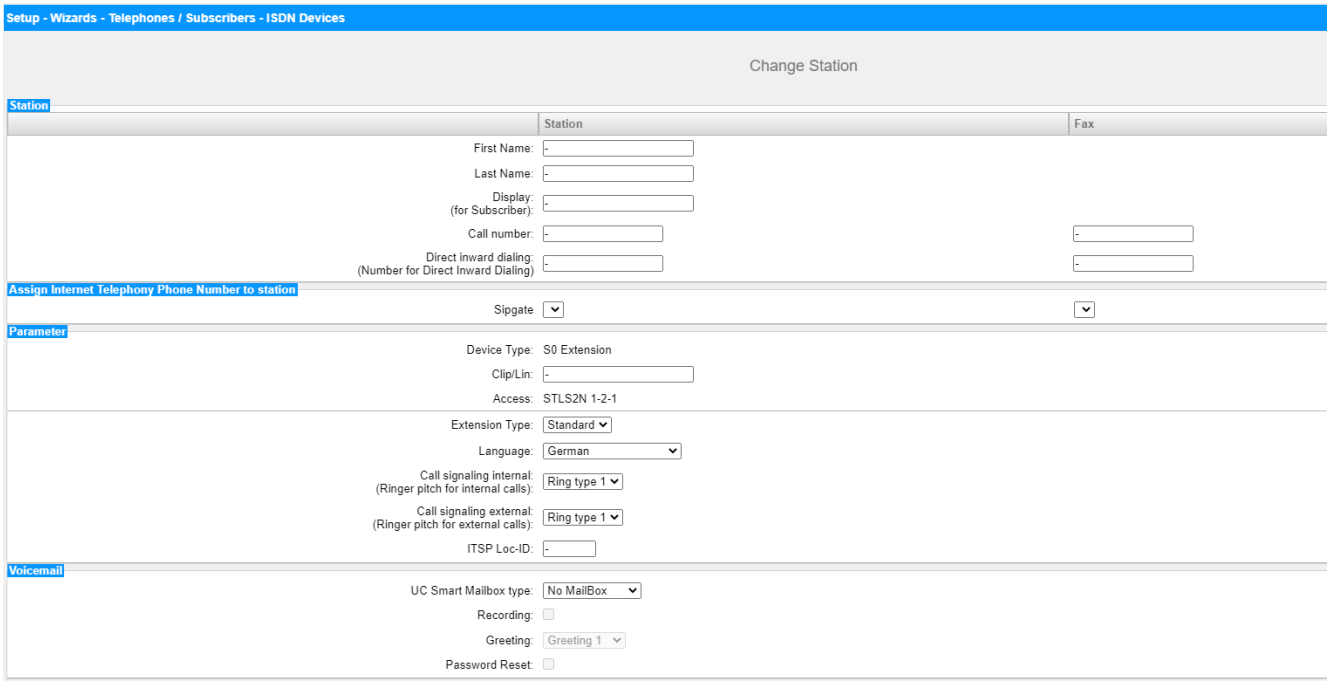
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

6) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

7) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

8) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf oder für ein SIP-Telefon durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Für SIP-Telefone: Wenn das SIP-Telefon zusammen mit einem Dual-Mode-Mobiltelefon betrieben werden soll, geben Sie im Bereich **Mobility** unter **mobile Rufnummer** die Amtskennziffer und gefolgt von der Rufnummer des Mobiltelefons ein (z.B. `0016012345678`). Wählen Sie zusätzlich aus der Aufklappliste **Web Feature ID** diesen SIP Client aus. (siehe Dual-Mode-Telefonie).

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).
g) Nur für SIP-Telefone: Geben Sie im Feld **Passwort** und im Feld **Passwort bestätigen** das Authentifizierungspasswort ein.
h) Nur für SIP-Telefone: Geben Sie im Feld **SIP User ID / Benutzername** die Benutzerkennung für die Authentifizierung ein.
i) Nur für SIP-Telefone: Geben Sie im Feld **Realm** die zugehörige Zone für die Authentifizierung ein.
j) Klicken Sie auf **OK & Weiter**.
k) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.
l) Klicken Sie auf **OK & Weiter**.

9) Wenn Sie einen weiteren IP-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 8.

10) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten Teilnehmer. Diese Liste entspricht einem Rufnumernplan.

11) Klicken Sie bei Bedarf auf **Drucken**, um die Daten der eingerichteten Teilnehmer auszudrucken.

12) Klicken Sie anschließend auf **OK & Weiter**.

Zugehörige Konzepte

Mehrsprachige Textausgabe auf Seite 1243

5.7.8 Konfiguration von UC Suite

Im Fenster **Automatische Konfiguration der Applikation-Suite** können Sie die automatische Konfiguration der UC-Lösung UC Suite durchführen.

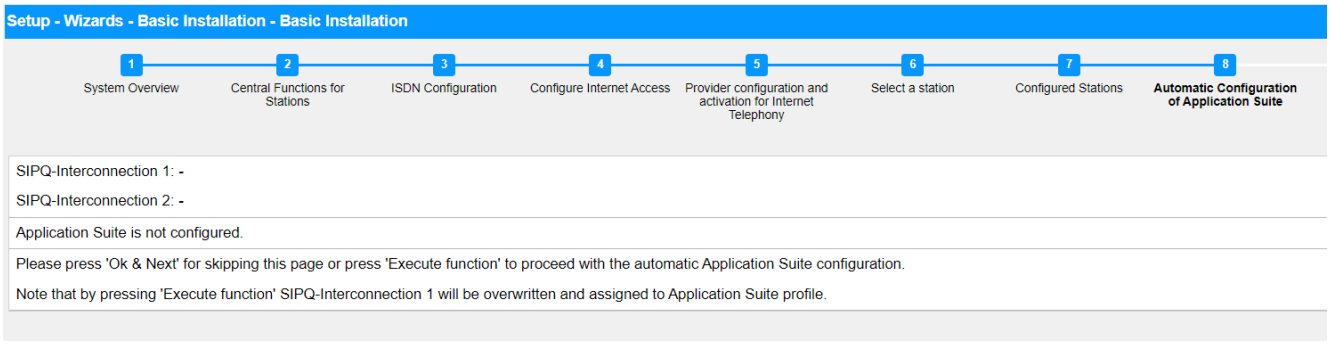
Anmerkung: Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Suite** gewählt wurde.

Die automatische Konfiguration der UC-Lösung UC Suite erfordert eine Anzahl von freien Amtsleitungen, die für die Anwendung statisch belegt werden. Diese Anzahl hängt von den Kapazitäten der Systemspezifikation ab und ist im Abschnitt Maximalwerte für Leitungen auf Seite 1457 aufgeführt (siehe *MEB-Leitungskanäle für UC Suite* in den Tabellen). Falls die Gesamtgrenze von 250 Leitungen überschritten wird, ist die Konfiguration der UC Suite nicht möglich.

5.7.8.1 So konfigurieren Sie die UC Suite

Voraussetzungen

Sie befinden sich im Fenster **Automatische Konfiguration der Anwendungssuite** des Assistenten für **Grundinstallation**.



Schritt für Schritt

1) Wenn keine UC Booster Card in das Kommunikationssystem integriert ist, klicken Sie auf **OK und Weiter**. Die Konfiguration wird übersprungen.
2) Wenn die UC Booster Card in das Kommunikationssystem integriert ist, klicken Sie auf **Funktion ausführen**. Die UC Suite wird automatisch konfiguriert. Sobald der Fortschrittsbalken 100 % anzeigt, klicken Sie auf **OK & Weiter**.

Anmerkung:

Für OpenScape Business X generiert der Assistent automatisch 76 Medienkanäle.

5.7.9 Konfiguration der UC Smart Sprachboxen

Im Fenster **Automatische Konfiguration der Smart VM** können Sie die automatische Konfiguration der UC Smart Sprachboxen (Smart VM, Smart VoiceMail) durchführen, wenn die UC-Lösung UC Smart genutzt wird.

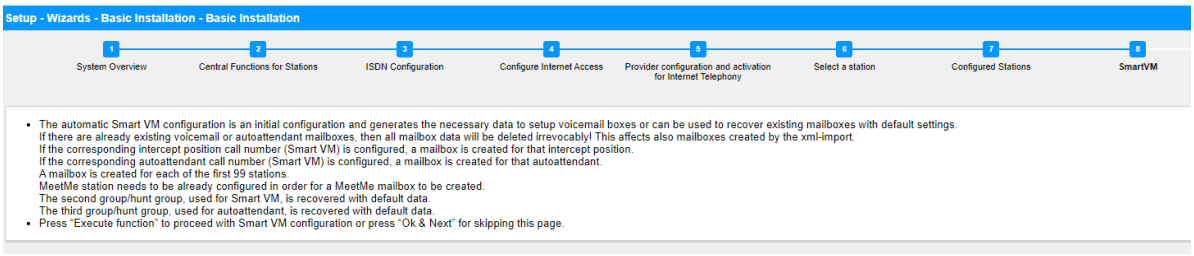
Anmerkung:

Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Smart** gewählt wurde.

5.7.9.1 Wie Sie die UC Smart Sprachboxen konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Automatische Konfiguration von Smart VM** des Assistenten für die **Grundinstallation**.



Schritt für Schritt

1) Wenn die UC Smart Sprachboxen nicht genutzt werden sollen, klicken Sie auf **OK & Weiter**. Die Konfiguration der Sprachboxen wird übersprungen.
2) Wenn die UC Smart Sprachboxen genutzt werden sollen, klicken Sie auf **Funktion ausführen**. Für die ersten 100 Teilnehmer werden automatisch Sprachboxen konfiguriert. Sobald der Verlaufsbalken 100 % anzeigt, klicken Sie auf **OK & Weiter**.

Anmerkung: Bereits vorhandene UC Smart Sprachboxen oder UC Smart AutoAttendant-Sprachboxen werden dabei unwiderruflich gelöscht.

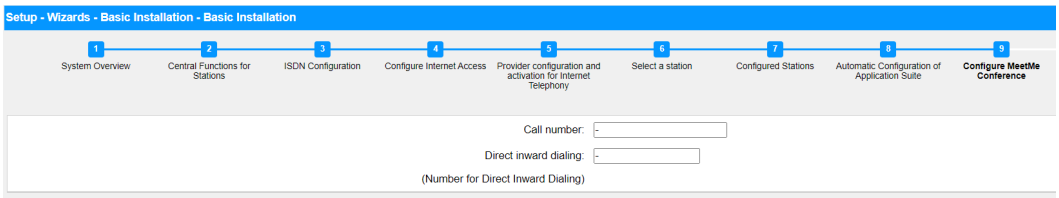
5.7.10 Konferenz-Server-Einstellungen

Im Fenster **MeetMe-Konferenz-Einstellungen ändern** können Sie die Rufnummer und die Einwahlnummer für Konferenzen festlegen.

5.7.10.1 Wie Sie die Konferenz-Server-Einstellungen ändern

Voraussetzungen

Sie befinden Sich im Fenster **MeetMe-Konferenz-Einstellungen ändern** im Assistenten für die **Grundinstallation**.



Schritt für Schritt

1) Geben Sie im Feld **Rufnummer** eine Rufnummer für die Konferenz ein.
2) Legen Sie im Feld **Durchwahl** die Einwahlnummer für die Konferenz (Konferenz-DUWA) fest, mit der sich Teilnehmer in eine bestehende Konferenz einwählen können.
3) Klicken Sie auf **OK & Weiter**.

5.7.11 E-Mail-Versand (optional)

Im Fenster **E-Mail-Weiterleitung ändern** können Sie den E-Mail-Versand konfigurieren. Teilnehmer werden dadurch über neue Sprach- und Faxnachrichten informiert und der Administrator erhält Systemmeldungen.

Sie haben folgende Möglichkeiten:

- E-Mail-Versand konfigurieren

  Sie können einen externen E-Mail-Server festlegen, über den OpenScape Business die E-Mails versenden soll. Sprach- und Faxnachrichten oder interne Systemmeldungen werden über diesen E-Mail-Server an eine oder verschiedene konfigurierbare E-Mail-Adressen versendet.

Anmerkung: Die Angabe eines E-Mail-Servers ist wichtig, wenn den Benutzern der UC Suite automatisch per E-Mail ein Link auf die Installationsdatei(en) geschickt werden soll.

5.7.11.1 E-Mail-Versand konfigurieren

Voraussetzungen

Wenn der externe E-Mail-Server für die Verwendung der einfachen Authentifizierung konfiguriert wurde, stellen Sie sicher, dass ein E-Mail-Konto mit Kennwort bei einem E-Mail-Anbieter vorhanden ist und Sie die Zugangsdaten für dieses Konto kennen.

Wenn der externe E-Mail-Server so konfiguriert wurde, dass er eine moderne Authentifizierung (Microsoft OAuth 2.0 tokenbasierte Autorisierung) verwendet, wie im Fall von Exchange Online, stellen Sie sicher, dass:

- Das E-Mail-Konto des Absenders muss für die Verwendung von SMTP mit Authentifizierung zugelassen sein (standardmäßig ist diese Option im Microsoft 365-Mandanten inaktiv). Sobald SMTP mit Authentifizierung aktiviert ist, funktioniert die OAUTH 2.0-E-Mail-Weiterleitung normal mit allen OpenScape Business-Mainboards.
- In Microsoft Azure Active Directory (Azure AD) eine Anwendung mit den erforderlichen Berechtigungen registriert wurde, damit Ihr OpenScape Business-System E-Mails versenden kann.
- Sie die Anwendungs- (Client-)ID und die Verzeichnis- (Mandanten-)ID der registrierten Anwendung kennen.

  Bitten Sie Ihren Azure AD-Administrator, diese Werte bei Bedarf bereitzustellen.
- Die E-Mail-Adresse, die als Absender der E-Mails angezeigt wird, gehört zum selben Azure AD oder Mandanten wie die registrierte Anwendung.

Sie befinden Sich im Fenster **E-Mail-Weiterleitung ändern** im Assistenten für die **Grundinstallation**.

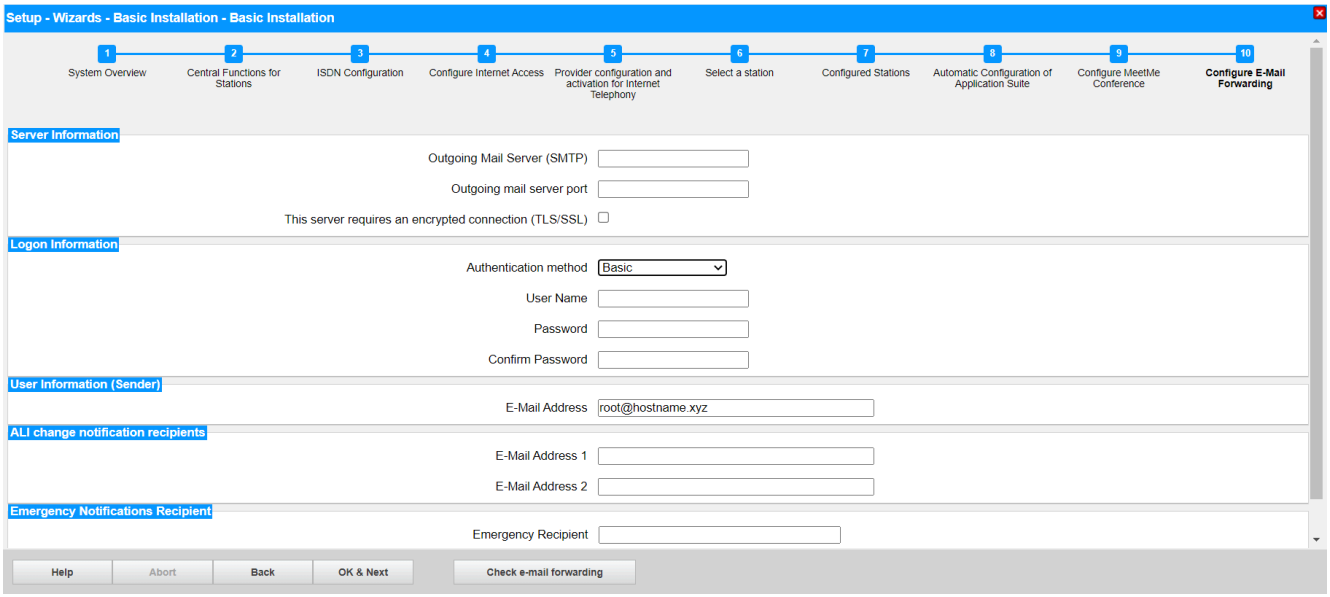


Abbildung 6: Optionen für die E-Mail-Weiterleitung bei Auswahl der einfachen Authentifizierungsmethode

Schritt für Schritt

1) Geben Sie den **Postausgangs-Server (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll, z. B. `smtp.web.de`. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.

   Anmerkung: Achten Sie darauf, dass der Name des Postausgangs-Servers aufgelöst werden kann. Falls nicht, müssen Sie den Assistenten für den E-Mail-Versand starten über **Service-Center** > **E-Mail-Weiterleitung** und anstelle des Namens des Postausgangsservers dessen IP-Adresse eingeben.

   ---

2) Geben Sie den **Postausgangs-Server-Port (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.
3) Wenn eine sichere Verbindung erforderlich ist, aktivieren Sie das Kontrollkästchen **Dieser Server benötigt eine verschlüsselte Verbindung (TLS/SSL)**. Erfragen Sie ggf. bei Ihrem E-Mail-Provider, ob diese Option aktiviert werden muss.
4) Wenn der externe E-Mail-Server für die Verwendung der einfachen Authentifizierung konfiguriert wurde, gehen Sie wie folgt vor:
   a) Wählen Sie in der Dropdown-Liste **Authentifizierungsmethode** die Option **Einfach**.
   b) Geben Sie den **Benutzernamen** des E-Mail-Kontos ein z. B. `max.mustermann`.
   c) Geben Sie unter **Kennwort** und **Kennwort wiederholen** das Kennwort des E-Mail-Kontos ein.

5) Wenn der externe E-Mail-Server so konfiguriert wurde, dass er eine moderne Authentifizierung verwendet, gehen Sie wie folgt vor:

a) Wählen Sie in der Dropdown-Liste **Authentifizierungsmethode** die Option **Microsoft OAuth 2.0**.

b) Geben Sie die Anwendungs- (Client-)ID, die Sie vom Microsoft Azure-Portal erhalten haben, in das Feld **Anwendungs-ID** ein.

c) Geben Sie in das Feld **Mandant** die Verzeichnis- (Mandanten-)ID ein, die Sie vom Microsoft Azure-Portal erhalten haben.

6) Geben Sie die **E-Mail-Adresse** ein, die als Absender der E-Mails erscheinen soll, z. B.: `john.doe@web.de`.

7) Geben Sie die **E-Mail-Adresse 1** ein, um eine Benachrichtigungs-E-Mail zu erhalten, wenn die ALI-Toleranz verwendet wurde. Sie können auch eine zweite E-Mail-Adresse in das Feld **E-Mail-Adresse 2** eingeben.

8) Geben Sie im Feld **Empfänger für Notfälle** die E-Mail-Adresse eines Sicherheitsbeauftragten vor Ort, an den eine E-Mail gesendet wird, wenn eine Notrufnummer gewählt wird.

Der Betreff der E-Mail lautet „Neuer Notruf“. Wenn dies konfiguriert wurde, sind die Rufnummer und der Name des Anrufers, die aus der Datenbank des Systems abgerufen werden, in der E-Mail enthalten.

9) Wenn Sie **Microsoft OAuth 2.0** als Authentifizierungsmethode ausgewählt haben, gehen Sie wie folgt vor:

a) Klicken Sie auf **OK & Weiter**.

b) Warten Sie, bis ein Autorisierungslink und ein Benutzercode erscheinen.

Der Autorisierungscode läuft nach einigen Minuten ab.

c) Öffnen Sie den Autorisierungslink und geben Sie den Benutzercode in das Pop-up-Fenster ein.

d) Melden Sie sich mit der E-Mail-Adresse an, die Sie in Schritt 6 auf Seite 207 **(E-Mail-Adresse**) eingegeben haben.

Die E-Mail-Adresse muss sich im selben Azure AD oder Mandanten befinden wie die registrierte Anwendung.

e) Nach erfolgreicher Authentifizierung zeigt das Pop-up-Fenster eine Meldung wie unten an:

```
Sie haben sich auf Ihrem Gerät bei <application-name>
angemeldet. Sie können dieses Fenster nun schließen.
```

f) Schließen Sie das Pop-up und kehren Sie zum WBM zurück.
Wenn die Authentifizierung erfolgreich war, wird die Meldung `Die Authentifizierung war erfolgreich!` angezeigt.

10) Falls Sie die eingegebenen E-Mail-Einstellungen überprüfen wollen, gehen Sie folgendermaßen vor:

a) Klicken Sie auf **E-Mail-Weiterleitung testen**.
b) Geben Sie unter **Senden an E-Mail-Adresse** die E-Mail-Adresse eines E-Mail-Postfachs ein, auf das Sie Zugriff haben. An diese E-Mail-Adresse wird die Test-E-Mail geschickt.
c) Geben Sie unter **Betreff in der E-Mail** einen beschreibenden Text ein, um die E-Mail in Ihrem E-Mail-Postfach identifizieren zu können.
d) Klicken Sie auf **Testmail senden**. Die E-Mail-Einstellungen werden überprüft und die E-Mail an das angegebene E-Mail-Postfach gesendet.
e) Überprüfen Sie, ob die E-Mail in Ihrem E-Mail-Postfach angekommen ist.
f) War der E-Mail-Versand erfolgreich, klicken Sie auf **Zurück** und gehen Sie zum nächsten Schritt.
g) War der E-Mail-Versand nicht erfolgreich, klicken Sie auf **Zurück** und überprüfen nochmal Ihre E-Mail-Einstellungen.

11) Klicken Sie auf **OK & Weiter** und anschließend auf **Fertig**. Die Basisinstallation ist beendet. Bevor Sie die im Wizard erwähnte Datensicherung durchführen, sollten Sie die Lizenzen aktivieren.

5.8 Abschließende Tätigkeiten

Nachdem die Erstinstallation und die Basisinstallation mit dem WBM abgeschlossen sind, müssen noch einige wichtige Einstellungen für den Betrieb von OpenScape Business getroffen werden.

Gehen Sie folgendermaßen vor:

1) Lizenzen aktivieren und zuordnen

Die mit OpenScape Business erworbenen Lizenzen müssen innerhalb einer Zeitspanne von 30 Tagen aktiviert werden. Die Zeitspanne startet beim ersten Anmelden am WBM. Nach Ablauf der Zeitspanne ist das Kommunikationssystem nur noch eingeschränkt nutzbar. Nach erfolgreicher Aktivierung müssen die Lizenzen den Teilnehmern und Leitungen zugeordnet werden. Systemweite Leistungsmerkmale sind in einem Standalone-System bereits mit der Aktivierung freigeschaltet.

2) UC Smart Client zur Installation bereitstellen (nur für UC Smart)

3) Wie Sie UC Suite Clients zur Installation bereitstellen (nur für UC Suite)

Die UC Suite Clients sind Bestandteil von UC Suite. Die Installationsdateien für die UC Clients sind über das WBM zugänglich und können den IP-Teilnehmern automatisch oder manuell zur Verfügung gestellt werden.

Zusätzlich gibt es für den Administrator die Möglichkeit der Silent Installation. Dabei handelt es sich um eine kommandozeilenbasierte Methode zur automatischen Installation, Deinstallation und Modifikation von UC Suite Clients auf einem PC ohne weitere erforderliche Eingaben. Weitere Informationen finden Sie unter Silent Installation/Deinstallation für UC Suite PC-Clients.

4) Datensicherung durchführen

Die bisherigen Änderungen an OpenScape Business müssen gesichert werden. Die Sicherung kann als Backup-Set z.B. auf einem USB-Medium oder im internen Netz gespeichert werden.

5.8.1 Wie Sie die Lizenzen aktivieren und zuordnen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Sie kennen den LAC (Lizenz-Autorisierungscode) für die Lizenzfreischaltung und haben eine Benutzerkennung und ein Passwort für den Zugang zum Lizenzserver.

Für die Verbindung zum Lizenzserver ist ein Internet-Zugang nötig.

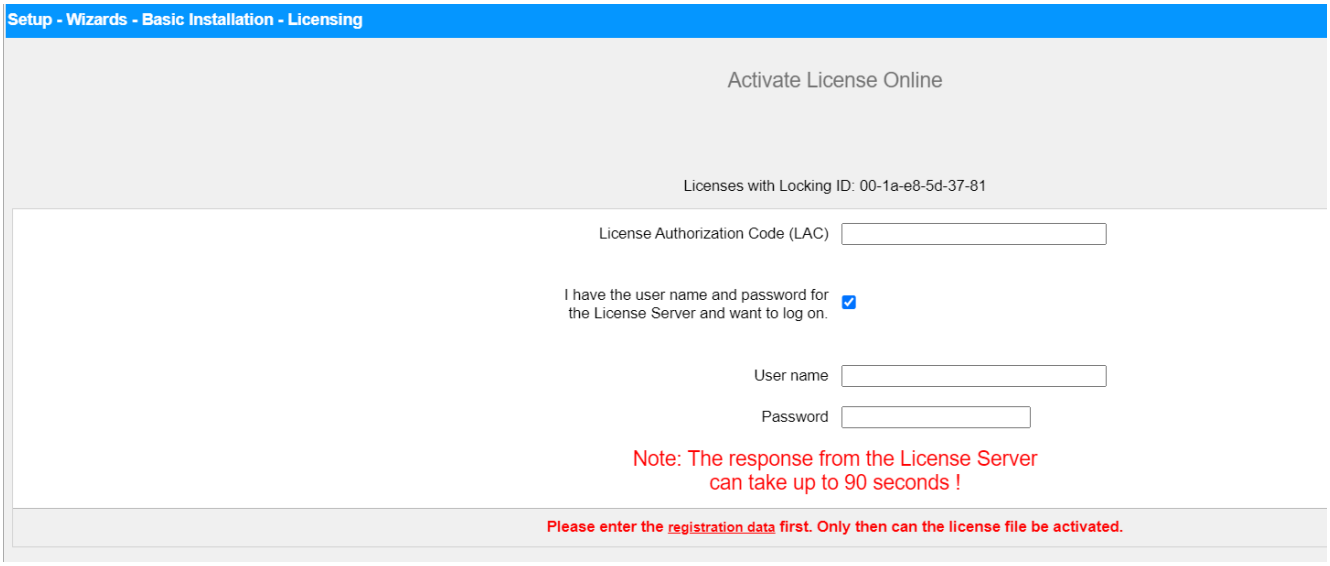
Schritt für Schritt

1) Lizenzen online aktivieren:

a) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

b) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.

c) Klicken Sie auf **Bearbeiten**, um den Wizard **Lizenzierung** zu starten.



d) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.

e) Aktivieren Sie das Kontrollkästchen **Ich habe Benutzernamen und Passwort für den Lizenzserver und möchte mich anmelden**.

f) Geben Sie **Benutzername** und **Passwort** für die Anmeldung am Lizenzserver ein.

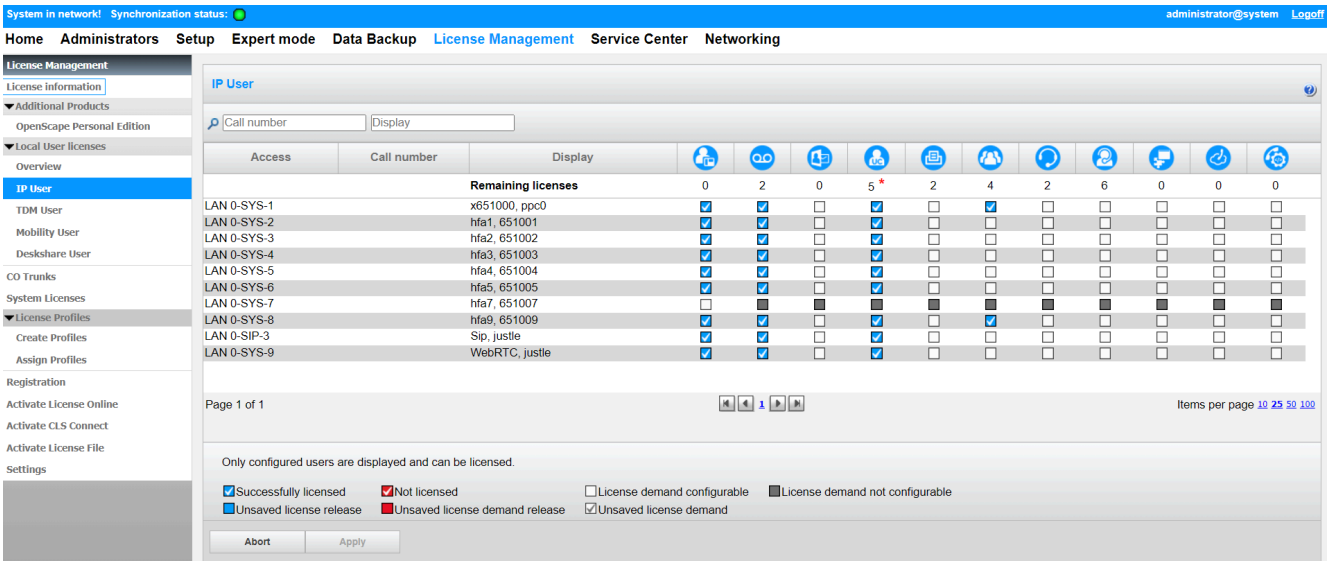
g) Klicken Sie auf **OK & Weiter**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen freigeschaltet.

2) Lizenzen den Teilnehmern zuordnen:

a) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

b) Navigieren Sie im Navigationsbaum unter **Lokale Benutzerlizenzen** > **...** zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.

c) Aktivieren Sie in der Zeile des gewünschten Teilnehmers das Kontrollkästchen in der Spalte **Benutzer-Lizenz** (erste Spalte mit Kontrollkästchen).



d) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.

Anmerkung: User-orientierte Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz (Benutzer-Lizenz) zugeordnet wurde (Schritt c).

---

e) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.

Sind ausreichend Lizenzen vorhanden ist die Lizenzierung der Teilnehmer beendet.

f) Fehlen Lizenzen, werden Ihnen die Fehler mit rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt e.

3) Lizenzen den Leitungen zuordnen:

a) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich **Amtsleitungen** wird Ihnen die Anzahl der erworbenen Leitungslizenzen angezeigt.

b) Für SIP-Leitungen: Geben Sie im Bereich **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der

Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.

c) Für S_{2M}-Leitungen: Wählen Sie im Bereich **S2M** in der Zeile des gewünschten Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.

d) Für T1-Leitungen (nur USA): Wählen Sie im Bereich **T1** in der Zeile des gewünschten Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.

e) Klicken Sie auf **OK & Weiter**.

Anmerkung: Die Anzahl der lizenzierten SIP- und S_{2M}/T1-Leitungen darf die Anzahl der erworbenen Leitungslizenzen nicht überschreiten.

5.8.2 Wie Sie den UC Smart Client zur Installation bereitstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Hard- und Software für die Nutzung von UC @work ist vorhanden.

Anmerkung: Für die Nutzung des UC Smart Clients myPortal @work sind Lizenzen erforderlich.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Software**.

3) Klicken Sie auf das Download-Symbol von **myPortal @work** und speichern Sie die Installationsdatei auf einem freigegebenen Netz-Laufwerk.

4) Senden Sie den Benutzern von myPortal @work die beiden Installationsdateien.

5) Alternativ können Sie den Benutzern von myPortal @work auch den Link zuschicken, über den sie direkt auf die Installationsdatei zugreifen können:

```
https://<IP-Adresse des Kommunikationssystems>/
management/downloads/myPortalAtWorkSetup.exe
```

5.8.3 Wie Sie die UC Suite Clients zur Installation bereitstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Hard- und Software für die Nutzung von UC Suite ist vorhanden.

Anmerkung: Für die Nutzung der UC Suite Clients sind Lizenzen nötig.

Schritt für Schritt

1) Damit die Installationsdateien einem Teilnehmer automatisch zur Verfügung gestellt werden können, vergewissern Sie sich, ob folgende Schritte durchgeführt worden sind:

a) Die E-Mail-Adressen der Teilnehmer müssen entweder zusammen mit den Teilnehmerdaten über eine XML-Datei importiert worden sein oder eingetragen werden unter **Einrichtung** > **UC Suite** > **Benutzerverzeichnis**.

b) Ein Mail-Server muss eingetragen sein.

Anmerkung: Einen E-Mail-Server können Sie auch nachträglich eintragen unter **Service-Center** > **Email-Weiterleitung**.

Alle Teilnehmer, deren E-Mail-Adressen bekannt sind, erhalten eine E-Mail mit dem Link auf das Installationsverzeichnis der UC Clients und mit einer Erste-Schritte-Anleitung. Im Installationsverzeichnis liegt zusätzlich eine Readme-Datei mit Informationen zur Installation der Software auf den Client-PCs.

2) Falls die nötigen Schritte für eine automatische Benachrichtigung nicht erfüllt sind, können Sie die Installationsdateien auch manuell zur Verfügung stellen. Gehen Sie dazu folgendermaßen vor:

a) Klicken Sie in der Navigationsleiste auf **Service-Center**.

b) Klicken Sie im Navigationsbaum auf **Software**.

c) Klicken Sie auf den gewünschten UC Client und speichern Sie die gezippte Installationsdatei auf einem freigegebenen Netz-Laufwerk.

d) Klicken Sie im Navigationsbaum auf **Dokumente** und wählen Sie die Aufklappliste **Bedienungsanleitung**.

e) Klicken Sie auf die Dokumentation zum gewünschten UC Client und speichern Sie die Dokumentationsdatei auf einem freigegebenen Netz-Laufwerk.

f) Senden Sie den Benutzern der UC Clients die gezippte Installationsdatei und die Dokumentationsdatei per E-Mail oder teilen Sie den Benutzern den Ablageort der Dateien mit.

g) In der Zip-Datei mit den Installationsdateien ist auch eine Readme-Datei enthalten. Weisen Sie die Benutzer darauf hin, dass die Installation der UC Clients anhand der Installationshinweise in der Readme-Datei durchgeführt werden muss.

3) Alternativ können Sie den UC Benutzern auch Links zuschicken, über die sie direkt auf die Installationsdateien der UC Clients zugreifen können.

a) Klicken Sie in der Navigationsleiste auf **Service-Center**.

b) Klicken Sie im Navigationsbaum auf **Software**.

c) Klicken Sie auf die Schaltfläche **Applikationslinks anzeigen**. Es werden Ihnen mehrere Links angezeigt, abhängig vom verwendeten Betriebssystem und vom gewünschten UC Client. Zum Beispiel:

```
https://<IP-Adresse des Kommunikationssystems>/
management/downloads/install-common.zip
```

5.8.4 Wie Sie eine Datensicherung durchführen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Für eine Datensicherung auf einem USB-Medium (USB-Stick oder USB-Festplatte) muss das USB-Medium an der USB-Server-Schnittstelle angeschlossen sein.

Anmerkung: Weitere Informationen zur Datensicherung siehe Sofortiges Sichern .

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup - sofort**.
3) Geben Sie im Bereich **Name** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.
4) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.
5) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.
6) Die Sicherung ist erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt!** erscheint. Klicken Sie auf **Beenden**.
7) Wenn Sie als Backup-Medium einen USB-Stick verwenden, warten Sie ab, bis die LED des USB-Sticks aufhört zu blinken. Erst dann ist die Sicherung erfolgreich auf dem USB-Stick gespeichert. Entfernen Sie anschließend den USB-Stick.
8) Die Erstinbetriebnahme mit dem WBM ist nun abgeschlossen. Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

Anmerkung: Falls eine neue Software-Version für das Kommunikationssystem vorliegt, wird Ihnen das auf der Startseite des WBM mitgeteilt - vorausgesetzt der Internet-Anschluss ist korrekt eingerichtet. Liegt eine neue Software-Version vor, führen Sie ein Update durch (siehe Update des Kommunikationssystems).

5.9 Inbetriebnahme der IP-Telefone

Eine komfortable Inbetriebnahme der IP-Telefone erfordert einen DHCP-Server, der das IP-Telefon mit den für die Anmeldung am Kommunikationssystem wichtigen Daten (netzwerkspezifische Daten) versorgt.

Netzwerkspezifische Daten

Ein IP-Telefon benötigt für die Anmeldung am Kommunikationssystem netzwerkspezifische Daten. Diese Daten können einerseits im DHCP-Server

gespeichert sein oder direkt am IP-Telefon eingegeben werden. Vorteil eines DHCP-Servers ist, dass alle angeschlossenen IP-Telefone automatisch mit den Daten versorgt werden.

Folgende Daten werden vom IP-Telefon benötigt:

- IP-Adresse des Kommunikationssystems
- IP-Adresse des DLS-Servers

Zusätzlich benötigt das IP-Telefon noch die eigene Rufnummer. Diese muss während der Anmeldung manuell am Telefon eingetragen werden.

Registrierung von SIP-Telefonen

Aus Sicherheitsgründen ist es empfehlenswert, dass sich SIP-Telefone am Kommunikationssystem registrieren. Dazu müssen die Registrationsdaten am IP-Telefon und im Kommunikationssystem übereinstimmen.

Folgende Daten werden für die Anmeldung benötigt:

- SIP-Benutzer-ID
- SIP-Passwort
- SIP-Realm (optional)

Verwenden Sie ein nicht triviales SIP-Passwort, das folgende Regeln erfüllt:

- Mindestens 8 Stellen
- Mindestens einen Großbuchstaben (A - Z)
- Mindestens einen Kleinbuchstaben (a - z)
- Mindestens eine Ziffer (0-9)
- Mindestens ein Sonderzeichen

Verwenden Sie eine SIP-Benutzer-ID, die nicht die Telefonnummer enthält.

Anmerkung: Weitere Informationen zur Einrichtung von SIP-Telefonen finden Sie unter `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Nutzung des internen DHCP-Servers

Wird der interne DHCP-Server des Kommunikationssystems genutzt, sind die netzwerkspezifischen Daten dort bereits hinterlegt. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, muss am IP-Telefon nur die festgelegte Rufnummer eintragen werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

Nutzung eines externen DHCP-Servers mit netzwerkspezifischen Daten

Wird ein externer DHCP-Server genutzt, sind die netzwerkspezifischen Daten dort zu hinterlegen. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, muss am IP-Telefon nur die festgelegte Rufnummer eintragen werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

Nutzung eines externen DHCP-Servers ohne netzwerkspezifische Daten

Wird ein externer DHCP-Server genutzt, bei dem die netzwerkspezifischen Daten nicht hinterlegt werden können, müssen diese am IP-Telefon eingegeben werden. Damit sich ein IP-Telefon am Kommunikationssystem registrieren

kann, müssen am IP-Telefon die festgelegte Rufnummer und die IP-Adresse des Kommunikationssystems eintragen und evtl. die Einstellungen für den Deployment Service geändert werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

5.9.1 Wie Sie ein IP-Telefon konfigurieren

Voraussetzungen

Das IP-Telefon ist an das interne Netz angeschlossen und betriebsbereit.

Anmerkung: Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 IP-Systemtelefons beschrieben. Für ein anderes IP-Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres IP-Telefons nach.

Schritt für Schritt

1) Um in den Administrationsmodus des IP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.

2) Blättern Sie im Register `Einstellungen` bis `Admin` und bestätigen Sie mit der OK-Taste.

3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.

4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.

5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des IP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für IP-Systemtelefone. Gehen Sie folgendermaßen vor:

a) Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
b) Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
c) Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.
d) Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
f) Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.
g) Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.
h) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
i) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
j) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

6) Legen Sie die Rufnummer des Telefons fest:
   a) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
   b) Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.
   c) Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.
   d) Geben Sie die festgelegte Rufnummer ein (z.B. `120`) und bestätigen Sie mit der OK-Taste.
   e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
7) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.
8) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

5.9.2 Wie Sie ein SIP-Telefon konfigurieren

Voraussetzungen

Das SIP-Telefon ist an das Kunden-LAN angeschlossen und betriebsbereit.

Anmerkung: Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 SIP-Systemtelefons beschrieben. Für ein anderes SIP-Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres SIP-Telefons nach.

Schritt für Schritt

1) Um in den Administrationsmodus des SIP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.
2) Blättern Sie im Register `Einstellungen` bis `Administrator (Admin)` und bestätigen Sie mit der OK-Taste.
3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.
4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.
5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des SIP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für SIP-Systemtelefone. Gehen Sie folgendermaßen vor:
   a) Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
   b) Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
   c) Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.

d) Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
f) Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.
g) Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.
h) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
i) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
j) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

6) Legen Sie die SNTP-Zeiteinstellungen fest:
a) Blättern Sie bis `Date and time` und bestätigen Sie mit der OK-Taste.
b) Blättern Sie bis `Time source` und bestätigen Sie mit der OK-Taste.
c) Blättern Sie bis `SNTP IP address` und bestätigen Sie mit der OK-Taste.
d) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
e) Blättern Sie bis `Timezone offset` und bestätigen Sie mit der OK-Taste.
f) Geben Sie die Abweichung der lokalen Uhrzeit von der UTC-Zeit (Universal Time Coordinated) in Stunden an (Deutschland: `1`) und bestätigen Sie mit der OK-Taste.
g) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
h) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

7) Legen Sie die Rufnummer des Telefons fest:
a) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
b) Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.
c) Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.
d) Geben Sie die festgelegte Rufnummer ein (z.B. `120`) und bestätigen Sie mit der OK-Taste.
e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

8) Legen Sie die SIP-Authentifizierungsdaten fest:
a) Blättern Sie bis `Registration` und bestätigen Sie mit der OK-Taste.
b) Blättern Sie bis `SIP session` und bestätigen Sie mit der OK-Taste.
c) Notieren Sie sich die `Realm` oder geben Sie bei Bedarf eine neue Realm (z.B. `OSBIZ-SIP`) ein.
d) Notieren Sie sich die `User ID` oder geben Sie bei Bedarf eine neue User ID (z.B. `SIP-120`) ein.
e) Vergeben Sie ein `Passwort` für die Registrierung am SIP Server.
f) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

9) Navigieren Sie mit der Zurück-Taste zum Menü `Admin` zurück.

10) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

5.10 Diagnose-Traces für einen Fehlerfall erfassen

Sie können automatisch die erforderlichen Diagnose-Traces für einen Fehlerfall erfassen. Der Wizard **Fehlermanagement** führt Sie durch den gesamten Prozess.

Sie müssen den **Fehlermanagement**-Wizard zweimal ausführen: vor und nach der Ausführung des problematischen Szenarios. Beim ersten Durchlauf (Phase 1) aktivieren Sie die Erfassung von Diagnose-Traces. Nach der Ausführung des problematischen Szenarios führen Sie den Assistenten erneut aus, um die Diagnose-Trace-Daten zu sammeln (Phase 2). Sobald Phase 2 abgeschlossen ist, können Sie die Trace-Datei herunterladen und in das Ticketsystem aufnehmen.

Führen Sie die folgenden Schritte durch, um die Diagnose-Trace-Daten für den Fehlerfall zu erfassen:

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten** neben **Fehlermanagement**.
3) Klicken Sie auf **OK & Weiter**.
4) Wenn Sie die Standard-Traces erfassen möchten, klicken Sie auf das Kontrollkästchen **Standard-Traces** .
5) Wenn Sie die Art der zu erfassenden Traces angeben möchten, wählen Sie die gewünschten Traces aus der entsprechenden Liste aus. Mehr als eine Auswahl ist möglich.

   Weitere Informationen zu Traces finden Sie im Handbuch zur Problembehebung.
6) Klicken Sie auf **OK & Weiter**.
7) Eine Liste mit zusätzlichen Informationen, relevanter Dokumentation und Hinweisen wird angezeigt. Klicken Sie auf **OK & Weiter**.
8) Die Szenarien und der Typ der Traces, die Sie erfassen möchten, werden angezeigt. Klicken Sie auf **Fertig**.
9) Fahren Sie mit der Ausführung des problematischen Szenarios fort.
10) Navigieren Sie nach Abschluss des Szenarios erneut zu **Setup > Fehlermanagement** und klicken Sie auf **Bearbeiten**.

    Sie werden zu Schritt 2 der Erfassung von Diagnose-Traces weitergeleitet. Wenn Sie den Prozess anhalten und erneut starten möchten, klicken Sie auf die Schaltfläche **Abbrechen**.
11) Klicken Sie auf **OK & Weiter**.
12) Geben Sie die erforderlichen Informationen ein und klicken Sie auf **OK & Weiter**.
13) Eine Liste mit den erforderlichen Informationen und einigen weiteren Aktionen wird angezeigt.
14) Klicken Sie auf **OK & Weiter**.
15) Klicken Sie auf **Fertigstellen** , um mit dem Herunterladen der Diagnose-Trace-Daten zu beginnen.

5.11 Neuflash

Mit den folgenden Schritten können Sie den Softwaretyp eines Geräts leicht ändern.

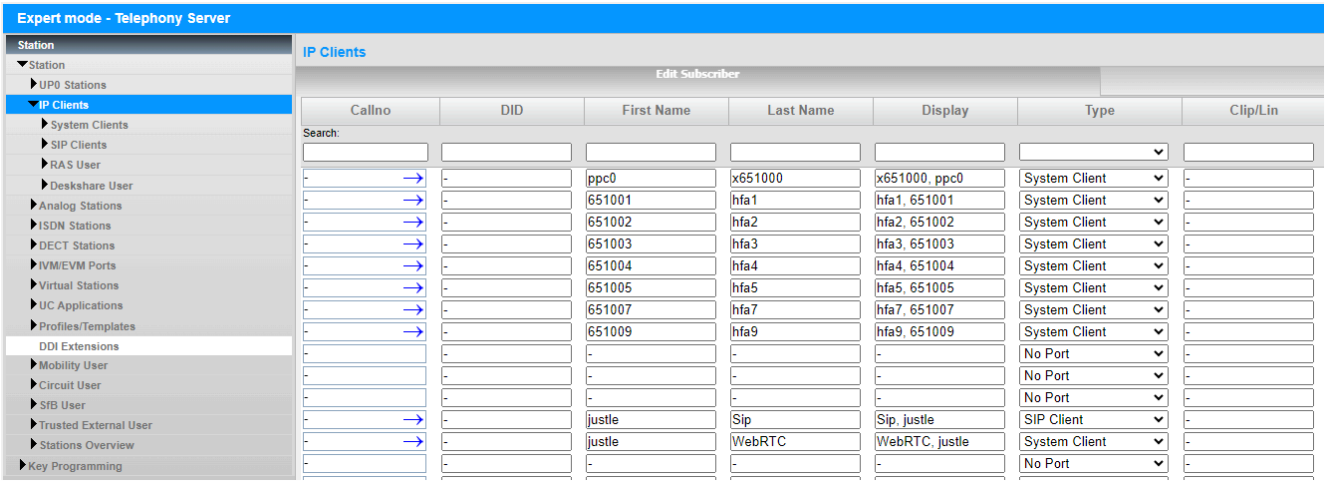
Das Konzept hinter diesem Merkmal ist es, die Art und Weise zu vereinfachen, ein SIP-Gerät (out of the box) zu bekommen und es im OSBiz-System als HFA-Gerät zu registrieren. Die einzigen Anforderungen sind:

- das Telefon muss die DLI-Adresse erhalten (entweder vom DHCP-Server oder manuell)
- der Administrator muss die Nummer des Telefons eingeben (das als System Client vorkonfiguriert sein muss)

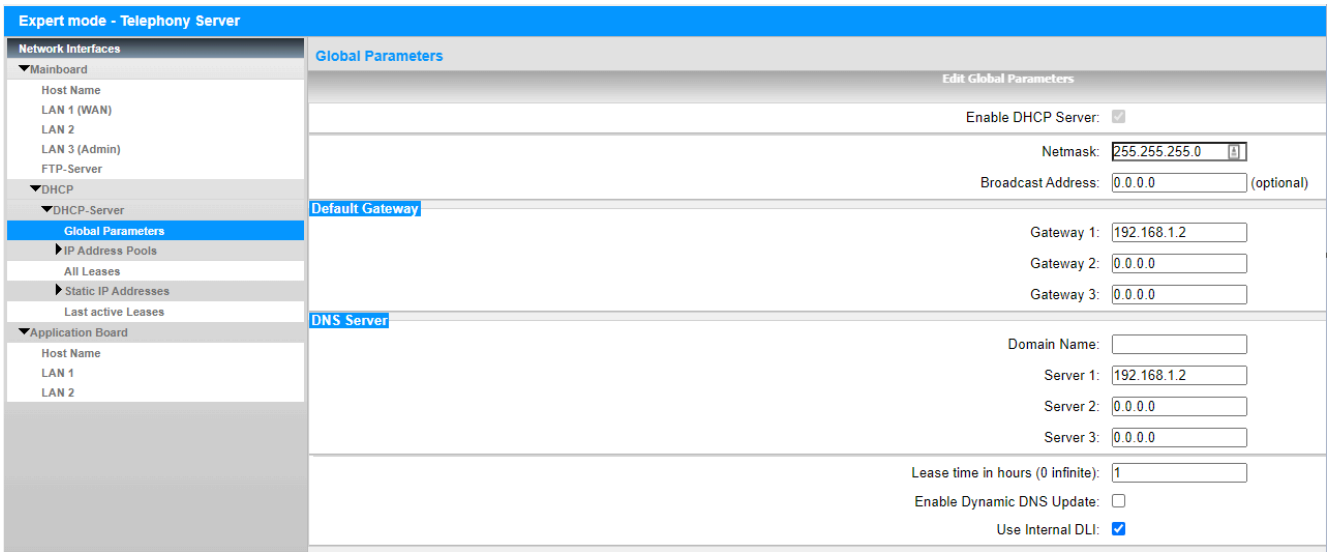
Sobald der Kunde ein neues Gerät erhält, wird es als SIP-Gerät vorkonfiguriert (Werkseinstellungen). Die Schritte zum Neuflashen dieses Geräts auf ein HFA-Gerät sind wie folgt:

Schritt für Schritt

1) Konfigurieren Sie in der OSBIZ-Datenbank die gewünschte Rufnummer als System Client (HFA).



2) Konfigurieren Sie den DHCP-Server, um die IP-Adresse des DLI zu senden. Dies kann entweder über den externen DHCP-Server oder den internen DHCP-Server erfolgen.



3) Wenn kein DHCP-Server verwendet wird, müssen Sie die DLI-IP auf dem Telefon manuell konfigurieren.

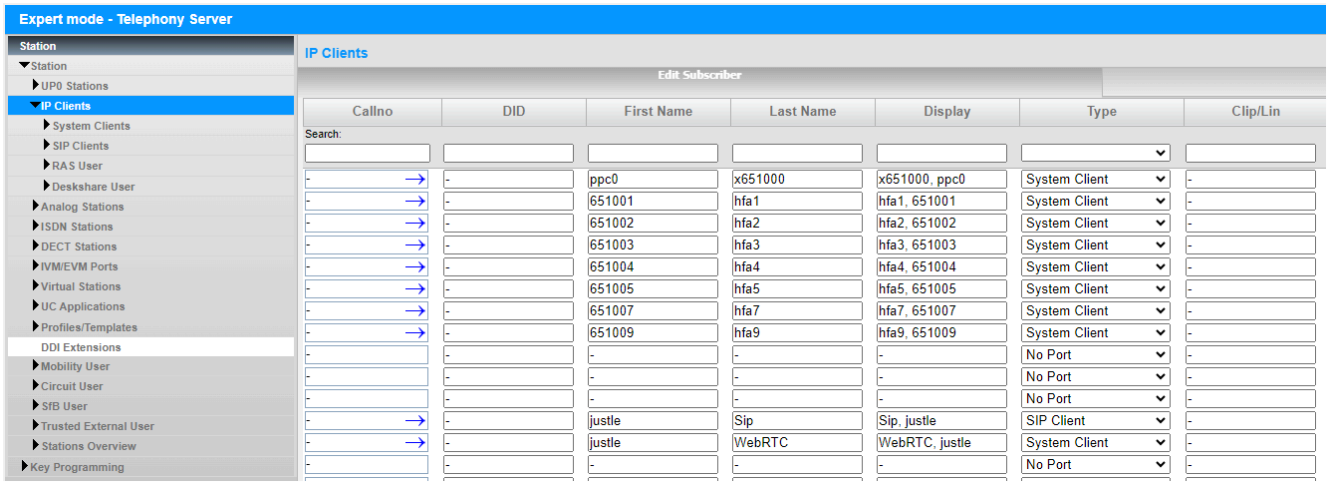
4) Sobald das SIP-Telefon eine IP und die DLI-IP erhalten hat, wird das Telefongerät in der DLI-Datenbank registriert, und es wird eine Aufforderung zur Eingabe der Nebenstellennummer angezeigt.

5) Geben Sie die Endgerätnummer am Telefon ein (die Nummer sollte dieselbe wie die im ersten Schritt konfigurierte sein, z. B. 4111).

6) Der Neuflash wird gestartet und das neue HFA-Image wird auf das Telefon heruntergeladen. Wenn das Telefon neu gestartet wird, wird es als HFA-Telefon registriert und die Plug-and-Play-Daten werden vom System an das Telefon gesendet.

7) **Um ein bereits registriertes SIP-Telefon neu zu flashen:**

8) Ändern Sie das SIP-Arbeitsgerät in "System Client".



9) Starten Sie das Telefon neu

10) Der Neuflash wird gestartet und das neue HFA-Image wird auf das Telefon heruntergeladen. Wenn das Telefon neu gestartet wird, wird es als HFA-

Telefon registriert und die Plug-and-Play-Daten werden vom System an das Telefon gesendet.

6 Ersteinrichtung von OpenScape Business S

Beschrieben wird die Ersteinrichtung von OpenScape Business S (kurz Softswitch genannt). Der Softswitch und die zugehörenden Komponenten werden in das bestehende Kunden-LAN integriert. Es werden der Internet-Zugang für die Internet-Telefonie eingerichtet und die angeschlossenen Teilnehmer konfiguriert.

Für OpenScape Business S ist die OpenScape Business-Kommunikationssoftware auf dem Linux Betriebssystem SLES 12 SP5 64-Bit oder SLES 15 SP6 64-Bit installiert. Die Kommunikationssoftware kann direkt auf einem Linux-Server oder in einer virtuellen Umgebung mit VMware vSphere oder Microsoft Hyper-V betrieben werden. Die Installation des Linux-Betriebssystems ist beschrieben in der Installationsanleitung *OpenScape Business, Installation Linux Server*.

Die Ersteinrichtung von OpenScape Business S wird mit dem Administrationsprogramm OpenScape Business Assistant (Web-based Management, kurz WBM genannt) durchgeführt.

Beschrieben wird die Konfiguration der am häufigsten verwendeten Komponenten. Nicht alle dieser Komponenten werden bei Ihnen zum Einsatz kommen. Daher werden Sie bei der Ersteinrichtung an einigen Stellen zwischen mehreren Möglichkeiten wählen oder Konfigurationen sogar ganz überspringen müssen, je nachdem, welche Komponenten bei Ihnen Anwendung finden.

Die ausführliche Administration der über die Ersteinrichtung hinausgehenden Leistungsmerkmale finden Sie in den anschließenden Kapiteln.

Voraussetzung für die Ersteinrichtung ist die Erstellung eines IP-Adress-Schemas und eines Rufnummernplans.

Übersicht über die wichtigsten Installationsschritte:

- Systemeinstellungen
- Systemrufnummern und Vernetzung
- Internet-Telefonie
- Teilnehmerkonfiguration
- Lizenzierung
- Systemhärtung
- Datensicherung

6.1 Voraussetzungen für die Ersteinrichtung

Die Erfüllung der Voraussetzungen für die Ersteinrichtung stellt den ordnungsgemäßen Betrieb von OpenScape Business S sicher.

Allgemein

Je nach verwendeter Hardware (Telefone, ...) und bestehender Infrastruktur gelten folgende Rahmenbedingungen:

- Die LAN-Infrastruktur (Internet-Router, Switches, etc.) ist vorhanden und nutzbar.
- Die IP-Telefone sind mit dem Kunden-LAN verbunden.

- Der für OpenScape Business S erforderliche Linux-Server wurde gemäß den Anweisungen im *OpenScape Business Linux-Server-Installationshandbuch* installiert und in das Kunden-LAN integriert und ist einsatzbereit.
- Alle für OpenScape Business S erforderlichen Lizenzen sind vorhanden (z.B. UC-Clients, Directory Services, etc.).
- Ein IP-Adressschema existiert und ist bekannt.
- Ein Wählplan (auch Nummerierungsplan genannt) ist vorhanden und bekannt.

Software

Für die Installation von OpenScape Business S ist die folgende Software erforderlich:

- DVD oder .ISO-Image mit der OpenScape Business-Kommunikationssoftware

  Enthält die OpenScape Business-Kommunikationssoftware. Diese DVD oder .ISO-Image ist im Lieferumfang enthalten.
- DVD oder USB-Stick mit Linux-Betriebssystem SLES 12 SP5 oder SLES 15 SP6.

  Die Linux-DVD wird möglicherweise während der Installation der OpenScape Business-Kommunikationssoftware benötigt, da einige für die Kommunikationssoftware erforderliche Softwarepakete (RPM) möglicherweise später von dieser DVD oder .ISO-Image installiert werden müssen.

Administration

Für die Ersteinrichtung von OpenScape Business S mit dem OpenScape Business Assistant (WBM) kann der Linux Server oder der Admin PC verwendet werden. Der WBM ist browserbasiert und somit unabhängig vom Betriebssystem.

- Webbrowser:

  Die folgenden HTML 5-fähigen Webbrowser werden unterstützt:

  – Microsoft Internet Explorer Version 11 und höher (Admin PC).
  – Microsoft Edge
  – Mozilla Firefox Version 37.x und 38.x
  – Mozilla Firefox ESR Version 24.x und 31.x
  – Google Chrome

  Wenn eine ältere Version des Webbrowsers installiert ist, müssen Sie eine aktuelle Version installieren, bevor Sie mit der Ersteinrichtung des Systems beginnen können.
- Java:

  Oracle Java 8 oder höher oder alternativ OpenJDK 8 muss installiert sein. Wenn eine ältere Version installiert ist, müssen Sie sie auf die neueste Version aktualisieren, bevor Sie das System zum ersten Mal einrichten können.

- Bildschirmauflösung: 1024x768 oder höher

Firewall

Bei Verbindung mit dem Internet wird eine Firewall für den Linux-Server benötigt, um unbefugten Zugriff von außen zu verhindern. Nach der Installation von Linux ist die Linux Firewall aktiviert. Das Installationsprogramm der Kommunikationssoftware passt die Firewall-Einstellungen so an, dass die Kommunikationssoftware ordnungsgemäß betrieben werden kann. Die Ports für die Kommunikationssoftware werden geöffnet und alle anderen Ports sind geschlossen.

Wenn eine externe Firewall im Netzwerk verwendet wird, muss die Linux Firewall deaktiviert und die für die Kommunikationssoftware erforderlichen Adressen und Ports geöffnet werden (siehe Verwendete Ports).

Internetzugang

Der Server-PC muss über einen Breitband-Internetzugang für verfügen:

- Sicherheitspatches und allgemeine Linux-Software-Updates

OpenScape Business erfordert eine Internetverbindung für:

- OpenScape Business-Software-Updates
- OpenScape Business-Merkmale wie z.B. Internettelefonie
- OpenScape Business Mobility Clients wie z.B. myPortal to go
- Remote Service

E-Mail-Server (optional)

OpenScape Business erfordert Zugriff auf einen E-Mail-Server für den Versand von E-Mails. Dazu müssen die Zugangsdaten zum E-Mail-Server in OpenScape Business eingegeben und die entsprechenden Accounts (IP-Adresse, URL, Anmeldedaten des E-Mail-Servers) im E-Mail-Server eingerichtet werden.

Wenn die E-Mail-Funktionalität innerhalb von OpenScape Business nicht verwendet wird, müssen diese Daten nicht eingegeben werden.

Internettelefonie, VoIP (optional)

Wenn Internettelefonie innerhalb von OpenScape Business verwendet wird, erfordert OpenScape Business Breitbandzugang zum Internet und einen Internettelefonie-Dienstanbieter (ITSP, SIP-Anbieter) für SIP-Telefonie über das Internet. Dazu müssen die entsprechenden Konten vom ITSP erhalten und die Zugangsdaten für den ITSP (IP-Adresse, URL, Anmeldedaten des SIP-Anbieters) in OpenScape Business eingerichtet werden.

Zweiter LAN-Port

Besitzt OpenScape Business S (bzw. der Linux-Server) einen zweiten LAN-Anschluss, können Sie diesen als WAN-Schnittstelle für den Internet-Zugang und für die Internet-Telefonie über ITSP einrichten. Der erste LAN-Anschluss dient wie gewohnt als LAN-Schnittstelle für die internen Telefone und PCs. Die Konfiguration des Internetzugangs erfolgt im externen Internetrouter des Kunden-LAN. Das Setup des zweiten LAN-Ports erfolgt direkt während der Ersteinrichtung von Linux oder kann später mit YaST durchgeführt werden. Im WBM muss lediglich der zweite LAN-Port als WAN-Schnittstelle aktiviert werden.

Fax als PDF

Sollen Faxe im PDF-Format gespeichert werden, erfordert der Server-PC mindestens 4 GB RAM. Wird OpenScape Business S in einer virtuellen Umgebung betrieben, muss der virtuellen Maschine auch 4GB RAM zugewiesen werden.

6.2 Komponenten

Die Komponenten des Installationsbeispiels sind im Folgenden beschrieben und skizziert.

Das Installationsbeispiel umfasst folgende Komponenten:

- OpenScape Business S

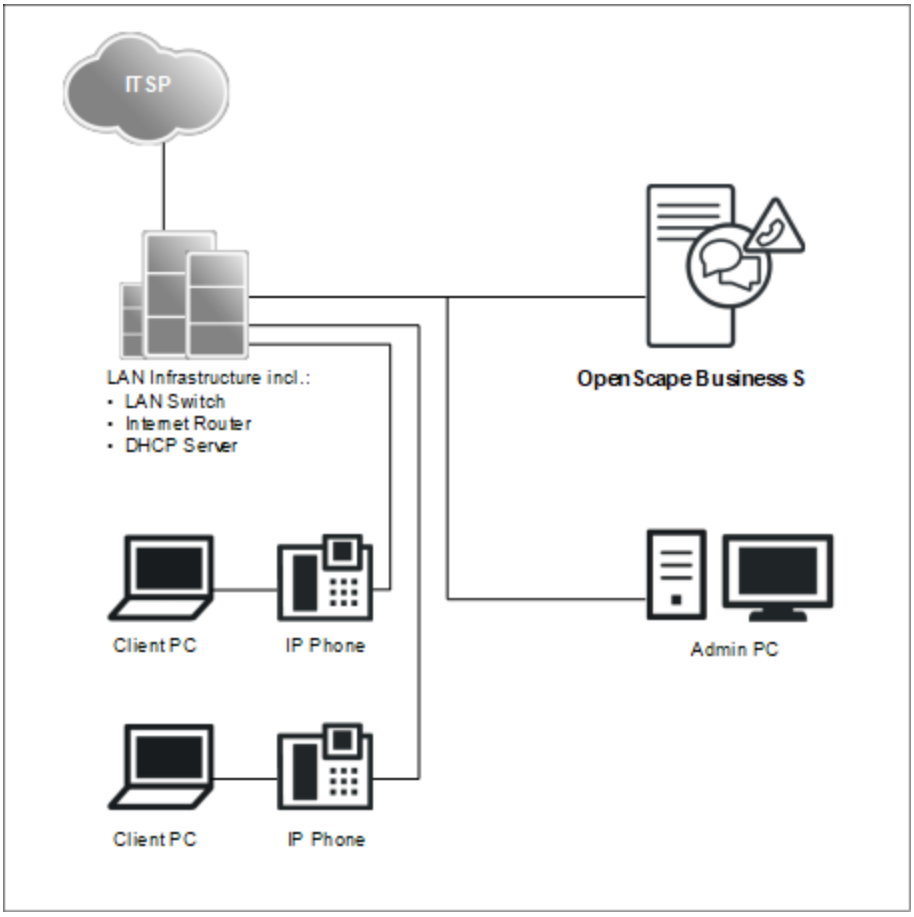
  Der Linux-Server mit der OpenScape Business S Kommunikationssoftware wird über seine LAN-Schnittstelle in das vorhandene Kunden-LAN eingebunden.
- Admin-PC

  Der Admin-PC wird ebenfalls über seine LAN-Schnittstelle in das vorhandene Kunden-LAN intergriert.
- IP-Teilnehmer (IP-Clients)

  Die IP-Teilnehmer (IP-Systemtelefone, Client-PCs, WLAN Access Points, ...) sind über einen oder mehrere Switches im LAN integriert.

Die IP-Clients erhalten ihre IP-Adressen dynamisch von einem internen DHCP-Server (DHCP-Server des Linux-Servers) oder von einem externen DHCP-Server (z.B. DHCP-Server des Internet-Routers).

Der Internet-Zugang ist im Internet-Router konfiguriert.



6.3 IP-Adressen-Schema

Ein IP-Adressen-Schema ist eine Festlegung, wie die IP-Adressen im Kunden-LAN vergeben sind. Es beinhaltet die IP-Adressen von PCs, Servern, Internet-Routern, IP-Telefonen usw.

Für eine bessere Übersicht bei der Zuordnung von IP-Adressen sollte ein IP-Adressen-Schema erstellt werden.

Beispiel eines IP-Adressen-Schemas mit dem IP-Adressband `192.168.5.x`:

IP-Adressbereich	Clients
192.168.5.1 bis **192.168.5.49**	Clients mit fester IP-Adresse
192.168.5.1	Internet-Router (Gateway)
192.168.5.10	Server-PC (OpenScape Business S)
192.168.5.20	E-Mail-Server
192.168.1.50 bis **192.168.1.254**	Client-PCs & IP-Telefone, zugleich IP-Adressband des DHCP-Servers, Zuweisung der IP-Adressen an die Clients erfolgt dynamisch

6.4 Rufnummernplan

Ein Rufnummernplan ist eine Liste aller im Kommunikationssystem verfügbaren Rufnummern. Er beinhaltet interne Rufnummern, Durchwahlnummern und Gruppenrufnummern.

Standard-Rufnummernplan

Die internen Rufnummern sind mit Standardwerten vorbelegt. Diese Werte können bei Bedarf an die eigenen Belange angepasst werden (individueller Rufnummernplan).

Auszug aus dem Standard-Rufnummernplan:

Art der Rufnummern	Standard-Rufnummern
Interne Teilnehmer-Rufnummern	100-349, 500-709
Teilnehmer-Durchwahlnummern	100-349, 500-709
Gruppenrufnummern	350-439
Voicemail-Rufnummer	71
Announcement Player Rufnummer	72
Richtungskennzahlen (Externkennzahlen): Amt ITSP	855-858
Rufnummer für Konferenzen	7400-7404
Rufnummer für Parken	7405
Rufnummer für AutoAttendant	7410-7429
Rufnummer für MeetMe-Konferenz	7430

Individueller Rufnummernplan

Ein individueller Rufnummernplan kann im WBM während der Basiskonfiguration über eine XML-Datei importiert werden.

Die XML-Datei enthält mehrere Register. Das Register "Kunde" enthält zusätzlich zu den Namen und den Rufnummern der Teilnehmer weitere Teilnehmerdaten, wie z.B. die Teilnehmer-Typen und die E-Mail-Adressen der Teilnehmer.

Ein Beispiel einer XML-Datei mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**. Die dort abgelegte XML-Datei können Sie auch als Vorlage für Ihre Daten verwenden. Sie kann z.B. mit Microsoft Excel bearbeitet werden.

6.5 Installation der Kommunikationssoftware

Die Kommunikationssoftware OpenScape Business S ist auf dem Linux-Server installiert.

Stellen Sie sicher, dass die zu konfigurierenden IP-Adressen und Netzwerkmasken für das Kunden-LAN geeignet sind.

DHCP-Server

Ein DHCP-Server weist jeder IP-Station (IP-Telefone, PCs etc.) automatisch eine eindeutige IP-Adresse zu und versorgt die IP-Stationen mit netzwerkspezifischen Daten wie z.B. der IP-Adresse des Standard-Gateways.

Als DHCP-Server kann entweder ein externer DHCP-Server (z.B. der DHCP-Server des Internetrouters oder des Kommunikationssystems) oder der DHCP-Server des Linux-Servers verwendet werden. Wenn der DHCP-Server des Linux-Servers verwendet wird, muss der externe DHCP-Server deaktiviert werden. Die Konfiguration des Linux DHCP-Servers kann während der Installation der OpenScape Business Kommunikationssoftware durchgeführt werden.

Anmerkung: Sie sollten DHCP entweder von yast oder von WBM aktivieren, aber nicht von beiden. Wenn Sie den DHCP während der Erstinstallation von OpenScape Business S aktivieren, entspricht dies der Aktivierung des DHCP durch yast. Wenn Sie DHCP auf OpenScape Business S aus WBM aktivieren möchten, sollte das DHCP bei der Erstinstallation der Kommunikationssoftware nicht aktiviert werden.

Virtuelle Umgebung

Die Kommunikationssoftware kann in einer virtuellen Umgebung ausgeführt werden. Es gibt zwei Weisen, die Installation durchzuführen:

- Separate Installation von Linux und der Kommunikationssoftware

  Dazu muss zunächst die Virtualisierungssoftware (Hostbetriebssystem) auf dem Server-PC installiert und konfiguriert werden. Linux wird in der virtuellen Umgebung als Gastbetriebssystem installiert. Innerhalb des Linux-Betriebssystems wird die Kommunikationssoftware zuletzt mit Hilfe der OpenScape Business DVD oder .ISO-Datei (siehe *OpenScape Business Linux Server, Installationsanleitung* für weitere Details).
- Kombinierte Installation von Linux und der Kommunikationssoftware (nur VMWare)

  Dazu muss zunächst die Virtualisierungssoftware (Hostbetriebssystem) auf dem Server-PC installiert und konfiguriert werden. In der virtuellen Umgebung wird ein OVA-Image (Open Virtualization Appliance) installiert, das Linux und die Kommunikationssoftware enthält. Das OVA-Image wird über den Software Supply Server (SWS) bereitgestellt.

  Für mehr als 50-Benutzer muss die Größe der Home-Partition nach der Installation auf 100-GB (für 50-bis 100-Benutzer) oder 200-GB (für bis zu 500-Benutzer oder für OpenScape Business Contact Center) oder 500-GB (für mehr als 500-Benutzer) geändert werden.

  Für Linux-Updates benötigen Sie auch den OpenScape Business SLES Upgrade-Schlüssel, um sich unter Linux registrieren zu können.

Verwendung von Snapshots auf virtuellen Maschinen (VM):

Snapshots können ein wertvoller Wartungsmechanismus sein, um beispielsweise einen schnellen Rollback in einen vordefinierten Betriebszustand der VM durchzuführen, nachdem ein Massenverteilungsskript fehlgeschlagen ist.

- Snapshots können während des normalen Betriebs nicht erstellt werden. Der aktuelle Betriebszustand der virtuellen Maschine wird während der Aufnahme eines Snapshots eingefroren. Folglich können angeschlossene Endgeräte und Anwendungen wie IP-Telefone oder UC-Clients die Verbindung zum Server verlieren.
- Snapshots können dazu führen, dass interne Server-Prozesse ihre Synchronisation verlieren, was bedeutet, dass der stabile Betrieb des Kommunikationssystems dann nicht mehr gewährleistet werden kann. Ein Server-Neustart nach dem Snapshot sollte daher auch innerhalb des Wartungszeitraums geplant werden.
- Frühere Snapshots sollten während des normalen Betriebs nicht in der Produktionsumgebung verbleiben.
- Snapshots können während eines geplanten Wartungsfensters oder im Rahmen der Installation gemacht werden.
- Snapshots werden intern von Backup-Tools wie VDP oder VDR verwendet. Es muss sichergestellt werden, dass es sich bei diesen Sicherungsvorgängen um Zeitpläne außerhalb der Geschäftszeiten handelt und dass die von diesen Tools generierten Snapshots am Ende des Vorgangs gelöscht werden.

Weitere Informationen zu Snapshots finden Sie in der VMware Knowledge Base (KB). Ein guter Ausgangspunkt ist der KB-Artikel 1025279 – Best Practices für Snapshots virtueller Maschinen in der VMware-Umgebung (englisch) (`http://kb.vmware.com/kb/1025279`).

Alle Informationen zu Snapshots in Microsoft Hyper-V finden Sie in der technet Bibliothek unter technet.microsoft.com im Hyper-V Kapitel.

6.5.1 Wie Sie die Kommunikationssoftware installieren

Voraussetzungen

- Das Betriebssystem SLES 12 SP5 oder SLES 15 SP6 wurde korrekt installiert und auf dem Linux-Server gestartet.
- DVD oder .ISO-Datei mit OpenScape Business-Kommunikationssoftware.
- DVD oder .ISO-Datei oder USB-Stick mit dem Linux-Betriebssystem SLES 12 SP5 64-Bit oder SLES 15 SP6 64-Bit, das für jede spätere Installation von Softwarepaketen (RPM) erforderlich sein kann.
- Die Root-Zugangsdaten (Benutzername und Passwort) für die Anmeldung am Linux-Server stehen zur Verfügung.

Wichtig: Die OpenScape Business-Kommunikationssoftware überschreibt während der Installation vorhandene Konfigurationsdateien (z.B. für DHCP, FTP, Postfix usw.).

Schritt für Schritt

1) Melden Sie sich mit Root-Rechten beim Linux-Server an.

2) Legen Sie die OpenScape Business-DVD oder .ISO-Datei in das DVD-Laufwerk ein.

3) Bestätigen Sie die Nachricht mit **Ausführen**. Das Fenster "Willkommen" erscheint.

4) Wählen Sie die gewünschte Einrichtungssprache aus (z.B. **Englisch**) und klicken Sie auf **Start**. Der Rest der Installation wird hier für die englische Sprache beschrieben.

5) Wählen Sie das gewünschte Produkt aus der Liste aus und klicken Sie auf **Auswählen**. Es wird geprüft, ob die Hardware alle Anforderungen für die Installation erfüllt. Bei geringfügigen Mängeln bei der Erfüllung der Anforderungen wird eine Warnung angezeigt. Nach Bestätigung kann dann die Installation fortgesetzt werden. Bei schweren Mängeln wird die Installation automatisch abgebrochen.

6) Es wird geprüft, ob zusätzliche RPM-Pakete installiert werden müssen. Wenn ja, bestätigen Sie dies mit **Bestätigen**. In diesem Fall müssen Sie später zurück zu SLES 12 oder SLES 15, DVD oder .ISO-Datei wechseln.

7) Es erscheint ein Fenster mit den Bedingungen der Lizenz (d. h. der Endbenutzer-Lizenzvereinbarung oder EULA). Lesen Sie die Lizenzbedingungen und akzeptieren Sie die Lizenzvereinbarung mit **Ja**.

8) Wenn bereits ein DHCP-Server im Kunden-LAN vorhanden ist (z.B. der DHCP-Server des Internet-Routers), stoppen Sie hier die Konfiguration des Linux-DHCP-Servers mit **Nein** und fahren Sie mit Schritt 12 fort, um fortzufahren.

Anmerkung: Damit die Software von Systemtelefonen auch bei Verwendung eines externen DHCP-Servers automatisch aktualisiert werden kann, haben Sie zwei Optionen:

a) Die IP-Adresse des Linux-Servers muss als DLS-Adresse an jedem Systemtelefon eingegeben werden.

b) Die netzwerkspezifischen Daten müssen auf dem externen DHCP-Server eingegeben werden. Die Parameter hierfür finden Sie unter `/var/log/OPTI.txt`.

---

9) Wenn Sie den Linux DHCP Server verwenden möchten, klicken Sie auf **Ja**, um den Linux DHCP Server zu aktivieren und zu konfigurieren.

10) Geben Sie die folgenden Werte ein (voreingestellt mit Standardwerten):

- **Standardroute**: IP-Adresse des Standard-Gateways; In der Regel die IP-Adresse des Internetrouters, z.B. `192.168.5.1`.
- **Domäne** (optional): die während der Linux-Installation angegebene Domäne, z.B.: `<customer>.com`
- **DNS-Server** (optional): IP-Adresse des DNS-Servers, der während der Linux-Installation angegeben wurde. Wenn im internen Netzwerk kein DNS-Server verfügbar ist, können Sie hier die IP-Adresse des Internetrouters (z.B. `192.168.5.1`) eingeben.
- **SNTP-Server**: IP-Adresse des internen oder externen NTP-Servers.
- **DLS/DLI-Server**: IP-Adresse des DLS-Servers, d. h. die IP-Adresse des Linux-Servers (z.B.: `192.168.5.10`).
- **Subnetz**: geeignetes Subnetz für den IP-Adressbereich, z.B.: `192.168.5.0`.
- **Netzmaske**: Subnetzmaske des Linux-Servers, die während der Linux-Installation angegeben wurde, z.B.: `255.255.255.0`.
- **IP-Bereichsanfang** und **IP-Bereichsende**: IP-Adressbereich, aus dem der DHCP-Server IP-Adressen zuweisen kann, z.B.: `192.168.5.100` bis `192.168.5.254`.

11) Klicken Sie auf **Weiter**.

12) Nach der Installation muss das Linux-Betriebssystem neu gestartet werden. Aktivieren Sie das Kontrollkästchen **PC-Neustart** und bestätigen Sie mit **Weiter**.

13) Wenn zusätzliche RPM-Pakete installiert werden müssen, werden Sie aufgefordert, den SLES 12 DVD oder SLES 15 USB-Stick einzulegen. Legen Sie die DVD oder den USB-Stick ein und bestätigen Sie mit **Weiter**. Legen Sie nach erfolgreicher Installation der RPM-Pakete die OpenScape Business-DVD erneut ein oder .ISO-Datei und bestätigen Sie dies mit **Weiter**, gefolgt von **Ausführen**.

14) Die OpenScape Business-Kommunikationssoftware ist installiert. Das Betriebssystem führt dann automatisch einen Neustart durch.

15) Melden Sie sich nach dem Neustart mit dem Benutzerkonto, das zuvor während der Linux-Installation eingerichtet wurde, an.

16) Klicken Sie mit der rechten Maustaste auf das DVD-Laufwerkssymbol auf dem Desktop und wählen Sie das Menü-Element **Auswerfen**. Entfernen Sie die OpenScape Business DVD aus dem DVD-Laufwerk.

Anmerkung: Es dauert wenige Minuten, bis alle Komponenten der OpenScape Business-Kommunikationssoftware aktiv sind.

6.6 Inbetriebnahme

Mit dem Wizard **Erstinstallation** des WBM werden die grundlegenden Einstellungen durchgeführt.

6.6.1 Wie Sie den Wizard Erstinstallation starten

Voraussetzungen

Das WBM ist gestartet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.

Anmerkung: Wenn bei niedrigen Bildschirmauflösungen der Arbeitsbereich aufgrund der Größe des Browserfensters nicht komplett angezeigt werden kann, so erscheinen horizontale oder vertikale Rollbalken an den Rändern, mit denen der angezeigte Ausschnitt verschoben werden kann.

Nächste Schritte

Führen Sie die Erstinstallation wie nachstehend beschrieben Schritt für Schritt durch. Felder, die hier nicht beschrieben werden, sind passend für den Standardfall vorbelegt und müssen nur geändert werden, wenn sie nicht zu Ihren Netzwerkdaten passen. Die ausführlichen Informationen finden Sie in der Administratordokumentation bei der Beschreibung der einzelnen Wizards.

6.6.2 Systemeinstellungen

Im Fenster **Systemeinstellungen** konfigurieren Sie die Systemeinstellungen des Kommunikationssystems.

Gehen Sie folgendermaßen vor:

1) Display-Logo und Produktbezeichnung festlegen

Sie können einen Display-Text festlegen, das im Display der Systemtelefone angezeigt wird. Zusätzlich können Sie die Produktbezeichnung auswählen.

2) Länderkennzeichen und Sprache für Event-Logs auswählen

Für eine korrekte Länderinitialisierung müssen Sie das Land auswählen, in dem das Kommunikationssystem betrieben wird. Zusätzlich können Sie die Sprache auswählen, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) abgespeichert werden.

3) Nur bei Bedarf: Weiteren LAN-Anschluss als WAN-Schnittstelle aktivieren

Besitzt OpenScape Business S (bzw. der Linux-Server) einen zweiten LAN-Anschluss, können Sie diesen als WAN-Schnittstelle für den Internet-Zugang und für die Internet-Telefonie über ITSP einrichten. Der erste LAN-Anschluss dient wie gewohnt als LAN-Schnittstelle für die internen Telefone und PCs.

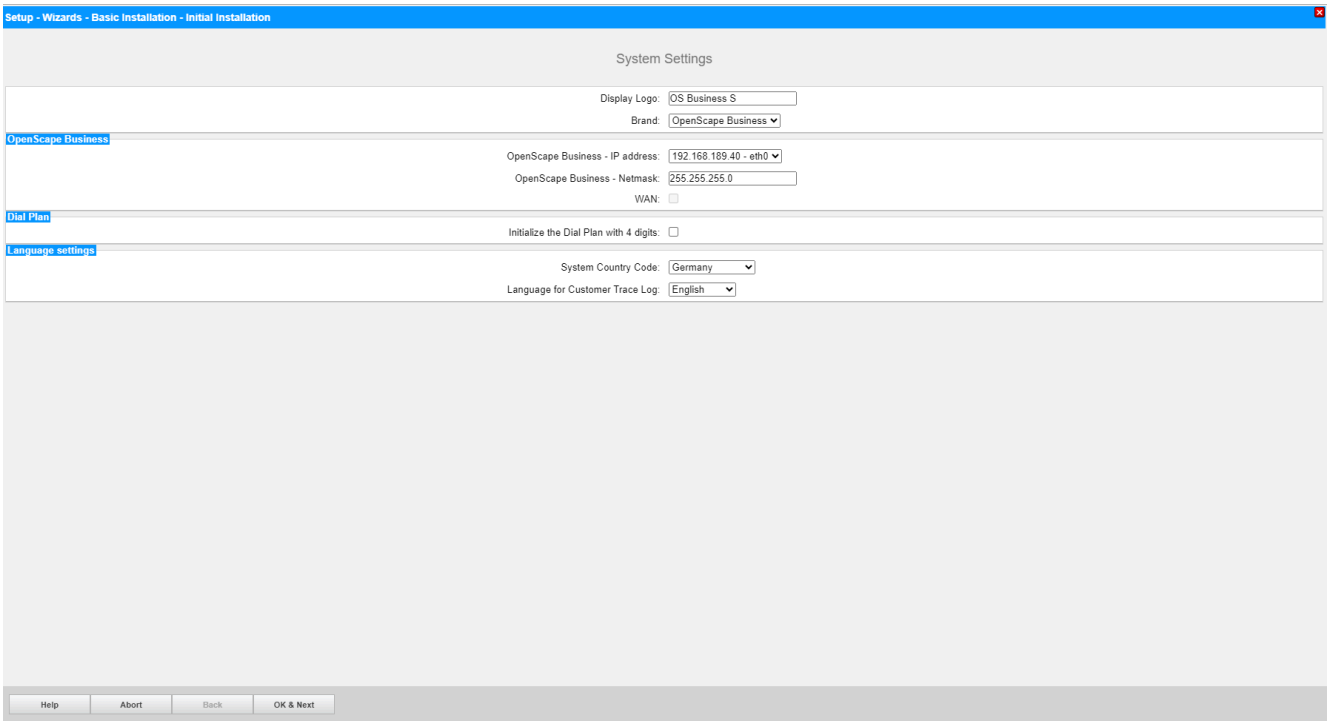
4) Ändern Sie den Standard-Wahlplan auf 4-stellige Nummern (nur für OSBiz S verfügbar)

Bei einer Neusysteminstallation können Sie den Wahlplan mit 4 statt 3 Ziffern initialisieren. Dadurch werden die Standardnummern des Systems von 100, 101, 102, ... in 1000, 1001, 1002 usw. geändert. Dies ermöglicht die automatische Rufnummernzuweisung für eine große Anzahl von Teilnehmerstationen. Beachten Sie, dass das System nach der Aktivierung dieses Flags neu gestartet wird.

6.6.2.1 Wie Sie das Sie das Anzeigelogo und den Produktnamen festlegen

Voraussetzungen

Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) Geben Sie in das Feld **Anzeigelogo** einen Text Ihrer Wahl ein (z. B. OS Business S). Der Text kann bis zu 16 Zeichen lang sein. Vermeiden Sie Umlaute und Sonderzeichen.
2) Wählen Sie den gewünschten Produktnamen in der Dropdown-Liste **Marke** aus.

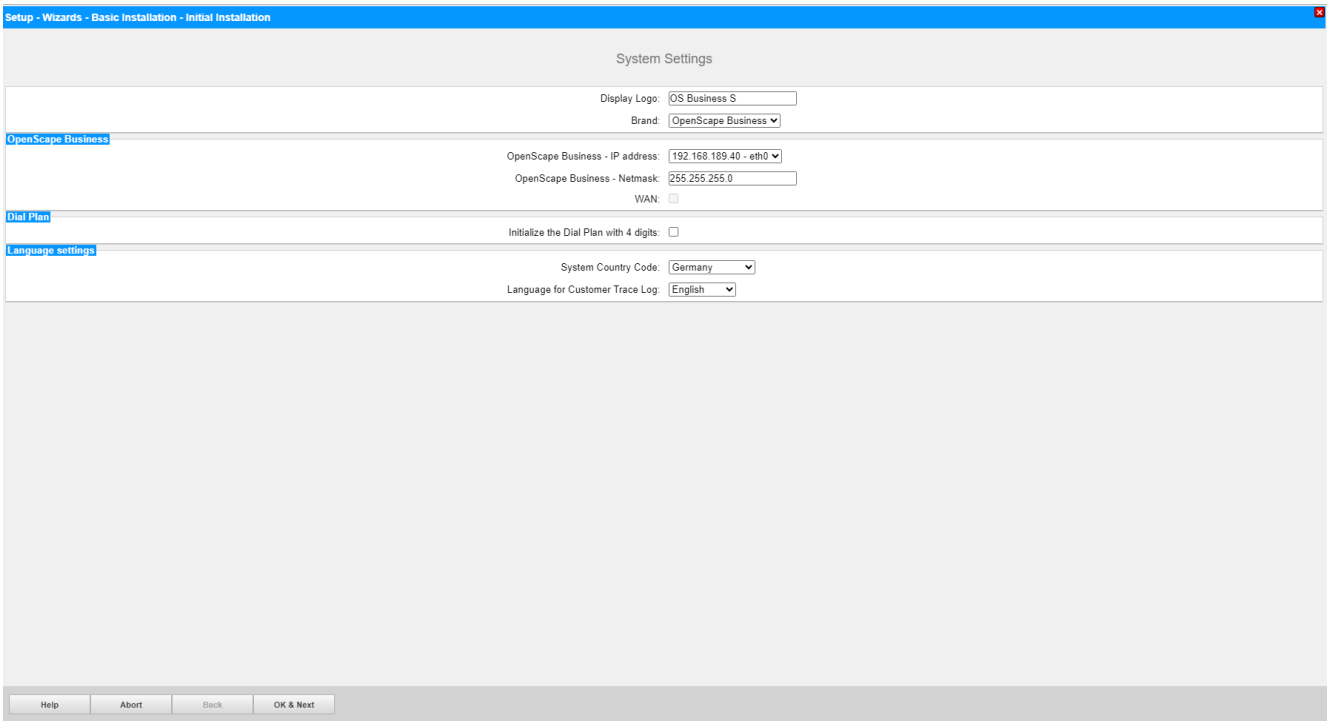
Nächste Schritte

Wählen Sie den Ländercode und die Sprache, die für die Trace-Protokolle verwendet werden sollen.

6.6.2.2 Wie wählen Sie den Ländercode und die Sprache für Trace-Protokolle aus

Voraussetzungen

Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) Wählen Sie in der Dropdown-Liste **Systemländercode** das Land, in dem das Kommunikationssystem betrieben wird.
2) Geben Sie im Feld **Sprache für Kunden-Trace-Protokoll** die Sprache ein, in der die Ereignisprotokolle (Systemereignisprotokolle, Fehlerprotokolle usw.) ausgegeben werden sollen.

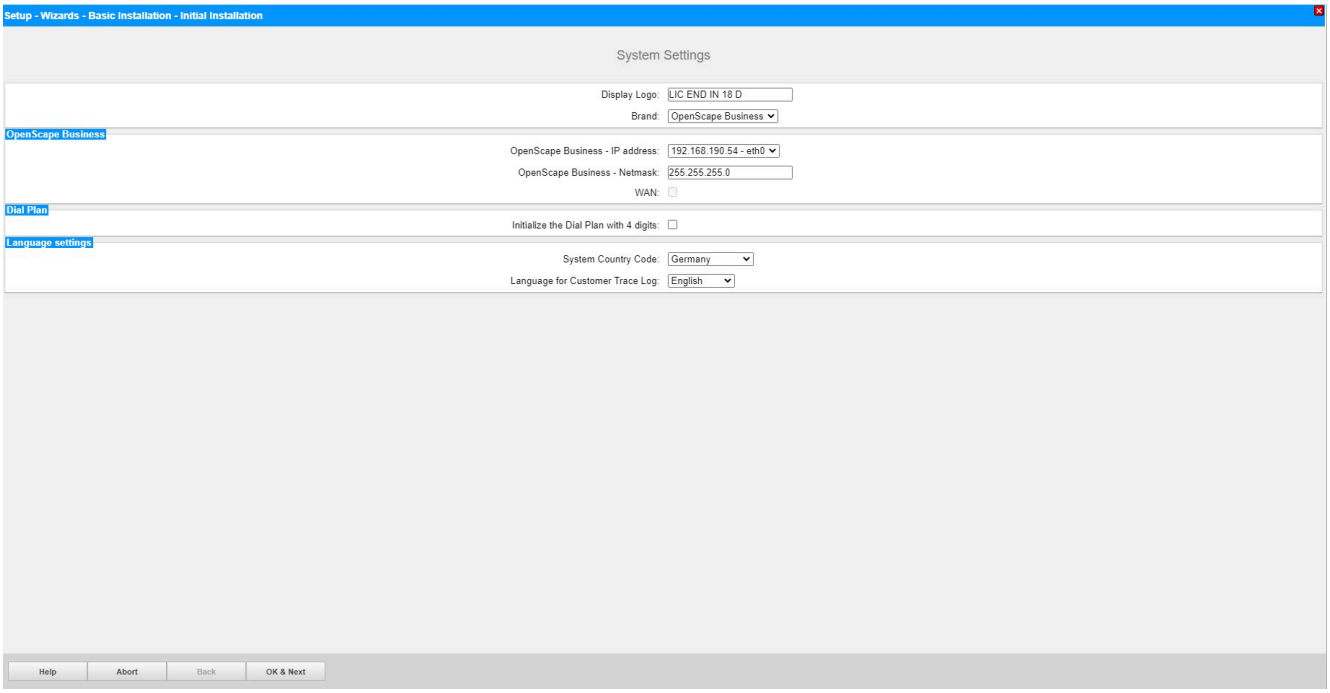
Nächste Schritte

Basiskonfiguration starten.

6.6.2.3 Wie Sie einen weiteren LAN-Anschluss als WAN-Schnittstelle aktivieren

Voraussetzungen

Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) Aktivieren Sie das Kontrollkästchen **WAN**.
2) Wählen Sie den gewünschten LAN-Port (z. B. `eth1` oder `eth2`) aus der Dropdown-Liste **OpenScape Business - IP-Adresse (WAN)** aus. Stehen nur zwei LAN-Ports zur Verfügung, wird der zweite LAN-Port `eth1` automatisch aktiviert.

Wichtig: Stellen Sie sicher, dass Sie anstelle des localhost die tatsächliche Netzwerkschnittstelle auswählen.

Anmerkung: Die Zuweisung von IP-Adressen und Subnetzmasken zu den LAN-Ports erfolgt bei der Erstinstallation von Linux oder anschließend über YaST.

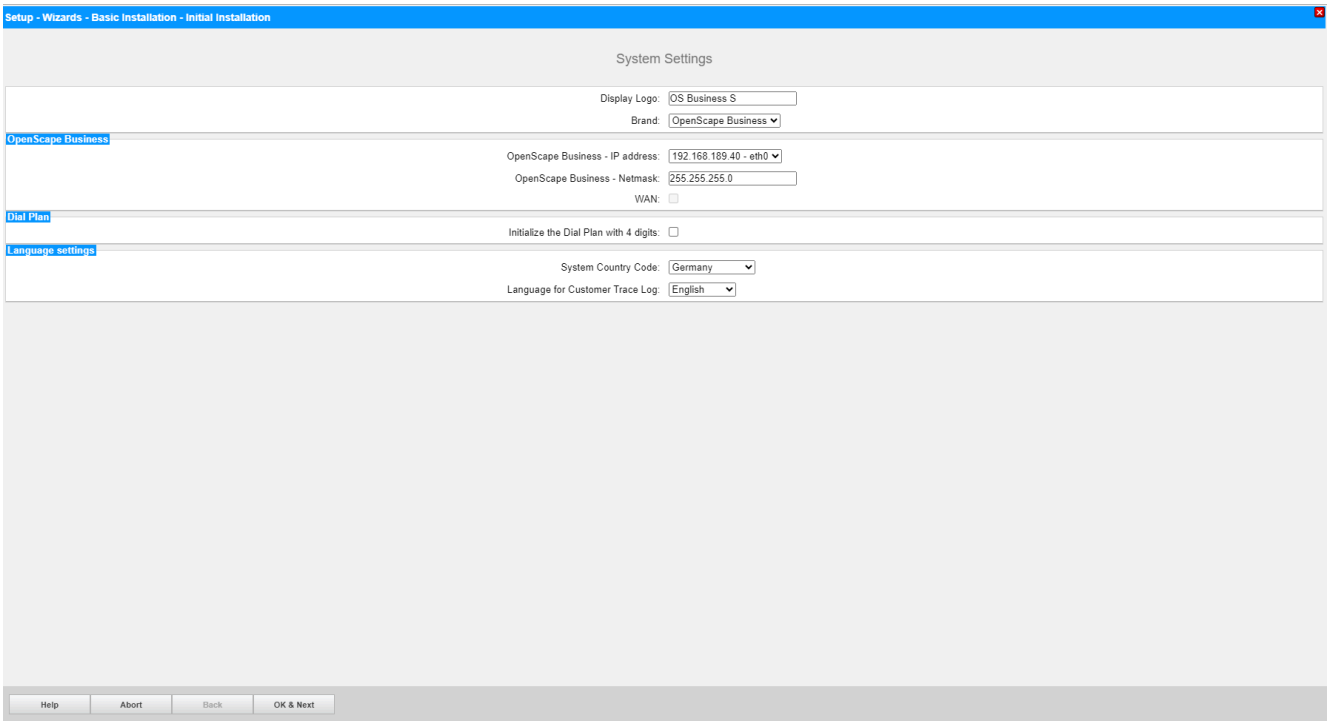
Nächste Schritte

UC-Lösung angeben.

6.6.2.4 Wie ändern Sie den Wahlplan auf 4 Ziffern

Voraussetzungen

Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

Klicken Sie auf das Kontrollkästchen des Feldes **Mit 4 Ziffern initialisieren** .

Nächste Schritte

Systemneustarts

6.6.3 UC-Lösung

Im Fenster **Applikationsauswahl ändern** legen Sie fest, welche UC-Lösung Sie nutzen.

Sie haben folgende Möglichkeiten:

- **Paket mit UC Smart**

  Die UC-Lösung UC Smart ist in OpenScape Business S intergiert.
- **Paket mit UC Suite**

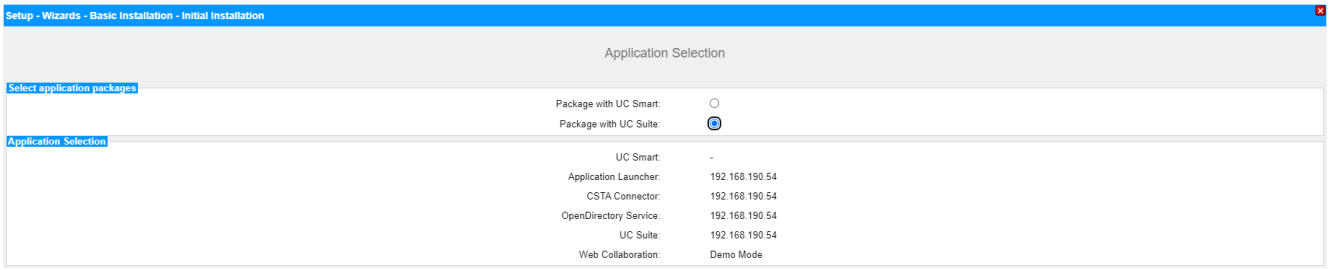
  Die UC-Lösung UC Suite ist in OpenScape Business S intergiert.

6.6.3.1 Wie Sie die UC-Lösung festlegen

Voraussetzungen

Sie haben Lizenzen erworben entweder für die UC-Lösung UC Smart oder für die UC-Lösung UC Suite.

Sie befinden sich im Fenster **Applikationsauswahl**.



Schritt für Schritt

1) Wenn Sie die UC-Lösung UC Smart nutzen, klicken Sie auf **Paket mit UC Smart**.
2) Wenn Sie die UC-Lösung UC Suite nutzen, klicken Sie auf **Paket mit UC Suite**.
3) Klicken Sie auf **OK & Weiter**.
4) Der Wizard **Erstinstallation** ist abgeschlossen. Klicken Sie auf **Beenden**.

Nächste Schritte

Basiskonfiguration starten.

6.7 Basiskonfiguration

Die Basiskonfiguration wird mit dem Wizard **Basisinstallation** des WBM durchgeführt. Dabei werden die wichtigsten Einstellungen für den Betrieb des Kommunikationssystems festgelegt.

Der Wizard Basisinstallation beinhaltet einen Progress Indicator, der den aktuellen Schritt sowie die darauf folgenden Schritte anzeigt.

6.7.1 Wie Sie den Wizard Basisinstallation starten

Voraussetzungen

Der Wizard **Erstinstallation** ist durchlaufen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

Nächste Schritte

Führen Sie die Basisinstallation wie nachstehend beschrieben Schritt für Schritt durch. Felder, die hier nicht beschrieben werden, sind passend für den Standardfall vorbelegt und müssen nur geändert werden, wenn sie nicht zu Ihren Netzwerkdaten passen. Die ausführlichen Informationen finden Sie in der Administratordokumentation bei der Beschreibung der einzelnen Wizards.

6.7.2 Systemrufnummern und Vernetzung

Im Fenster **Übersicht** geben Sie die Systemrufnummern ein (Anlagenrufnummer, Länder- und Ortsvorwahl, Internationales Präfix) und legen fest, ob OpenScape Business mit anderen OpenScape Business-Systemen vernetzt werden soll.

Gehen Sie folgendermaßen vor:

1) Systemrufnummern eingeben

- Systemrufnummern für Anlagenanschluss eingeben

  Hier geben Sie die Anlagenrufnummer für Ihren Anlagenanschluss ein sowie die Länder- und Ortsvorwahl.

  Die Eingabe der Ländervorwahl ist für Internet-Telefonie und Konferenz-Server-Funktionalitäten zwingend erforderlich.

  Das internationale Präfix ist abhängig von der zuvor gewählten Länderkennzahl vorbelegt.
- Systemrufnummern für Mehrgeräteanschluss eingeben

  Hier geben Sie Länder- und Ortsvorwahl für Ihren Mehrgeräteanschluss ein.

  Die Eingabe der Ländervorwahl ist für Internet-Telefonie und für MeetMee-Konferenzen zwingend erforderlich.

  Das internationale Präfix ist abhängig von der zuvor gewählten Länderkennzahl vorbelegt.

2) Vernetzung aktivieren oder deaktivieren

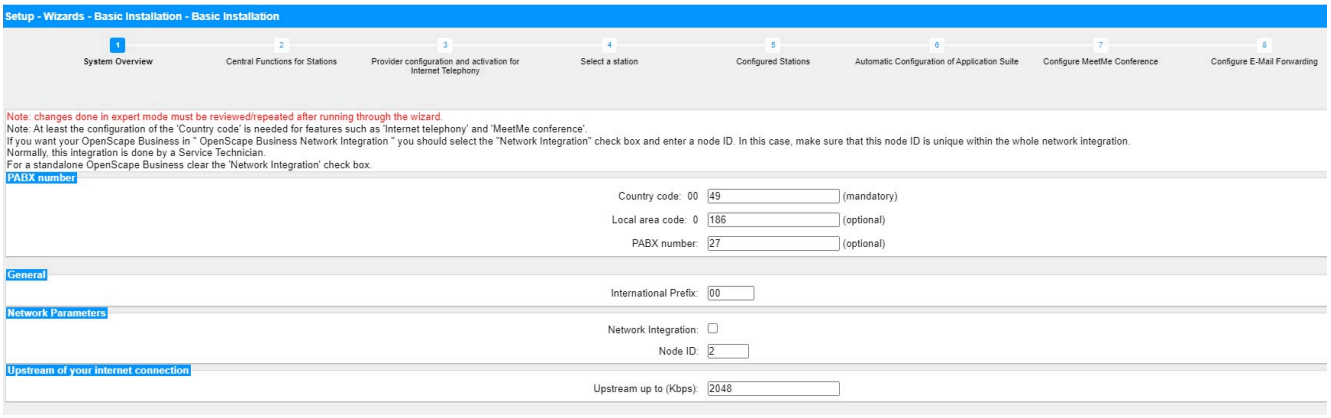
Soll OpenScape Business mit anderen OpenScape Business vernetzt werden, muss die Vernetzung aktiviert und OpenScape Business eine Knoten-ID zugewiesen werden. Jede OpenScape Business muss im Netzverbund eine eindeutige Knoten-ID besitzen.

6.7.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben

Voraussetzungen

Sie haben einen Anlagenanschluss.

Sie befinden sich im Fenster **Systemüberblick** des Assistenten **Basisinstallation**.



Schritt für Schritt

1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.
2) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. `89` für München.
3) Geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z. B. `7007` (Ihre Anschlussnummer).
4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

   Bei Telefonaten ins Ausland werden der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. bei einem Telefonat von Deutschland nach USA die "00-1-..." und bei einem Telefonat von USA nach Deutschland die "011-49-...".

Nächste Schritte

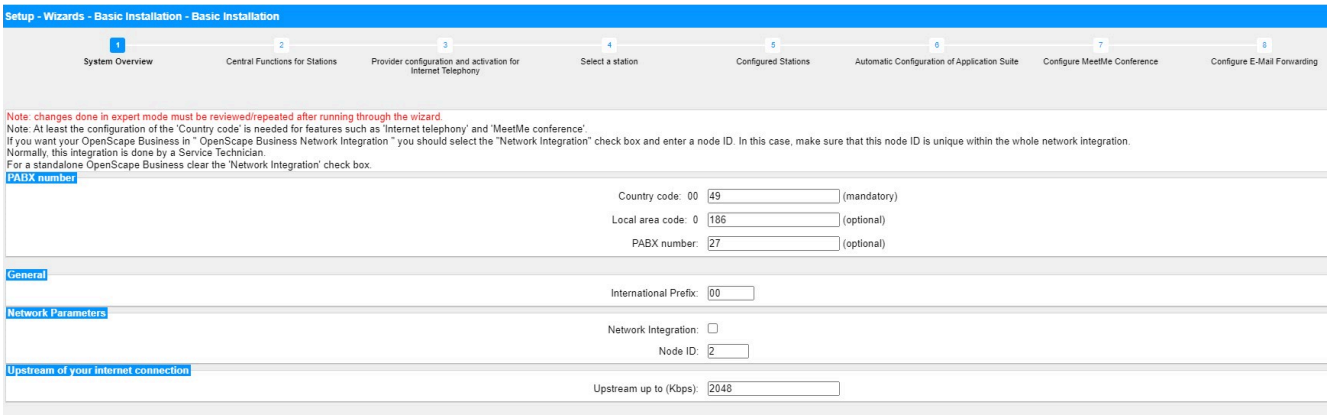
Vernetzung aktivieren oder deaktivieren

6.7.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben

Voraussetzungen

Sie haben einen Mehrgeräteanschluss.

Sie befinden sich im Fenster **Systemüberblick** des Assistenten **Basisinstallation**.



Schritt für Schritt

1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.
2) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. `89` für München.
3) Lassen Sie das Feld **Anlagenrufnummer** leer.
4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

   Bei Telefonaten ins Ausland werden der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. bei einem Telefonat von Deutschland nach USA die "00-1-..." und bei einem Telefonat von USA nach Deutschland die "011-49-...".

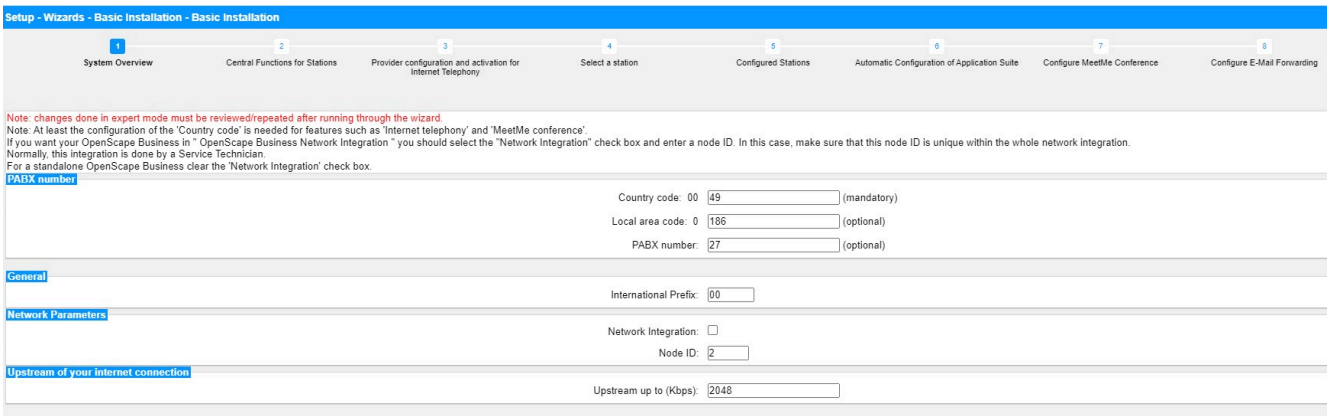
Nächste Schritte

Vernetzung aktivieren oder deaktivieren

6.7.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren

Voraussetzungen

Sie befinden sich im Fenster **Systemüberblick** des Assistenten **Basisinstallation**.



Schritt für Schritt

1) Wenn das Kommunikationssystem mit anderen Kommunikationssystemen vernetzt werden soll:
   a) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
   b) Vergeben Sie im Feld **Knoten-ID** für das Kommunikationssystem eine im Netzverbund eindeutige Knoten-ID (Ziffern von `1` bis `100` möglich).
2) Wenn das Kommunikationssystem nicht mit anderen Kommunikationssystemen vernetzt werden soll, lassen Sie das Kontrollkästchen **Netzwerk-Integration** deaktiviert.

Nächste Schritte

Konfigurieren Sie den Upstream Ihrer Internetverbindung.

6.7.2.4 Wie Sie die Upstream-Strecke Ihrer Internetverbindung konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Übersicht**.

Schritt für Schritt

1) Geben Sie im Feld **Upstream bis zu (Kbit/s)** die Geschwindigkeit Ihrer Internetverbindung an.
2) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

Teilnehmerdaten konfigurieren.

6.7.3 Teilnehmerdaten

Im Fenster **Zentrale Teilnehmer-Funktionen** können Sie bei Bedarf anstelle des vordefinierten Standardrufnummernplans Ihren individuellen Rufnummernplan konfigurieren und weitere Teilnehmerdaten importieren. Im Netzverbund muss der Standard-Rufnummernplan an den Rufnummernplan des Netzverbunds angepasst werden.

Der Standardrufnummernplan enthält vordefinierte Rufnummern für verschiedene Teilnehmertypen (IP-Telefone, analoge Telefone, ...) und für spezielle Funktionen (Internet-Telefonie, Sprachbox, AutoAttendant, ...).

Die Teilnehmerdaten enthalten u.a. die internen Rufnummern, die Durchwahlnummern und die Namen der Teilnehmer. Über eine XML-Datei im UTF-8-Format können diese Daten und weitere Teilnehmerdaten während der Basiskonfiguration in das Kommunikationssystem importiert werden.

Anmerkung:

Eine XML-Vorlage mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**. In diese Vorlage können Sie z.B. mit Microsoft Excel Ihre Daten eintragen.

Sie haben folgende Möglichkeiten:

- **Teilnehmerdaten ohne Netzverbund konfigurieren**

  Gehen Sie folgendermaßen vor:

  1) Teilnehmerdaten anzeigen

  Sie können sich alle vorkonfigurierten Rufnummern und Teilnehmerdaten anzeigen lassen.

  2) Alle Rufnummern löschen (optional)

  Verwenden Sie einen individuellen Rufnummernplan, müssen Sie alle vorkonfigurierten Rufnummern löschen.

  3) Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen (optional)

  Verwenden Sie einen individuellen Rufnummernplan, können Sie die vorkonfigurierten Rufnummern an den eigenen Rufnummernplan anpassen.

  Anmerkung:

  Geht der Benutzer die Option **Vorkonfigurierte Rufnummern ändern** durch, muss eine bereits in UC Suite vorhandene, benutzerdefinierte Konfiguration geändert oder wiederholt werden (z.B. Pilot-Warteschlangen)

  ---

  4) Teilnehmerdaten über XML-Datei importieren (optional)

  Ihre individuellen Rufnummern inkl. zusätzlicher Teilnehmerdaten können Sie bequem über eine XML-Datei während der Basiskonfiguration importieren.

- **Teilnehmerdaten mit Netzverbund konfigurieren**

  Gehen Sie folgendermaßen vor:

  1) Alle Rufnummern löschen

  Falls im Netzverbund die UC Suite zum Einsatz kommt, ist ein geschlossener Rufnummernplan erforderlich, d.h. alle Rufnummern im Netzverbund müssen eindeutig sein. Daher müssen die vorkonfigurierten Rufnummern gelöscht und an den Netzverbund angepasste Rufnummern verwendet werden.

  2) Teilnehmerdaten über XML-Datei importieren

  Die an den Netzverbund angepassten Rufnummern sind inkl. zusätzlicher Teilnehmerdaten bequem über eine XML-Datei während der Basiskonfiguration zu importieren. Diese Datei kann alle Teilnehmer des Netzverbundes enthalten. Beim Import werden nur die Rufnummern und Teilnehmerdaten übernommen, die der zuvor angegebenen Knoten-ID des Kommunikationssystems zugeordnet sind.

Zugehörige Tasks

Anzeigen von Massendaten auf Seite 164
Wie Sie die LCR-Einträge zurücksetzen auf Seite 1430

Zugehörige Verweise

LCR > LCR-Flags auf Seite 1625

6.7.3.1 Wie Sie die Teilnehmerdaten anzeigen

Voraussetzungen

Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen**.
2) Klicken Sie auf **Funktion ausführen**. Es wird eine Teilnehmerliste mit den vorkonfigurierten Rufnummern (Standardrufnummernplan) angezeigt.
3) Klicken Sie auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
4) Wenn Sie keine Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

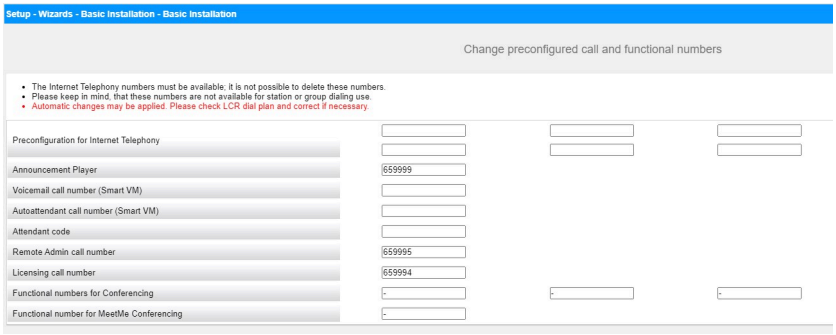
6.7.3.2 Wie Sie alle Rufnummern löschen

Voraussetzungen

Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Alle Rufnummern löschen**.
2) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen**.
3) Klicken Sie auf **Funktion ausführen**. Alle vorbelegten Rufnummern, außer **Wiedergabegerät für Ansagen, Remote-Admin Rufnummer** und **Licensing Rufnummer** werden gelöscht. Anschließend erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



4) Passen Sie die Kennzahlen und speziellen Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
5) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

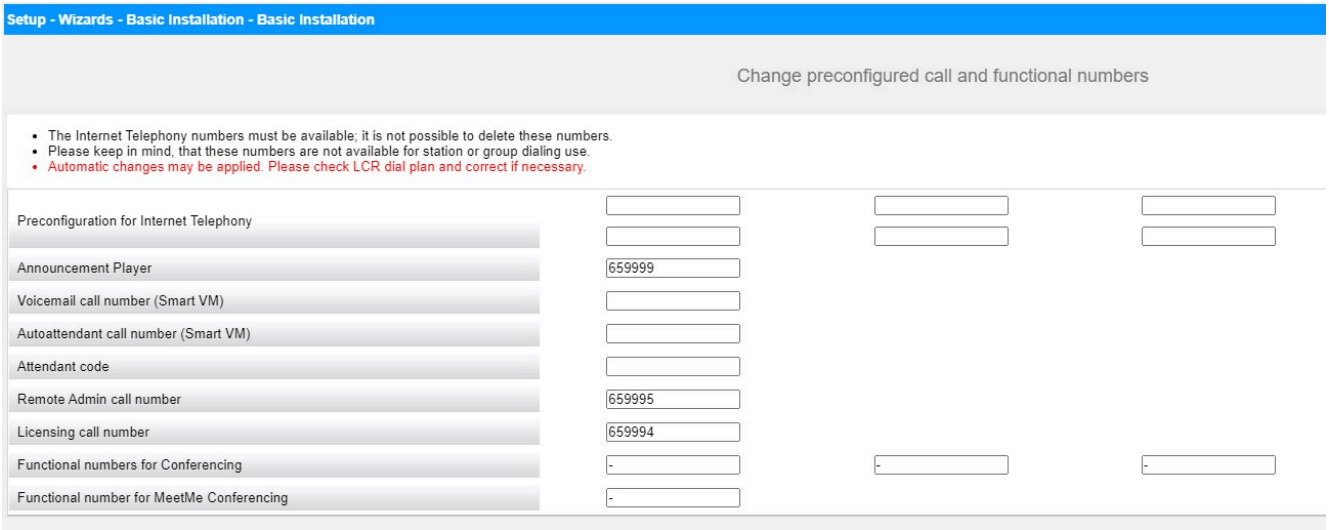
6.7.3.3 Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen

Voraussetzungen

Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Vorkonfigurierte Rufnummern ändern**.
2) Klicken Sie auf **Funktion ausführen**. Es erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



3) Passen Sie die vorkonfigurierten Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
4) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

6.7.3.4 Teilnehmerdaten über eine XML-Datei importieren

Voraussetzungen

Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen** des Assistenten **Basisinstallation**.

Eine XML-Datei im UTF-8-Format mit den eingetragenen Daten liegt vor. Eine XML-Vorlage finden Sie unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **CSV/XML-Datei mit Teilnehmerdaten importieren**.
2) Klicken Sie auf **Funktion ausführen**.
3) Wählen Sie mit **Durchsuchen** die erstellte XML-Datei aus und klicken Sie auf **Öffnen**.
4) Klicken Sie anschließend auf **OK**. Die Teilnehmerdaten werden importiert.
5) Klicken Sie auf **OK & Weiter**.

6.7.4 Internetzugang

6.7.4.1 Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port

Voraussetzungen

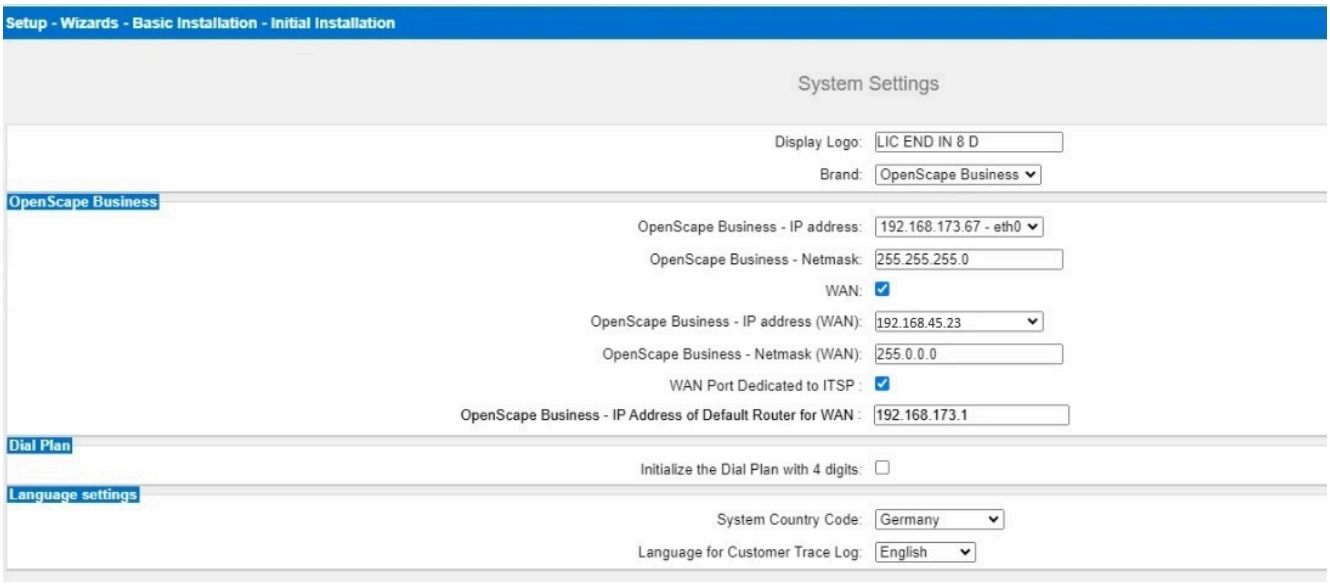
Sie haben im SLES eine neue Netzwerkschnittstelle erstellt.

Sie befinden sich im Fenster **Systemeinstellungen** des Assistenten für die **Erstinstallation**.

Bitte beachten Sie, dass diese Funktion nur für ITSPs, die in den Anbieter-Einstellungen nicht STUN verwenden müssen, gilt.

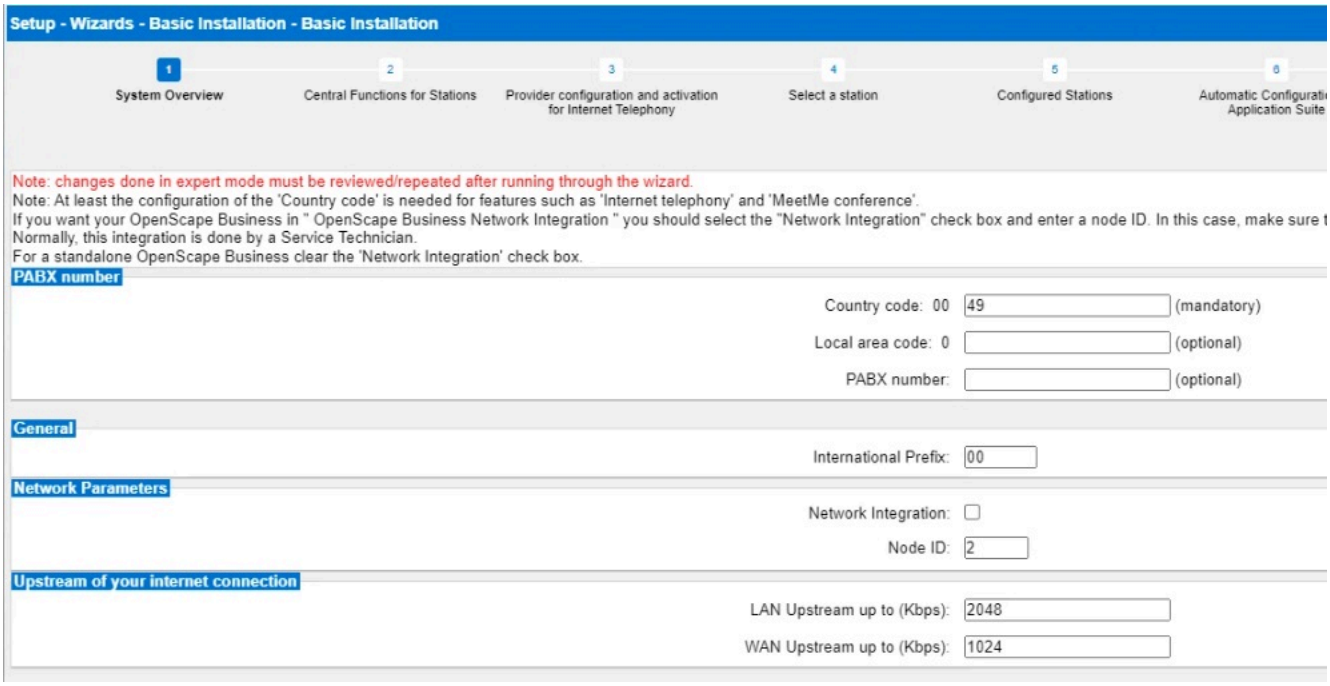
Schritt für Schritt

1) Aktivieren Sie das Kontrollkästchen **WAN** und wählen Sie die entsprechende Netzwerkschnittstelle aus.
   Die Option **WAN-Schnittstelle für ITSP** wird verfügbar.
2) Klicken Sie, um die **WAN-Schnittstelle für ITSP** zu aktivieren.



3) Klicken Sie auf **OK & Weiter**.
4) Navigieren Sie zu **Setup > Basisinstallation** und führen Sie den Assistenten für **Basisinstallation** aus.

5) Konfigurieren Sie die maximalen Upstream-Werte in den entsprechenden Feldern **LAN Upstream bis zu (Kbps)** und **WAN Upstream bis zu (Kbps)**.



6) Klicken Sie auf **OK & Weiter**.

7) Nach dem Anwenden der Konfiguration ist ein Neustart des Systems erforderlich.

6.7.5 Internet-Telefonie

Im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** konfigurieren Sie die Internet-Telefonie. Sie können vorkonfigurierte oder neue Internet-Telefonie-Service-Provider (ITSP) konfigurieren. Für jeden ITSP können Sie einen oder mehrere Accounts konfigurieren. Es können bis zu 8 ITSP gleichzeitig aktiv sein.

Sie haben folgende Möglichkeiten:

- **Vordefinierten ITSP konfigurieren**

  Sie können vordefinierte ITSP-Vorlagen verwenden. Dazu werden in diese Vorlage die eigenen Zugangsdaten und Rufnummern eingetragen und diese anschließend aktiviert.
- **Neuen ITSP konfigurieren**

  Sie können auch neue ITSP hinzufügen und aktivieren.

  Einen neuen ITSP zu konfigurieren ist nur in seltenen Fällen nötig und sehr aufwändig. Deshalb wird diese Möglichkeit nicht in der Erstinstallation beschrieben. Genauere Informationen finden Sie im Kapitel Konfiguration eines ITSP.
- **Internet-Telefonie deaktivieren**

  Sie können die Internet-Telefonie deaktivieren.

Anmerkung:

Einrichtebeispiele finden Sie im Internet im **Unify Experts Wiki** unter *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Zuordnung der ITSP-Rufnummern

- Bei einem **Internet-Telefonie-Teilnehmeranschluss** stellt der ITSP Einzelrufnummern zur Verfügung, z.B. 70005555, 70005556, ... Diese Einzelrufnummern werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.
- Bei einem **Internet-Telefonie-Anlagenanschluss** stellt der ITSP ein Rufnummernband (Rufnummernbereich) zur Verfügung, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Bereich werden dann manuell als interne Rufnummern der Teilnehmer vergeben.

Die beiden Anschlussarten können kombiniert werden.

Alternativ können für beide Anschlussarten die ITSP-Rufnummern bei der Teilnehmer-Konfiguration als Durchwahlrufnummern der Teilnehmer eingetragen werden.

Interne Rufnummer	Name	Durchwahl
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Somit ergeben sich die ITSP-Rufnummern aus der eingerichteten Anlagenrufnummer (z.B. Länderkennzahl 49) und den eingetragenen Durchwahlnummern im Langformat. Das hat Vorteile bei der Wahlbewertung und dem Call-Management, auch in einem Netzverbund. So ist der ITSP-Anschluss z. B. durchwahlfähig zu einem anderen Knoten.

Ein weiterer Amtsanschluss über ISDN ist in diesem Fall nur eingeschränkt möglich (sinnvoll z.B. für Notrufe).

6.7.5.1 Vordefinierten ITSP konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** des Assistenten für die **Grundinstallation**.

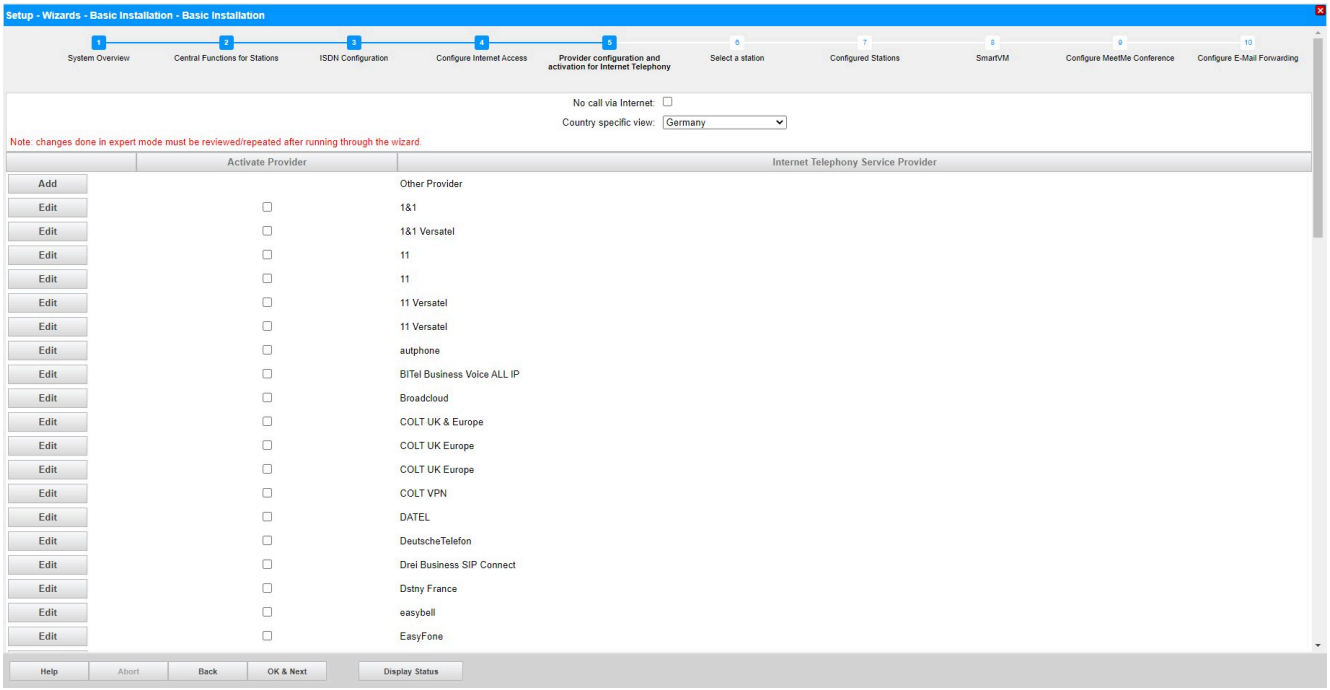
Die Verbindung zum Internet ist betriebsbereit.

Die Internet-Telefonie-Zugangsdaten Ihres ITSP liegen Ihnen vor (z. B. Benutzerkennung, Passwort, Internet-Telefonie-Rufnummern).

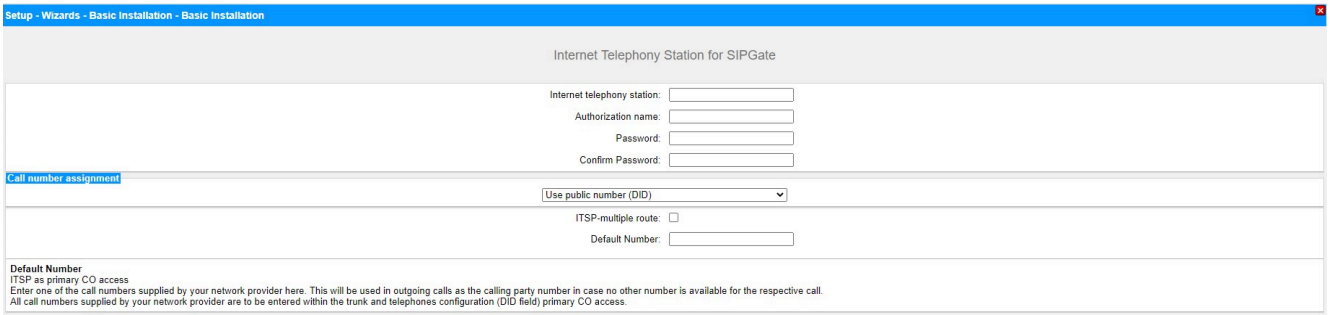
Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt.

Die Liste enthält die für das gewählte Land vordefinierten ITSP und die eventuell bereits angelegten ITSP.



2) Wenn Sie das voreingestellte Land ändern möchten, wählen Sie aus der Aufklappliste **Länderspezifische Ansicht** das gewünschte Land aus. Es werden die für das gewählte Land möglichen ITSP angezeigt.
3) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie 8 ITSP aktivieren. Klicken Sie anschließend auf **OK**.
4) Klicken Sie in der Zeile des entsprechenden ITSP auf **Bearbeiten**, um einen vordefinierten ITSP zu konfigurieren.
5) Aktivieren Sie das Kontrollkästchen **Provider aktivieren**.
6) Klicken Sie auf **OK & Weiter**.
7) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.



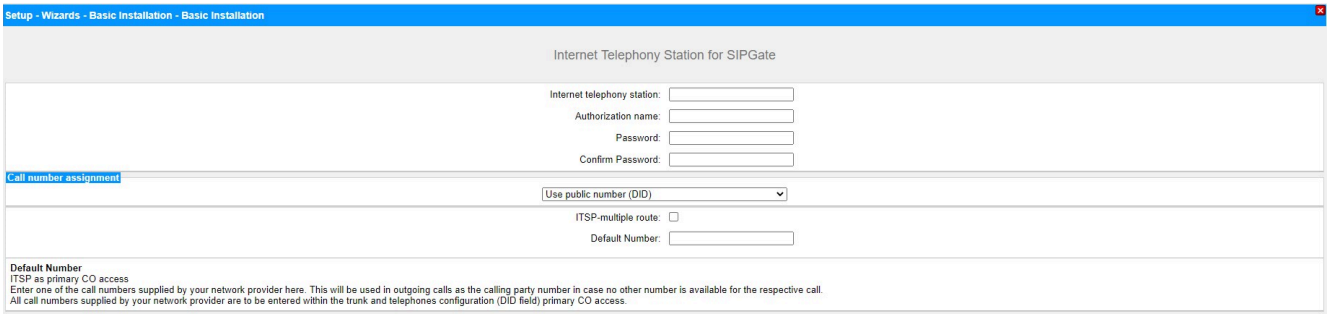
8) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: SIP-Benutzer, SIP-ID usw.

9) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen Autorisierungsnamen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

10) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, dass Sie vom ITSP erhalten haben. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: Kennwort, SIP-Kennwort usw.

11) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

Öffentliche Rufnummer (DuWa): die Internet-Telefonie-Rufnummern Ihres Internet-Telefonie-Teilnehmeranschlusses oder Internet-Telefonie-Anlagenanschlusses werden nicht hier bei der ITSP-Konfiguration, sondern bei der Teilnehmer-Konfiguration in den Feldern **DuWa** eingetragen.



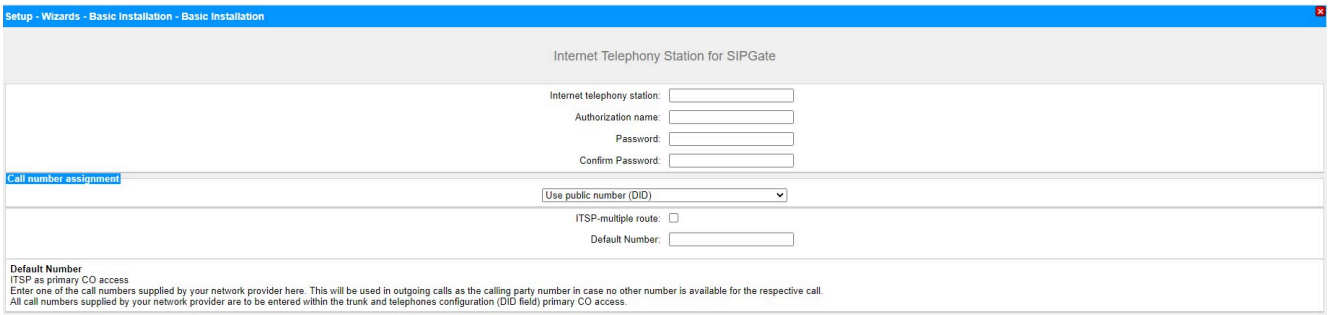
a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.

b) Unter **Standardnummer**, geben Sie die Telefonnummer, die für ausgehende Anrufe verwendet werden soll, wenn keine DID-Nummer des Anrufers verfügbar ist, ein.

c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern).

12) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

Interne Nummer (Rufnr.) verwenden / Einzeleinträge: Sie haben einen Internet-Telefonie-Teilnehmeranschluss und als Internet-Telefonie-Rufnummern Einzelrufnummern erhalten (z. B. 70005555, 70005556,...). Diese Einzelrufnummern ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.

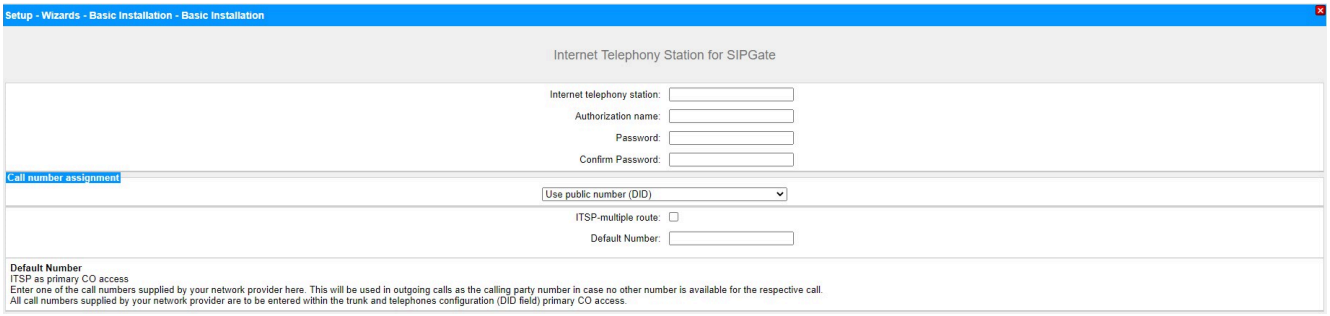
b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP

mitgeteilten Internet-Telefonie-Teilnehmerrufnummern ein und klicken Sie auf **Hinzufügen**.

c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).

13) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:

Interne Nummer (Rufnr.) verwenden / Bereichseintrag: Sie besitzen einen Internet-Telefonie-Anlagenanschluss und haben als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z.B. (+49) 89 7007-100 bis (+49) 89 7007-147. Sie weisen dann die Rufnummern aus dem Rufnummernbereich den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.

b) Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.

c) Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.

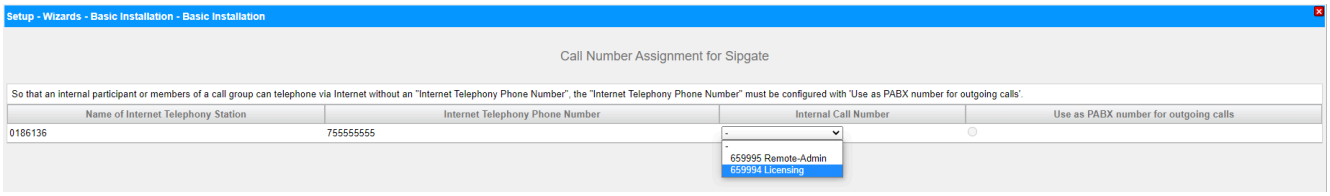
14) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie weitere Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern einrichten möchten, wiederholen Sie die Schritte 7 bis 14.

16) Klicken Sie auf **OK & Weiter**. Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.

17) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.

Dieser Schritt entfällt, wenn Sie für die Zuordnung der Internet-Telefonie-Rufnummern die Möglichkeit 1 gewählt haben. Die Zuordnung treffen Sie in diesem Fall bei der Teilnehmer-Konfiguration im Feld **DuWa**.



a) Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.

b) Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.

18) Klicken Sie auf **OK & Weiter**. Hier sehen Sie nochmals die Liste der vordefinierten und neu hinzugefügten ITSP. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit **Restart ITSP** können Sie sich bei Verbindungsproblemen bei bereits aktivierten ITSP neu registrieren

19) Klicken Sie auf **OK & Weiter**.

20) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!

Anmerkung: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig zu führenden Internet-Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

Weitere Informationen über die Anzahl der gleichzeitigen Internetanrufe finden Sie unter Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP auf Seite 827.

---

21) Klicken Sie auf **OK & Weiter**.

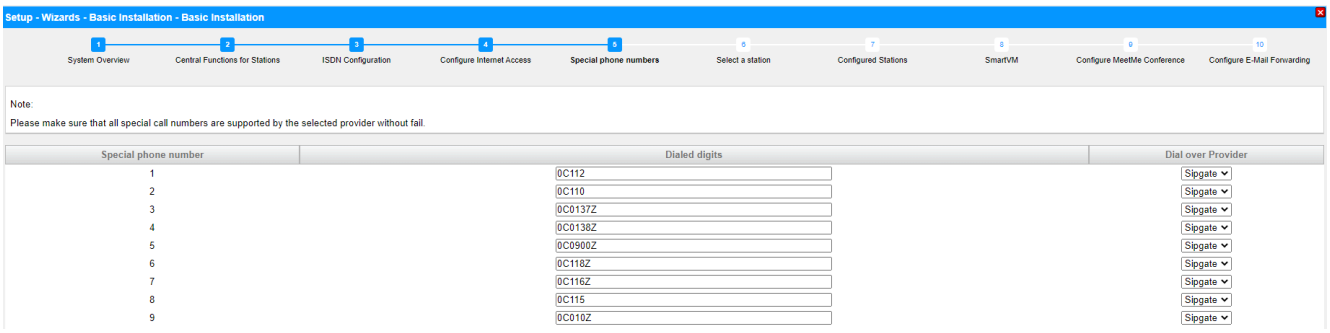
22) Falls Sie bei der Einrichtung Ihres Internet-Zugangs die Dauerverbindung noch nicht aktiviert haben, können Sie das hier nachholen. Ohne Dauerverbindung können Sie keine Anrufe über das Internet empfangen. Ist die Dauerverbindung bereits eingerichtet, erscheinen die unter a) bis c) beschriebenen Felder nicht.

a) Aktivieren Sie unter **Dauerverbindung** das Optionsfeld **An**.

b) Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).

c) Klicken Sie auf **OK & Weiter**.

23) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.



Folgende Rufnummerneinträge sind gültig:

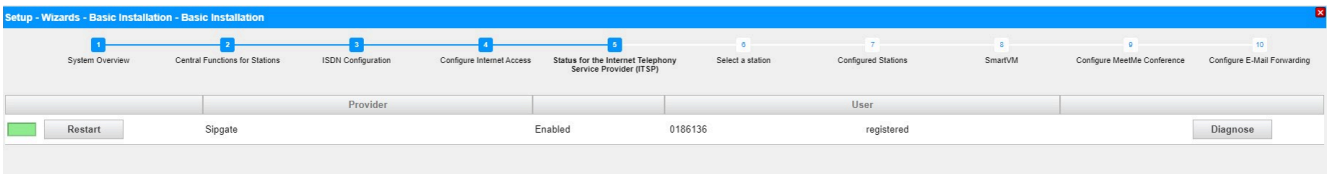
- 0 bis 9: Zulässige Ziffern
- -: Feldtrennzeichen
- X: beliebige Ziffer von 0 bis 9
- N: beliebige Ziffer von 2 bis 9
- Z: Eine oder mehrere Ziffern folgen bis Wahlende
- C: Simulierter Wählton (kann max. dreimal eingetragen werden)

24) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

Anmerkung: Stellen Sie sicher, dass Notrufnummern immer gewählt werden können. Falls Notrufnummern über einen Internet-Telefonie-Service-Provider gewählt werden sollen, muss der ITSP dies unterstützen.

---

25) Klicken Sie auf **OK & Weiter**. Der Status Ihres ITSP wird angezeigt.



Grün markiert sind ITSP, die eingerichtet und an denen Sie bereits registriert sind.

Orange markiert sind ITSP, die eingerichtet und an denen Sie noch nicht registriert sind.

26) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

6.7.5.2 Wie Sie Internet-Telefonie deaktivieren

Voraussetzungen

Sie befinden sich im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** des Assistenten für die **Grundinstallation**.

Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **Keine Telefonie über Internet** aktiviert.
2) Klicken Sie zweimal auf **OK & Weiter**.

6.7.6 Teilnehmer

In den Fenstern **Teilnehmer auswählen - ...** konfigurieren Sie die an dem Kommunikationssystem angeschlossenen Teilnehmer.

Gehen Sie folgendermaßen vor:

1) IP- und SIP-Teilnehmer konfigurieren

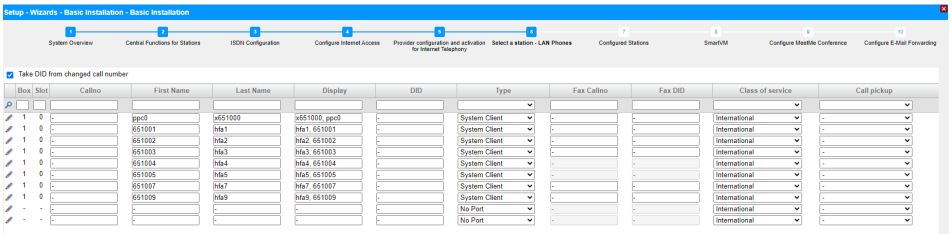
   IP-Teilnehmer und SIP-Teilnehmer sind z.B. LAN-Telefone oder WLAN-Telefone.

6.7.6.1 Wie Sie IP- und SIP-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - LAN-Telefone** im Assistenten für die **Grundinstallation**.

Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless LAN-Netzwerk.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- Nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- Nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- Bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

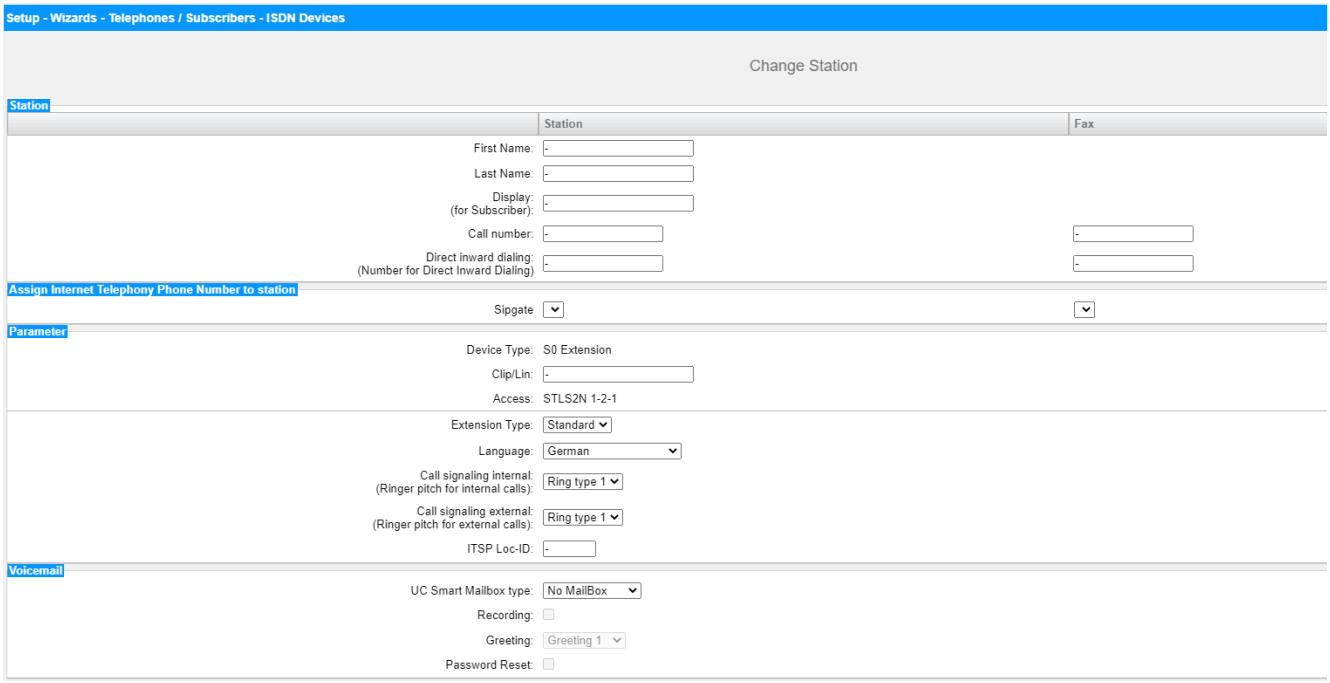
3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` ein.

Anmerkung: Der Name kann aus bis zu 16 Zeichen bestehen, sollte aber keine Umlaute oder Sonderzeichen enthalten. Der Name wird wie hier angegeben bei den UC Clients als Nachname eingetragen, kann dort aber nachbearbeitet werden.

---

4) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ des IP-Teilnehmers aus (z. B. "System Client" oder "SIP Client").

5) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:
   a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
   b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
6) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.
7) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.
8) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf oder für ein SIP-Telefon durch:
   a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



   b) Für SIP-Telefone: Wenn das SIP-Telefon zusammen mit einem Dual-Mode-Mobiltelefon betrieben werden soll, geben Sie im Bereich **Mobility** unter **mobile Rufnummer** die Amtskennziffer und gefolgt von der Rufnummer des Mobiltelefons ein (z.B. `0016012345678`). Wählen Sie zusätzlich aus der Aufklappliste **Web Feature ID** diesen SIP Client aus. (siehe Dual-Mode-Telefonie).

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur für SIP-Telefone: Geben Sie im Feld **Passwort** und im Feld **Passwort bestätigen** das Authentifizierungspasswort ein.

h) Nur für SIP-Telefone: Geben Sie im Feld **SIP User ID / Benutzername** die Benutzerkennung für die Authentifizierung ein.

i) Nur für SIP-Telefone: Geben Sie im Feld **Realm** die zugehörige Zone für die Authentifizierung ein.

j) Klicken Sie auf **OK & Weiter**.

k) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

l) Klicken Sie auf **OK & Weiter**.

9) Wenn Sie einen weiteren IP-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 8.

10) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten Teilnehmer. Diese Liste entspricht einem Rufnumernplan.

11) Klicken Sie bei Bedarf auf **Drucken**, um die Daten der eingerichteten Teilnehmer auszudrucken.

12) Klicken Sie anschließend auf **OK & Weiter**.

Zugehörige Konzepte

Mehrsprachige Textausgabe auf Seite 1243

6.7.7 Konfiguration von UC Suite

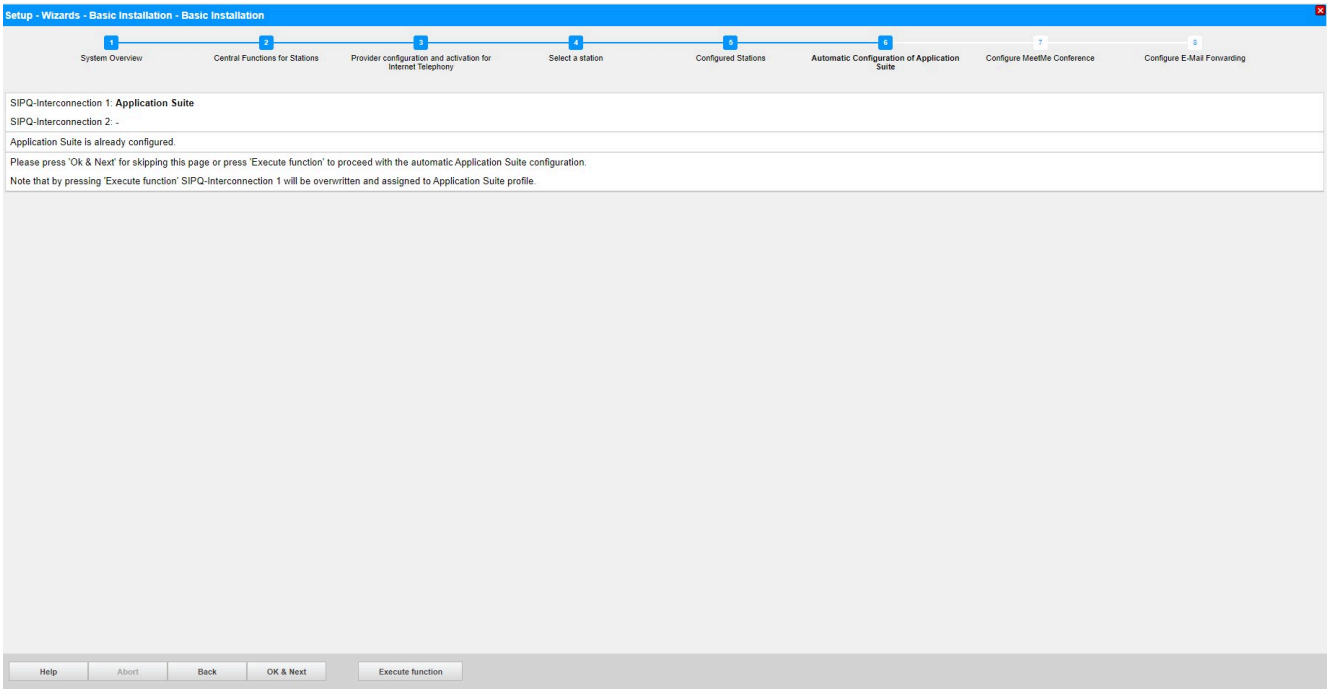
Im Fenster **Automatische Konfiguration der Applikation-Suite** können Sie die automatische Konfiguration der UC-Lösung UC Suite durchführen.

Anmerkung: Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Suite** gewählt wurde.

6.7.7.1 So konfigurieren Sie die UC Suite

Voraussetzungen

Sie befinden sich im Fenster **Automatische Konfiguration der Anwendungssuite**.



Schritt für Schritt

Klicken Sie auf **Funktion ausführen**. Die UC Suite wird automatisch konfiguriert. Sobald der Fortschrittsbalken 100 % anzeigt, klicken Sie auf **OK & Weiter**.

Anmerkung:

Für OpenScape Business S generiert der Assistent automatisch 60 Medienkanäle in UC Suite. Parallel dazu können 16 Kanäle für Ankündigungen genutzt werden, ohne dass zusätzliche Medienkanäle konfiguriert werden müssen.

6.7.8 Konfiguration der UC Smart Sprachboxen

Im Fenster **Automatische Konfiguration der Smart VM** können Sie die automatische Konfiguration der UC Smart Sprachboxen (Smart VM, Smart VoiceMail) durchführen, wenn die UC-Lösung UC Smart genutzt wird.

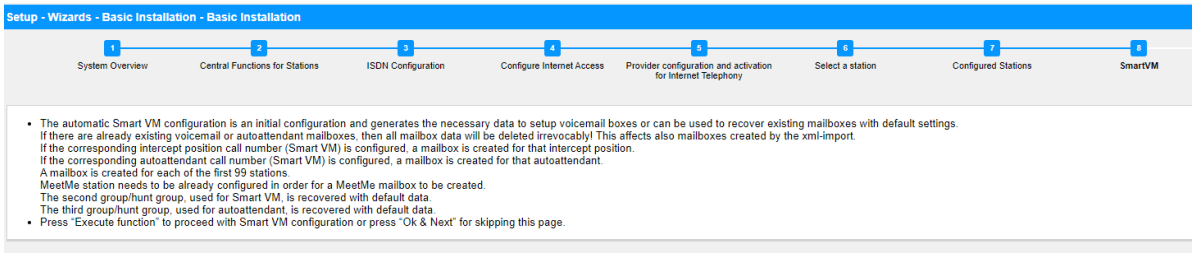
Anmerkung:

Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Smart** gewählt wurde.

6.7.8.1 Wie Sie die UC Smart Sprachboxen konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Automatische Konfiguration von Smart VM**.



Schritt für Schritt

1) Wenn die UC Smart Sprachboxen nicht genutzt werden sollen, klicken Sie auf **OK & Weiter**. Die Konfiguration der Sprachboxen wird übersprungen.
2) Wenn die UC Smart Sprachboxen genutzt werden sollen, klicken Sie auf **Funktion ausführen**. Für die ersten 100 Teilnehmer werden automatisch Sprachboxen konfiguriert. Sobald der Verlaufsbalken 100% anzeigt, klicken Sie auf **OK & Weiter**.

Anmerkung: Bereits vorhandene UC Smart Sprachboxen oder UC Smart AutoAttendant-Sprachboxen werden dabei unwiderruflich gelöscht.

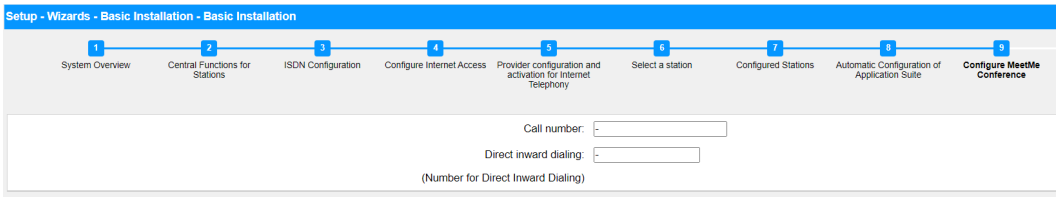
6.7.9 Konferenz-Server-Einstellungen

Im Fenster **MeetMe-Konferenz-Einstellungen ändern** können Sie die Rufnummer und die Einwahlnummer für Konferenzen festlegen.

6.7.9.1 Wie Sie die Konferenz-Server-Einstellungen ändern

Voraussetzungen

Sie befinden Sich im Fenster **MeetMe-Konferenz-Einstellungen ändern** im Assistenten für die **Grundinstallation**.



Schritt für Schritt

1) Geben Sie im Feld **Rufnummer** eine Rufnummer für die Konferenz ein.
2) Legen Sie im Feld **Durchwahl** die Einwahlnummer für die Konferenz (Konferenz-DUWA) fest, mit der sich Teilnehmer in eine bestehende Konferenz einwählen können.
3) Klicken Sie auf **OK & Weiter**.

6.7.10 E-Mail-Versand (optional)

Im Fenster **E-Mail-Weiterleitung ändern** können Sie den E-Mail-Versand konfigurieren. Teilnehmer werden dadurch über neue Sprach- und Faxnachrichten informiert und der Administrator erhält Systemmeldungen.

Sie haben folgende Möglichkeiten:

- E-Mail-Versand konfigurieren

  Sie können einen externen E-Mail-Server festlegen, über den OpenScape Business die E-Mails versenden soll. Sprach- und Faxnachrichten oder interne Systemmeldungen werden über diesen E-Mail-Server an eine oder verschiedene konfigurierbare E-Mail-Adressen versendet.

Anmerkung: Die Angabe eines E-Mail-Servers ist wichtig, wenn den Benutzern der UC Suite automatisch per E-Mail ein Link auf die Installationsdatei(en) geschickt werden soll.

6.7.10.1 E-Mail-Versand konfigurieren

Voraussetzungen

Wenn der externe E-Mail-Server für die Verwendung der einfachen Authentifizierung konfiguriert wurde, stellen Sie sicher, dass ein E-Mail-Konto mit Kennwort bei einem E-Mail-Anbieter vorhanden ist und Sie die Zugangsdaten für dieses Konto kennen.

Wenn der externe E-Mail-Server so konfiguriert wurde, dass er eine moderne Authentifizierung (Microsoft OAuth 2.0 tokenbasierte Autorisierung) verwendet, wie im Fall von Exchange Online, stellen Sie sicher, dass:

- Das E-Mail-Konto des Absenders muss für die Verwendung von SMTP mit Authentifizierung zugelassen sein (standardmäßig ist diese Option im Microsoft 365-Mandanten inaktiv). Sobald SMTP mit Authentifizierung aktiviert ist, funktioniert die OAUTH 2.0-E-Mail-Weiterleitung normal mit allen OpenScape Business-Mainboards.

- In Microsoft Azure Active Directory (Azure AD) eine Anwendung mit den erforderlichen Berechtigungen registriert wurde, damit Ihr OpenScape Business-System E-Mails versenden kann.
- Sie die Anwendungs- (Client-)ID und die Verzeichnis- (Mandanten-)ID der registrierten Anwendung kennen.

  Bitten Sie Ihren Azure AD-Administrator, diese Werte bei Bedarf bereitzustellen.
- Die E-Mail-Adresse, die als Absender der E-Mails angezeigt wird, gehört zum selben Azure AD oder Mandanten wie die registrierte Anwendung.

Sie befinden Sich im Fenster **E-Mail-Weiterleitung ändern** im Assistenten für die **Grundinstallation**.

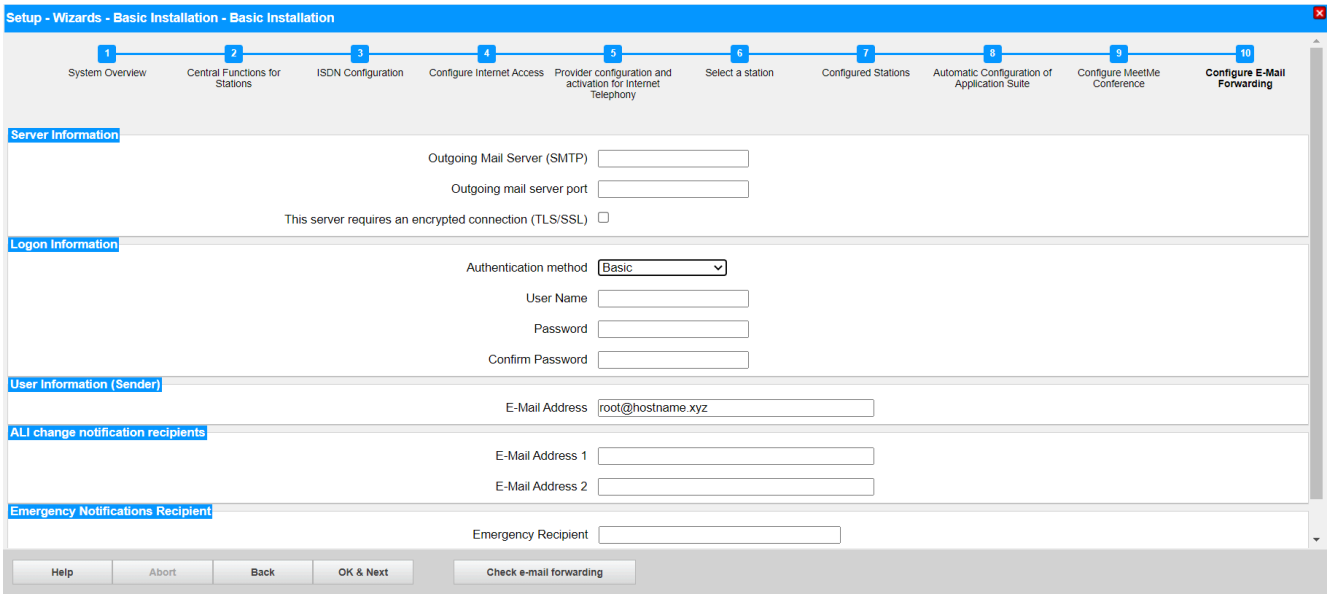


Abbildung 7: Optionen für die E-Mail-Weiterleitung bei Auswahl der einfachen Authentifizierungsmethode

Schritt für Schritt

1) Geben Sie den **Postausgangs-Server (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll, z. B. `smtp.web.de`. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.

Anmerkung: Achten Sie darauf, dass der Name des Postausgangs-Servers aufgelöst werden kann. Falls nicht, müssen Sie den Assistenten für den E-Mail-Versand starten über **Service-Center** > **E-Mail-Weiterleitung** und anstelle des Namens des Postausgangsservers dessen IP-Adresse eingeben.

---

2) Geben Sie den **Postausgangs-Server-Port (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.

3) Wenn eine sichere Verbindung erforderlich ist, aktivieren Sie das Kontrollkästchen **Dieser Server benötigt eine verschlüsselte Verbindung (TLS/SSL)**. Erfragen Sie ggf. bei Ihrem E-Mail-Provider, ob diese Option aktiviert werden muss.

4) Wenn der externe E-Mail-Server für die Verwendung der einfachen Authentifizierung konfiguriert wurde, gehen Sie wie folgt vor:
   a) Wählen Sie in der Dropdown-Liste **Authentifizierungsmethode** die Option **Einfach**.
   b) Geben Sie den **Benutzernamen** des E-Mail-Kontos ein z. B. `max.mustermann`.
   c) Geben Sie unter **Kennwort** und **Kennwort wiederholen** das Kennwort des E-Mail-Kontos ein.
5) Wenn der externe E-Mail-Server so konfiguriert wurde, dass er eine moderne Authentifizierung verwendet, gehen Sie wie folgt vor:
   a) Wählen Sie in der Dropdown-Liste **Authentifizierungsmethode** die Option **Microsoft OAuth 2.0**.
   b) Geben Sie die Anwendungs- (Client-)ID, die Sie vom Microsoft Azure-Portal erhalten haben, in das Feld **Anwendungs-ID** ein.
   c) Geben Sie in das Feld **Mandant** die Verzeichnis- (Mandanten-)ID ein, die Sie vom Microsoft Azure-Portal erhalten haben.
6) Geben Sie die **E-Mail-Adresse** ein, die als Absender der E-Mails erscheinen soll, z. B.: `john.doe@web.de`.
7) Geben Sie die **E-Mail-Adresse 1** ein, um eine Benachrichtigungs-E-Mail zu erhalten, wenn die ALI-Toleranz verwendet wurde. Sie können auch eine zweite E-Mail-Adresse in das Feld **E-Mail-Adresse 2** eingeben.
8) Geben Sie im Feld **Empfänger für Notfälle** die E-Mail-Adresse eines Sicherheitsbeauftragten vor Ort, an den eine E-Mail gesendet wird, wenn eine Notrufnummer gewählt wird.

   Der Betreff der E-Mail lautet „Neuer Notruf“. Wenn dies konfiguriert wurde, sind die Rufnummer und der Name des Anrufers, die aus der Datenbank des Systems abgerufen werden, in der E-Mail enthalten.
9) Wenn Sie **Microsoft OAuth 2.0** als Authentifizierungsmethode ausgewählt haben, gehen Sie wie folgt vor:
   a) Klicken Sie auf **OK & Weiter**.
   b) Warten Sie, bis ein Autorisierungslink und ein Benutzercode erscheinen.

      Der Autorisierungscode läuft nach einigen Minuten ab.
   c) Öffnen Sie den Autorisierungslink und geben Sie den Benutzercode in das Pop-up-Fenster ein.
   d) Melden Sie sich mit der E-Mail-Adresse an, die Sie in Schritt 6 auf Seite 260 **(E-Mail-Adresse**) eingegeben haben.

      Die E-Mail-Adresse muss sich im selben Azure AD oder Mandanten befinden wie die registrierte Anwendung.
   e) Nach erfolgreicher Authentifizierung zeigt das Pop-up-Fenster eine Meldung wie unten an:

      `Sie haben sich auf Ihrem Gerät bei <application-name> angemeldet. Sie können dieses Fenster nun schließen.`
   f) Schließen Sie das Pop-up und kehren Sie zum WBM zurück.
      Wenn die Authentifizierung erfolgreich war, wird die Meldung `Die Authentifizierung war erfolgreich!` angezeigt.

10) Falls Sie die eingegebenen E-Mail-Einstellungen überprüfen wollen, gehen Sie folgendermaßen vor:

a) Klicken Sie auf **E-Mail-Weiterleitung testen**.

b) Geben Sie unter **Senden an E-Mail-Adresse** die E-Mail-Adresse eines E-Mail-Postfachs ein, auf das Sie Zugriff haben. An diese E-Mail-Adresse wird die Test-E-Mail geschickt.

c) Geben Sie unter **Betreff in der E-Mail** einen beschreibenden Text ein, um die E-Mail in Ihrem E-Mail-Postfach identifizieren zu können.

d) Klicken Sie auf **Testmail senden**. Die E-Mail-Einstellungen werden überprüft und die E-Mail an das angegebene E-Mail-Postfach gesendet.

e) Überprüfen Sie, ob die E-Mail in Ihrem E-Mail-Postfach angekommen ist.

f) War der E-Mail-Versand erfolgreich, klicken Sie auf **Zurück** und gehen Sie zum nächsten Schritt.

g) War der E-Mail-Versand nicht erfolgreich, klicken Sie auf **Zurück** und überprüfen nochmal Ihre E-Mail-Einstellungen.

11) Klicken Sie auf **OK & Weiter** und anschließend auf **Fertig**. Die Basisinstallation ist beendet. Bevor Sie die im Wizard erwähnte Datensicherung durchführen, sollten Sie die Lizenzen aktivieren.

6.8 Abschließende Tätigkeiten

Nachdem die Erstinstallation und die Basisinstallation mit dem WBM abgeschlossen sind, müssen noch einige wichtige Einstellungen für den Betrieb von OpenScape Business getroffen werden.

Gehen Sie folgendermaßen vor:

1) Lizenzen aktivieren und zuordnen

Die mit OpenScape Business erworbenen Lizenzen müssen innerhalb einer Zeitspanne von 30 Tagen aktiviert werden. Die Zeitspanne startet beim ersten Anmelden am WBM. Nach Ablauf der Zeitspanne ist das Kommunikationssystem nur noch eingeschränkt nutzbar. Nach erfolgreicher Aktivierung müssen die Lizenzen den Teilnehmern und Leitungen zugeordnet werden. Systemweite Leistungsmerkmale sind bereits mit der Aktivierung freigeschaltet.

2) UC Smart Client zur Installation bereitstellen (nur für UC Smart)

3) UC Clients zur Installation bereitstellen

Die UC Clients sind Bestandteil der UC Suite. Die Installationsdateien für die UC Clients sind über das WBM zugänglich und können den IP-Teilnehmern automatisch oder manuell zur Verfügung gestellt werden.

Zusätzlich gibt es für den Administrator die Möglichkeit der Silent Installation. Dabei handelt es sich um eine kommandozeilenbasierte Methode zur automatischen Installation, Deinstallation und Modifikation von UC Suite Clients auf einem PC ohne weitere erforderliche Eingaben. Weitere Informationen finden Sie unter Silent Installation/Deinstallation für UC Suite PC-Clients.

4) Datensicherung durchführen

Die bisherigen Änderungen an OpenScape Business müssen gesichert werden. Die Sicherung kann als Backup-Set z.B. im internen Netz gespeichert werden.

6.8.1 Wie Sie die Lizenzen aktivieren und zuordnen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Sie kennen den LAC (Lizenz-Autorisierungscode) für die Lizenzfreischaltung und haben eine Benutzerkennung und ein Passwort für den Zugang zum Lizenzserver.

Für die Verbindung zum Lizenzserver ist ein Internet-Zugang nötig.

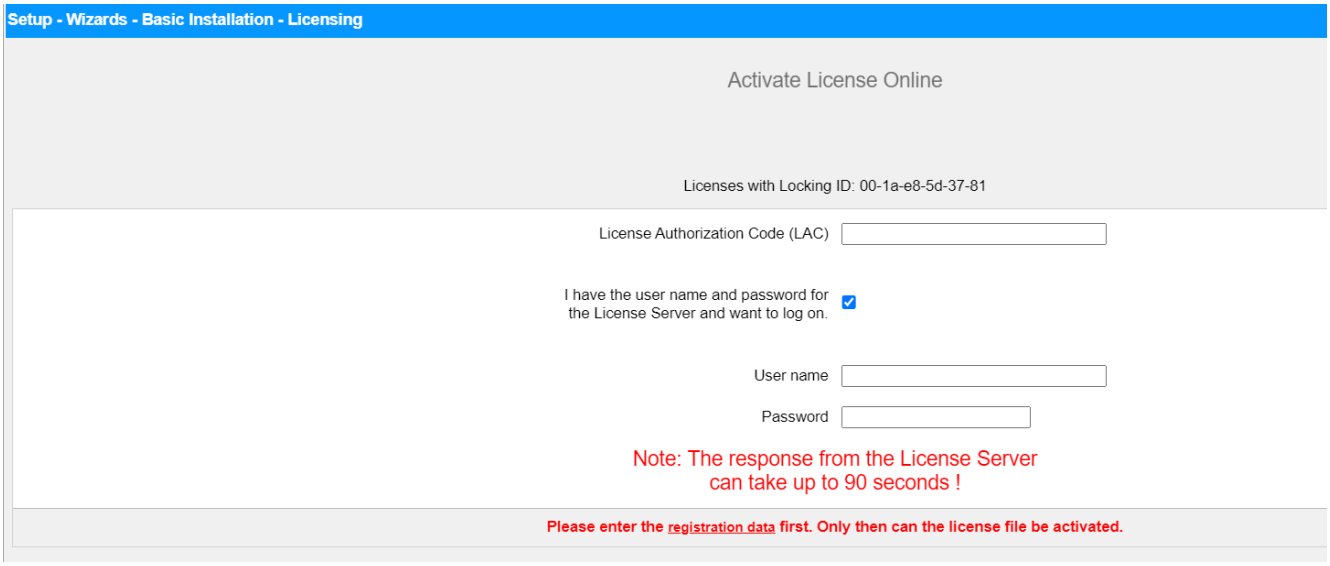
Schritt für Schritt

1) Lizenzen online aktivieren:

a) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

b) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.

c) Klicken Sie auf **Bearbeiten**, um den Wizard **Lizenzierung** zu starten.



d) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.

e) Aktivieren Sie das Kontrollkästchen **Ich habe Benutzernamen und Passwort für den Lizenzserver und möchte mich anmelden**.

f) Geben Sie **Benutzername** und **Passwort** für die Anmeldung am Lizenzserver ein.

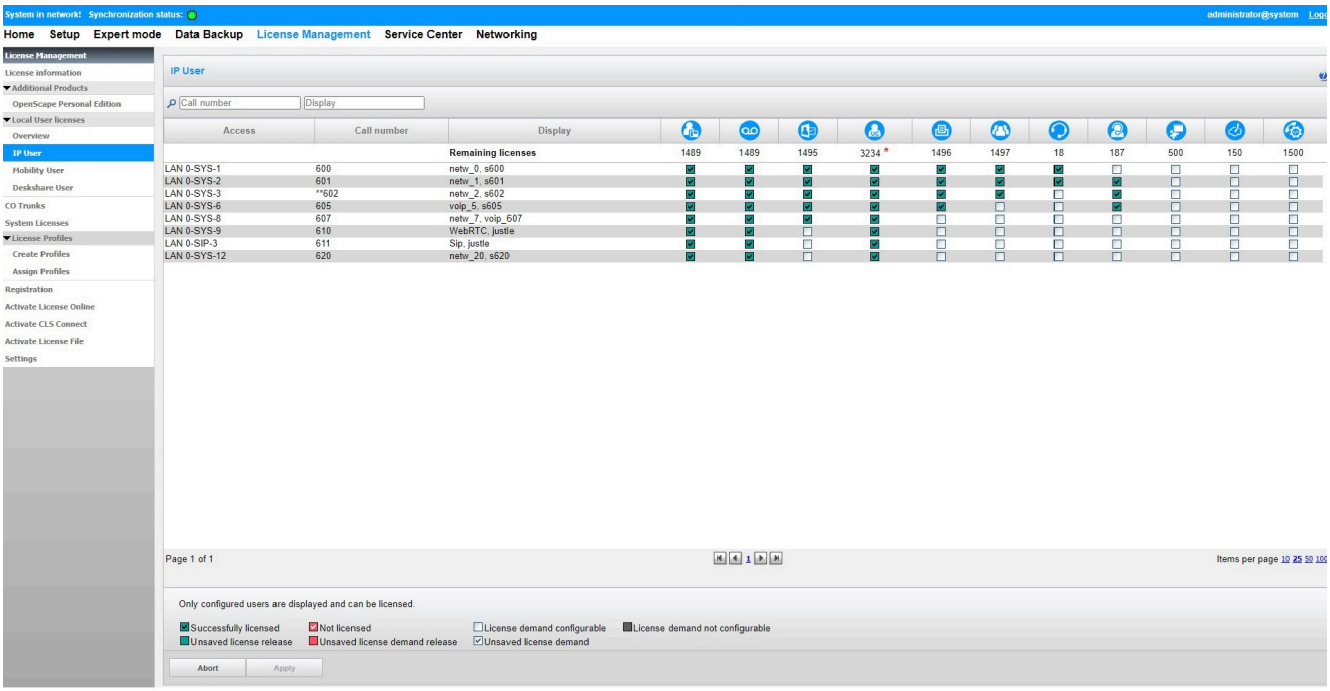
g) Klicken Sie auf **OK & Weiter**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen freigeschaltet.

2) Lizenzen den Teilnehmern zuordnen:

a) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

b) Navigieren Sie im Navigationsbaum unter **Lokale Benutzerlizenzen > ...** zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.

c) Aktivieren Sie in der Zeile des gewünschten Teilnehmers das Kontrollkästchen in der Spalte **Benutzer-Lizenz** (erste Spalte mit Kontrollkästchen).



d) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.

Anmerkung: User-orientierte Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz (Benutzer-Lizenz) zugeordnet wurde (Schritt c).

---

e) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.

Sind ausreichend Lizenzen vorhanden ist die Lizenzierung der Teilnehmer beendet.

f) Fehlen Lizenzen, werden Ihnen die Fehler mit rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt e.

3) Lizenzen den Leitungen zuordnen:

a) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich **Amtsleitungen** wird Ihnen die Anzahl der erworbenen Leitungslizenzen angezeigt.

b) Für SIP-Leitungen: Geben Sie im Bereich **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der

Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.

c) Klicken Sie auf **OK & Weiter**.

6.8.2 Wie Sie den UC Smart Client zur Installation bereitstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Hard- und Software für die Nutzung von UC @work ist vorhanden.

Anmerkung: Für die Nutzung des UC Smart Clients myPortal @work sind Lizenzen erforderlich.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Software**.

3) Klicken Sie auf das Download-Symbol von **myPortal @work** und speichern Sie die Installationsdatei auf einem freigegebenen Netz-Laufwerk.

4) Senden Sie den Benutzern von myPortal @work die beiden Installationsdateien.

5) Alternativ können Sie den Benutzern von myPortal @work auch den Link zuschicken, über den sie direkt auf die Installationsdatei zugreifen können:

```
https://<IP-Adresse des Kommunikationssystems>/
management/downloads/myPortalAtWorkSetup.exe
```

6.8.3 Wie Sie die UC Suite Clients zur Installation bereitstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Hard- und Software für die Nutzung von UC Suite ist vorhanden.

Anmerkung: Für die Nutzung der UC Suite Clients sind Lizenzen nötig.

Schritt für Schritt

1) Damit die Installationsdateien einem Teilnehmer automatisch zur Verfügung gestellt werden können, vergewissern Sie sich, ob folgende Schritte durchgeführt worden sind:

a) Die E-Mail-Adressen der Teilnehmer müssen entweder zusammen mit den Teilnehmerdaten über eine XML-Datei importiert worden sein oder eingetragen werden unter **Einrichtung** > **UC Suite** > **Benutzerverzeichnis**.

b) Ein Mail-Server muss eingetragen sein.

> **Anmerkung:** Einen E-Mail-Server können Sie auch nachträglich eintragen unter **Service-Center** > **Email-Weiterleitung**.

Alle Teilnehmer, deren E-Mail-Adressen bekannt sind, erhalten eine E-Mail mit dem Link auf das Installationsverzeichnis der UC Clients und mit einer Erste-Schritte-Anleitung. Im Installationsverzeichnis liegt zusätzlich eine Readme-Datei mit Informationen zur Installation der Software auf den Client-PCs.

2) Falls die nötigen Schritte für eine automatische Benachrichtigung nicht erfüllt sind, können Sie die Installationsdateien auch manuell zur Verfügung stellen. Gehen Sie dazu folgendermaßen vor:

a) Klicken Sie in der Navigationsleiste auf **Service-Center**.
b) Klicken Sie im Navigationsbaum auf **Software**.
c) Klicken Sie auf den gewünschten UC Client und speichern Sie die gezippte Installationsdatei auf einem freigegebenen Netz-Laufwerk.
d) Klicken Sie im Navigationsbaum auf **Dokumente** und wählen Sie die Aufklappliste **Bedienungsanleitung**.
e) Klicken Sie auf die Dokumentation zum gewünschten UC Client und speichern Sie die Dokumentationsdatei auf einem freigegebenen Netz-Laufwerk.
f) Senden Sie den Benutzern der UC Clients die gezippte Installationsdatei und die Dokumentationsdatei per E-Mail oder teilen Sie den Benutzern den Ablageort der Dateien mit.
g) In der Zip-Datei mit den Installationsdateien ist auch eine Readme-Datei enthalten. Weisen Sie die Benutzer darauf hin, dass die Installation der UC Clients anhand der Installationshinweise in der Readme-Datei durchgeführt werden muss.

3) Alternativ können Sie den UC Benutzern auch Links zuschicken, über die sie direkt auf die Installationsdateien der UC Clients zugreifen können.

a) Klicken Sie in der Navigationsleiste auf **Service-Center**.
b) Klicken Sie im Navigationsbaum auf **Software**.
c) Klicken Sie auf die Schaltfläche **Applikationslinks anzeigen**. Es werden Ihnen mehrere Links angezeigt, abhängig vom verwendeten Betriebssystem und vom gewünschten UC Client. Zum Beispiel:

```
https://<IP-Adresse des Kommunikationssystems>/
management/downloads/install-common.zip
```

6.8.4 Wie Sie eine Datensicherung durchführen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

> **Anmerkung:** Weitere Informationen zur Datensicherung siehe Sofortiges Sichern .

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup - sofort**.
3) Geben Sie im Bereich **Name** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.
4) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll (z B. auf einem Netzlaufwerk).
5) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.
6) Die Sicherung ist erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt!** erscheint. Klicken Sie auf **Beenden**.
7) Die Erstinbetriebnahme mit dem WBM ist nun abgeschlossen. Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

6.9 Inbetriebnahme der IP-Telefone

Eine komfortable Inbetriebnahme der IP-Telefone erfordert einen DHCP-Server, der das IP-Telefon mit den für die Anmeldung am Kommunikationssystem wichtigen Daten (netzwerkspezifische Daten) versorgt.

Netzwerkspezifische Daten

Ein IP-Telefon benötigt für die Anmeldung am Kommunikationssystem netzwerkspezifische Daten. Diese Daten können einerseits im DHCP-Server gespeichert sein oder direkt am IP-Telefon eingegeben werden. Vorteil eines DHCP-Servers ist, dass alle angeschlossenen IP-Telefone automatisch mit den Daten versorgt werden.

Folgende Daten werden vom IP-Telefon benötigt:

- IP-Adresse des Kommunikationssystems
- IP-Adresse des DLS-Servers

Zusätzlich benötigt das IP-Telefon noch die eigene Rufnummer. Diese muss während der Anmeldung manuell am Telefon eingetragen werden.

Registrierung von SIP-Telefonen

Aus Sicherheitsgründen ist es empfehlenswert, dass sich SIP-Telefone am Kommunikationssystem registrieren. Dazu müssen die Registrationsdaten am IP-Telefon und im Kommunikationssystem übereinstimmen.

Folgende Daten werden für die Anmeldung benötigt:

- SIP-Benutzer-ID
- SIP-Passwort
- SIP-Realm (optional)

Verwenden Sie ein nicht triviales SIP-Passwort, das folgende Regeln erfüllt:

- Mindestens 8 Stellen
- Mindestens einen Großbuchstaben (A - Z)
- Mindestens einen Kleinbuchstaben (a - z)

- Mindestens eine Ziffer (0-9)
- Mindestens ein Sonderzeichen

Verwenden Sie eine SIP-Benutzer-ID, die nicht die Telefonnummer enthält.

Anmerkung: Weitere Informationen zur Einrichtung von SIP-Telefonen finden Sie unter `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Nutzung des internen DHCP-Servers

Wird der interne DHCP-Server des Kommunikationssystems genutzt, sind die netzwerkspezifischen Daten dort bereits hinterlegt. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, muss am IP-Telefon nur die festgelegte Rufnummer eintragen werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

Nutzung eines externen DHCP-Servers mit netzwerkspezifischen Daten

Wird ein externer DHCP-Server genutzt, sind die netzwerkspezifischen Daten dort zu hinterlegen. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, muss am IP-Telefon nur die festgelegte Rufnummer eintragen werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

Nutzung eines externen DHCP-Servers ohne netzwerkspezifische Daten

Wird ein externer DHCP-Server genutzt, bei dem die netzwerkspezifischen Daten nicht hinterlegt werden können, müssen diese am IP-Telefon eingegeben werden. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, müssen am IP-Telefon die festgelegte Rufnummer und die IP-Adresse des Kommunikationssystems eintragen und evtl. die Einstellungen für den Deployment Service geändert werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

6.9.1 Wie Sie ein IP-Telefon konfigurieren

Voraussetzungen

Das IP-Telefon ist an das interne Netz angeschlossen und betriebsbereit.

Anmerkung: Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 IP-Systemtelefons beschrieben. Für ein anderes IP-Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres IP-Telefons nach.

Schritt für Schritt

1) Um in den Administrationsmodus des IP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.

2) Blättern Sie im Register `Einstellungen` bis `Admin` und bestätigen Sie mit der OK-Taste.
3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.
4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.
5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des IP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für IP-Systemtelefone. Gehen Sie folgendermaßen vor:
   a) Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
   b) Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
   c) Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.
   d) Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
   e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
   f) Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.
   g) Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.
   h) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
   i) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
   j) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.
6) Legen Sie die Rufnummer des Telefons fest:
   a) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
   b) Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.
   c) Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.
   d) Geben Sie die festgelegte Rufnummer ein (z.B. `120`) und bestätigen Sie mit der OK-Taste.
   e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
7) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.
8) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

6.9.2 Wie Sie ein SIP-Telefon konfigurieren

Voraussetzungen

Das SIP-Telefon ist an das Kunden-LAN angeschlossen und betriebsbereit.

Anmerkung: Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 SIP-Systemtelefons beschrieben. Für ein anderes SIP-Telefon müssen diese Einstellungen analog

durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres SIP-Telefons nach.

Schritt für Schritt

1) Um in den Administrationsmodus des SIP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.
2) Blättern Sie im Register `Einstellungen` bis `Administrator (Admin)` und bestätigen Sie mit der OK-Taste.
3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.
4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.
5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des SIP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für SIP-Systemtelefone. Gehen Sie folgendermaßen vor:
   a) Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
   b) Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
   c) Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.
   d) Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
   e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
   f) Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.
   g) Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.
   h) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
   i) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
   j) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.
6) Legen Sie die SNTP-Zeiteinstellungen fest:
   a) Blättern Sie bis `Date and time` und bestätigen Sie mit der OK-Taste.
   b) Blättern Sie bis `Time source` und bestätigen Sie mit der OK-Taste.
   c) Blättern Sie bis `SNTP IP address` und bestätigen Sie mit der OK-Taste.
   d) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
   e) Blättern Sie bis `Timezone offset` und bestätigen Sie mit der OK-Taste.
   f) Geben Sie die Abweichung der lokalen Uhrzeit von der UTC-Zeit (Universal Time Coordinated) in Stunden an (Deutschland: `1`) und bestätigen Sie mit der OK-Taste.
   g) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
   h) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

7) Legen Sie die Rufnummer des Telefons fest:
   a) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
   b) Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.
   c) Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.
   d) Geben Sie die festgelegte Rufnummer ein (z.B. `120`) und bestätigen Sie mit der OK-Taste.
   e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

8) Legen Sie die SIP-Authentifizierungsdaten fest:
   a) Blättern Sie bis `Registration` und bestätigen Sie mit der OK-Taste.
   b) Blättern Sie bis `SIP session` und bestätigen Sie mit der OK-Taste.
   c) Notieren Sie sich die `Realm` oder geben Sie bei Bedarf eine neue Realm (z.B. `OSBIZ-SIP`) ein.
   d) Notieren Sie sich die `User ID` oder geben Sie bei Bedarf eine neue User ID (z.B. `SIP-120`) ein.
   e) Vergeben Sie ein `Passwort` für die Registrierung am SIP Server.
   f) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

9) Navigieren Sie mit der Zurück-Taste zum Menü `Admin` zurück.

10) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

6.10 Deinstallation der Kommunikationssoftware

Die Deinstallation der Kommunikationssoftware ist über eine Text-Konsole möglich.

6.10.1 Wie Sie die Kommunikationssoftware deinstallieren

Schritt für Schritt

1) Öffnen Sie ein Terminal (z.B. GNOME Terminal).

2) Geben Sie in der Shell-Oberfläche den Befehl `su` (für superuser = root) ein und bestätigen Sie mit der Eingabetaste.

3) Geben Sie in der Shell-Oberfläche das Passwort für den Benutzer "root" ein und bestätigen Sie mit der Eingabetaste.

4) Geben Sie in der Shell-Oberfläche den Befehl `oso_deinstall.sh` ein und bestätigen Sie mit der Eingabetaste. Folgen Sie den Anweisungen des Deinstallationsprogramms.

6.11 Verwendete Ports

Die OpenScape Business Systemkomponenten nutzen verschiedene Ports, die bei Bedarf in der Firewall freigeschaltet werden müssen. Für die Ports der Webbased Clients (z.B. myPortal to go) muss ein Port Forwarding im Router eingerichtet werden.

Eine tatsächliche und vollständige Liste aller verwendeten Ports von OpenScape Business finden Sie in der "Interface Management Database" (IFMD), die über das Partnerportal von Unify abgerufen werden kann (https://unify.com/en/partners/partner-portal.

Anmerkung: Die in der folgenden Liste mit "O" identifizierten Ports sind optional, d. h. Sie sind in der Firewall nicht dauerhaft geöffnet.

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Systemkomponenten							
Admin Portal (https)	X		443	X	X	X	X
CAR-Lebendigkeitsprüfungen	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (bis zu V3R3) 7780, 7791 (ab V3R3.1 und höher)	O		O	
Communication Client-Installationsprogramm	X		8101	X	X	X	X
Csta Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
Csta Service Provider (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP Server	X		389		X	X	X

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
xNAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
xOpenfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X
OpenScape Business Benutzerportal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (eingebettet)		X	29100-30530	X	X	X	X
RTP (Server)		X	29100-30888	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (Traps)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

Anmerkung: Aus Sicherheitsgründen wird empfohlen für die Webbased Clients ausschließlich https zu verwenden und ein Port Forwarding von extern TCP/443 nach intern TCP/8802 einzurichten.

CLS-Zertifikat

Ab V3R3.1 wird über einen neu eingeführten Port ein neues CLS-Zertifikat mit aktualisiertem Common Name (CN) bereitgestellt. Dies bietet einen verbesserten und stärkeren Digest-Algorithmus sowie aktualisierte juristische Personen an. Die online über den CLS Connect-Modus lizenzierten Systeme erfordern die folgenden zwei Voraussetzungen:

- Die IP-Adresse 188.64.16.4 ist für ausgehenden Datenverkehr in der Firewall aktiviert.
- Die Ports 7780 und 7791 sind für ausgehenden Datenverkehr in der Firewall aktiviert.

Der zuvor verwendete Port 7790 kann nach dem Upgrade auf V3R3.1 aus der Firewall-Konfiguration entfernt werden, um die Sicherheit zu erhöhen.

6.12 Diagnose-Traces für einen Fehlerfall erfassen

Sie können automatisch die erforderlichen Diagnose-Traces für einen Fehlerfall erfassen. Der Wizard **Fehlermanagement** führt Sie durch den gesamten Prozess.

Sie müssen den **Fehlermanagement**-Wizard zweimal ausführen: vor und nach der Ausführung des problematischen Szenarios. Beim ersten Durchlauf (Phase 1) aktivieren Sie die Erfassung von Diagnose-Traces. Nach der Ausführung des problematischen Szenarios führen Sie den Assistenten erneut aus, um die Diagnose-Trace-Daten zu sammeln (Phase 2). Sobald Phase 2 abgeschlossen ist, können Sie die Trace-Datei herunterladen und in das Ticketsystem aufnehmen.

Führen Sie die folgenden Schritte durch, um die Diagnose-Trace-Daten für den Fehlerfall zu erfassen:

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten** neben **Fehlermanagement**.

3) Klicken Sie auf **OK & Weiter**.

4) Wenn Sie die Standard-Traces erfassen möchten, klicken Sie auf das Kontrollkästchen **Standard-Traces** .

5) Wenn Sie die Art der zu erfassenden Traces angeben möchten, wählen Sie die gewünschten Traces aus der entsprechenden Liste aus. Mehr als eine Auswahl ist möglich.

Weitere Informationen zu Traces finden Sie im Handbuch zur Problembehebung.

6) Klicken Sie auf **OK & Weiter**.

7) Eine Liste mit zusätzlichen Informationen, relevanter Dokumentation und Hinweisen wird angezeigt. Klicken Sie auf **OK & Weiter**.

8) Die Szenarien und der Typ der Traces, die Sie erfassen möchten, werden angezeigt. Klicken Sie auf **Fertig**.

9) Fahren Sie mit der Ausführung des problematischen Szenarios fort.

10) Navigieren Sie nach Abschluss des Szenarios erneut zu **Setup > Fehlermanagement** und klicken Sie auf **Bearbeiten**.

    Sie werden zu Schritt 2 der Erfassung von Diagnose-Traces weitergeleitet. Wenn Sie den Prozess anhalten und erneut starten möchten, klicken Sie auf die Schaltfläche **Abbrechen**.

11) Klicken Sie auf **OK & Weiter**.

12) Geben Sie die erforderlichen Informationen ein und klicken Sie auf **OK & Weiter**.

13) Eine Liste mit den erforderlichen Informationen und einigen weiteren Aktionen wird angezeigt.

14) Klicken Sie auf **OK & Weiter**.

15) Klicken Sie auf **Fertigstellen** , um mit dem Herunterladen der Diagnose-Trace-Daten zu beginnen.

6.13 Neuflash

Mit den folgenden Schritten können Sie den Softwaretyp eines Geräts leicht ändern.

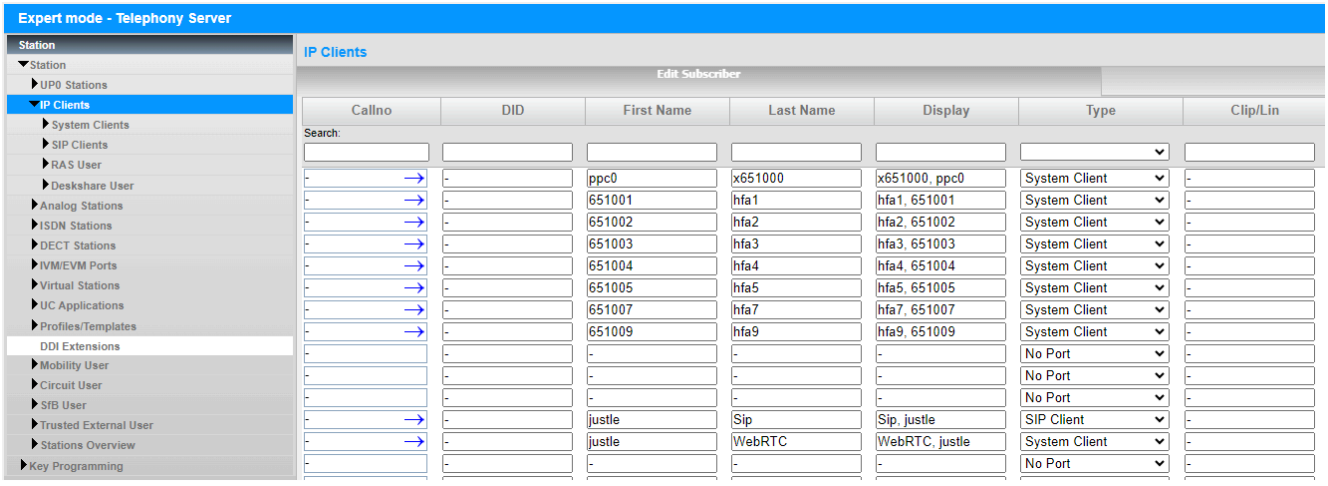
Das Konzept hinter diesem Merkmal ist es, die Art und Weise zu vereinfachen, ein SIP-Gerät (out of the box) zu bekommen und es im OSBiz-System als HFA-Gerät zu registrieren. Die einzigen Anforderungen sind:

- das Telefon muss die DLI-Adresse erhalten (entweder vom DHCP-Server oder manuell)
- der Administrator muss die Nummer des Telefons eingeben (das als System Client vorkonfiguriert sein muss)

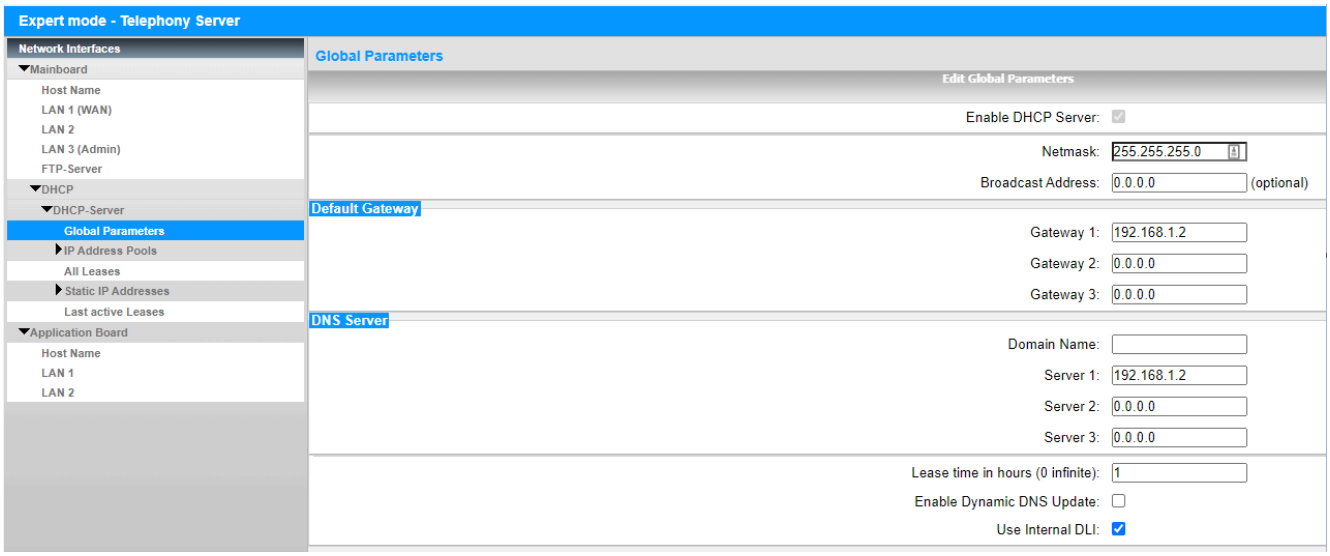
Sobald der Kunde ein neues Gerät erhält, wird es als SIP-Gerät vorkonfiguriert (Werkseinstellungen). Die Schritte zum Neuflashen dieses Geräts auf ein HFA-Gerät sind wie folgt:

Schritt für Schritt

1) Konfigurieren Sie in der OSBIZ-Datenbank die gewünschte Rufnummer als System Client (HFA).



2) Konfigurieren Sie den DHCP-Server, um die IP-Adresse des DLI zu senden. Dies kann entweder über den externen DHCP-Server oder den internen DHCP-Server erfolgen.



3) Wenn kein DHCP-Server verwendet wird, müssen Sie die DLI-IP auf dem Telefon manuell konfigurieren.

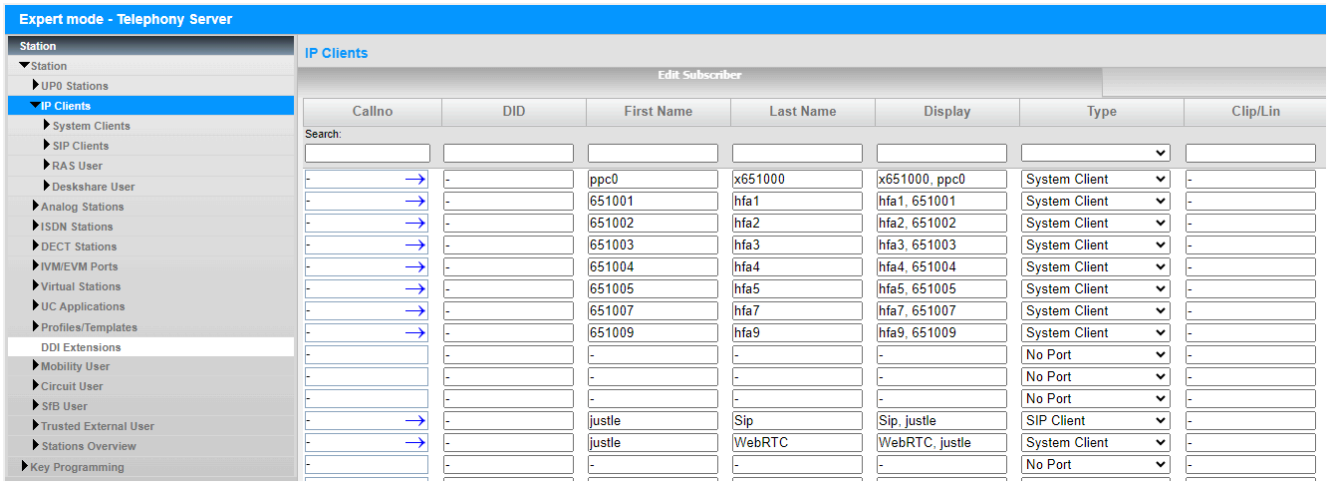
4) Sobald das SIP-Telefon eine IP und die DLI-IP erhalten hat, wird das Telefongerät in der DLI-Datenbank registriert, und es wird eine Aufforderung zur Eingabe der Nebenstellennummer angezeigt.

5) Geben Sie die Endgerätnummer am Telefon ein (die Nummer sollte dieselbe wie die im ersten Schritt konfigurierte sein, z. B. 4111).

6) Der Neuflash wird gestartet und das neue HFA-Image wird auf das Telefon heruntergeladen. Wenn das Telefon neu gestartet wird, wird es als HFA-Telefon registriert und die Plug-and-Play-Daten werden vom System an das Telefon gesendet.

7) **Um ein bereits registriertes SIP-Telefon neu zu flashen:**

8) Ändern Sie den SIP-Arbeitsgerätetyp in "System Client".



9) Starten Sie das Telefon neu.

10) Der Neuflash wird gestartet und das neue HFA-Image wird auf das Telefon heruntergeladen. Wenn das Telefon neu gestartet wird, wird es als HFA-

Telefon registriert und die Plug-and-Play-Daten werden vom System an das Telefon gesendet.

7 Ersteinrichtung OpenScape Business UC Booster

Dieser Abschnitt beschreibt die Erstinstallation und Konfiguration des OpenScape Business UC Boosters am OpenScape Business X3/X5/X8-Kommunikationssystem. Beachten Sie, dass hier unterschieden wird, je nachdem, ob die OpenScape Business UC Booster Card oder der OpenScape Business UC Booster Server für die UC Booster Funktionalität verwendet werden soll.

Die Ersteinrichtung des OpenScape Business UC Boosters erfolgt über das OpenScape Business Assistant-Verwaltungsprogramm (webbasiertes Management, kurz auch als WBM genannt).

Die ausführliche Administration der über die Ersteinrichtung hinausgehenden Leistungsmerkmale finden Sie in den anschließenden Kapiteln.

Ersteinrichtung der OpenScape Business UC Booster Card

Die OpenScape Business UC Booster Card wird im OpenScape Business X3/X5/X8-Kommunikationssystem installiert und für den Betrieb konfiguriert. Darauf folgt die Konfiguration der OpenScape Business UC Booster-Funktionalität.

Die konkreten Installationsschritte, die für die Ersteinrichtung erforderlich sind, unterscheiden sich, je nachdem, ob die UC Booster Card erstmalig mit dem OpenScape Business X3/X5/X8-Kommunikationssystem in Betrieb genommen wird oder ob sie später in ein bestehendes und bereits konfiguriertes OpenScape Business X3/X5/X8-Kommunikationssystem integriert wird.

Übersicht der Installationsschritte für beide Optionen:

Integration in ein neues Kommunikationssystem	Integration in ein bestehendes Kommunikationssystem
	Sichern der Konfigurationsdaten des Kommunikationssystems
Installation der UC Booster Card Die UC Booster Card wird im OpenScape Business X3/X5/X8-Kommunikationssystem installiert. Eine Beschreibung finden Sie in der OpenScape Business Service Dokumentation, Hardware-Installation und Beschreibung der Platinen.	Installation der UC Booster Card Die UC Booster Card wird im OpenScape Business X3/X5/X8-Kommunikationssystem installiert. Eine Beschreibung finden Sie in der OpenScape Business Service Dokumentation, Hardware-Installation und Beschreibung der Platinen.
Konfigurieren der UC Booster Card Die Konfiguration der UC Booster Card erfolgt zusammen mit der Erstinstallation des OpenScape Business X3/X5/X8-Kommunikationssystems. Eine Beschreibung finden Sie unter Integration in das Kunden-LAN.	Konfigurieren der UC Booster Card Die Konfiguration der UC Booster Card wird später auf einem bereits konfigurierten OpenScape Business X3/X5/X8-Kommunikationssystem durchgeführt. Eine Beschreibung finden Sie unter Integration in das Kunden-LAN. Einzelheiten zur Konfiguration finden Sie unter Konfigurieren der UC Booster Card

Integration in ein neues Kommunikationssystem	Integration in ein bestehendes Kommunikationssystem
Grundkonfiguration Die Grundkonfiguration erfolgt zusammen mit der Erstinstallation des OpenScape Business X3/X5/X8-Kommunikationssystems. Eine Beschreibung finden Sie unter Grundkonfiguration.	Grundkonfiguration Die Grundkonfiguration wird später auf einem bereits konfigurierten OpenScape Business X3/X5/X8-Kommunikationssystem durchgeführt. Eine Beschreibung finden Sie unter Grundkonfiguration. Die Besonderheiten der Basiskonfiguration finden Sie unter Grundkonfiguration
Abschlussaktivitäten Die Abschlussaktivitäten (einschließlich der Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business X3/X5/X8-Kommunikationssystems durchgeführt. Eine Beschreibung finden Sie unter Abschlussaktivitäten.	Abschlussaktivitäten Die Abschlussaktivitäten (einschließlich der Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business X3/X5/X8-Kommunikationssystems durchgeführt. Eine Beschreibung finden Sie unter Abschlussaktivitäten. Die Besonderheiten der Abschlussaktivitäten finden Sie unter Abschlussaktivitäten

Erstinstallation des OpenScape Business UC Booster Servers

Der OpenScape Business UC Booster Server ist zusammen mit dem OpenScape Business X3/X5/X8-Kommunikationssystem in das Kunden-LAN integriert.

Die OpenScape Business-Kommunikationssoftware für den OpenScape Business UC Booster Server, die OpenScape Business UC Booster-Funktionalität bietet, wird auf dem Linux Betriebssystem SLES 12 SP5 64-Bit oder SLES 15 SP6 64-Bit installiert. Die Kommunikationssoftware kann direkt auf einem Linux-Server oder in einer virtuellen Umgebung mit VMware vSphere betrieben werden. Die Installation des Linux-Betriebssystems ist im Installationshandbuch *OpenScape Business, Installation des Linux-Servers* beschrieben.

Der OpenScape Business UC Booster Server verfügt über einen eigenen WBM. Dieser WBM wird für Software-Updates, Sicherung der Konfigurationsdaten und Diagnose des OpenScape Business UC Booster Servers verwendet. Die Erstinstallation des OpenScape Business UC Booster Servers erfolgt mit dem WBM des Kommunikationssystems.

Je nachdem, ob der UC Booster Server zum ersten Mal mit dem OpenScape Business X3/X5/X8-Kommunikationssystem in Betrieb genommen wird oder ob er später an ein bestehendes und bereits konfiguriertes OpenScape Business X3/X5/X8-Kommunikationssystem angeschlossen wird, unterscheiden sich die spezifischen Installationsschritte für die Erstinstallation.

Übersicht der Installationsschritte für beide Optionen:

Integration in ein neues Kommunikationssystem	Integration in ein bestehendes Kommunikationssystem
	Sichern der Konfigurationsdaten des Kommunikationssystems
Installation des Linux-Servers Die Installation des Linux-Servers wird im OpenScape Business Linux Server Installationshandbuch beschrieben.	Installation des Linux-Servers Die Installation des Linux-Servers wird im OpenScape Business Linux Server Installationshandbuch beschrieben.
Installation der Kommunikationssoftware	Installation der Kommunikationssoftware
Konfigurieren des UC Booster Servers Die Konfiguration des UC Booster Servers erfolgt zusammen mit der Erstinstallation des OpenScape Business X3/X5/X8-Kommunikationssystems. Eine Beschreibung finden Sie unter Integration in das Kunden-LAN.	Konfigurieren des UC Booster Servers Die Konfiguration des UC Booster Servers wird später auf einem bereits konfigurierten OpenScape Business X3/X5/X8-Kommunikationssystem durchgeführt. Eine Beschreibung finden Sie unter Integration in das Kunden-LAN. Einzelheiten zur Konfiguration finden Sie unter Konfigurieren des UC Booster Servers
Grundkonfiguration Die Grundkonfiguration erfolgt zusammen mit der Erstinstallation des OpenScape Business X3/X5/X8-Kommunikationssystems. Eine Beschreibung finden Sie unter Grundkonfiguration.	Grundkonfiguration Die Grundkonfiguration wird später auf einem bereits konfigurierten OpenScape Business X3/X5/X8-Kommunikationssystem durchgeführt. Eine Beschreibung finden Sie unter Grundkonfiguration. Die Besonderheiten der Basiskonfiguration finden Sie unter Grundkonfiguration
Abschlussaktivitäten Die Abschlussaktivitäten (einschließlich der Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business X3/X5/X8-Kommunikationssystems durchgeführt. Eine Beschreibung finden Sie unter Abschlussaktivitäten.	Abschlussaktivitäten Die Abschlussaktivitäten (einschließlich der Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business X3/X5/X8-Kommunikationssystems durchgeführt. Eine Beschreibung finden Sie unter Abschlussaktivitäten. Die Besonderheiten der Abschlussaktivitäten finden Sie unter Abschlussaktivitäten

7.1 Voraussetzungen für die Ersteinrichtung

Die Erfüllung der Voraussetzungen für die Erstinstallation stellt den ordnungsgemäßen Betrieb des OpenScape Business UC Boosters sicher.

Allgemein

Je nach verwendeter Hardware (Telefone, ...) und bestehender Infrastruktur gelten folgende Rahmenbedingungen:

- Das OpenScape Business X3/X5/X8-Kommunikationssystem ist konfiguriert und einsatzbereit.
- Die LAN-Infrastruktur (Internet-Router, Switches, etc.) ist vorhanden und nutzbar.
- Die IP-Telefone sind mit dem Kunden-LAN verbunden.
- Für Software-Updates und Fernzugriff wird eine Breitband-Internetverbindung empfohlen.
- Alle für OpenScape Business UC Booster erforderlichen Lizenzen sind vorhanden (z.B. UC-Clients, Directory Services, etc.). Bei der Integration in ein bereits lizenziertes Kommunikationssystem gibt es keine Aktivierungszeit.
- Ein IP-Adressschema existiert und ist bekannt.
- Ein Wählplan (auch Nummerierungsplan genannt) ist vorhanden und bekannt.

Für UC Booster Card

Für den Betrieb der UC Booster Card sind folgende Voraussetzungen zu beachten.

- OpenScape Business-Hardware:

  Die UC Booster Card ist installiert.
- Netzwerkausrüstung:

  Voraussetzung für den ordnungsgemäßen Betrieb ist ein IPv6-fähiges Netzwerkgerät, über das die UC Booster Card mit dem Kommunikationssystem verbunden ist. Dadurch erhält die UC Booster Card automatisch eine IP-Adresse während der Ersteinrichtung und nach jedem Neustart des Systems.

  Ist das Netzwerkgerät nicht IPv6-fähig, blinkt die rote LED des Kommunikationssystems. In diesem Fall muss der Admin-Port des Systems über ein zusätzliches Ethernet-Kabel mit dem zweiten LAN-Port der UC Booster Card verbunden werden. Dadurch erhält die UC Booster Card automatisch eine IPv4 IP-Adresse über das IPv6-Protokoll. Sobald die UC Booster Card über IP erreichbar ist, erlischt die rote LED des Kommunikationssystems. Die gewünschte IP-Adresse für die UC Booster Card kann dann während der Ersteinrichtung und nach jedem Neustart des Systems eingegeben werden. Die Kommunikation zwischen System und UC Booster Card erfolgt nun über die IPv4-Verbindung des Switches.

  Anmerkung: Das zusätzliche Ethernet-Kabel sollte angeschlossen bleiben, falls ein Neustart oder ein Nachladen erforderlich ist.
- Lüfterkit:

  Die UC Booster Card erfordert einen zusätzlichen Lüfter. Das Lüfterkit hängt vom Kommunikationssystem ab.
- Gehäuseabdeckung:

  Für das OpenScape Business X3W ist eine neue Gehäuseabdeckung für das Lüfterkit der UC Booster Card erforderlich.

  Bei der Migration von HiPath 3000-Systemen sind für OpenScape Business X3W/X5W und X3R/X5R neue Gehäuseabdeckungen erforderlich, um das Lüfterkit der UC Booster Card aufzunehmen.

- Kommunikationssoftware:

  Die Software des Kommunikationssystems muss auf die neueste Version aktualisiert werden. Beachten Sie, dass hierfür das Image inklusive der Software für UC Booster Card verwendet werden muss.
- Webbrowser:

  Der Admin-PC dient zur Ersteinrichtung der UC Booster Card mit dem OpenScape Business Assistant (WBM). Der WBM ist browserbasiert und somit unabhängig vom Betriebssystem. Eine Bildschirmauflösung von 1024 x 768 oder höher ist erforderlich.

  Die folgenden HTML 5-fähigen Webbrowser werden unterstützt:

  – Microsoft Internet Explorer Version 10 und höher.
  – Microsoft Edge
  – Mozilla Firefox Version 17 und höher
  – Google Chrome

  Wenn eine ältere Version des Webbrowsers installiert ist, müssen Sie eine aktuelle Version installieren, bevor Sie mit der Ersteinrichtung des Systems beginnen können.

  Anmerkung: Zwischen OSCC und OCAB ist ein uneingeschränkter Netzwerkzugriff erforderlich.

Für UC Server Booster

Für den Betrieb des UC Booster Servers sind folgende Voraussetzungen zu beachten.

- Linux-Server:

  Der für OpenScape Business S erforderliche Linux-Server wurde gemäß den Anweisungen im *OpenScape Business Linux-Server-Installationshandbuch* installiert und in das Kunden-LAN integriert und ist einsatzbereit.
- OpenScape Business-Kommunikationssoftware:

  Die Installations-DVD mit der OpenScape Business-Kommunikationssoftware ist verfügbar. Nach der Softwareinstallation muss die Software des Kommunikationssystems und die Kommunikationssoftware des UC Booster Servers separat auf die gleiche, neueste Softwareversion aktualisiert werden.
- DVD oder USB-Stick mit Linux Betriebssystem SLES 12 SP5 64-Bit oder SLES 15 SP6 64-Bit.

  Die Linux-DVD wird möglicherweise während der Installation der OpenScape Business-Kommunikationssoftware benötigt, da einige für die Kommunikationssoftware erforderliche Softwarepakete (RPM) möglicherweise später von dieser DVD installiert werden müssen.
- Webbrowser:

  Für die Ersteinrichtung des UC Booster Servers mit dem OpenScape Business Assistant (WBM) kann entweder der Linux-Server oder der Admin PC verwendet werden. Der WBM ist browserbasiert und somit unabhängig

vom Betriebssystem. Eine Bildschirmauflösung von 1024 x 768 oder höher ist erforderlich.

Die folgenden HTML 5-fähigen Webbrowser werden unterstützt:

– Microsoft Internet Explorer Version 10 und höher (Admin-PC).
– Microsoft Edge
– Mozilla Firefox Version 17 und höher (Linux-Server / Admin-PC)
– Google Chrome

Wenn eine ältere Version des Webbrowsers installiert ist, müssen Sie eine aktuelle Version installieren, bevor Sie mit der Ersteinrichtung des Systems beginnen können.

- Firewall:

  Bei Verbindung mit dem Internet wird eine Firewall für den Linux-Server benötigt, um unbefugten Zugriff von außen zu verhindern. Nach der Installation von Linux ist die Linux Firewall aktiviert. Das Installationsprogramm der Kommunikationssoftware passt die Firewall-Einstellungen so an, dass die Kommunikationssoftware ordnungsgemäß betrieben werden kann. Die Ports für die Kommunikationssoftware werden geöffnet und alle anderen Ports sind geschlossen.

  Wenn eine externe Firewall im Netzwerk verwendet wird, muss die Linux Firewall deaktiviert und die für die Kommunikationssoftware erforderlichen Adressen und Ports geöffnet werden (siehe Verwendete Ports).

7.2 Sicherung der Konfigurationsdaten des Kommunikationssystems

Bevor OpenScape Business UC Booster installiert wird, sollte unbedingt eine Sicherung der bestehenden Konfigurationsdaten des OpenScape Business Kommunikationssystems durchgeführt werden.

Die Sicherung erfolgt am WBM des OpenScape Business Kommunikationssystems.

Es kann auf unterschiedliche Backup-Medien gesichert werden (wie z.B. auf ein USB-Medium oder ein Netzlaufwerk).

7.2.1 Wie Sie eine Datensicherung durchführen

Voraussetzungen

Sie sind am WBM des Kommunikationssystems mit dem Profil **Advanced** angemeldet.

Für eine Datensicherung auf einem USB-Medium muss das USB-Medium an der USB-Server-Schnittstelle des Kommunikationssystems angeschlossen sein.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup - sofort**.
3) Geben Sie im Bereich **Name** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.

4) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.
5) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.
6) Die Sicherung ist erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt!** erscheint. Klicken Sie auf **Beenden**.
7) Wenn Sie als Backup-Medium einen USB-Stick verwenden, warten Sie ab, bis die LED des USB-Sticks aufhört zu blinken. Erst dann ist die Sicherung erfolgreich auf dem USB-Stick gespeichert. Entfernen Sie anschließend den USB-Stick.
8) Die Datensicherung mit dem WBM ist nun abgeschlossen. Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

7.3 Inbetriebnahme UC Booster Card

Die Inbetriebnahme der UC Booster Card umfasst die Montage in das OpenScape Business Kommunikationssystem und die erstmalige Konfiguration für den korrekten Betrieb.

Nach erfolgreicher Konfiguration muss ein Software-Update durchgeführt werden.

7.3.1 Montage der UC Booster Card

Die UC Booster Card wird in das OpenScape Business Kommunikationssystem integriert. Der Steckplatz der UC Booster Card ist abhängig vom Kommunikationssystem.

Die Montage der UC Booster Card ist in der Servicedokumentation, Montage der Hardware im Kapitel "Beschreibung der Baugruppen" ausführlich beschrieben.

Die UC Booster Card kann in folgende OpenScape Business Kommunikationssysteme integriert werden:

- OpenScape Business X3R und X5R (OCCMR)

  UC Booster Card mit zusätzlichem Lüfterkit.
- OpenScape Business X3W und X5W (OCCM)

  UC Booster Card mit zusätzlichem Lüfterkit.

  Für OpenScape Business X3W wird für den Lüfterkit zusätzlich eine neue Gehäusekappe benötigt.
- OpenScape Business X8 (OCCL)

  UC Booster Card mit zusätzlichem Lüfterkit.

7.3.2 Konfiguration der UC Booster Card

Während der Konfiguration werden die grundlegenden Einstellungen für den Betrieb der UC Booster Card festgelegt.

Die Konfiguration der UC Booster Card wird mit dem Wizard **Erstinstallation** des WBM des Kommunikationssystems durchgeführt. Die Beschreibung der Konfiguration finden Sie im Kapitel Erstinstallation OpenScape Business X3/X5/X8.

Der Wizard **Erstinstallation** des WBM umfasst die erstmalige Konfiguration des gesamten Kommunikationssystems. Für den Betrieb der OpenScape Business UC Booster Card sind folgende Konfigurationsanteile wichtig:

- IP-Adresse der UC Booster Card

  Die UC Booster Card benötigt eine eigenständige IP-Adresse aus dem Netzsegment des Kommunikationssystems.
- Auswahl der UC-Lösung

  Es kann ausgewählt werden, ob die UC-Lösung UC Smart oder UC Suite genutzt werden soll.

Das Ändern der IP-Adresse der UC Booster Card oder der UC-Lösung führt zu einem Neustart des Kommunikationssystems.

7.3.3 Software-Update für die UC Booster Card

Für den korrekten Betrieb der UC Booster Card muss die Software des Kommunikationssystems aktualisiert werden. Dadurch werden alle fehlenden Software-Komponenten für die UC Booster Card nachinstalliert.

Ist die Software des Kommunikationssystems bereits auf dem aktuellen Stand, muss das System nochmals mit der aktuellen Software aktualisiert werden, damit alle für die UC Booster Funktionalität benötigten Komponenten nachinstalliert werden.

Das Software-Update kann einerseits über das Internet durchgeführt werden oder andererseits über eine Image-Datei, die vom Software Download Server bezogen werden kann. Beim Update über die Image-Datei ist darauf zu achten, dass diejenige Image-Datei verwendet wird, die die UC Booster Card Anteile enthält (osbiz..._ocab.tar).

7.3.3.1 Wie Sie ein Software-Update durchführen

Voraussetzungen

Ein Zugang zum Internet ist vorhanden.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Software Update** > **Update via Internet**. Es wird Ihnen die aktuell installierte Softwareversion angezeigt.
3) Klicken Sie auf **OK & Weiter**.
4) Lesen Sie sich die Lizenzvereinbarung (EULA) durch und aktivieren Sie anschließend das Optionsfeld **Ich stimme der Lizenzvereinbarung zu**.
5) Klicken Sie auf **OK & Weiter**.
6) Aktivieren Sie das Optionsfeld **Start der Aktion - Sofort / Sofort nach der Übertragung**.

7) Klicken Sie auf **OK & Weiter**. Das Software-Update wird im Hintergrund in das Kommunikationssystem geladen und nach der Übertragung automatisch aktiviert. Nach zwei Neustarts ist die Software aktualisiert.

Anmerkung: Sie können das Browser-Fenster jederzeit schließen.

---

8) Den aktuellen Status des Updates können Sie mit dem WBM unter **Service-Center** > **Software-Update** > **Status** abfragen.

7.4 Inbetriebnahme UC Booster Server

Die Inbetriebnahme des UC Booster Servers umfasst die Installation der OpenScape Business Kommunikationssoftware auf dem Linux-Server und die erstmalige Konfiguration für den korrekten Betrieb.

Nach erfolgreicher Konfiguration muss ein Software-Update durchgeführt werden.

7.4.1 Installation der Kommunikationssoftware

Die OpenScape Business Kommunikationssoftware wird auf dem Linux-Server mit Hilfe der OpenScape Business DVD installiert.

Achten Sie darauf, dass die zu konfigurierenden IP-Adressen und Netzmasken zu dem Kunden-LAN passen.

DHCP-Server

Ein DHCP-Server weist den IP-Teilnehmern (IP-Telefone, PCs, usw.) automatisch eine IP-Adresse zu und versorgt sie mit netzwerkspezifischen Daten, wie z.B. der IP-Adresse des Standard-Gateways.

Als DHCP-Server kann ein externer DHCP-Server genutzt werden (z.B. der DHCP-Server des Internet-Routers oder des Kommunikationssystems) oder der DHCP-Server des Linux-Servers. Soll der DHCP-Server des Linux-Servers verwendet werden, muss der externe DHCP-Server deaktiviert werden. Die Konfiguration des Linux-DHCP-Servers kann während der Installation der OpenScape Business Kommunikationssoftware durchgeführt werden.

Virtuelle Umgebung

Die Kommunikationssoftware kann in einer virtuellen Umgebung laufen. Dazu wird auf dem Server-PC zuerst die Virtualisierungssoftware (Hostbetriebssystem) installiert und konfiguriert. Anschließend wird Linux als Gastbetriebssystem installiert. Innerhalb des Linux-Betriebssystems wird zuletzt die Kommunikationssoftware installiert (siehe hierzu *OpenScape Business Linux Server Installationsanleitung*).

Einsatz von Snapshots auf Virtuellen Maschinen (VM):

Snapshots können ein wertvoller Wartungsmechanismus sein, z.B. um einen schnellen Rollback auf einen vordefinierten Betriebszustand der VM durchzuführen, nachdem ein Massenverteiler-Skript fehlgeschlagen ist.

- Snapshots dürfen nicht während des laufenden Betriebes durchgeführt werden. Während ein Snapshot gezogen wird, wird der aktuelle

Betriebszustand der virtuellen Maschine eingefroren. Daher können verbundene Endgeräte und Applikationen, wie IP-Telefone oder die UC-Clients die Verbindung zum Server verlieren.

- Snapshots können zur Folge haben, dass interne Serverprozesse ihre Synchronisation verlieren und ein stabiler Betrieb des Kommunikationssystems nicht mehr gewährleistet ist. Daher sollte im Anschluss an den Snapshot ein Server-Neustart mit in das Wartungsfenster eingeplant werden.
- Vorherige Snapshots dürfen auf der Produktionsumgebung während des normalen Betriebes nicht verbleiben.
- Snapshots können während eines vorgesehenen Wartungsfensters oder im Rahmen der Installation gezogen werden.
- Snapshots werden intern von Backup-Tools wie VDP oder VDR genutzt. Es muss sichergestellt sein, dass diese Backup-Vorgänge außerhalb der Geschäftszeiten geplant werden und dass Snapshots, die durch diese Tools generiert werden, am Ende des Vorgangs gelöscht werden.

Weitere Informationen bezüglich Snapshots können der VMware Knowledge Base (KB) entnommen werden. Ein guter Einstiegspunkt ist der KB-Artikel 1025279 - Best Practices for virtual machine snapshots in the VMware environment (`http://kb.vmware.com/kb/1025279`).

7.4.1.1 Wie Sie die Kommunikationssoftware installieren

Voraussetzungen

- Das Betriebssystem SLES 12 SP5 oder SLES 15 SP6 wurde korrekt installiert und auf dem Linux-Server gestartet.
- DVD oder .ISO-Datei mit OpenScape Business-Kommunikationssoftware.
- DVD oder .ISO-Datei oder USB-Stick mit dem Linux-Betriebssystem SLES 12 SP5 64-Bit oder SLES 15 SP6 64-Bit, das für jede spätere Installation von Softwarepaketen (RPM) erforderlich sein kann.
- Die Root-Zugangsdaten (Benutzername und Passwort) für die Anmeldung am Linux-Server stehen zur Verfügung.

Wichtig: Die OpenScape Business-Kommunikationssoftware überschreibt während der Installation vorhandene Konfigurationsdateien (z.B. für DHCP, FTP, Postfix usw.).

Schritt für Schritt

1) Melden Sie sich mit Root-Rechten beim Linux-Server an.

2) Legen Sie die OpenScape Business-DVD oder .ISO-Datei in das DVD-Laufwerk ein.

3) Bestätigen Sie die Nachricht mit **Ausführen**. Das Fenster "Willkommen" erscheint.

4) Wählen Sie die gewünschte Einrichtungssprache aus (z.B. **Englisch**) und klicken Sie auf **Start**. Der Rest der Installation wird hier für die englische Sprache beschrieben.

5) Wählen Sie das gewünschte Produkt aus der Liste aus und klicken Sie auf **Auswählen**. Es wird geprüft, ob die Hardware alle Anforderungen für die Installation erfüllt. Bei geringfügigen Mängeln bei der Erfüllung der

Anforderungen wird eine Warnung angezeigt. Nach Bestätigung kann dann die Installation fortgesetzt werden. Bei schweren Mängeln wird die Installation automatisch abgebrochen.

6) Es wird geprüft, ob zusätzliche RPM-Pakete installiert werden müssen. Wenn ja, bestätigen Sie dies mit **Bestätigen**. In diesem Fall müssen Sie später zurück zu SLES 12 oder SLES 15, DVD oder .ISO-Datei wechseln.

7) Es erscheint ein Fenster mit den Bedingungen der Lizenz (d. h. der Endbenutzer-Lizenzvereinbarung oder EULA). Lesen Sie die Lizenzbedingungen und akzeptieren Sie die Lizenzvereinbarung mit **Ja**.

8) Wenn bereits ein DHCP-Server im Kunden-LAN vorhanden ist (z.B. der DHCP-Server des Internet-Routers), stoppen Sie hier die Konfiguration des Linux-DHCP-Servers mit **Nein** und fahren Sie mit Schritt 12 fort, um fortzufahren.

Anmerkung: Damit die Software von Systemtelefonen auch bei Verwendung eines externen DHCP-Servers automatisch aktualisiert werden kann, haben Sie zwei Optionen:

a) Die IP-Adresse des Linux-Servers muss als DLS-Adresse an jedem Systemtelefon eingegeben werden.

b) Die netzwerkspezifischen Daten müssen auf dem externen DHCP-Server eingegeben werden. Die Parameter hierfür finden Sie unter `/var/log/OPTI.txt`.

---

9) Wenn Sie den Linux DHCP Server verwenden möchten, klicken Sie auf **Ja**, um den Linux DHCP Server zu aktivieren und zu konfigurieren.

10) Geben Sie die folgenden Werte ein (voreingestellt mit Standardwerten):

- **Standardroute**: IP-Adresse des Standard-Gateways; In der Regel die IP-Adresse des Internetrouters, z.B. `192.168.5.1`.
- **Domäne** (optional): die während der Linux-Installation angegebene Domäne, z.B.: `<customer>.com`
- **DNS-Server** (optional): IP-Adresse des DNS-Servers, der während der Linux-Installation angegeben wurde. Wenn im internen Netzwerk kein DNS-Server verfügbar ist, können Sie hier die IP-Adresse des Internetrouters (z.B. `192.168.5.1`) eingeben.
- **SNTP-Server**: IP-Adresse des internen oder externen NTP-Servers.
- **DLS/DLI-Server**: IP-Adresse des DLS-Servers, d. h. die IP-Adresse des Linux-Servers (z.B.: `192.168.5.10`).
- **Subnetz**: geeignetes Subnetz für den IP-Adressbereich, z.B.: `192.168.5.0`.
- **Netzmaske**: Subnetzmaske des Linux-Servers, die während der Linux-Installation angegeben wurde, z.B.: `255.255.255.0`.
- **IP-Bereichsanfang** und **IP-Bereichsende**: IP-Adressbereich, aus dem der DHCP-Server IP-Adressen zuweisen kann, z.B.: `192.168.5.100` bis `192.168.5.254`.

11) Klicken Sie auf **Weiter**.

12) Nach der Installation muss das Linux-Betriebssystem neu gestartet werden. Aktivieren Sie das Kontrollkästchen **PC-Neustart** und bestätigen Sie mit **Weiter**.

13) Wenn zusätzliche RPM-Pakete installiert werden müssen, werden Sie aufgefordert, den SLES 12 DVD oder SLES 15 USB-Stick einzulegen.

Legen Sie die DVD oder den USB-Stick ein und bestätigen Sie mit **Weiter**. Legen Sie nach erfolgreicher Installation der RPM-Pakete die OpenScape Business-DVD erneut ein oder .ISO-Datei und bestätigen Sie dies mit **Weiter**, gefolgt von **Ausführen**.

14) Die OpenScape Business-Kommunikationssoftware ist installiert. Das Betriebssystem führt dann automatisch einen Neustart durch.

15) Melden Sie sich nach dem Neustart mit dem Benutzerkonto, das zuvor während der Linux-Installation eingerichtet wurde, an.

16) Klicken Sie mit der rechten Maustaste auf das DVD-Laufwerkssymbol auf dem Desktop und wählen Sie das Menü-Element **Auswerfen**. Entfernen Sie die OpenScape Business DVD aus dem DVD-Laufwerk.

Anmerkung: Es dauert wenige Minuten, bis alle Komponenten der OpenScape Business-Kommunikationssoftware aktiv sind.

7.4.2 Konfiguration des UC Booster Servers

Während der Erstkonfiguration werden die grundlegenden Einstellungen für den Betrieb des UC Booster Servers festgelegt.

Die Konfiguration des UC Booster Servers wird mit dem Wizard **Erstinstallation** des WBM des Kommunikationssystems durchgeführt. Die Beschreibung der Konfiguration finden Sie im Kapitel Erstinstallation OpenScape Business X.

Der Wizard **Erstinstallation** des WBM umfasst die erstmalige Konfiguration des gesamten Kommunikationssystems. Für den Betrieb der OpenScape Business UC Booster Card sind folgende Konfigurationsanteile wichtig.

- Auswahl der UC-Lösung

  Es kann ausgewählt werden, ob die UC-Lösung UC Smart oder UC Suite genutzt werden soll. Dazu muss auch die IP-Adresse des Linux-Servers eingetragen werden.

  Das Ändern der UC-Lösung führt zu einem Neustart des Kommunikationssystems.

Zusätzlich muss am WBM des UC Booster Servers die IP-Adresse des Kommunikationssystems bekannt gegeben werden.

7.4.2.1 IP-Adresse des Kommunikationssystems bekannt geben

Voraussetzungen

Der UC Booster Server ist in das Kunden-LAN integriert und betriebsbereit.

Das OpenScape Business Kommunikationssystem ist betriebsbereit.

Schritt für Schritt

1) Starten Sie auf dem Linux-PC den Webbrowser und rufen Sie das WBM des OpenScape Business Servers unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z.B. `https://192.168.1.10`

2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).

a) Schließen Sie den Webbrowser.

b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.

c) Erlauben Sie die Benutzerkontensteuerung.

d) Rufen Sie das WBM des OpenScape Business Servers unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z.B. `https://192.168.1.10`

e) Klicken Sie auf **Laden dieser Website fortsetzen**.

f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.

g) Klicken Sie auf **Zertifikate anzeigen**.

h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).

i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.

j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.

k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.

l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.

m) Schließen Sie den Webbrowser.

n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie das WBM des OpenScape Business Servers unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z.B. `https://192.168.1.10`

3) Klicken Sie oben rechts auf das Sprachkürzel und wählen Sie aus dem Menü die Sprache aus, in der die Oberfläche des WBM angezeigt werden soll. Die Anmeldeseite wird in der ausgewählten Sprache angezeigt.

4) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

Anmerkung: Wenn Sie nach Eingabe von `administrator` in das Feld **Passwort** wechseln, wird `@system` automatisch ergänzt.

---

5) Geben Sie im zweiten Feld unter **Login** das Standard-Passwort `administrator` für den Zugang als Administrator ein.

6) Klicken Sie auf **Login**.

7) Folgende Schritte sind nur einmalig beim ersten Anmelden am WBM nötig:

a) Geben Sie im Feld **Passwort** nochmal das Standard-Passwort `administrator` ein.

b) Geben Sie in den Feldern **Neues Passwort** und **Neues Passwort bestätigen** ein neues Passwort ein, um das System gegen Missbrauch zu schützen. Berücksichtigen Sie Groß-/Kleinschreibung und den Zustand der Tasten `Num` und `CapsLock` (Feststelltaste). Das Passwort erscheint verdeckt durch Sternchen (*).

Anmerkung: Das Passwort muss mindestens 8 Zeichen lang sein und eine Ziffer enthalten. Bitte merken Sie sich Ihr neues Passwort genau.

---

c) Klicken Sie auf **Login**.

d) Wählen Sie das aktuelle Datum aus und tragen Sie die Uhrzeit korrekt ein.

e) Klicken Sie auf **OK & Weiter**. Sie werden automatisch vom WBM abgemeldet.

f) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

Anmerkung: Wenn Sie nach Eingabe von `administrator` in das Feld **Passwort** wechseln, wird `@system` automatisch ergänzt.

---

g) Geben Sie im zweiten Feld unter **Login** Ihr neu definiertes Passwort für den Zugang als Administrator ein.

h) Klicken Sie auf **Login**. Es erscheint die Startseite des WBM.

i) Klicken Sie in der Navigationsleiste auf **Administratoren**.

j) Aktivieren Sie in der **Administratoren-Liste** das Kontrollkästchen vor dem Listeneintrag **Administrator**.

k) Klicken Sie auf **Bearbeiten**.

l) Wählen Sie in der Aufklappliste **Benutzerrolle** das Benutzerprofil **Expert** aus.

m) Klicken Sie auf **OK & Weiter**.

n) Melden Sie sich am WBM ab über den Link **Abmelden** rechts oben.

o) Melden Sie sich erneut am WBM an mit dem Standard-Benutzernamen `administrator@system` und dem neu definierten Passwort.

8) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

9) Klicken Sie im Navigationsbaum auf **Wartung** > **Konfiguration**.

10) Geben Sie im Register **Gateway IP-Adresse ändern** unter **Gateway IP-Adresse** die IP-Adresse des Kommunikationssystems ein, z.B. `192.168.1.2`.

11) Klicken Sie auf **Übernehmen**.

7.4.3 Software-Update für die UC Booster Server

Für den korrekten Betrieb des UC Booster Servers muss die Software des Kommunikationssystems und die Software der Kommunikationssoftware des UC Booster Servers auf den gleichen Software-Stand aktualisiert werden.

Ist die Software des Kommunikationssystems bereits auf dem aktuellen Stand, muss nur noch die Software des UC Booster Servers aktualisiert werden.

Das Software-Update kann einerseits über das Internet durchgeführt werden oder andererseits über eine Image-Datei, die vom Software Download Server bezogen werden kann. Beim Update des UC Booster Servers über die Image-Datei ist darauf zu achten, dass diejenige Image-Datei verwendet wird, die die UC Booster Server Anteile enthält (osbiz..._pcx.tar).

7.5 Basiskonfiguration

Während der Basiskonfiguration werden die wichtigsten Einstellungen für den Betrieb von OpenScape Business UC Booster festgelegt.

Die Basiskonfiguration wird sowohl für die UC Booster Card als auch für den UC Booster Server mit dem Wizard **Basisinstallation** des WBM des Kommunikationssystems durchgeführt. Die Beschreibung der Basiskonfiguration finden Sie im Kapitel Erstinstallation OpenScape Business X.

Die Basiskonfiguration umfasst die Konfiguration des gesamten Kommunikationssystems. Für den Betrieb von OpenScape Business UC Booster sind folgende Konfigurationsanteile wichtig:

- Teilnehmerdaten

  Spezielle Rufnummern, die für den Betrieb von OpenScape Business UC Booster benötigt werden, können angepasst werden. Hier muss z.B. die Rufnummer der UC Suite Sprachbox (VoiceMail) angegeben werden.
- Konfiguration der UC Booster Card

  Ist eine UC Booster Card in das Kommunikationssystem integriert, muss die automatische Konfiguration der UC Booster Card eingeleitet werden.
- Meet-Me-Konferenzeinstellungen

  Mit OpenScape Business UC Booster steht das Leistungsmerkmal Meet-Me-Konferenz zur Verfügung. Die vorbelegte Rufnummer und die vorbelegte Einwahlnummer für die Meet-Me-Konferenz können geändert werden.

7.6 Abschließende Tätigkeiten

Nachdem die Erstinstallation und die Basisinstallation mit dem WBM abgeschlossen sind, müssen noch einige wichtige Einstellungen für den Betrieb von OpenScape Business UC Booster getroffen werden.

Die abschließenden Tätigkeiten werden sowohl für die UC Booster Card als auch für den UC Booster Server mit dem WBM des Kommunikationssystems durchgeführt. Die Beschreibung der abschließenden Tätigkeiten finden Sie in der Online-Hilfe oder in der OpenScape Business Administratordokumentation, Kapitel Erstinstallation OpenScape Business X.

Für den Betrieb von OpenScape Business UC Booster sind folgende abschließende Tätigkeiten wichtig:

- Lizenzen aktivieren und zuordnen

  Um die OpenScape Business UC Booster Funktionalität nutzen zu können, müssen bei einer Integration in ein bereits lizenziertes

Kommunikationssystem die Lizenzen sofort aktiviert werden. Bei einer Integration in ein noch nicht lizenziertes Kommunikationssystem sind die Lizenzen innerhalb einer Zeitspanne von 30 Tagen zu aktivieren. Nach erfolgreicher Aktivierung müssen die Lizenzen den Teilnehmern zugeordnet werden. Systemweite Leistungsmerkmale sind in einem Standalone-System bereits mit der Aktivierung freigeschaltet.

- UC Clients zur Installation bereitstellen

  Die UC Clients sind Bestandteil der UC Suite. Die Installationsdateien für die UC Clients sind über das WBM zugänglich und können den IP-Teilnehmern automatisch oder manuell zur Verfügung gestellt werden.
- Datensicherung durchführen

  Die bisherigen Änderungen an OpenScape Business müssen gesichert werden. Die Sicherung kann als Backup-Set z.B. auf einem USB-Medium oder im internen Netz gespeichert werden.

  Bei der UC Booster Card reicht es, eine Datensicherung des Kommunikationssystems durchzuführen. Bei dem UC Booster Server müssen die Daten des Kommunikationssystems und separat die Daten der Kommunikationssoftware des UC Booster Servers gesichert werden.

7.7 Deinstallation der Kommunikationssoftware

Die Deinstallation der Kommunikationssoftware ist über eine Text-Konsole möglich.

7.7.1 Wie Sie die Kommunikationssoftware deinstallieren

Schritt für Schritt

1) Öffnen Sie ein Terminal (z.B. GNOME Terminal).
2) Geben Sie in der Shell-Oberfläche den Befehl `su` (für superuser = root) ein und bestätigen Sie mit der Eingabetaste.
3) Geben Sie in der Shell-Oberfläche das Passwort für den Benutzer "root" ein und bestätigen Sie mit der Eingabetaste.
4) Geben Sie in der Shell-Oberfläche den Befehl `oso_deinstall.sh` ein und bestätigen Sie mit der Eingabetaste. Folgen Sie den Anweisungen des Deinstallationsprogramms.

7.8 Hochrüstung von UC Booster Card auf UC Booster Server

Um ein OpenScape Business Kommunikationssystem mit integrierter UC Booster Card auf ein OpenScape Business Kommunikationssystem mit angeschlossenem UC Booster Server hochzurüsten, sind die nachstehend beschriebenen Schritte durchzuführen.

Hochrüst-Schritte

Führen Sie folgende Schritte der Reihe nach durch:

1) **Sicherung der Konfigurationsdaten**

   Führen Sie eine Sicherung der Konfigurationsdaten des Kommunikationssystems durch.

   Beschreibung der Datensicherung siehe Sicherung der Konfigurationsdaten des Kommunikationssystems.

2) **Änderung der IP-Adresse der UC Booster Card**

   Ändern Sie im WBM des Kommunikationssystems mit dem Wizard **Erstinstallation** die IP-Adresse der UC Booster Card in eine nicht benutzte IP-Adresse. Die Verbindung zu den UC Clients wird getrennt.

   Beschreibung der IP-Adressänderung siehe Systemeinstellungen .

3) **Änderung der Applikationsauswahl**

   Ändern Sie im WBM des Kommunikationssystems mit dem Wizard **Erstinstallation** bei der Nutzung von UC Suite die Applikationsauswahl von **Paket mit UC Suite** auf **Paket mit UC Suite auf OSBiz UC Booster Server** oder bei der Nutzung von UC Smart die Applikationsauswahl von **Paket mit UC Smart** auf **Paket mit UC Smart auf OSBiz UC Booster Server**) und geben Sie als IP-Adresse des UC Booster Servers die ehemalige IP-Adresse der UC Booster Card an.

   Beschreibung der Applikationsauswahl siehe UC-Lösung.

4) **Installation des Linux-Servers**

   Auf dem Linux-Server ist das für den UC Booster Server freigegebene Linux-Betriebssystem zu installieren.

   Beschreibung der Linux-Installation siehe OpenScape Business Linux-Server Installationsanleitung.

5) **Änderung der IP-Adresse des UC Booster Servers**

   Für die IP-Adresse des UC Booster Servers (= IP-Adresse des Linux-Servers) muss die ehemalige IP-Adresse der UC Booster Card angegeben werden. Die IP-Adresse des Linux-Servers können Sie während der Installation des Linux-Betriebssystems eingeben oder nachträglich über YaST ändern.

   Beschreibung der IP-Adressvergabe während der Linux-Installation siehe OpenScape Business Linux-Server Installationsanleitung.

6) **Installation der Kommunikationssoftware**

   Auf dem Linux-Server ist die OpenScape Business Kommunikationssoftware zu installieren.

   Beschreibung der Installation der Kommunikationssoftware siehe Installation der Kommunikationssoftware.

7) **Konfiguration des UC Booster Servers**

   Geben Sie im WBM des UC Booster Servers die IP-Adresse des Kommunikationssystems ein.

   Beschreibung der IP-Adressvergabe des Kommunikationssystems siehe Konfiguration des UC Booster Servers.

8) **Neustart der Kommunikationssoftware**

   Führen Sie im WBM des UC Booster Servers einen Neustart der Kommunikationssoftware des UC Booster Servers durch.

   Beschreibung des Neustarts siehe Restart (Neustart) der UC Applikation .

9) **Update der Software**

   Die Software des Kommunikationssystems und des UC Booster Servers müssen auf den gleichen Software-Stand gebracht werden.

   Beschreibung des Software-Update siehe Updates.

10) **Wiederherstellung der Konfigurationsdaten**

    Spielen Sie im WBM des Kommunikationssystems die Sicherung der Konfigurationsdaten des Kommunikationssystems ein. Kommunikationssystem und Kommunikationssoftware führen anschließend einen Neustart durch. Die Verbindung zu den UC Clients ist wieder hergestellt.

    Beschreibung der Datenwiederherstellung siehe Wiederherstellen .

7.9 Verwendete Ports

Die OpenScape Business Systemkomponenten nutzen verschiedene Ports, die bei Bedarf in der Firewall freigeschaltet werden müssen. Für die Ports der Webbased Clients (z.B. myPortal to go) muss ein Port Forwarding im Router eingerichtet werden.

Eine tatsächliche und vollständige Liste aller verwendeten Ports von OpenScape Business finden Sie in der "Interface Management Database" (IFMD), die über das Partnerportal von Unify abgerufen werden kann (https://unify.com/en/partners/partner-portal.

Anmerkung: Die in der folgenden Liste mit "O" identifizierten Ports sind optional, d. h. Sie sind in der Firewall nicht dauerhaft geöffnet.

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Systemkomponenten							
Admin Portal (https)	X		443	X	X	X	X
CAR-Lebendigkeitsprüfungen	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (bis zu V3R3) 7780, 7791 (ab V3R3.1 und höher)	O		O	
Communication Client-Installationsprogramm	X		8101	X	X	X	X
Csta Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Csta Service Provider (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP Server	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
xNAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
xOpenfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X
OpenScape Business Benutzerportal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (eingebettet)		X	29100-30530	X	X	X	X
RTP (Server)		X	29100-30888	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
SNMP (Get/Set)		X	161	X		X	
SNMP (Traps)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

Anmerkung: Aus Sicherheitsgründen wird empfohlen für die Webbased Clients ausschließlich https zu verwenden und ein Port Forwarding von extern TCP/443 nach intern TCP/8802 einzurichten.

CLS-Zertifikat

Ab V3R3.1 wird über einen neu eingeführten Port ein neues CLS-Zertifikat mit aktualisiertem Common Name (CN) bereitgestellt. Dies bietet einen verbesserten und stärkeren Digest-Algorithmus sowie aktualisierte juristische Personen an. Die online über den CLS Connect-Modus lizenzierten Systeme erfordern die folgenden zwei Voraussetzungen:

- Die IP-Adresse 188.64.16.4 ist für ausgehenden Datenverkehr in der Firewall aktiviert.
- Die Ports 7780 und 7791 sind für ausgehenden Datenverkehr in der Firewall aktiviert.

Der zuvor verwendete Port 7790 kann nach dem Upgrade auf V3R3.1 aus der Firewall-Konfiguration entfernt werden, um die Sicherheit zu erhöhen.

8 Lizenzierung

Das flexible Lizenzkonzept von OpenScape Business bietet dem Kunden die Möglichkeit, den Leistungsumfang über Lizenzen genau seinen Anforderungen anzupassen. Alle Kommunikationssysteme OpenScape Business X und OpenScape Business S unterliegen diesem Lizenzkonzept. Telefone, UC Clients, UC-Funktionen und systemweite Leistungsmerkmale können so nach individuellem Kundenbedarf freigeschaltet werden. Für alle OpenScape Business Kommunikationssysteme werden einheitliche Lizenzen verwendet.

Soll OpenScape Business zu einem späteren Zeitpunkt erweitert oder mit zusätzlichen Leistungsmerkmalen ausgestattet werden, ist dies jederzeit durch den Erwerb weiterer Lizenzen möglich.

Alle Lizenzen sind immer an die Basislizenz des Kommunikationssystems gebunden und erlauben die Nutzung der erworbenen Leistungsmerkmale für die zugeordnete Version von OpenScape Business.

Um besondere Leistungsmerkmale dem Kunden zum Test oder zum Kennenlernen zur Verfügung zu stellen, können Evaluierungslizenzen mit einer Laufzeit von 90 Tagen bestellt werden.

Anmerkung: Es empfiehlt sich, keine Lizenzdateien zu installieren oder einen Assistenten auszuführen, wenn das System aktiv ist, da dadurch aktive Anrufe möglicherweise beendet werden könnten.

Activation Period

Innerhalb der Activation Period (Zeitspanne von 30 Tagen) muss die Lizenzaktivierung vorgenommen werden. Die Activation Period beginnt, wenn im WBM das aktuelle Datum eingeben wird. Dabei wird das Ablaufdatum der Activation Period gespeichert.

Das Produkt ist während der Activation Period voll funktionsfähig und die maximale Anzahl an Lizenzen steht zur Nutzung zur Verfügung.

Verliert das System innerhalb der Activation Period das aktuelle Datum (z. B. durch eine Entladung des Akkus auf dem Mainboard), muss zeitnah im WBM das Datum aktualisiert werden, damit das System innerhalb der Activation Period weiterhin uneingeschränkt genutzt werden kann.

Ist nach Ablauf der Activation Period keine Lizenzierung erfolgt, ist das Kommunikationssystem nur noch sehr eingeschränkt nutzbar. Eine interne Kommunikation zwischen den Teilnehmern ist möglich, aber nach extern können nur die beiden ersten aktiven Telefone telefonieren (z. B. für Notrufe). Der Zugang zum Kommunikationssystem über die Fernverwaltung (Remote-Zugang) ist weiterhin möglich. Das System befindet sich ebenfalls in diesem eingeschränkt nutzbaren Zustand, wenn die Erstinstallation nur mit dem Manager E durchgeführt wurde, da hierüber die Activation Period nicht gestartet wird.

Struktur der Lizenzen

Die Lizenzen für das Kommunikationssystem sind folgendermaßen strukturiert:

- Eine Basislizenz aktiviert die Software des Kommunikationssystems dauerhaft. Dis ist auch die Voraussetzung für die Aktivierung aller weiteren Lizenzen.

- Teilnehmer-Lizenzen zur Aktivierung der Telefone für die externe Sprachkommunikation.
- User-orientierte Lizenzen zum Freischalten spezifischer Leistungsmerkmale für die Benutzer.
- Systemlizenzen um allgemeine Leistungsmerkmale systemweit freizuschalten.

Migration

Für bestehende HiPath 3000 V9 Kunden wird eine Lizenzmigration über eine Upgradelizenz angeboten. Die Lizenzmigration bietet Investitionsschutz für den Kunden für die weitere Nutzung der Telefone und der Sprachleistungsmerkmale.

Anmerkung: Informationen zur Lizenzierung und zum Upgrade oder zur Migration von Systemen in einem Netzwerk finden Sie im Abschnitt **Netzwerk - Lizenzierung** im Kapitel Updates.

Zugehörige Konzepte

Teilnehmer auf Seite 428

8.1 Lizenzierungsverfahren

Für die Lizenzierung steht mit dem OpenScape Lizenz-Management ein zentralisiertes Verfahren zur Verwaltung und Aktivierung von Lizenzen zur Verfügung. Dieses stellt sicher, dass ein Kunde jeweils genau den Systemausbau bzw. diejenigen Leistungsmerkmale verwenden kann, für die er die entsprechenden Lizenzen (Nutzungsrechte) erworben hat.

Die Lizenzen der OpenScape Business Kommunikationssysteme werden an die Locking ID bzw. die Advanced Locking ID des Kommunikationssystems gebunden (siehe Locking ID und Advanced ID Locking).

Der Kunde bestellt die gewünschten Leistungsmerkmale und erhält einen Lizenzaktivierungsschlüssel (LAC). Nach erfolgreicher Erstinstallation des Kommunikationssystems aktiviert der Kunde die erworbenen Lizenzen mit Hilfe einer Lizenzdatei. Die Lizenzdatei stellt dem System einen Lizenzpool mit allen erworbenen Lizenzen für die anschließende Lizenzzuordnung zur Verfügung.

Das WBM bietet Wizard-gesteuert die Funktionen für die Kunden-Registrierung, die Lizenzaktivierung und die Lizenzzuordnung für Standalone-Systeme und Systeme in einem OpenScape Business Netzverbund an. Eine Lizenzierung mit dem Manager E ist nicht möglich.

Schritte zur erfolgreichen Lizenzierung

1) Konfiguration des Systems innerhalb der Activation Period
2) Registrierung der Kundendaten
3) Lizenzaktivierung
4) Lizenzzuordnung

Kunden-Registrierung

Im Rahmen der Lizenzierung sind für die Registrierung des Kunden die Kundendaten des jeweiligen Systems zwingend einzugeben. Die Kundendaten

werden verwendet, um im Fall von sicherheitsrelevanten Sachverhalten, insbesondere Produktrückrufen schnell informieren zu können. Zusätzlich erhalten die Kunden Informationen zur Vermeidung von Lizenzmissbrauch durch Dritte, z.B. über die Neuverknüpfung der Lizenzinformationen.

Lizenzaktivierung

Bei der Lizenzaktivierung werden über die Lizenzverwaltung des WBM die erworbenen Lizenzen an das Kommunikationssystem gebunden. Dafür stehen 2 Methoden zur Verfügung:

- Online-Aktivierung

  Bei der Online-Aktivierung wird nach Eingabe des LAC über das Internet eine Verbindung zum zentralen Lizenzserver (Central License Server, CLS) hergestellt und die Lizenzdatei automatisch an den im Kommunikationssystem integrierten Lizenzagenten (Customer License Agent, CLA) übertragen. Anschließend werden die Lizenzen automatisch aktiviert.
- Offline-Aktivierung

  Bei der Offline-Aktivierung besteht keine Verbindung des Kommunikationssystems zum zentralen Lizenzserver (Central License Server, CLS). Die Lizenzdatei wird von einem autorisierten Partner am CLS generiert und muss während der Lizenzaktivierung manuell an den im Kommunikationssystem integrierten Lizenzagenten (Customer License Agent, CLA) übertragen werden.

Lizenzzuordnung

Alle erworbenen Lizenzen werden über die Lizenzverwaltung des WBM den Teilnehmern fest zugeordnet.

Um Teilnehmern Lizenzen zuordnen zu können, müssen die Teilnehmer zuerst mit dem WBM eingerichtet werden, z.B. bei der Erstinstallation. Jede Systemkonfiguration kann unabhängig von den vorhandenen Lizenzen eingerichtet werden. Erst mit der Lizenzzuordnung kann das entsprechende Leistungsmerkmal genutzt werden.

Bei der Lizenzzuordnung wird zwischen Konfiguration und Vergabe von Lizenzen unterschieden. Für Teilnehmer und User-orientierte Lizenzen werden Lizenzanforderungen konfiguriert. Ist für eine Lizenzanforderung eine Lizenz in dem Lizenzpool vorhanden, wird das entsprechende Leistungsmerkmal freigeschaltet. Ist keine Lizenz in dem Lizenzpool vorhanden, bleibt die konfigurierte Lizenzanforderung erhalten, aber das entsprechende Leistungsmerkmal ist nicht freigeschaltet. Bei Bedarf müssen fehlende Lizenzen nachgekauft werden.

Lizenzierung im Netzverbund

Für einen OpenScape Business Netzverbund wird eine netzweite Lizenzdatei (Netzwerklizenzdatei) von einem autorisierten Partner am zentralen Lizenzserver (CLS) generiert. Diese netzweite Lizenzdatei wird vom zentralen Lizenzagenten (CLA) des Master-Knoten verwaltet und stellt den einzelnen Knoten die Lizenzen zur Verfügung. Die Zuordnung der Lizenzen erfolgt über das WBM jedes einzelnen Knotens. Innerhalb eines Netzverbunds können die Lizenzen über das WBM verschoben werden.

Bei der Lizenzierung eines Netzverbunds ist eine Online-Aktivierung nicht möglich.

Pay As You Go

Neben dem traditionellen Lizenzierungsmodell unterstützt OpenScape Business auch ein Abonnement-Lizenzierungsmodell (Pay As You Go). "Pay As You Go" bietet die Möglichkeit, nur die genutzten Lizenzen pro Abrechnungszeitraum in Rechnung zu stellen und zusätzliche Lizenzen zu nutzen, ohne die Lizenzdatei zu erweitern. Es ist nicht erforderlich, die Anzahl der Lizenzen im Voraus festzulegen.

Eine permanente Internetverbindung vom OpenScape Business-System zum Central License Server (CLS) ist erforderlich. Sie kann entweder online mit einem Lizenzaktivierungscode (LAC) oder per Datei-Upload aktiviert werden. Nach der Installation, der kundenspezifischen Konfiguration der Lösung und der Aktivierung von "Pay As You Go" wird in regelmäßigen Abständen ein Bericht über die genutzten Lizenzen an den Central License Server (CLS) gesendet und ausgewertet. Einmal im Monat wird ein Abschlussbericht auf der Produktseite des Central License Server (CLS) erstellt, und der Inhalt dieses Abschlussberichts wird für die Lizenzabrechnung verwendet.

Mit der Abonnementlizenzierung wird ein neuer Zeitraum eingeführt, die Wartezeit. Die Wartezeit beginnt mit dem Systemstart, oder wenn eine "Pay As You Go"-Lizenzdatei aktiviert wird. Nachfolgend beginnt der Zeitraum. Eine während dieses Zeitraums im WBM vorgenommene Lizenzkonfiguration führt zudem nicht zu einer Aktualisierung der Lizenznutzung. Die maximale Dauer der Wartezeit beträgt 2 Stunden.

Anmerkung: Damit die Firewall auf das CLS zugreifen kann, sind folgende Maßnahmen erforderlich:

- Der Port 7790 wurde für ausgehenden IP-Datenverkehr freigegeben

- 188.64.16.4 wurde für ausgehenden IP-Datenverkehr freigegeben

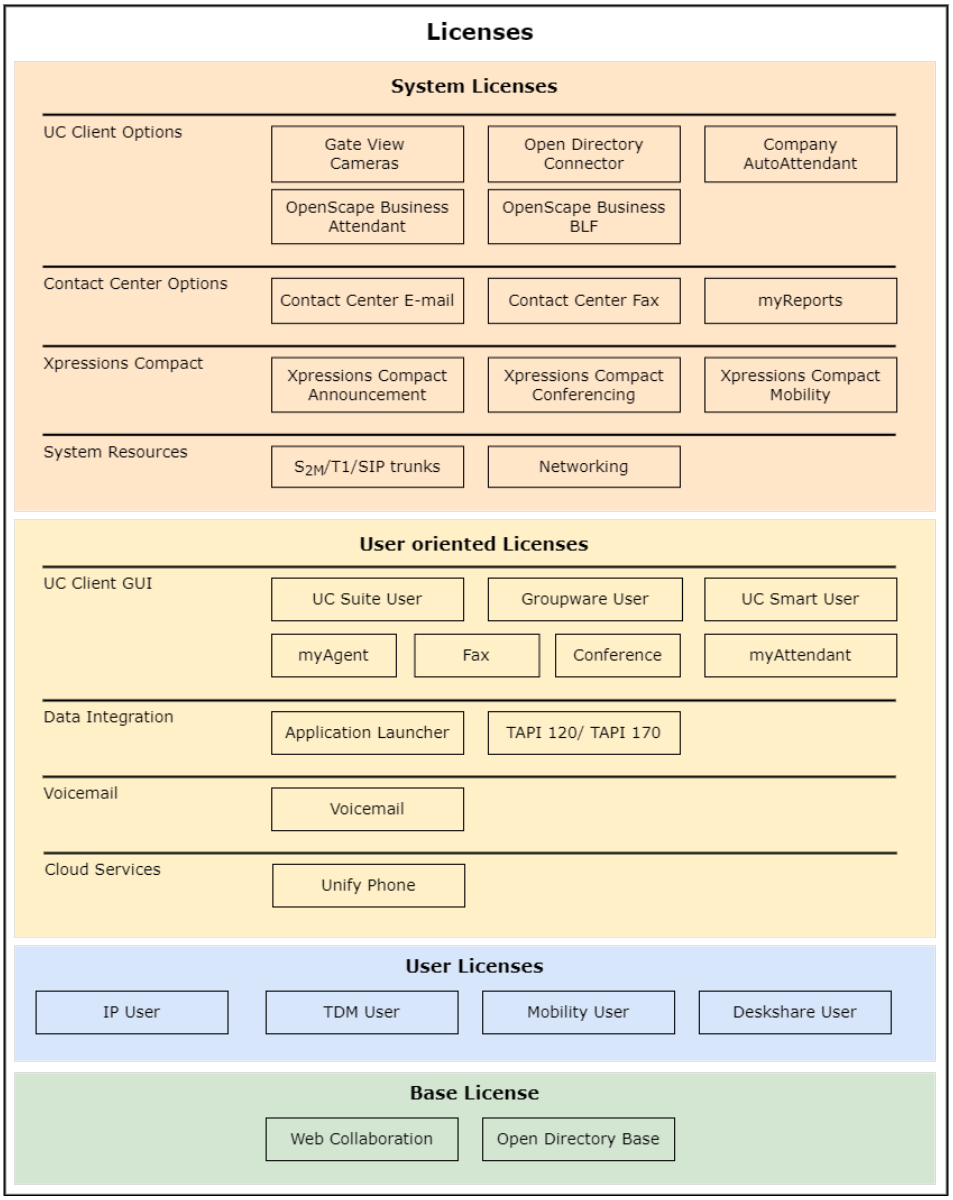
Neuere V3R3-Softwaresysteme verwenden Port 7791 für die Online-Lizenzaktivierung.

8.2 Lizenzen

Um die Leistungsmerkmale des Kommunikationssystems nutzen zu können, sind Lizenzen zu erwerben. Innerhalb einer gewissen Zeitspanne (Activation Period) müssen die erworbenen Lizenzen aktiviert werden.

Die Lizenzen sind thematisch zu Lizenzgruppen zusammengefasst. Folgende Lizenzgruppen stehen zur Verfügung:

- Basislizenzen
- Teilnehmer-Lizenzen
- User-orientierte Lizenzen
- Systemlizenzen



Die o.a. Lizenzen können für OpenScape Business X, OpenScape Business S und OpenScape Business UC Booster Server verwendet werden. Der UC Booster Server hat keine eigene Basislizenz. Die Lizenzen decken alle Leistungsmerkmale ab und können nach den Wünschen des Kunden zusammengestellt werden. Die Kombinationsmöglichkeiten der Lizenzen werden bei der Lizenz- und Lizenzprofilzuordnung genauer erklärt.

Teilnehmer-Lizenzen und User-orientierte Lizenzen werden den Teilnehmern fest zugeordnet.

8.2.1 Basislizenz

Die Basislizenz erlaubt die generelle Nutzung des Kommunikationssystems und ist Voraussetzung für die Aktivierung aller weiteren Lizenzen.

Internet-Telefonie und Notbetrieb ist auch ohne Basislizenz möglich.

Folgende Basislizenzen stehen zur Verfügung:

- **OpenScape Business V2 X1 Base**

  Für die Freischaltung des V2-Funktionsumfangs von

  – OpenScape Business X1

  Die Basislizenz enthält zusätzlich die Lizenzen OpenDirectory Base für die Nutzung von Open Directory Service (ODS) und Web Collaboration für das Starten einer Web Collaboration Sitzung. Damit kann die UC-Lösung UC Smart mit einer externen Datenbank verbunden werden.
- **OpenScape Business V2 Base**

  Für die Freischaltung des V2-Funktionsumfangs von

  – OpenScape Business X3/X5/X8 mit oder ohne UC Booster (UC Booster Card oder UC Booster Server) oder
  – OpenScape Business S

  Die Basislizenz enthält zusätzlich die Lizenz OpenDirectory Base für die Nutzung von Open Directory Service (ODS) und Web Collaboration für das Starten einer Web Collaboration Sitzung. Damit können die UC-Lösungen UC Suite oder UC Smart mit einer externen Datenbank verbunden werden.

8.2.2 Benutzerlizenzen

Jeder am Kommunikationssystem angeschlossene Teilnehmer benötigt für die externe Telefonie eine Benutzerlizenz. Diese Lizenz wird der Rufnummer des Teilnehmers über das WBM fest zugeordnet.

Benutzerlizenzen beinhalten die umfassende Sprachfunktionalität von OpenScape-Business. Für die Nutzung der UC-Lösungen UC Smart oder UC Suite sind weitere Lizenzen nötig (siehe User-orientierte Lizenzen).

Folgende Teilnehmer-Lizenzen stehen zur Verfügung:

- **IP-Teilnehmer**

  Für die Nutzung von IP-Systemtelefonen (HFA) und SIP-Telefonen.
- **TDM-Benutzer**

  Für die Nutzung von UP0-Systemtelefonen, analogen Telefonen, analogem FAX, ISDN-Telefonen, ISDN-Fax und DECT-Telefonen.
- **Mobility-Teilnehmer**

  Für die Nutzung von GSM-/Mobiltelefonen, Smartphones und Tablet-PCs als Nebenstelle des Kommunikationssystems. Für die Nutzung von myPortal to go und Mobility Entry. Die Zuordnung eines zusätzlichen Tischtelefons (Desk Phone) ist nicht erforderlich. Für die Verwendung des Unify Phone Clients zusammen mit OpenScape Business.
- **DeskShare User**

  Für die Nutzung des Leistungsmerkmals DeskSharing. Diesen Teilnehmern ist nur eine Rufnummer und kein physikalisches Telefon fest zugeordnet. DeskShare User können bestimmte IP-Systemtelefone unter ihrer eigenen, fest zugeordneten Rufnummer nutzen und haben an den Telefonen Zugriff auf ihre persönlichen Telefoneinstellungen.
- **Fallback-Benutzer**

  Für die grundlegende Telefonie im Falle des Ausfalls eines Systemknotens. Die Lizenz wird als zeitbasierte Pay As You Go-Lizenz unterstützt. Daher

wird die Nutzungszeit basierend auf den Tagen berechnet, an denen das System Benutzer von anderen Knoten hostet. Die Lizenzen sind nur während dieser Host-Zeit gültig. Bei normalem Betriebsmodus werden Fallback User wie nicht lizenzierte Benutzer behandelt.

Flexible Teilnehmer-Lizenzierung

Mit der flexiblen Teilnehmer-Lizenzierung können TDM-, Mobility- und DeskShare User auch mit IP-Benutzerlizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility-Benutzerlizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility-Teilnehmer, können übrige IP-Benutzerlizenzen verwendet werden, um diesen Bedarf zu decken.

Voraussetzung für die Nutzung der flexiblen Teilnehmer-Lizenzierung ist die Software-Version V1R3.3 und eine am CLS neu generierte Lizenzdatei, die in OpenScape Business eingespielt und aktiviert werden muss.

Flexible Teilnehmer-Lizenzierung für UC Suite

Mit der flexiblen Teilnehmer-Lizenzierung für UC Suite können myPortal for Desktop-Teilnehmer auch mit myPortal for Outlook-Benutzerlizenzen lizenziert werden. Sind alle erworbenen myPortal for Desktop-Lizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere Benutzer, können übrige myPortal for Outlook-Benutzerlizenzen verwendet werden, um diesen Bedarf zu decken.

Voraussetzung für die Nutzung der flexiblen Teilnehmer-Lizenzierung ist die Software-Version V2 und eine am CLS neu generierte Lizenzdatei, die in OpenScape Business eingespielt und aktiviert werden muss.

8.2.3 User-orientierte Lizenzen

User-orientierte Lizenzen sind teilnehmerbezogen und berechtigen zur Nutzung der Unified Communications Leistungsmerkmale und der Applikationen zur Datenintegration. Eine User-orientierte Lizenz setzt immer eine Teilnehmer-Lizenz voraus und ist der Rufnummer des Teilnehmers fest zugeordnet.

Folgende User-orientierte Lizenzen stehen zur Verfügung:

Voicemail

- **Voicemail**

  Für die Nutzung einer persönlichen Sprachbox (VoiceMail) über das Telefon (TUI) und über die Oberfläche der UC-Lösungen UC Smart oder UC Suite.

  Anmerkung: Wird die UC-Lösung UC Smart auf UC Suite erweitert, bleiben die vorhandenen VoiceMail-Lizenzen und die Zuordnung zu den Teilnehmern erhalten.

  Anmerkung: Wenn Sie einer Nebenstelle eine VoiceMail-Lizenz zuweisen, wird ein UC Suite-Benutzer erstellt und alle aktiven Anrufweiterleitungen werden zurückgesetzt.

Cloud-Dienste

- **Unify Phone**

  Für die Nutzung des Unify Phone-Clients in Kombination mit OpenScape Business.

UC Client Benutzeroberfläche

- **UC Smart User**

  Für die Nutzung der UC Smart Funktionen der Communications Clients myPortal @Work, myPortal to go und weiterer Web Services-Clients.
- **UC Suite User**

  Für die Nutzung der UC Suite Funktionen der Communications Clients myPortal @work, myPortal for Desktop, myPortal to go und weiterer Web Services-Clients.
- **Groupware User**

  Für die Nutzung der UC Suite Funktionen der Communications Clients myPortal @work, myPortal for Outlook, myPortal to go und weiterer Web Services-Clients.
- **Fax**

  Für die Nutzung einer Faxbox innerhalb der UC Suite. Voraussetzung ist eine zusätzliche UC User- oder eine Groupware User-Lizenz.
- **Konferenz**

  Für die Nutzung der Konferenz-Verwaltung innerhalb der UC Suite, wie z.B. Verwalten und Einleiten von permanenten und wiederkehrenden Konferenzen. Voraussetzung ist eine zusätzliche UC User-Lizenz oder eine Groupware User-Lizenz.

  Für die Teilnahme an Konferenzen wird keine Lizenz benötigt.
- **myAttendant**

  Für die Nutzung der UC Suite-Vermittlungsfunktionen.
- **myAgent**

  Für die Nutzung der Contact Center Funktionen, wie z.B. Informationen zu Warteschlangen, Popups mit Kundeninformationen bei ankommenden Anrufen und Zugriff auf die Anrufhistorie.

Anmerkung: Für den mobilen Client myPortal to go ist neben der Mobility User-Lizenz eine zusätzliche UC User-Lizenz oder Groupware User-Lizenz für die UC-Lösung UC Smart oder die UC-Lösung UC Suite erforderlich.

Datenintegration

- **Application Launcher**

  Für die anrufbezogene Steuerung von Applikationen auf einem Client-PC bei ankommenden und gehenden Anrufen, z. B. Aufruf einer Applikation oder Anzeige von Anruferdaten. Der Application Launcher kann mit UC Smart, UC Suite oder myAgent betrieben werden und benötigt zusätzlich eine eine UC User-/Groupware User-Lizenz oder eine myAgent-Lizenz. Optional kann er den Open Directory Service nutzen.

- **OpenScape Business TAPI**

  Für die Nutzung von TAPI-konformen Applikationen und zum PC-unterstützten Telefonieren mit kundeneigenen Programmen verschiedener Software-Hersteller. Voraussetzung ist UC Booster (UC Booster Card oder UC Booster Server).

8.2.4 Systemlizenzen

Systemlizenzen sind nicht teilnehmerbezogen und schalten die systemweiten Leistungsmerkmale frei. Diese Leistungsmerkmale können von allen Teilnehmern des Kommunikationssystems genutzt werden.

Übersicht über Systemlizenzanforderungen

Trunktype	SSP-Lizenz	Leitungslizenzen/ Kanal	Networking-Lizenz
ITSP	Ja	Ja	Nein
Native SIP-Trunk	Ja	Nein	Ja
Skype for Business	Ja	Ja	Nein
Unify Phone	Ja	Nein	Nein
SIPQ-Verbindung	Nein	Nein	Ja

Folgende Systemlizenzen stehen zur Verfügung.

System Ressourcen

- **S_{2M}/T1/SIP Trunks**

  Für die Nutzung von S_{2M}-/T1- und ITSP-Kanälen. S_0-Kanäle müssen nicht lizenziert werden. Dazu zählen auch Anschaltungen zu S_0-Fax-Servern im PP-Modus. Bei Primärmultiplex-Verbindungen S_{2M} oder T1 (USA) werden die einzelnen Sprachkanäle lizenziert. Bei ITSP-Verbindungen wird die Anzahl der gleichzeitigen Verbindungen zu einem oder mehreren ITSP-Providern (SIP-Providern) lizenziert. Die Anzahl der möglichen gleichzeitigen Verbindungen ist abhängig von der Bandbreite des Anschlusses.
- **Vernetzung**

  Für die IP-Vernetzung via SIP-Q/native SIP und/oder die TDM-Vernetzung via CorNet-NQ oder QSIG. Für die Vernetzung der UC Suite Applikationen. Pro Knoten ist eine Lizenz nötig.

Anmerkung: Die Networking-Lizenz schaltet für einen Knoten die Leitungen für die Sprachvernetzung und die UC Suite Vernetzung frei. Für Vernetzungsleitungen werden keine S_{2M}/T1/SIP Trunk-Lizenzen benötigt.

Tabelle 3: Übersicht über die Systemressourcenlizenzen (S_{2M}/ITSP)

Protokoll	Lizenzen			
	Keine Lizenz	OpenScape Business Networking (1x pro System)	OpenScape Business S_{2M} / ITSP (1x pro Kanal)	TDM-Benutzer
S_0 intern				
Fax-Server (DSS1/QSIG)	X			
Euro-Bus				Pro S_0-Teilnehmer
S_0 - Amtsleitungen				
Euro-Amt PP	X			
Euro-Amt PMP	X			
S_{2M} - Amtsleitungen				
Euro-Amt PP			X	
ITSP - Provider				
ITSP 1 bis 8			X	
S_0 Vernetzung				
QSIG		X		
CorNet-NQ		X		
S_{2M} - Vernetzung				
QSIG		X		
CorNet-NQ		X		
SIP-Vernetzung				
SIP-Q		X		
native SIP		X		

Contact Center Optionen

- **Contact Center Mail**

  Für die Einrichtung von einer oder mehreren E-Mail-Boxen für das Empfangen und Senden von E-Mails für Contact-Center-Agenten. Voraussetzung ist eine Teilnehmer-Lizenz und eine myAgent Lizenz. Pro Knoten ist eine Lizenz nötig.
- **Contact Center Fax**

  Für die Einrichtung von einer oder mehreren Faxboxen für das Empfangen und Senden von Faxen für Contact-Center-Agenten. Voraussetzung ist eine Teilnehmer-Lizenz und eine myAgent Lizenz. Pro Knoten ist eine Lizenz nötig.
- **myReports**

  Für die Erstellung von Statistiken über die Auslastung der Contact Center-Ressourcen nach unterschiedlichen Kriterien. Mit dem Schedule Manager können aus über 100 vordefinierten Berichtsvorlagen für Telefon-, E-

Mail- und Fax-Kontakte Berichte erstellt werden. Die Verwaltung der Berichtsvorlagen erfolgt über den Report Manager mit der Möglichkeit zur Umgruppierung sowie zum Hinzufügen und Löschen neu erstellter Report-Vorlagen.

UC Client Optionen

- **Open Directory Connector**

  Für die Verbindung zum Open Directory Service (ODS), um auf eine externe Datenbank oder ein externes Verzeichnis zugreifen zu können. Pro Knoten können bis zu vier Datenbanken angebunden werden.
- **Company AutoAttendant**

  Für die Nutzung eines zentralen, UC Smart oder UC Suite basierten AutoAttendant zur automatischen Vermittlung von Gesprächen. Pro Knoten ist eine Lizenz nötig.

  Ansagen vom Typ "Wartemusik" (endlos) werden nur mit dieser Lizenz abgespielt.
- **OpenScape Business Attendant**

  Für die Nutzung des PC-Vermittlungsplatzes OpenScape Business Attendant. Pro Knoten können bis zu 8 OpenScape Business Attendant lizenziert werden.

  Soll OpenScape Business Attendant auch Zugriff auf Präsenz-Informationen haben, ist zusätzlich eine oder UC User-Lizenz nötig.
- **OpenScape Business BLF**

  Für die Nutzung der zusätzlichen Besetztlampenfeldanzeige von OpenScape Business BLF. Pro Teilnehmer ist eine BLF-Lizenz und eine UC User-Lizenz erforderlich. Pro Knoten können bis zu 50 OpenScape Business BLF lizenziert werden.

8.2.5 Evaluierungslizenzen

Mit einer Evaluierungslizenz können besondere Leistungsmerkmale über einen bestimmten Zeitraum (Evaluation Period) mit vollem Leistungsumfang kostenlos getestet werden. Wird während der Evaluation Period eine reguläre Lizenz für das Leistungsmerkmal aktiviert, wird die Evaluierungslizenz deaktiviert.

Folgende Evaluierungslizenzen stehen zur Verfügung:

- **OpenScape Business V3 Service Evaluierung**

  Diese Evaluierungslizenz ist für Partner bestimmt, die das Kommunikationssystem in ihrer Firma vorkonfigurieren und später beim Kunden in Betrieb nehmen möchten. Während der Vorkonfiguration startet die Activation Period von 30 Tagen. Damit nach Inbetriebnahme

des Systems die Activation Period von 30 Tagen neu startet, muss diese Evaluierungslizenz nach der Inbetriebnahme beim Kunden aktiviert werden.#

Die Aktivierung ist einmal pro System und nur innerhalb der Activation Period möglich. Ist die Activation Period abgelaufen muss das System mit dauerhaften Lizenzen lizenziert werden.

Anmerkung: Wenn die Service-Evaluierung aktiviert ist, kann CLS Connect nicht aktiviert werden.

- **OpenScape Business V3 UC Smart Evaluierung**

  Diese Evaluierungslizenz ist für Kunden bestimmt, die die UC-Funktionen von UC Smart testen möchten. Mit dieser Evaluierungslizenz können alle Leistungsmerkmale von UC Smart genutzt werden.

  Anmerkung: Diese Evaluierungslizenz ist nicht einsetzbar, falls sich das Kommunikationssystem in einem Netzverbund befindet und die Lizenz "Networking" aktiv ist. Sind bereits Voicemail Lizenzen vorhanden, werden diese in Kombination mit den neuen UC Evaluierungslizenzen verwendet.

- **OpenScape Business V3 UC Suite Evaluierung**

  Diese Evaluierungslizenz ist für Kunden bestimmt, die die UC-Funktionen von UC Suite testen möchten. Mit dieser Evaluierungslizenz können alle Leistungsmerkmale von UC Suite genutzt werden.

  Anmerkung: Diese Evaluierungslizenz ist nicht einsetzbar, falls sich das Kommunikationssystem in einem Netzverbund befindet und die Lizenz "Networking" aktiv ist. Sind bereits Voicemail Lizenzen vorhanden, werden diese in Kombination mit den neuen UC Evaluierungslizenzen verwendet.

- **OpenScape Business V3 UC Suite Contact Center Evaluierung**

  Diese Evaluierungslizenz ist für Kunden bestimmt, die das Multimedia Contact Center testen möchten. Mit dieser Evaluierungslizenz können alle Leistungsmerkmale des Multimedia Contact Centers genutzt werden.

  Anmerkung: Wird das Multimedia Contact Center nicht innerhalb der Evaluation Period lizenziert, muss der Administrator vor Ablauf der Evaluierungslizenz die Einstellungen am Contact Center wieder rückgängig machen (z.B. Zeitpläne und Warteschlangen löschen, Agenten deaktivieren, usw.). Andernfalls können in OpenScape Business Fehler auftreten.

- **OpenScape Business V3 CRM Evaluierung**

  Diese Evaluierungslizenz ist für Kunden bestimmt, Application Launcher, Open Directory Service und TAPI testen möchten.

- **OpenScape Business V3 Attendant Evaluierung**

  Diese Evaluierungslizenz ist für Kunden bestimmt, die die Applikation OpenScape Business Attendant testen möchten.

- **OpenScape Business V3 BLF Evaluierung**

  Diese Evaluierungslizenz ist für Kunden bestimmt, die die Applikation OpenScape Business BLF testen möchten, z.B. für die eigenständige Anzeige von Besetztlampenfeld- und Präsenz-Informationen.

Regeln

- Die Aktivierung einer Evaluierungslizenz erfolgt am Customer License Server (CLS) und ist nur einmal möglich.
- Die Evaluation Period beträgt 90 Tage. Nach 60 Tagen wird im Display der Systemtelefone die verbleibende Zeit in Tagen rückwärts gezählt.
- Nach Ablauf der Evaluation Period erfolgt die automatische Deaktivierung des Leistungsmerkmals.
- Evaluierungslizenzen können gleichzeitig im System aktiv sein, enden dann aber zu unterschiedlichen Zeiten.
- Ist eine zeitlich unbefristete Lizenz aktiv, wird die Evaluierungslizenz nicht gestartet oder, falls bereits vorhanden, gestoppt.

8.2.6 Upgrade-Lizenzen

Upgrade-Lizenzen sind nötig, um von HiPath 3000 V9, OpenScape Office V3 und OpenScape Business V1 Systemen auf OpenScape Business V2 Systeme hochzurüsten.

Die Lizenzmigration von HiPath 3000 Systemen setzt ein laufendes und ggf. lizenziertes HiPath 3000 V9 System voraus. Die Schritte zur Hardware- und Lizenzmigration sind genau zu beachten (siehe Migration). Reine HiPath 3000 TDM Systeme ohne Lizenzen sind zuerst auf Version 9 hochzurüsten und können anschließend mit einer Upgrade-Lizenz auf OpenScape Business hochgerüstet werden.

Folgende Upgrade-Lizenzen stehen zur Verfügung:

- **HiPath 3000 V9 Upgrade auf OpenScape Business V2**

  Für die Migration von HiPath 3000 V9 auf OpenScape Business V2 X3/X5/X8.
- **HiPath 3000 V8 Upgrade auf OpenScape Business V2**

  Für die Migration von HiPath 3000 V8 auf HiPath 3000 V9 und anschließend auf OpenScape Business V2 X3/X5/X8.
- **HiPath 3000 V7 Upgrade auf OpenScape Business V2**

  Für die Migration von HiPath 3000 V7 auf HiPath 3000 V9 und anschließend auf OpenScape Business V2 X3/X5/X8.
- **OpenScape Office V3 MX/LX Upgrade auf OpenScape Business V2**

  Für die Migration von OpenScape Office V3 MX/LX auf OpenScape Business V2.

8.2.7 Vorschläge für Lizenzkombinationen

Lizenzen können beliebig kombiniert werden. Im Folgenden sind einige Vorschläge aufgelistet, wie Lizenzen sinnvoll kombiniert werden können, um die gewünschten Funktionen zu nutzen.

Bitte beachten Sie, dass für manche Funktionen mehrere Lizenzen benötigt werden.

Telefonie

- Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User

---

Anmerkung: Ohne gültige Lizenz ist das Telefon nur für interne Verbindungen freigeschaltet.

Tefefonie mit UC Smart

- Telefonie mit Sprachbox (UC Smart)
  - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
  - Erforderlich: User-orientierte VoiceMail-Lizenz
- Telefonie mit Mobility Entry (DISA-basiertes Mobility)
  - Erforderlich: Teilnehmer-Lizenz Mobility-Teilnehmer
- Telefonie mit myPortal to go
  - Erforderlich: Teilnehmer-Lizenz Mobility-Teilnehmer

    In der Betriebsart **Desktelefon** (Steuerung des Bürotelefons) ist keine Lizenz Mobility-Teilnehmer erforderlich.
  - Erforderlich: User-orientierte Lizenz UC User
  - Optional: User-orientierte VoiceMail-Lizenz
- Telefonie mit myPortal @work
  - Erforderlich: IP-Teilnehmer
  - Erforderlich: User-orientierte Lizenz UC User
  - Optional: User-orientierte VoiceMail-Lizenz
  - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myPortal @work VoIP
  - Erforderlich: IP-Teilnehmer
  - Erforderlich: User-orientierte Lizenz UC User
  - Optional: User-orientierte VoiceMail-Lizenz
  - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit optiClient Attendant
  - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
  - Erforderlich: Systemlizenz OpenScape Business Attendant
  - Optional: User-orientierte VoiceMail-Lizenz
  - Optional: User-orientierte Lizenz UC User (zum Anzeigen des Anwesenheitsstatus)

Telefonie mit UC Suite

- Telefonie mit Sprachbox (UC Suite)
  - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
  - Erforderlich: User-orientierte VoiceMail-Lizenz
- Telefonie mit myPortal for Desktop
  - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
  - Erforderlich: User-orientierte Lizenz UC User
  - Optional: User-orientierte VoiceMail-Lizenz
  - Optional: User-orientierte Lizenz Fax
  - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myPortal for Outlook
  - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
  - Erforderlich: User-orientierte Lizenz Groupware User
  - Optional: User-orientierte VoiceMail-Lizenz
  - Optional: User-orientierte Lizenz Fax
  - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myPortal to go
  - Erforderlich: Teilnehmer-Lizenz Mobility-Teilnehmer

    In der Betriebsart **Desktelefon** (Steuerung des Bürotelefons) ist keine Lizenz Mobility-Teilnehmer erforderlich.
  - Erforderlich: User-orientierte Lizenz Groupware User oder UC User
  - Optional: User-orientierte VoiceMail-Lizenz
- Telefonie mit myPortal @work
  - Erforderlich: IP-Teilnehmer
  - Erforderlich: User-orientierte Lizenz Groupware User oder UC User
  - Optional: User-orientierte VoiceMail-Lizenz
  - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myPortal @work VoIP
  - Erforderlich: IP-Teilnehmer
  - Erforderlich: User-orientierte Lizenz Groupware User oder UC User
  - Optional: User-orientierte VoiceMail-Lizenz
  - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myAttendant
  - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
  - Erforderlich: User-orientierte Lizenz myAttendant
  - Optional: User-orientierte VoiceMail-Lizenz

Telefonie mit Unify Phone

- Erforderlich: IP-Teilnehmer
- Erforderlich: User-orientierte Unify Phone-Lizenz

- Optional: User-orientierte VoiceMail-Lizenz und zusätzliche IP-User-Lizenz für die Teamkonfiguration

Nutzung des Contact Centers

- Erforderlich: Teilnehmer-Lizenz IP-Teilnehmer, DeskShare User oder Mobility-Teilnehmer
- Erforderlich: User-orientierte Lizenz myAgent

  Damit das System Contact Center-Anrufe weiterleiten und adressieren kann, muss mindestens eine myAgent-Lizenz aktiv sein.
- Optional: Systemlizenz Contact Center E-Mail
- Optional: Systemlizenz Contact Center Fax
- Optional: Systemlizenz myReports

Nutzung des Company AutoAttendant

- Erforderlich: Systemlizenz Company AutoAttendant

  Die AutoAttendant-Systemlizenz des Unternehmens muss aktiv sein, damit das System AutoAttendant-Anrufe weiterleiten und adressieren kann.

8.3 Lizenzierung eines Kommunikationssystems (Standalone)

Die Lizenzierung eines Standalone-Systems ist in einer bestimmten Reihenfolge durchzuführen. Diese Reihenfolge ist am Beispiel eines der Kommunikationssysteme OpenScape Business X dargestellt.

Wie Sie Schritt 3 und Schritt 4 mit Hilfe des WBM durchführen, ist in den nachfolgenden Unterkapiteln beschrieben.

1) **Lizenz-Autorisierungscode (LAC)**

   Der Kunde erhält beim Kauf von Lizenzen einen Lizenz-Autorisierungscode (LAC). Die Daten über die erworbenen Lizenzen sind in der Datenbank des zentralen Lizenzservers (CLS) gespeichert.
2) **Installation und Konfiguration**

   Der Kunde oder Servicetechniker installiert und konfiguriert das Kommunikationssystem mit Hilfe der WBM-Wizards (u.a. Teilnehmer und Leitungen). Beim ersten Starten des WBM ist das aktuelle Datum einzugeben. Ab diesem Zeitpunkt startet die Activation Period (Zeitspanne von 30 Tagen, in der die Lizenzierung des Kommunikationssystems vorgenommen werden muss).
3) **Lizenzaktivierung**

   Der Kunde oder Servicetechniker aktiviert die Lizenzen mit dem WBM entweder online über den Lizenz-Autorisierungscode (Online-Lizenzaktivierung) oder offline direkt über die Lizenzdatei (Offline-Lizenzaktivierung).
4) **Lizenzzuordnung**

   Der Kunde oder Servicetechniker ordnet mit dem WBM den Teilnehmern und den Leitungen die erworbenen Lizenzen zu. Nach erfolgreicher Zuordnung werden die lizenzierten Leistungsmerkmale freigeschaltet.

8.3.1 CLS Connect

CLS Connect ermöglicht Ihnen unbegrenzte Rehosts Ihrer OpenScape Business-Systeme. Zu diesem Zweck muss das **CLS Connect**-Flag aktiviert werden.

Anmerkung: Nach der Aktivierung kann dieses Flag nicht mehr ausgeschaltet werden.

Wenn das System die Verbindung zum CLS verliert, beginnt der Failover-Zeitraum. Wenn die Verbindung nach 30 Tagen nicht wiederhergestellt ist, wird das System in den Notfallmodus versetzt und gilt als unlizenziert.

Anmerkung: Wenn ein OpenScape Business-System mit aktivem CLS Connect neu programmiert werden muss, kann keine Sicherungsdatei erstellt werden. Ein Reload muss mit der gleichen MAC-ID und SIEL-ID durchgeführt werden. CLS Connect lässt sich ohne aktive Basislizenz nicht aktivieren. Die vorhandene Lizenzdatei aus dem CLS kann manuell über das WBM in das System hochgeladen werden.

8.3.1.1 Aktivierung von CLS Connect

CLS Connect ermöglicht Ihnen unbegrenzte Rehosts Ihrer OpenScape Business-Systeme.

Voraussetzungen

Sie sind am WBM mit dem Profil **Erweitert** angemeldet.

Für die Verbindung zum CLS ist ein Internet-Zugang nötig.

Die folgenden Firewall-Einstellungen sind aktiv:

a) Der Port 7790 ist für gehenden IP-Datenverkehr freigegeben.

Neuere V3R3-Softwaresysteme verwenden Port 7791 für die Online-Lizenzaktivierung.

b) IP 188.64.16.4 ist für gehenden IP-Datenverkehr freigegeben.

Anmerkung: Um die Firewall-Regeln sicherer zu machen, wird empfohlen, nur gehende Kommunikation zuzulassen.

Eine Verbindung zum CLS ist möglich; siehe Überprüfen des zentralen Lizenzservers (Central License Server, CLS)

Anmerkung: Wenn Sie CLS Connect aktivieren, kann es nicht wieder deaktiviert werden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **CLS Connect aktivieren**.
3) Aktivieren Sie **CLS Connect** über das Kontrollkästchen.
4) Klicken Sie auf **Aktivieren**.

Anmerkung: Im Infobereich der Startseite erscheint folgender Hinweis, wenn die Online-Lizenzkontrolle aktiviert ist:

'License mode: "CLS Connect".'

8.3.1.2 Umschaltung von CLS Connect

Weg von der CLS Connect- hin zu einer permanenten oder PAYGO-Lizenz.

Wenn Sie derzeit ein „CLS Connect“-Lizenzprogramm nutzen und auf eine permanente oder PAYGO-Lizenz umsteigen möchten, müssen Sie einige Schritte beachten, um einen reibungslosen Übergang zu gewährleisten:

Schritt für Schritt

1) Aktivieren Sie die Funktion CLS Connect Stop für die Lizenzdatei des Systems. Dies kann über ein CLS-Support-Ticket erfolgen.
2) Aktivieren Sie eine neue Lizenzdatei für das OSBiz, um das Secure Bit zurückzusetzen. Danach können Sie PAYGO oder die permanente lokale Lizenz für das System auf CLS aktivieren. Sie erhalten dann eine neue Datei, die Sie auf dem System aktivieren können.

Anmerkung: Wenn Sie eine vernetzte OSBiz-Umgebung haben, die in CLS Connect lizenziert ist, wird auch bei den Slave-Knoten das Secure Bit gesetzt. Wenn Sie planen, einen Slave-Knoten irgendwann als separates, eigenständiges System mit einer Nicht-CLS Connect-Lizenz zu verwenden, erstellen Sie bitte ein Support-Ticket für die erforderlichen Schritte.

8.3.2 Lizenzaktivierung (Standalone)

Nachdem ein Produkt oder ein Leistungsmerkmal erworben wurde, müssen zuerst die mit dem Produkt/Leistungsmerkmal bereitgestellten Lizenzen aktiviert werden. Nach erfolgreicher Aktivierung erfolgt dann die Lizenzzuordnung.

Um Lizenzen zu aktivieren gibt es zwei Möglichkeiten:

- **Online-Lizenzaktivierung** (über den Lizenz-Autorisierungscode)

  Der Kunde oder Servicetechniker überträgt mit Hilfe des WBM den Lizenz-Autorisierungscode via Internet an den zentralen Lizenzserver (CLS). Zusammen mit dem LAC wird die Locking ID des Kommunikationssystems für die Lizenzaktivierung verwendet. Der CLS erzeugt aus den Daten eine

Lizenzdatei und schickt diese zurück an das System, das daraufhin die erworbenen Lizenzen aktiviert.

Für den Zugang zum CLS benötigen Sie eine Internet-Verbindung. Die IP-Adresse des CLS ist im WBM unter **Lizenzverwaltung** > **Einstellungen** und kann falls nötig vom Administrator mit Profil **Expert** geändert werden.

Anmerkung: Für die Online-Lizenzaktivierung wird standardmäßig der Port 7790 verwendet. Dieser Port muss in der Firewall des Kundennetzes freigegeben sein.

Neuere V3R3-Softwaresysteme verwenden Port 7791 für die Online-Lizenzaktivierung.

Anmerkung: Bevor die Online-Lizenzierung durchgeführt werden kann, müssen zuerst die Registrierungsdaten korrekt erfasst werden.

- **Offline-Lizenzaktivierung** (direkt über die Lizenzdatei)

  Der Kunde oder Servicetechniker meldet sich am zentralen Lizenzserver (CLS) an und gibt dort den Lizenz-Autorisierungscode zusammen mit der Locking ID des Kommunikationssystems ein. Der CLS erzeugt aus den Daten eine Lizenzdatei. Der Kunde oder Servicetechniker lädt sich die Lizenzdatei herunter und spielt diese in das WBM ein. Das System aktiviert daraufhin die erworbenen Lizenzen.

  Die IP-Adresse des CLS ist im WBM unter **Lizenzverwaltung** > **Einstellungen** und kann falls nötig vom Administrator mit Profil **Expert** geändert werden.

Wenn das Kommunikationssystem erweitert werden soll, können weitere Lizenzen zugekauft werden. Beim Erwerb zusätzlicher Lizenzen wird ein weiterer Lizenz-Autorisierungscode (LAC) ausgeliefert, mit dem die neu erworbenen Lizenzen aktiviert werden können.

Anmerkung: Zusätzlich erworbene Lizenzen können auch über Remote aktiviert werden.

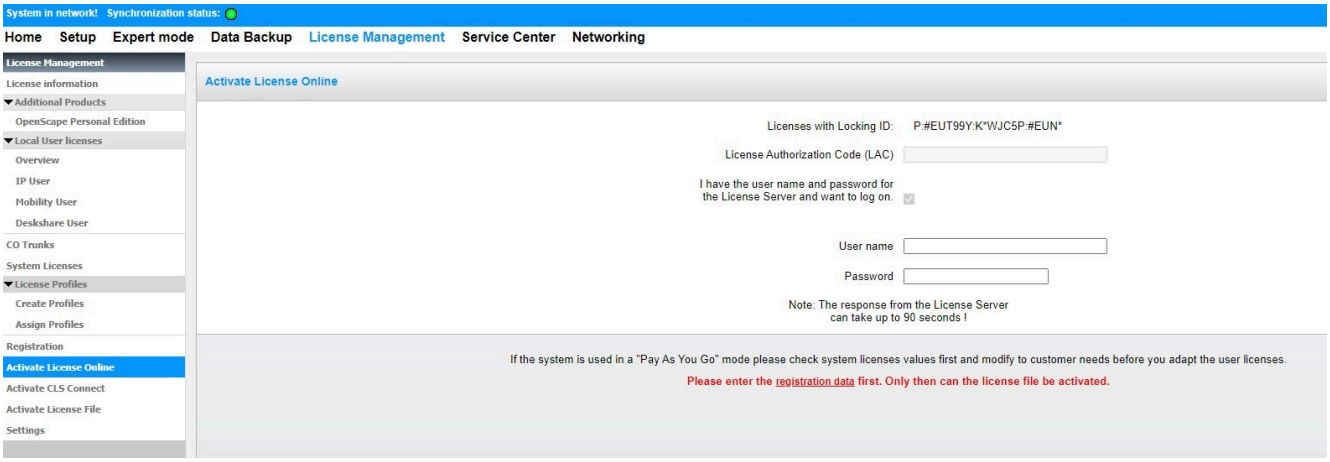
8.3.2.1 Wie Sie Lizenzen online aktivieren (Standalone)

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Sie kennen den Lizenz-Autorisierungscode (LAC) für die Lizenzfreischaltung.

Für die Verbindung zum Lizenzserver muss das Kommunikationssystem eine Verbindung zum Internet haben.



Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Registrierung**.
3) Geben Sie Ihre Daten ein und klicken Sie auf **OK**.
4) Klicken Sie im Navigationsbaum auf **Lizenz Online aktivieren**.
5) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.
6) Aktivieren Sie das Kontrollkästchen **Ich habe Benutzernamen und Passwort für den Lizenzserver und möchte mich anmelden**.
7) Geben Sie **Benutzername** und **Passwort** für die Anmeldung am Lizenzserver ein.
8) Klicken Sie auf **Aktivieren**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen in das Kommunikationssystem übertragen. Nach erfolgreicher Freischaltung wird die Verbindung automatisch wieder abgebaut.

8.3.2.2 Wie Sie Lizenzen offline aktivieren (Standalone)

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Lizenzdatei wurde am zentralen Lizenzserver erzeugt und abgespeichert. Sie kennen den Ablageort der Lizenzdatei.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Lizenzdatei aktivieren**.
3) Klicken Sie unter **Lizenzdatei** auf **Durchsuchen** und wählen Sie den Ablageort der Lizenzdatei aus.
4) Klicken Sie auf **Aktivieren**.

8.3.3 Lizenzzuordnung (Standalone)

Nach erfolgreicher Aktivierung müssen die erworbenen Lizenzen den Teilnehmern und Leitungen zugeordnet werden. Systemweite Leistungsmerkmale sind in einem Standalone-System bereits mit der Aktivierung freigeschaltet.

Zuordnung von Benutzerlizenzen und User-orientierten Lizenzen

Den Teilnehmern können Benutzerlizenzen und User-orientierte Lizenzen zugeordnet werden.

Folgenden Anwender-Typen können Benutzerlizenzen zugeordnet werden:

Symbol	Benutzerlizenz	Beschreibung
	IP-Teilnehmer	Für die Nutzung von IP-Systemtelefonen (HFA oder SIP) und SIP-Telefonen
	TDM-Teilnehmer	Für die Nutzung von UP0-Systemtelefonen, ISDN-Telefonen, analogen Telefonen und DECT-Telefonen
	Mobility-Teilnehmer	Für die Nutzung von myPortal to go, Mobility Entry und DISA (One Number Service)
	Deskshare User	Für die Nutzung von DeskSharing für IP-Teilnehmer

Die Benutzerlizenzen werden den Rufnummern der Teilnehmer fest zugeordnet. Wird ein Teilnehmer gelöscht oder einer Rufnummer ein anderer Teilnehmer-Typ zugeordnet, wird die zugehörige Benutzerlizenz freigegeben.

Neben einigen Lizenzen befindet sich ein Sternchen. Ein rotes Sternchen bedeutet, dass die Lizenzen auch durch die Zuweisung einer anderen Lizenz gedeckt werden können.

Mit der flexiblen Lizenzierung können TDM-, Mobility- und DeskShare-Teilnehmer auch mit IP-Benutzerlizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility-Benutzerlizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility-Teilnehmer, können übrige IP-Benutzerlizenzen verwendet werden, um diesen Bedarf zu decken.

Nachdem dem Teilnehmer eine Benutzerlizenz zugeordnet wurde, können diesem Teilnehmer auch User-orientierte Lizenzen zugeordnet werden.

Folgende User-orientierte Lizenzen können den Teilnehmern zugeordnet werden:

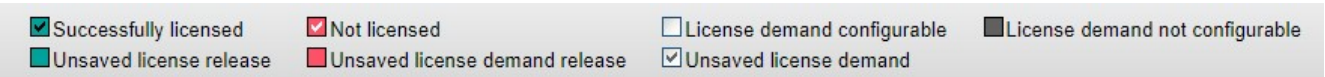
Symbol	User-orientierte Lizenz	Beschreibung
	Voicemail	Für die Nutzung der Sprachbox.
	Groupware User	Für die Nutzung der UC Suite-Funktionen über myPortal for Outlook.

Symbol	User-orientierte Lizenz	Beschreibung
	RAS-Benutzer	Für die Nutzung der UC Suite-Funktionen über myPortal for Desktop.
	Fax	Für die Nutzung einer Faxbox innerhalb der UC Suite. Voraussetzung ist eine UC User- oder eine Groupware User-Lizenz.
	Konferenz	Für die Nutzung der Konferenz-Funktionen der UC Suite. Voraussetzung ist eine UC User- oder eine Groupware User-Lizenz.
	myAttendant	Für die Nutzung der UC Suite-Vermittlungsfunktionen.
	myAgent	Für die Nutzung der Contact Center-Funktionen.
	Application Launcher	Für die anrufbezogene Steuerung von Applikationen auf einem Client-PC bei ankommenden und gehenden Anrufen, z. B. Aufruf einer Applikation oder Anzeige von Anruferdaten.
	Unify Phone	Für die Nutzung des Unify Phone-Clients in Kombination mit OpenScape Business.
	TAPI	Für die Nutzung von TAPI-konformen Applikationen und zum PC-unterstützten Telefonieren mit kundeneigenen Programmen verschiedener Software-Hersteller.

Sie können sich eine Übersicht über alle Benutzerlizenzen und User-orientierte Lizenzen anzeigen lassen (über **Lokale Benutzerlizenzen** > **Übersicht)**.

In dieser Übersicht werden Ihnen auch zu jedem Teilnehmer die Zustände seiner Lizenzen angezeigt.

Es gibt folgende Lizenzzustände:



Zuordnung von System-Lizenzen

System-Lizenzen enthalten Lizenzen für Leitungen und systemweite Leistungsmerkmale.

Folgenden Typen von Leitungen können Lizenzen zugeordnet werden:

- S_{2M}-/T1-Leitungen: Anzahl der B-Channels
- ITSP-Leitungen: Anzahl der gleichzeitig über einen ITSP geführten Rufe

Lizenzen für systemweite Leistungsmerkmale werden bei einem Standalone-System bereits bei der Lizenzaktivierung standardmäßig freigeschaltet. Eine weitere Zuordnung ist nicht erforderlich.

Vorgehensweise bei der Lizenzzuordnung

Voraussetzung: Die Lizenzdatei ist aktiviert und die Teilnehmer sind eingerichtet.

- Teilnehmer lizenzieren

  1) Teilnehmer eine User-Lizenz zuordnen. Durch diese Zuordnung wird für den Teilnehmer eine Lizenzanforderung generiert und zugleich die Zuordnung der User-orientierten Lizenzen freigeschaltet.
  2) Teilnehmer die User-orientierten Lizenzen zuordnen. Durch diese Zuordnungen werden für den Teilnehmer weitere Lizenzanforderungen generiert. Bitte beachten Sie, dass einige Lizenzen andere Lizenzen voraussetzen (siehe Vorschläge für Lizenzkombinationen).
  3) Lizenzanforderungen prüfen und freischalten.
  4) Liegen nicht genügend Lizenzen für die Freischaltung vor, werden Ihnen die fehlerhaften Zuordnungen über die Lizenzzustände (rot) angezeigt. Die Lizenzzuordnungen korrigieren und die Lizenzen erneut prüfen und freischalten.

  Anmerkung: Zur besseren Übersicht können Sie sich die Lizenzzuordnungen für alle Teilnehmer als Vorab-Ausdruck anzeigen lassen (über **Lokale Benutzerlizenzen** > **Übersicht** > **Drucken**). Am Ende des Ausdrucks werden alle ungültigen Zuordnungen in einer separaten Tabelle aufgeführt.

- Leitungslizenzen zuordnen

  Die Leitungslizenzen müssen auf die benötigten S_{2M}-/T1- und ITSP-Leitungen aufgeteilt werden.

8.3.3.1 Teilnehmer lizenzieren (Standalone)

Verteilen Sie die verfügbaren Teilnehmer-Lizenzen und User-orientierten Lizenzen auf die Teilnehmer. Nach erfolgreicher Zuordnung sind die Teilnehmer lizenziert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

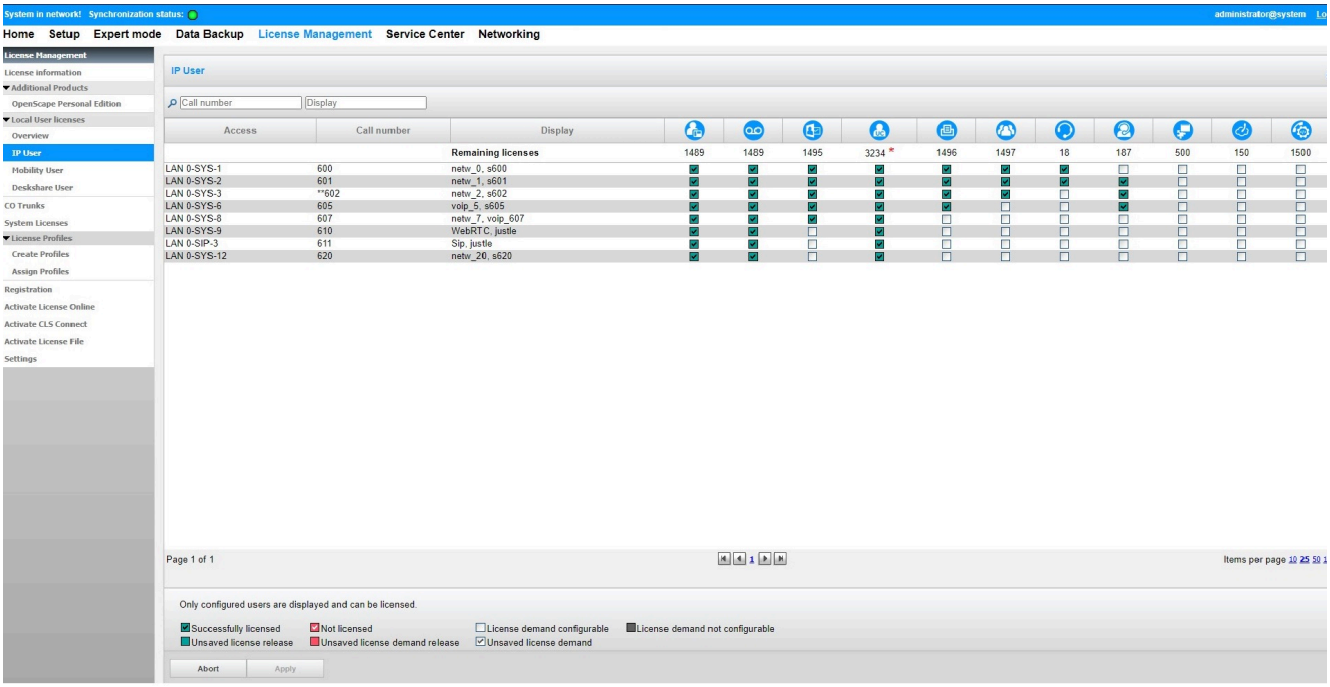
1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Navigieren Sie im Navigationsbaum unter **Lokale Benutzerlizenzen** > **...** zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.

   Unter **Verbleibende Lizenzen** wird Ihnen angezeigt, wie viele Lizenzen Sie noch den Teilnehmern zuordnen können. Bei den TDM-, Mobility- und DeskShare-Teilnehmern beinhaltet die Anzeige auch alle noch übrigen IP User Lizenzen, da diese Lizenzen auch für die Lizenzierung von TDM-, Mobility- und DeskShare-Teilnehmern verwendet werden dürfen (flexible Teilnehmer-Lizenzierung).

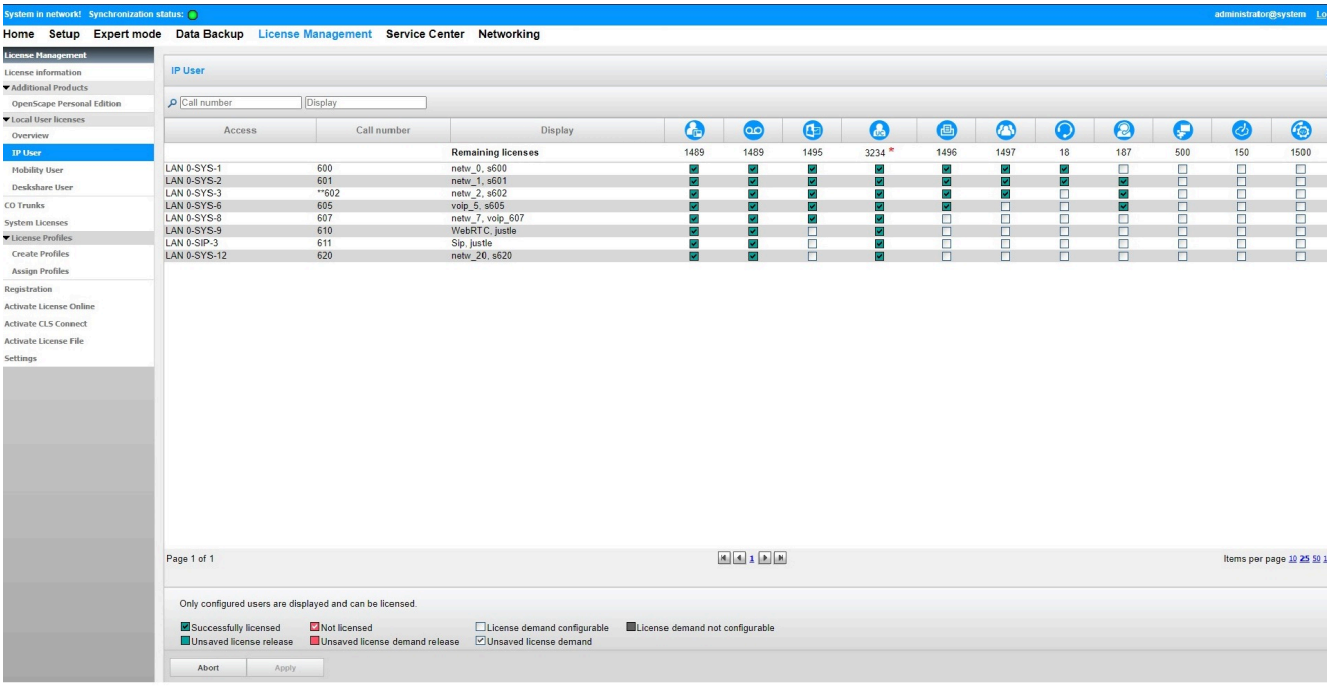
   Wenn der ausgewählte Teilnehmertyp der eines Mobility-Teilnehmers ist, sehen Sie auch die Gesamtzahl der verfügbaren Unify Phone-Lizenzen und deren Ablaufdatum.

3) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die Teilnehmer-Lizenz, indem Sie das hell hinterlegte Kontrollkästchen (erste Spalte mit Kontrollkästchen) aktivieren. Die Kontrollkästchen in den anderen Spalten werden aktiviert.

Anmerkung: Sie können sich auch einen ausgewählten Teilnehmer anzeigen lassen, indem Sie in die Suchfelder **Rufnummer** oder **Name** einen Suchbegriff eingeben und anschließend die Eingabetaste drücken oder auf das Lupen-Symbol klicken. Alle Teilnehmer werden aufgelistet, wenn beide Suchfelder leer sind und Sie anschließend die Eingabetaste drücken oder auf das Lupen-Symbol klicken.



4) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.



Anmerkung: Benutzerbezogene Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz zugeordnet wurde (Schritt 3).

Anmerkung: Wenn Sie einer Nebenstelle eine VoiceMail-Lizenz zuweisen, wird ein UC Suite-Benutzer erstellt und alle aktiven Anrufweiterleitungen werden zurückgesetzt.

Anmerkung: Die "Pay As You Go“-Voicemail-Lizenz wird automatisch aktiviert/deaktiviert, wenn eine Voice-Benutzerlizenz lizenziert/nicht-lizenziert ist; unabhängig davon kann eine Voicemail-Lizenz jederzeit deaktiviert werden.

Groupware, UC User, Fax, myAttendant und myAgent sind Lizenzmerkmale, die im UC Smart-Modus nicht konfigurierbar sind.

Groupware- und UC User-Lizenzen schließen sich im UC Suite-Modus gegenseitig aus.

5) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.

   Sind ausreichend Lizenzen vorhanden, ist die Lizenzierung des Teilnehmers hiermit beendet.

   Anmerkung: Bei "Pay As You Go" erscheint ein Popup-Fenster. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.

6) Fehlen Lizenzen, werden Ihnen die Fehler mit rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt 5.

   Anmerkung: Wenn Sie eine Teilnehmer-Lizenz entfernen wollen, müssen Sie eine Warnmeldung bestätigen. Anschließend erscheint ein neues Kontrollkästchen **Warnungen aktiviert**. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie weitere Teilnehmer-Lizenzen ohne Warnmeldung entfernen.

8.3.3.2 Wie Sie Leitungen lizenzieren (Standalone)

Verteilen Sie die erworbenen Leitungslizenzen auf die SIP- und S_{2M}-/T1-Leitungen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich **Amtsleitungen** wird Ihnen die Anzahl der verfügbaren Lizenzen für SIP- und S_{2M}-/T1-Amtsleitungen angezeigt.
3) Für SIP-Leitungen: Geben Sie im Bereich **SIP trunks** unter **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.
4) Für S_{2M}-Leitungen: Wählen Sie im Bereich **PRI (S2M/T1)** in der Zeile des gewünschten S_{2M}-Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.
5) Für digitale T1-Leitungen (nur USA): Wählen Sie im Bereich **PRI (S2M/T1)** in der Zeile des gewünschten T1-Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.
6) Für analoge T1-Leitungen (nur USA): Aktivieren Sie die analoge T1-Leitung, indem Sie im Bereich **PRI (S2M/T1)** in der Zeile der analoge T1-Leitung in der Aufklappliste der Spalte **Demands** den Eintrag **1** auswählen (**0** bedeutet: die Leitung ist deaktiviert).

7) Klicken Sie auf **OK & Weiter**.

Anmerkung: Die Anzahl der lizenzierten SIP-Leitungen und die Anzahl der lizenzierten S_{2M}-/T1-Leitungen darf die Anzahl der verfügbaren Leitungslizenzen nicht überschreiten.

8.4 Lizenzierung mehrerer Kommunikationssysteme (Netzverbund)

Die Lizenzierung mehrerer Kommunikationssysteme ist in einer bestimmten Reihenfolge durchzuführen. Diese Reihenfolge ist am Beispiel eines Netzverbunds aus einer OpenScape Business S (Master) und zweier OpenScape Business X3 (Slave) dargestellt.

Sind mehrere OpenScape Business (Knoten) zu einem Netzverbund zusammengeschlossen, erfolgt die Lizenzierung zentral über eine Netzwerklizenzdatei, die am Master-Knoten aktiviert wird. Zusätzlich benötigt jeder Slave-Knoten im Netzverbund eine eigene Networking-Systemlizenz. Der Knoten mit der größten Bandbreite sollte der Master-Knoten sein.

Mit dem Netzwerk-Wizard des WBM werden die Knoten im Netzverbund als Master-Knoten und Slave-Knoten konfiguriert. Der Master-Knoten enthält den zentralen Lizenzagenten (zentraler CLA, central Customer License Agent). Alle Slave-Knoten im Netzverbund nutzen diesen CLA für die Lizenzierung. Dafür wird den Slave-Knoten mit Hilfe des WBM die IP-Adresse des Master-Knotens bekannt gegeben.

Für den gesamten Netzverbund existiert nur eine Netzwerklizenzdatei. Diese ist an den Master-Knoten über seine Locking ID gebunden. Ist eine OpenScape Business S (Soft Switch) der Master-Knoten, ist die Netzwerklizenzdatei über die Locking ID des Linux-Servers des Soft Switches oder über die Advanced Locking ID des Soft Switches gebunden, wenn der Soft Switch in einer virtuellen Umgebung eingesetzt wird. Die Netzwerklizenzdatei ist im zentralen CLA gespeichert und enthält alle Lizenzinformationen des Netzverbunds. Sie kann nur am Master-Knoten über das WBM aktiviert werden. Nur der Master-Knoten hat Zugang zum CLS, an allen anderen Knoten ist der Zugang deaktiviert.

Im Netzverbund sollte eine knotenspezifische Lizenzierung nicht vorgenommen werden. Liegt für jeden Knoten bereits eine eigene Netzwerkdatei vor, können Sie diese am CLS zu einer Netzwerklizenzdatei zusammenführen.

Verhalten bei Netzproblemen (Failover)

Fällt die Verbindung zum Master-Knoten und somit zum zentralen CLA aus, wird im Display der Systemtelefone "Failover Period" angezeigt. Innerhalb dieser Failover Period (max. 30 Tage) sind alle Knoten und deren Leistungsmerkmale weiterhin funktionsfähig. Sind die Netzprobleme beseitigt und ist die Verbindung zum zentralen CLA wiederhergestellt, gehen alle Knoten wieder in den regulären Lizenzstatus über.

Werden die Netzprobleme nicht innerhalb der Failover Period behoben, gehen die Knoten in den Notbetrieb über. Anschließend muss der Netzverbund neu lizenziert werden.

Lizenzierungsablauf im Netzverbund anhand des o.g. Beispiels

OpenScape Business S (Master) und beide OpenScape Business X3 (Slave) sind bereits installiert, konfiguriert und zu einem Netzverbund zusammengeschlossen.

1) **Lizenz-Autorisierungscode (LAC)**

   Der Kunde erhält beim Kauf von Lizenzen einen Lizenz-Autorisierungscode (LAC). Die Daten über die erworbenen Lizenzen sind in der Datenbank des zentralen Lizenzservers (CLS) gespeichert.

2) **OpenScape Business S als Master-Knoten**

   Der Kunde oder Servicetechniker meldet sich am WBM der OpenScape Business S an und installiert mit Hilfe des Netzwerk-Wizards die OpenScape Business S als Master-Knoten.

   Das System wurde bereits installiert und konfiguriert und läuft in der Activation Period (Zeitspanne von 30 Tagen, in der die Lizenzierung vorgenommen werden muss).

3) **Locking ID des Master-Knotens**

   Der Kunde oder Servicetechniker notiert sich die Locking ID oder die Advanced Locking ID von OpenScape Business S.

   Beschreibung siehe Wie Sie die Locking ID des Kommunikationssystems abfragen

4) **OpenScape Business X3 als Slave-Knoten**

   Der Kunde oder Servicetechniker meldet sich zuerst am WBM der ersten OpenScape Business X3 an und installiert mit Hilfe des Netzwerk-Wizards die erste OpenScape Business X3 als Slave-Knoten und wiederholt diese Prozedur am WBM der zweiten OpenScape Business X3.

   Die Systeme wurden bereits installiert und konfiguriert und laufen in der Activation Period.

5) **Locking IDs von OpenScape Business X3**

   Der Kunde oder Servicetechniker notiert sich die Locking IDs der beiden OpenScape Business X3.

   Beschreibung siehe Wie Sie die Locking ID des Kommunikationssystems abfragen

6) **Lizenzaktivierung**

   Der Kunde oder Servicetechniker meldet sich am CLS an und generiert zusammen mit dem Lizenz-Autorisierungscode und den Locking IDs eine Netzwerklizenzdatei. Diese Datei lädt er mit Hilfe des WBM in den Master-Knoten.

   Beschreibung siehe Wie Sie Lizenzen offline aktivieren (Netzverbund)

   Das System aktiviert daraufhin die erworbenen Lizenzen.

7) **Lizenzzuordnung**

   Der Kunde oder Servicetechniker verteilt nun die Lizenzen auf die Knoten. Dazu meldet er sich am WBM jedes Knotens an und ordnet dem Knoten die gewünschte Anzahl von Lizenzen zu. Wichtig ist, dass jedem Knoten eine Networking-Systemlizenz zugewiesen ist, ansonsten ist er nicht in den Netzverbund integriert.

   Beschreibung siehe Wie Sie Systemlizenzen einem Knoten zuordnen

8.4.1 Lizenzaktivierung (Netzverbund)

Nachdem ein Produkt oder ein Leistungsmerkmal erworben wurde, müssen zuerst die mit dem Produkt/Leistungsmerkmal bereitgestellten Lizenzen aktiviert werden. Dafür wird direkt die Lizenzdatei benötigt. Nach erfolgreicher Aktivierung erfolgt dann die Lizenzzuordnung.

Um Lizenzen zu aktivieren gibt es folgende Möglichkeit:

- **Offline-Lizenzaktivierung** (direkt über die Lizenzdatei)

  Der Kunde oder Servicetechniker meldet sich am zentralen Lizenzserver (CLS) an und gibt dort den Lizenz-Autorisierungscode zusammen mit den Locking IDs der Kommunikationssysteme ein. Der CLS erzeugt aus den Daten eine Lizenzdatei. Der Kunde oder Servicetechniker lädt sich die Lizenzdatei herunter und spielt diese in das WBM des Master-Knotens ein.

  Am Master-Knoten wird geprüft, ob die in der Lizenzdatei gespeicherten Locking IDs mit denen der Systeme übereinstimmen. Ist die Prüfung erfolgreich, werden die Lizenzen aktiviert und die Systeme wechseln in den regulären Lizenzstatus. Ist die Prüfung nicht erfolgreich, laufen die Systeme weiter in der Activation Period und nach Ablauf der Activation Period nur noch im Notbetrieb.

  Die IP-Adresse des CLS ist im WBM unter **Lizenzverwaltung** > **Einstellungen** hinterlegt.

Um Lizenzdateien zusammen zu führen gibt es folgende Möglichkeit:

- **Wie Sie Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen**

  Sind bereits ein oder mehrere Knoten lizenziert und sollen diese in einem Netzverbund zusammengeführt werden, so muss der Administrator über den CLS die einzelnen Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen und diese in den zentralen CLA laden. An allen anderen Knoten muss die IP-Adresse des Master-Knotens mit dem zentralen Lizenzagenten über den Netzwerk-Wizard des WBM eingegeben werden.

8.4.1.1 Wie Sie Lizenzen offline aktivieren (Netzverbund)

Am Beispiel einer OpenScape Business S als Master-Knoten (Knoten 1) und zwei weiteren OpenScape Business X3 (Knoten 2 und Knoten 3) wird die Generierung und Aktivierung der gemeinsamen Netzwerklizenzdatei beschrieben.

Voraussetzungen

Es besteht ein Zugang zum CLS.

Alle Knoten sind installiert und miteinander vernetzt, siehe Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway).

Schritt für Schritt

1) Melden Sie sich am CLS mit Ihrem Benutzernamen und Passwort an.
2) Wählen Sie unter **Lizenzen** den Eintrag **Lizenzschlüssel generieren und herunterladen**.

3) Geben Sie unter **LAC** den Lizenz-Autorisierungscode (LAC) ein und klicken Sie auf **Suchen**.
4) Öffnen Sie das Produkt OpenScape Business S und wählen Sie die Leistungsmerkmale aus, die dem Knoten 1 zugeordnet werden sollen.
5) Klicken Sie auf **Lizenzschlüssel generieren**.
6) Geben Sie unter **MAC Adresse** die MAC-Adresse oder Advanced Locking ID von OpenScape Business S (Knoten 1) ein und unter **MAC-Adresse des Netzwerk-CLA** nochmal die MAC-Adresse oder Advanced Locking ID von OpenScape Business S (Master-Knoten) ein.

Anmerkung: Die MAC-Adresse von OpenScape Business S ist die MAC-Adresse der Netzwerkkarte des OpenScape Business S Linux-Servers, die bei der Installation des Linux-Betriebssystems verwendet wurde. Die Advanced Locking ID von OpenScape Business S wird anstelle der MAC-Adresse verwendet, wenn OpenScape Business S in einer virtuellen Umgebung betrieben wird.

---

7) Geben Sie bei den Leistungsmerkmalen die gewünschte Anzahl ein und klicken Sie auf **Weiter**.
8) Kontrollieren Sie die Kundendaten und klicken Sie auf **Weiter**.
9) Lesen Sie sich den rechtlichen Hinweis durch und klicken Sie anschließend auf **Ich stimme diesen Bedingungen zu**.
10) Klicken Sie auf **Ausführen**, um den Lizenzschlüssel generieren zu lassen.
11) Wählen Sie für den Knoten 2 unter **Lizenzen** den Eintrag **Lizenzschlüssel generieren und herunterladen**.
12) Geben Sie unter **LAC** erneut den Lizenz-Autorisierungscode (LAC) ein und klicken Sie auf **Suchen**.
13) Öffnen Sie das Produkt OpenScape Business X3 und wählen Sie die Leistungsmerkmale aus, die dem Knoten 2 zugeordnet werden sollen.
14) Klicken Sie auf **Lizenzschlüssel generieren**.
15) Geben Sie unter **MAC Adresse** die MAC-Adresse des Knoten 2 ein und unter **MAC-Adresse des Netzwerk-CLA** die MAC-Adresse des Knoten 1 (Master-Knoten) ein.
16) Geben Sie bei den Leistungsmerkmalen die gewünschte Anzahl ein und klicken Sie auf **Weiter**.
17) Klicken Sie auf **Weiter**.
18) Bestätigen Sie den rechtlichen Hinweis, indem Sie das Kontrollkästchen **Ich stimme diesen Bedingungen zu** anklicken.
19) Klicken Sie auf **Ausführen**, um den Lizenzschlüssel generieren zu lassen.
20) Wiederholen Sie die Schritte 11 bis 19 für den Knoten 3.
21) Klicken Sie auf **Lizenzschlüssel** und anschließend auf **Download**, um die Netzwerklizenzdatei herunterzuladen.
22) Speichern Sie die Netzwerklizenzdatei.
23) Melden Sie sich am WBM des Master-Knotens an, indem Sie in Ihrem Webbrowser die Adresse `https://<IP-Adresse des Master-Knotens>` aufrufen und anschließend Benutzernamen und Passwort eingeben.
24) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
25) Klicken Sie im Navigationsbaum auf **Lizenzdatei aktivieren**.

26) Klicken Sie unter **Lizenzdatei** auf **Durchsuchen** und wählen Sie den Ablageort der Netzwerklizenzdatei aus.
27) Klicken Sie auf **Aktivieren**.

8.4.1.2 Wie Sie Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen

Werden mehrere vorher nicht vernetzte Knoten in einen Netzverbund integriert, müssen die Lizenzdateien der einzelnen Knoten mit Hilfe des CLS zu einer gemeinsamen Netzwerklizenzdatei zusammengeführt werden.

Voraussetzungen

Es besteht ein Zugang zum CLS und Sie besitzen die Zugriffsrechte für die Lizenzpakete der einzelnen Knoten.

Alle Knoten sind installiert und miteinander vernetzt, siehe Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway).

Schritt für Schritt

1) Melden Sie sich am CLS mit Ihrem Benutzernamen und Passwort an.
2) Wählen Sie unter **Netzwerk Lizenzierung** den Eintrag **System hinzufügen/entfernen** aus.
3) Wählen Sie die MAC-Adresse des Knotens aus, der in den Netzverbund integriert werden soll.
4) Klicken Sie auf die **Rehost**.
5) Geben Sie unter **MAC-Adresse** die MAC-Adresse des Knotens ein.
6) Geben Sie unter **MAC-Adresse des Netzwerk-CLA** die MAC-Adresse des Master-Knotens ein. In der Regel ist OpenScape Business S der Master-Knoten.

   Anmerkung: Die MAC-Adresse von OpenScape Business S ist die MAC-Adresse der Netzwerkkarte des OpenScape Business S Linux-Servers, die bei der Installation des Linux-Betriebssystems verwendet wurde.

7) Klicken Sie auf **Weiter**.
8) Kontrollieren Sie die Kundendaten und klicken Sie auf **Weiter**.
9) Lesen Sie sich den rechtlichen Hinweis durch und klicken Sie anschließend auf **Ich stimme diesen Bedingungen zu**.
10) Klicken Sie auf **Ausführen**, um den Lizenzschlüssel generieren zu lassen.
11) Wiederholen Sie für weitere Knoten die Schritte 2 bis 10.
12) Klicken Sie auf **Lizenzschlüssel** und anschließend auf **Download**, um die Netzwerklizenzdatei herunterzuladen.
13) Speichern Sie die Netzwerklizenzdatei.
14) Melden Sie sich am WBM des Master-Knotens an, indem Sie in Ihrem Webbrowser die Adresse `https://<IP-Adresse des Master-Knotens>` aufrufen und anschließend Benutzernamen und Passwort eingeben.
15) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
16) Klicken Sie im Navigationsbaum auf **Lizenzdatei aktivieren**.

17) Klicken Sie unter **Lizenzdatei** auf **Durchsuchen** und wählen Sie den Ablageort der Netzwerklizenzdatei aus.
18) Klicken Sie auf **Aktivieren**.

8.4.2 Lizenzzuordnung (Netzverbund)

Nach erfolgreicher Aktivierung müssen die erworbenen Lizenzen den Teilnehmern und Leitungen zugeordnet werden. Diese Zuordnung wird an jedem Knoten separat durchgeführt.

Zuordnung von Benutzerlizenzen und User-orientierten Lizenzen

Den Teilnehmern können Benutzerlizenzen und User-orientierte Lizenzen zugeordnet werden.

Folgenden Anwender-Typen können Benutzerlizenzen zugeordnet werden:

Symbol	Benutzerlizenz	Beschreibung
	IP-Teilnehmer	Für die Nutzung von IP-Systemtelefonen (HFA oder SIP) und SIP-Telefonen
	TDM-Teilnehmer	Für die Nutzung von UP0-Systemtelefonen, ISDN-Telefonen, analogen Telefonen und DECT-Telefonen
	Mobile Teilnehmer	Für die Nutzung von myPortal to go, Mobility Entry und DISA (One Number Service)
	DeskSharing-Teilnehmer	Für die Nutzung von DeskSharing für IP-Teilnehmer
	Fallback User	Für die grundlegende Telefonie im Falle eines Fehlerereignisses.

Die Benutzerlizenzen werden den Rufnummern der Teilnehmer fest zugeordnet. Wird ein Teilnehmer gelöscht oder einer Rufnummer ein anderer Teilnehmer-Typ zugeordnet, wird die zugehörige Benutzerlizenz freigegeben.

Mit der flexiblen Lizenzierung können TDM-, Mobility- und DeskShare-Teilnehmer auch mit IP-Benutzerlizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility-Benutzerlizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility-Teilnehmer, können übrige IP-Benutzerlizenzen verwendet werden, um diesen Bedarf zu decken.

Nachdem dem Teilnehmer eine Benutzerlizenz zugeordnet wurde, können diesem Teilnehmer auch User-orientierte Lizenzen zugeordnet werden.

Folgende User-orientierte Lizenzen können den Teilnehmern zugeordnet werden:

Symbol	User-orientierte Lizenz	Beschreibung
	Voicemail	Für die Nutzung der Sprachbox.

Symbol	User-orientierte Lizenz	Beschreibung
	Groupware User	Für die Nutzung der UC Suite-Funktionen über myPortal for Outlook.
	UC Suite	Für die Nutzung der UC Suite-Funktionen über myPortal for Desktop.
	Fax	Für die Nutzung einer Faxbox innerhalb der UC Suite. Voraussetzung ist eine UC User- oder eine Groupware User-Lizenz.
	Konferenz	Für die Nutzung der Konferenz-Funktionen der UC Suite. Voraussetzung ist eine UC User- oder eine Groupware User-Lizenz.
	myAttendant	Für die Nutzung der UC Suite-Vermittlungsfunktionen.
	myAgent	Für die Nutzung der Contact Center-Funktionen.
	Application Launcher	Für die anrufbezogene Steuerung von Applikationen auf einem Client-PC bei ankommenden und gehenden Anrufen, z. B. Aufruf einer Applikation oder Anzeige von Anruferdaten.
	Unify Phone	Für die Nutzung des Unify Phone-Clients in Kombination mit OpenScape Business.
	TAPI 120/170	Für die Nutzung von TAPI-konformen Applikationen und zum PC-unterstützten Telefonieren mit kundeneigenen Programmen verschiedener Software-Hersteller.

Sie können sich eine Übersicht über alle Benutzerlizenzen und User-orientierte Lizenzen anzeigen lassen (über **Lokale Benutzerlizenzen** > **Übersicht)**.

In dieser Übersicht werden Ihnen auch zu jedem Teilnehmer die Zustände seiner Lizenzen angezeigt.

Es gibt folgende Lizenzzustände:

Zuordnung von System-Lizenzen

System-Lizenzen enthalten Lizenzen für Leitungen und systemweite Leistungsmerkmale.

Folgenden Typen von Leitungen können Lizenzen zugeordnet werden:

- S_{2M}-/T1-Leitungen: Anzahl der B-Channels
- ITSP-Leitungen: Anzahl der gleichzeitig über einen ITSP geführten Rufe

Systemweite Lizenzen werden im Netzverbund jedem System (Knoten) zugeordnet. Diese Konfiguration ist direkt nacheinander an jedem Knoten

durchzuführen. Die Gesamtzahl der systemweiten Lizenzen, die in der Netzwerklizenzdatei auf dem Master-Knoten gespeichert sind, wird um die an dem Knoten konfigurierte Anzahl reduziert.

Vorgehensweise bei der Lizenzzuordnung

Voraussetzung: Die Lizenzdatei ist aktiviert und die Teilnehmer sind eingerichtet.

- Teilnehmer lizenzieren

  1) Teilnehmer eine User-Lizenz zuordnen. Durch diese Zuordnung wird für den Teilnehmer eine Lizenzanforderung generiert und zugleich die Zuordnung der User-orientierten Lizenzen freigeschaltet.
  2) Teilnehmer die User-orientierten Lizenzen zuordnen. Durch diese Zuordnungen werden für den Teilnehmer weitere Lizenzanforderungen generiert. Bitte beachten Sie, dass einige Lizenzen andere Lizenzen voraussetzen (siehe Vorschläge für Lizenzkombinationen).
  3) Lizenzanforderungen prüfen und freischalten.
  4) Liegen nicht genügend Lizenzen für die Freischaltung vor, werden Ihnen die fehlerhaften Zuordnungen über die Lizenzzustände (rot) angezeigt. Die Lizenzzuordnungen korrigieren und die Lizenzen erneut prüfen und freischalten.

  Anmerkung: Zur besseren Übersicht können Sie sich die Lizenzzuordnungen für alle Teilnehmer als Vorab-Ausdruck anzeigen lassen (über **Lokale Benutzerlizenzen** > **Übersicht** > **Drucken**). Am Ende des Ausdrucks werden alle ungültigen Zuordnungen in einer separaten Tabelle aufgeführt.

- Leitungslizenzen zuordnen

  Die Leitungslizenzen müssen auf die benötigten S_{2M}-/T1- und ITSP-Leitungen aufgeteilt werden.

8.4.2.1 Wie Sie Teilnehmer lizenzieren (Netzverbund)

Verteilen Sie die verfügbaren Teilnehmer-Lizenzen und User-orientierten Lizenzen auf die Teilnehmer. Nach erfolgreicher Zuordnung sind die Teilnehmer lizenziert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Navigieren Sie im Navigationsbaum unter **Lokale Benutzerlizenzen** > **...** zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.

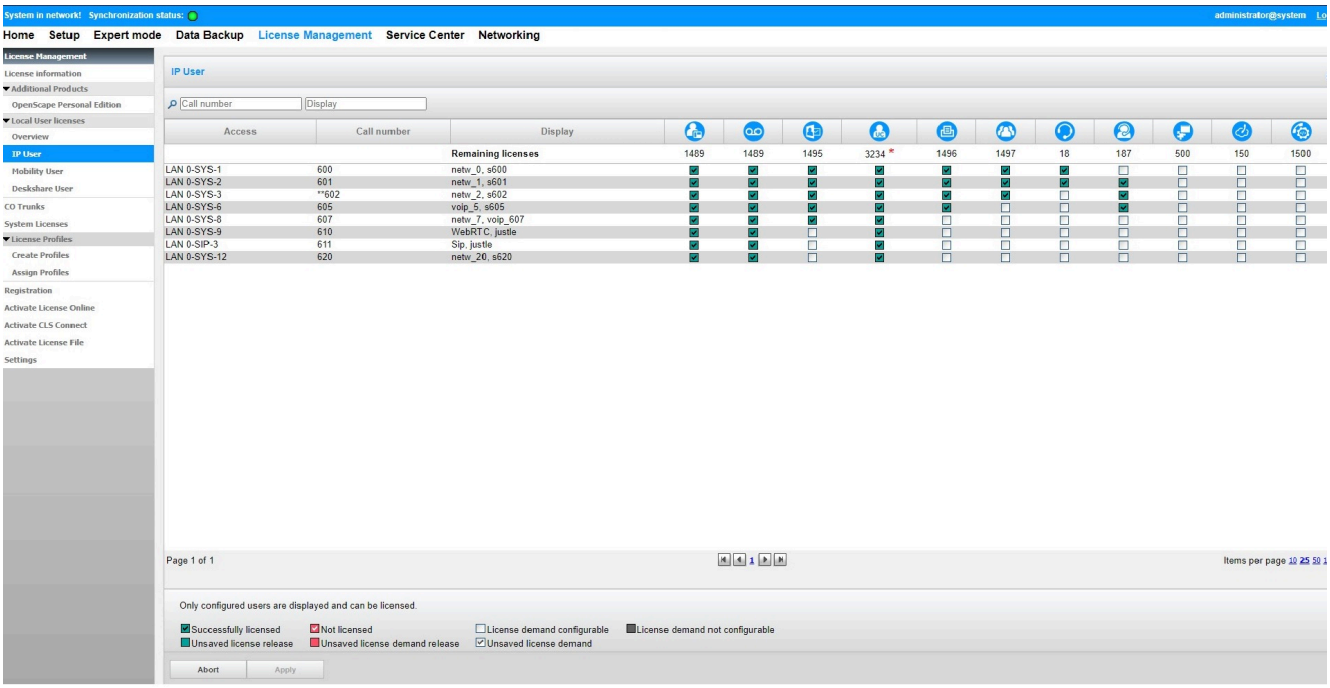
   Unter **Verbleibende Lizenzen** wird Ihnen angezeigt, wie viele Lizenzen Sie noch den Teilnehmern zuordnen können. Bei den TDM-, Mobility- und DeskShare-Teilnehmern beinhaltet die Anzeige auch alle noch übrigen IP User Lizenzen, da diese Lizenzen auch für die Lizenzierung von TDM-,

Mobility- und DeskShare-Teilnehmern verwendet werden dürfen (flexible Teilnehmer-Lizenzierung).

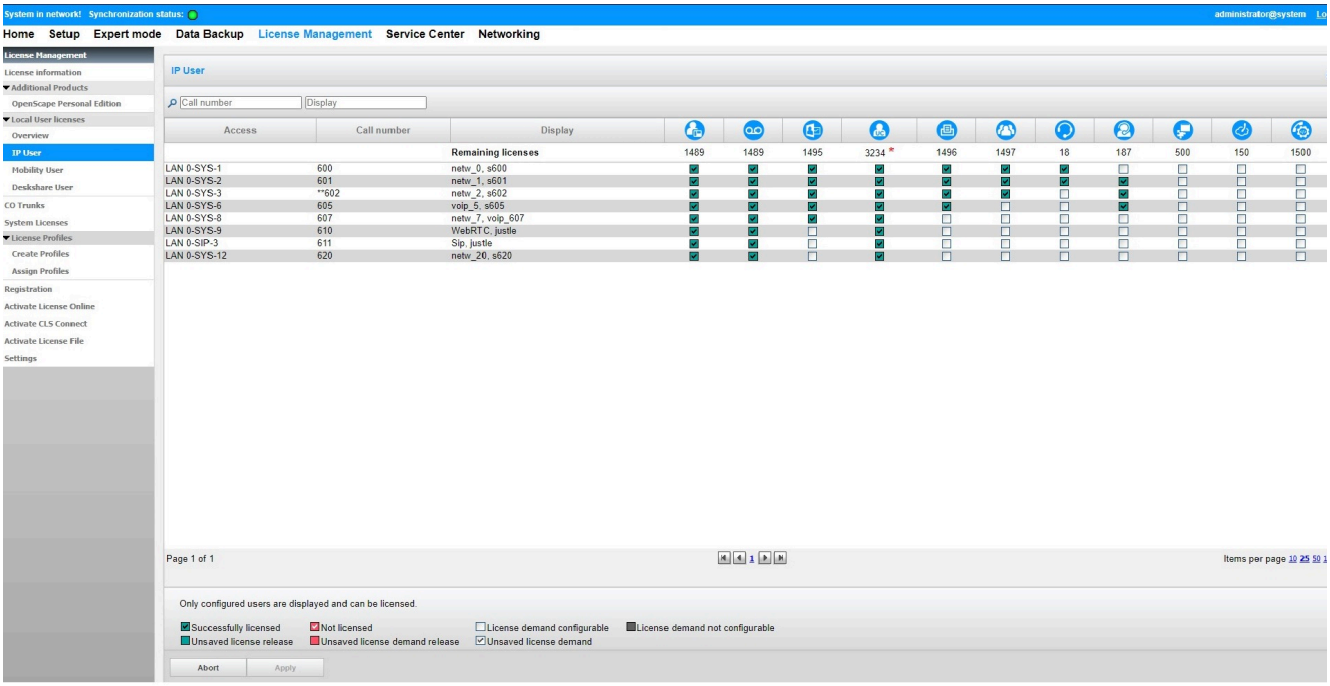
Wenn der ausgewählte Teilnehmertyp der eines Mobility-Teilnehmers ist, sehen Sie auch die Gesamtzahl der verfügbaren Unify Phone-Lizenzen und deren Ablaufdatum.

3) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die Teilnehmer-Lizenz, indem Sie das hell hinterlegte Kontrollkästchen (erste Spalte mit Kontrollkästchen) aktivieren. Die Kontrollkästchen in den anderen Spalten werden aktiviert.

Anmerkung: Sie können sich auch einen ausgewählten Teilnehmer anzeigen lassen, indem Sie in die Suchfelder **Rufnummer** oder **Name** einen Suchbegriff eingeben und anschließend die Eingabetaste drücken oder auf das Lupen-Symbol klicken. Alle Teilnehmer werden aufgelistet, wenn beide Suchfelder leer sind und Sie anschließend die Eingabetaste drücken oder auf das Lupen-Symbol klicken.



4) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.



Anmerkung: Benutzerbezogene Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz zugeordnet wurde (Schritt 3).

Anmerkung: „Pay As You Go“ ist nicht verfügbar, wenn es sich um eine Netzwerklizenzdatei handelt.

Im Falle eines Netzwerks von OpenScape Business-Systemen kann jedes der Systeme Pay As You Go über den lokalen zentralen Lizenzagenten (CLA) nutzen.

---

5) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.

   Sind ausreichend Lizenzen vorhanden, ist die Lizenzierung des Teilnehmers hiermit beendet.

6) Fehlen Lizenzen, werden Ihnen die Fehler mit rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt 5.

Anmerkung: Wenn Sie eine Teilnehmer-Lizenz entfernen wollen, müssen Sie eine Warnmeldung bestätigen. Anschließend erscheint ein neues Kontrollkästchen **Warnungen aktiviert**. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie weitere Teilnehmer-Lizenzen ohne Warnmeldung entfernen.

8.4.2.2 Wie Sie Leitungen lizenzieren (Netzverbund)

Verteilen Sie die erworbenen Leitungslizenzen auf die SIP- und S_{2M}-/T1-Leitungen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich $_{\text{Amtsleitungen}}$ wird Ihnen die Anzahl der verfügbaren Lizenzen für SIP- und S**2M**-/T1-Amtsleitungen angezeigt.
3) Für SIP-Leitungen: Geben Sie im Bereich **SIP trunks** unter **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.
4) Für S_{2M}-Leitungen: Wählen Sie im Bereich **S2M** in der Zeile des gewünschten Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.
5) Für T1-Leitungen (nur USA): Wählen Sie im Bereich **T1** in der Zeile des gewünschten Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.
6) Klicken Sie auf **OK & Weiter**.

Anmerkung: Die Anzahl der lizenzierten SIP-Leitungen und die Anzahl der lizenzierten S_{2M}-/T1-Leitungen darf die Anzahl der verfügbaren Leitungslizenzen nicht überschreiten.

8.4.2.3 Wie Sie Systemlizenzen einem Knoten zuordnen

Voraussetzungen

Sie sind am WBM des gewünschten Knotens angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **System-Lizenzen**. Es werden Ihnen alle verfügbaren Systemlizenzen angezeigt.
3) Wählen Sie in der Spalte **benutzte Lizenzen** bei den gewünschten Systemlizenzen die Anzahl der Systemlizenzen aus, die dem Knoten zugeordnet werden sollen.

   In der Spalte **verfügbar für Verteilung** wird Ihnen angezeigt, wie viele Lizenzen für den gesamten Netzverbund zur Verfügung stehen.

Anmerkung: Achten Sie darauf, dass dem Knoten die Systemlizenz "Networking" zugeordnet ist, ansonsten ist der Konten nicht in den Netzverbund integriert.

---

4) Klicken Sie auf **Speichern**.

8.4.2.4 Wie Sie die Systemlizenz "Networking" einem Knoten zuordnen

Voraussetzungen

Sie sind am WBM des gewünschten Knotens angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **System-Lizenzen**. Es werden Ihnen alle verfügbaren Systemlizenzen angezeigt.

3) Wählen Sie bei der Systemlizenz **Networking** in der Spalte **benutzte Lizenzen** aus der Aufklappliste den Eintrag **1** aus.

In der Spalte **verfügbar für Verteilung** wird Ihnen angezeigt, wie viele Lizenzen für den gesamten Netzverbund zur Verfügung stehen.

4) Klicken Sie auf **Speichern**.

8.5 Lizenzinformationen

Informationen zu den zur Verfügung stehenden und zugewiesenen Lizenzen, Produkten und Leistungsmerkmalen werden mit dem WBM angezeigt. Im Netzverbund können die Lizenzinformationen zu allen im Netz vorhandenen Knoten abgerufen werden.

Folgende Informationen können angezeigt werden:

- **MAC-Adresse**: MAC-Adresse der Hardware-Plattform oder des Softswitch Linux Servers, an die die Lizenzen gebunden sind.

  Anmerkung: Befindet sich das Kommunikationssystem in der Activation Period, wird hier evtl. eine falsche MAC-Adresse angezeigt. Die richtige MAC-Adresse kann über das **Service-Center** unter **Inventory**Inventar auf Seite 1284 abgefragt werden.

- **Advanced Locking ID**: Advanced Locking ID des Softswitches in einer virtuellen Umgebung, an die die Lizenzen gebunden sind.
- **Locking ID**: Locking ID des Application Servers, an die die Lizenzen gebunden sind.
- **Knoten**: Name des Kommunikationssystems, an die die Lizenzen gebunden sind.
- **Produktname**: Name des Produkts, das der Lizenz zugeordnet ist.
- **Leistungsmerkmal**: Leistungsmerkmal, das der Lizenz zugeordnet ist.
- **Benutzte Lizenzen**: Anzeige der benutzten und der vorhandenen Lizenzen.
- **verteilbare Lizenzen**: Anzeige der im Netzverbund noch verfügbaren Lizenzen.
- **Status**: Status der Lizenz.

Das Produkt OpenScape Personal Edition ist über eine eigene Lizenzdatei lizenziert. Die Lizenzinformationen dazu werden unter **Zusätzliche Produkte** angezeigt.

8.5.1 Lizenzinformationen ohne Netzverbund (Standalone)

Es können alle dem Kommunikationssystem zugeordneten Lizenzen und die Informationen dazu angezeigt werden.

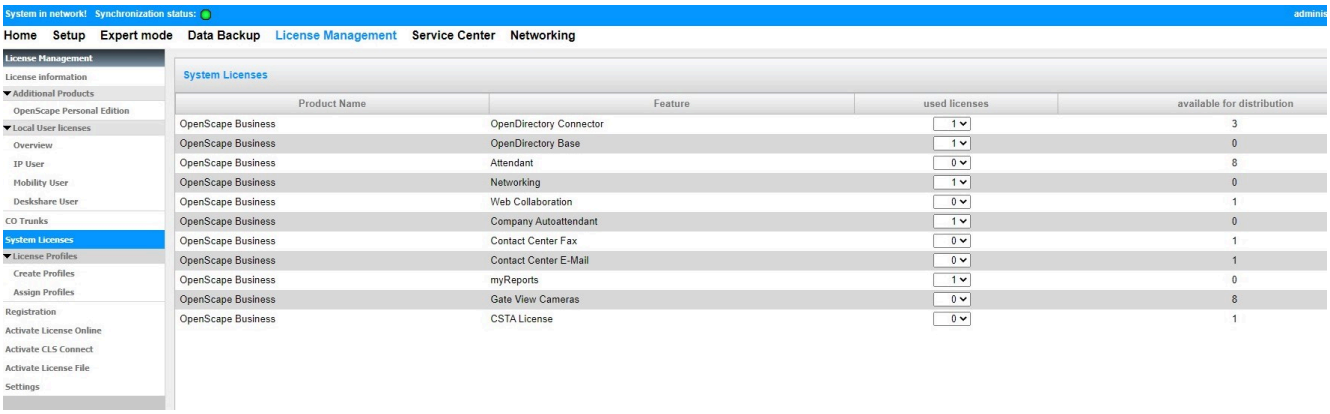
8.5.1.1 Wie Sie Lizenzinformationen anzeigen

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**. Es werden Ihnen die Lizenzinformationen zu Ihrem Kommunikationssystem angezeigt.



Anmerkung: Im Falle von „Pay As You Go“ sind die verwendeten Lizenzen konfigurierbar, mit Ausnahme von Contact Center Fax, Contact Center E-Mail und myReports im UC Smart-Modus.

8.5.2 Lizenzinformationen im Netzverbund

In einem Netzverbund können alle Lizenzen und die Informationen dazu angezeigt werden. Diese Informationen werden aus der Netzwerklizenzdatei ausgelesen.

Die Lizenzen in einem Netzverbund sind bis auf die Basis-Lizenzen vom Typ "floating" und befinden sich in einem Lizenz-Pool. Wird eine Lizenz an einem Knoten (Kommunikationssystem) nicht mehr benötigt und freigegeben, kann sie an einem anderen Knoten genutzt werden.

In einem Netzverbund können sowohl alle Lizenzen des Netzverbundes als auch die gemeinsam genutzten Lizenzen (floating) oder die speziell an einen Knoten gebundenen Lizenzen angezeigt werden.

Zusätzlich können die Teilnehmer-Lizenzen und die User-orientierten Lizenzen nach Knoten sortiert in einer Übersicht angezeigt werden.

8.5.2.1 Wie Sie alle Lizenzen des Netzverbundes anzeigen

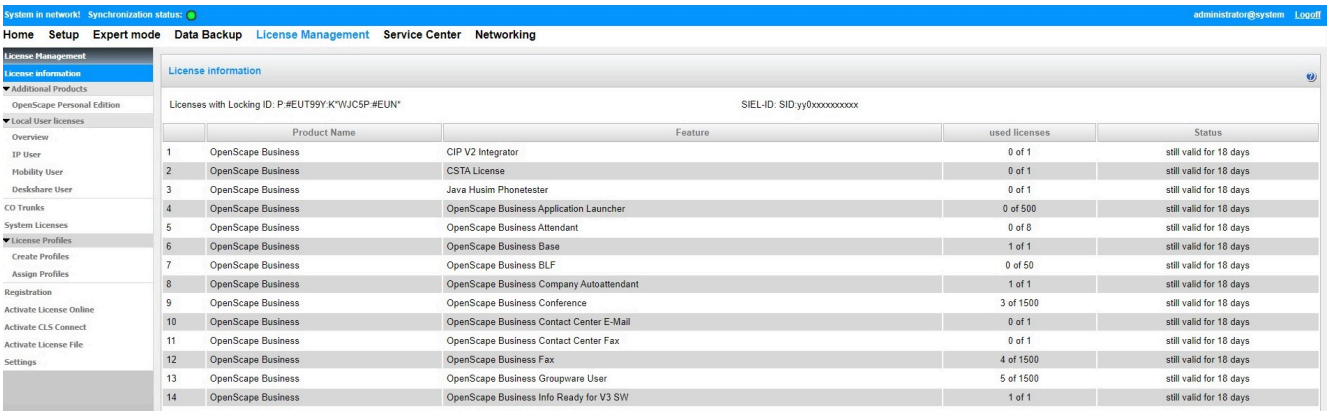
Voraussetzungen

Das Kommunikationssystem befindet sich in einem Netzverbund.

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Lizenzinformationen**. Es werden Ihnen alle Lizenzen im Netzverbund angezeigt.



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.2 Wie Sie die an einen Knoten gebundenen Lizenzen anzeigen

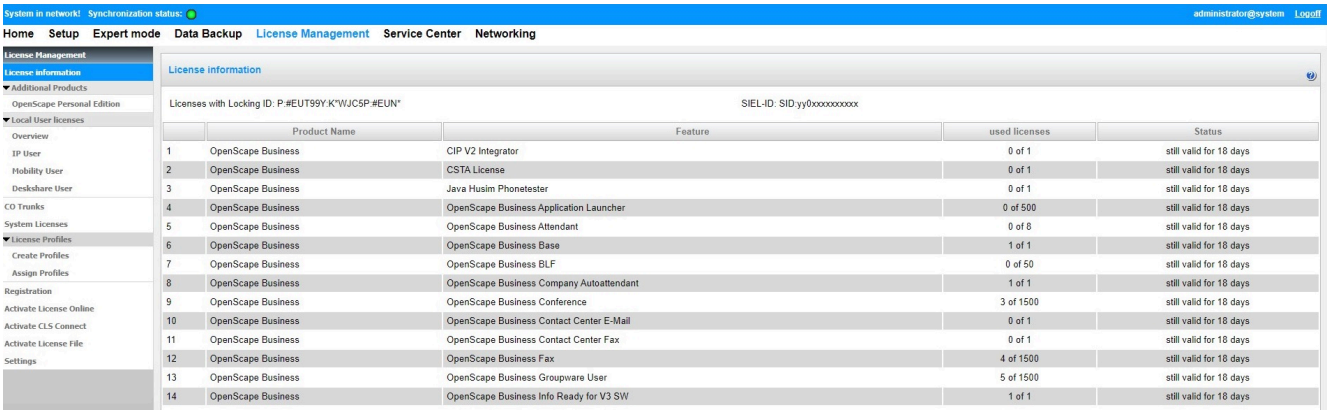
Voraussetzungen

Das Kommunikationssystem befindet sich in einem Netzverbund.

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Lizenzinformationen**.
3) Klicken Sie im Navigationsbaum auf den Systemnamen oder die Locking ID des gewünschten Knotens. Es werden Ihnen die speziell an diesen Knoten gebundenen Lizenzen angezeigt, wie z.B. die Basislizenz.



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.3 Wie Sie alle im Netzverbund gemeinsam genutzten Lizenzen anzeigen

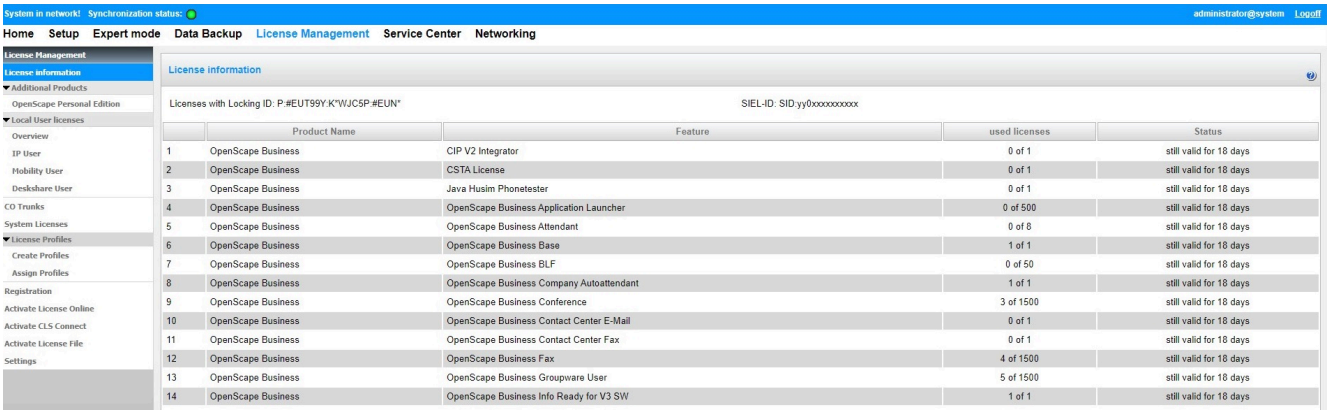
Voraussetzungen

Das Kommunikationssystem befindet sich in einem Netzverbund.

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Lizenzinformationen**.
3) Klicken Sie im Navigationsbaum auf **Unverankert**. Es werden Ihnen alle gemeinsam genutzten Lizenzen im Netzverbund angezeigt.



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.4 Wie Sie Teilnehmer- und User-orientierte Lizenzen knotenabhängig anzeigen

Voraussetzungen

Das Kommunikationssystem befindet sich in einem Netzverbund.

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Netzweite Lizenzübersicht**. Es werden Ihnen alle Teilnehmer-Lizenzen und User-orientierten Lizenzen im Netzverbund nach Knoten sortiert angezeigt.

8.6 Lizenzprofilzuordnung

Lizenzprofile enthalten vordefinierte Lizenzzuordnungen und können einem oder mehreren Teilnehmern zugewiesen werden. Lizenzprofile sind nützlich, wenn mehrere Teilnehmer dieselben Lizenzen bekommen sollen.

Es können vordefinierte Lizenzprofile verwendet oder neue Lizenzprofile erstellt werden.

Ein Lizenzprofil gilt immer für einen Teilnehmer-Typ und kann nur Teilnehmern dieses Typs zugeordnet werden. Es können mehrere Lizenzprofile für einen Teilnehmer-Typ angelegt und benannt werden.

Für folgende Teilnehmer-Typen können Lizenzprofile erstellt werden:

- IP-Teilnehmer (IP-Systemtelefone, SIP-Telefone)
- TDM-Teilnehmer (UP0-Telefone, ISDN-Telefone, analoge Telefone, DECT-Telefone)
- DeskSharing-Teilnehmer
- Mobile Teilnehmer

Innerhalb eines Lizenzprofils können Sie dem Teilnehmer-Typ nach Ihren Wünschen User-orientierte Lizenzen zuordnen.

Wird die Lizenzzuordnung eines Teilnehmers eines Lizenzprofils separat geändert, wird die Zuordnung des Teilnehmers zum Lizenzprofil automatisch aufgehoben.

8.6.1 Wie Sie ein Lizenzprofil hinzufügen

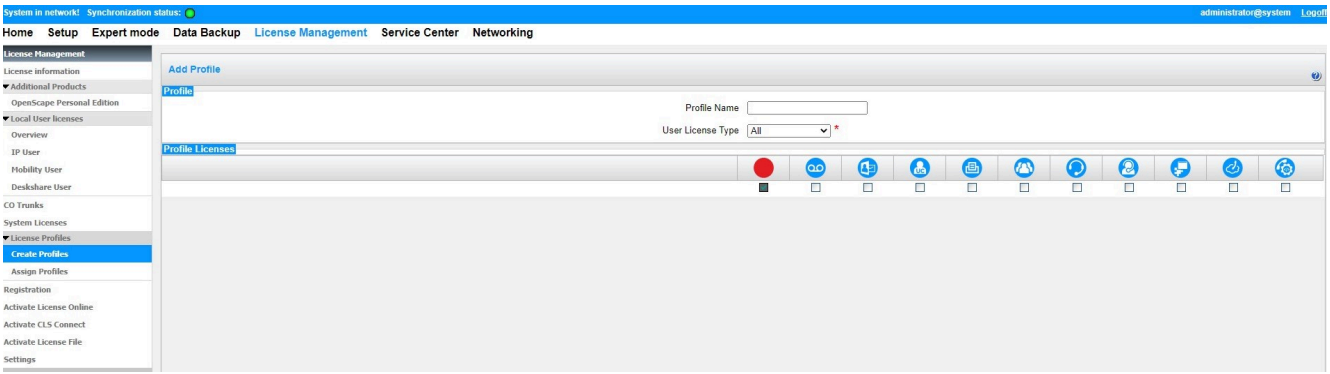
Erstellen Sie ein neues Lizenzprofil.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Lizenzprofile** > **Profile erstellen**. Es werden Ihnen alle vorhandenen Lizenzprofile angezeigt.
3) Klicken Sie auf **Hinzufügen**.



4) Geben Sie im Feld **Profilname** einen Namen Ihrer Wahl für das neue Profil ein.
5) Wählen Sie aus der Aufklappliste **Lizenztyp Benutzer** den Teilnehmer-Typ aus, für den das Profil gelten soll.
6) Wählen Sie die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.
7) Klicken Sie auf **OK & Weiter**. Ihre Zuordnung wird auf Richtigkeit geprüft.

   Bei fehlerfreier Zuordnung ist die Lizenzierung der Teilnehmer beendet.
8) Bei fehlerhafter Zuordnung werden Ihnen die Fehler mit einem rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt 7.

8.6.2 Wie Sie ein Lizenzprofil bearbeiten

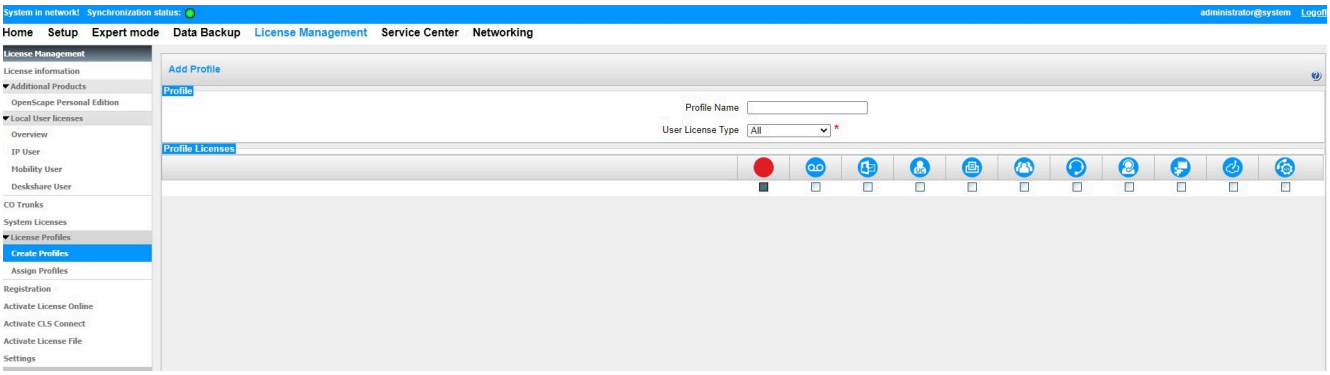
Bearbeiten Sie ein bestehendes Lizenzprofil.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Lizenzprofile** > **Profile erstellen**. Es werden Ihnen alle vorhandenen Lizenzprofile angezeigt.



3) Aktivieren Sie das Optionsfeld vor dem gewünschten Lizenzprofil und klicken Sie auf **Bearbeiten**.
4) Ändern Sie das Lizenzprofil wie gewünscht.
5) Klicken Sie auf **OK & Weiter**. Ihre Zuordnung wird auf Richtigkeit geprüft.

   Bei fehlerfreier Zuordnung ist die Bearbeitung des Lizenzprofils beendet.
6) Bei fehlerhafter Zuordnung werden Ihnen die Fehler mit einem rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt 5.

8.6.3 Wie Sie Teilnehmern ein Lizenzprofil zuordnen

Ordnen Sie ein Lizenzprofil den verfügbaren Teilnehmern zu.

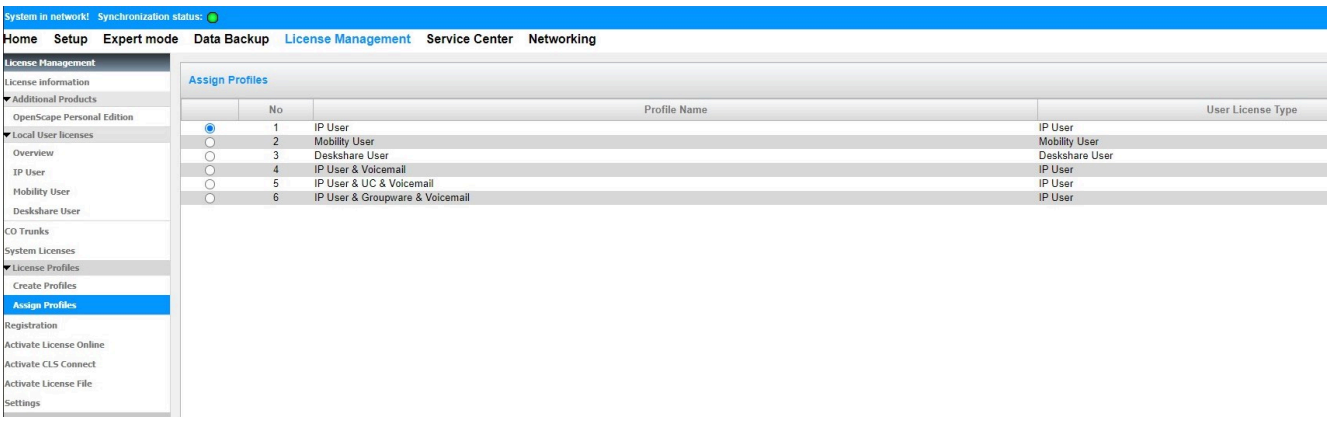
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzprofile** > **Profile zuweisen**. Es werden Ihnen alle vorhandenen Lizenzprofile angezeigt.



3) Aktivieren Sie das Optionsfeld vor dem gewünschten Lizenzprofil und klicken Sie auf **OK & Weiter**.
4) Markieren Sie im linken Feld **Auswahl** alle Teilnehmer, denen das Lizenzprofil zugewiesen werden soll.
5) Klicken Sie auf **Hinzufügen**. Die ausgewählten Teilnehmer erscheinen im rechten Fenster **Mitglieder**.
6) Klicken Sie auf **OK & Weiter**. Die im Lizenzprofil ausgewählten Lizenzen werden den Teilnehmern zugeordnet.

Anmerkung: Bei "Pay As You Go" erscheint ein Popup-Fenster. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.

Anmerkung: Teilnehmer können auch nachträglich aus einem Lizenzprofil entfernt oder neue Teilnehmer hinzugefügt werden.

8.6.4 Wie Sie ein Lizenzprofil löschen

Löschen Sie ein bestehendes Lizenzprofil.

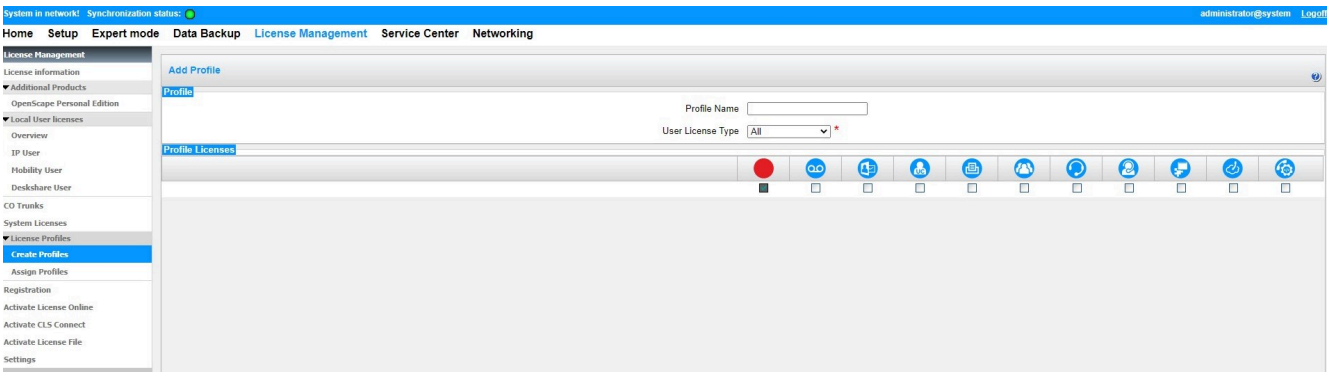
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzprofile** > **Profile erstellen**. Es werden Ihnen alle vorhandenen Lizenzprofile angezeigt.



3) Aktivieren Sie das Optionsfeld vor dem gewünschten Lizenzprofil und klicken Sie auf **Löschen**.

4) Bestätigen Sie die Meldung mit **OK**. Das Lizenzprofil ist gelöscht.

8.7 Rehost nach Hardwaretausch

Lizenzen müssen aktualisiert werden, wenn das Mainboard der Hardwareplattform oder die Netzwerkkarte des Linux-Servers im Kommunikationssystem ausgestauscht wird. Für den Rehost werden die MAC-Adresse der alten Hardware, die MAC-Adresse der neuen Hardware und die Anmeldedaten für den zentralen Lizenzserver (CLS) benötigt.

Nach Austausch der Hardware müssen die Konfigurationsdaten mit Hilfe des aktuellen Backup-Sets wiederhergestellt werden (siehe Wiederherstellen).

Da die Lizenzen an die MAC-Adresse der Hardware gebunden sind, ändert sich nach Austausch der Hardware die MAC-Adresse und somit sind die Lizenzen nicht mehr gültig. Nach Hardwaretausch befindet sich das Kommunikationssystem wieder in der Activation Period. Nachdem alte und neue MAC-Adresse am CLS eingetragen wurden, kann die neue Lizenzdatei generiert werden. Diese wird per Offline-Aktualisierung in das Kommunikationssystem geladen und anschließend werden alle vorhandenen Lizenzen automatisch aktiviert.

Für den Soft Switch wird die MAC-Adresse der Netzwerkkarte des Linux-Servers verwendet, die bei der Installation des Linux-Betriebssystems ausgewählt wurde (sichtbar über YaST). Die MAC-Adresse kann auch mit Hilfe des WBMs ausgelesen werden.

Anmerkung: Jeder Rehost wird im CLS protokolliert. Eine Lizenz kann maximal dreimal für einen Rehost verwendet werden.

Anmerkung: Die IP-Adresse des CLS kann über das WBM unter **Lizenzverwaltung** > **Einstellungen** abgefragt und falls nötig geändert werden.

8.7.1 Wie Sie einen Rehost nach einem Hardwaretausch ausführen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Hardware ist getauscht worden und Sie haben am CLS einen Rehost durchgeführt.

Die Konfigurationsdaten wurde mit Hilfe des aktuellen Backup-Sets wiederhergestellt.

Sie kennen den Lizenz-Autorisierungscode (LAC) für die Lizenzfreischaltung.

Für die Verbindung zum Lizenzserver muss das Kommunikationssystem eine Verbindung zum Internet haben.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Lizenz Online aktivieren**.
3) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.
4) Lassen Sie das Kontrollkästchen für den Zugang zum Lizenzserver über Benutzername und Kennwort deaktiviert. Der Zugang zum Lizenzserver erfolgt automatisch. (Die Eingabe von Benutzername und Kennwort ist nur für Vertriebspartner nötig.)
5) Klicken Sie auf **Aktivieren**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen aktualisiert. Nach erfolgreicher Aktualisierung wird die Verbindung automatisch wieder abgebaut.
6) Starten Sie das Kommunikationssystem neu.

Nächste Schritte

Speichern Sie Ihre Konfigurationsdaten in einem neuen Backup-Set (siehe Sofortiges Sichern).

8.8 Lizenzserver (Central License Server, CLS)

Der Lizenzserver (CLS) erzeugt und verwaltet die Lizenzdateien.

Eine Lizenzdatei wird generiert, wenn der Kunde über das WBM den Lizenz-Autorisierungscode an den CLS sendet. Die Übertragung der Lizenzdatei an das Kommunikationssystem erfolgt automatisch über das Internet. Ist eine automatische Übertragung nicht möglich, kann die Lizenzdatei auch manuell in das Kommunikationssystem geladen werden.

8.8.1 Wie Sie die IP-Adresse des Lizenzservers abfragen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Hat sich die IP-Adresse des zentralen Lizenzservers geändert, müssen Sie die aktuelle IP-Adresse wissen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Einstellungen**. Es wird Ihnen im Feld **IP-Adresse des zentralen Lizenzservers** die IP-Adresse des zentralen Lizenzservers (CLS) angezeigt. Die aktuell gültige IP-Adresse lautet `188.64.16.4`.
3) Wenn Sie die IP-Adresse des zentralen Lizenzservers ändern müssen, geben Sie im Feld **IP-Adresse des zentralen Lizenzservers** die neue IP-Adresse des zentralen Lizenzservers in der Form `123.124.125.126` ein.
4) Klicken Sie auf **Aktivieren**.

8.8.2 So überprüfen Sie die Verbindung zum Central License Server (CLS)

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Einstellungen**.
3) Klicken Sie im Bereich **Central License Server** auf **CLS-Verbindung testen**.

Wenn eine aktive Internetverbindung besteht, erscheint die Meldung **Erfolgreich mit CLS verbunden**.

Wenn keine Internetverbindung besteht, erscheint die Meldung **Keine Verbindung zu CLS!**

8.9 Lizenzagent (Customer License Agent, CLA)

Der Lizenzagent (CLA) ist Teil der OpenScape Business Kommunikationssoftware und läuft automatisch im Hintergrund. Er verwaltet die Lizenzdatei und die darin enthaltenen Lizenzen. Der CLA prüft die Lizenzanforderungen und schaltet bei genügend vorhandenen Lizenzen die Lizenzen frei. Pro Kommunikationssystem gibt es nur einen CLA (lokaler CLA). Sind mehrere Kommunikationssysteme (Knoten) in einem Netzverbund, sollte nur ein CLA (zentraler CLA) auf dem Master-Knoten verwendet werden.

Folgende Konfigurationen sind möglich:

- **Wie Sie eine Verbindung zum lokalen Lizenzagenten konfigurieren**

  Wird ein Knoten aus dem Netzverbund genommen, wird die Verbindung zum zentralen CLA aufgehoben. Es wird automatisch der auf dem Knoten installierte lokale CLA genutzt. Funktioniert dieser Automatismus nicht, kann die Verbindung zum lokalen CLa manuell hergestellt werden.
- **Wie Sie die Verbindung zum zentralen Lizenzagenten ändern**

  Jeder Knoten im Netzverbund benötigt die Verbindung zum zentralen CLA auf dem Master-Knoten. Diese Verbindung wird beim Durchlaufen des WBM-Wizards **Vernetzung** automatisch hergestellt. Ändert sich die IP-Adresse des Master-Knotens, ist an allen Slave-Knoten die Verbindung zum zentralen CLA neu zu konfigurieren.

8.9.1 Wie Sie eine Verbindung zum lokalen Lizenzagenten konfigurieren

Voraussetzungen

Sie sind am WBM des gewünschten Knotens angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Einstellungen**.
3) Aktivieren Sie das Optionsfeld **Lokaler Lizenzagent (CLA)**.
4) Klicken Sie auf **Aktivieren**.

8.9.2 Wie Sie die Verbindung zum zentralen Lizenzagenten ändern

Voraussetzungen

Das Kommunikationssystem befindet sich in einem Netzverbund.

Sie sind am WBM des gewünschten Knotens angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Einstellungen**.
3) Aktivieren Sie das Optionsfeld **Zentraler Lizenzagent** und geben Sie unter **IP-Adresse des zentralen Lizenzagenten** die IP-Adresse des Master-Knotens (Knoten 1) in der Form `123.124.125.126` ein.
4) Klicken Sie auf **Aktivieren**.

8.10 Locking ID und Advanced Locking ID

Jedem Kommunikationssystem ist eine Locking ID oder eine Advanced Locking ID zugeordnet. Um eine eindeutige Lizenzierung zu gewährleisten, werden die Lizenzen an diese Locking IDs gebunden.

Locking-ID

Bei Hardware-Plattformen ist die Locking ID die MAC-Adresse des Kommunikationssystems.

Bei einem Soft Switch ist die Locking ID die MAC-Adresse der Netzwerkkarte des Linux-Servers. Enthält der Linux-Server mehrere Netzwerkkarten, ist die Netzwerkkarte auszuwählen, die bei der Erstinbetriebnahme des Linux-Servers verwendet wurde.

Befindet sich das Kommunikationssystem in der Activation Period, wird unter den Lizenzinformationen evtl. eine falsche MAC-Adresse angezeigt. Die richtige MAC-Adresse kann über das **Service-Center** unter **Inventory** abgefragt werden.

Advanced Locking ID

Läuft ein Soft Switch in einer virtuellen Umgebung, wird anstelle der Locking ID die Advanced Locking ID (ALI) verwendet. Die Advanced Locking ID wird am CLS mittels ALI-Calculator generiert.

Folgende System- und Netzwerkparameter müssen konfiguriert sein, da sie für die Generierung der 24-stelligen Advanced Locking ID verwendet werden.

- IP-Adresse des Default-Gateways (Linux-Server)
- Hostname des Linux-Servers
- IP-Adresse des Linux-Servers
- IP-Adresse des DNS-Servers (konfiguriert im Linux-Server)
- Zeitzone (Linux-Server)

Sind einer oder mehrere dieser System- und Netzwerkparameter nicht eingerichtet, so kann die Advanced Locking ID nicht generiert werden.

Die Advanced Locking ID wird im WBM angezeigt. In einigen Fällen ist es möglich, dass die ALI, die am CLS für die Lizenzdatei generiert wurde, abweicht von der ALI, die während der Activation Period im WBM angezeigt wird. Die Lizenzdatei mit der abweichenden ALI wird vom System trotzdem akzeptiert.

Ändert sich einer der oben aufgeführten System- und Netzwerkparameter, fällt der Soft Switch in den nicht lizenzierten Zustand zurück und eine neue Advanced Locking ID wird generiert. Um die gekaufte Lizenzdatei wieder nutzen zu können, muss am Zentralen Lizenzserver (CLS) ein Rehost von der alten auf die neue Advanced Locking ID durchgeführt werden.

Wenn das System eine Änderung in ALI feststellt, wird auf der WBM-Startseite im Lizenzbereich eine Meldung angezeigt, die den Benutzer darüber informiert, dass ALI geändert wurde. Der Benutzer muss auf „Bestätigen“ klicken, um zu bestätigen, dass er über die Änderung informiert wurde. Dann wird die Nachricht von der WBM-Startseite entfernt, bis eine neue Instanz einer ALI-Änderung erkannt wird. Wenn der Benutzer nicht auf „Bestätigen“ klickt, wird die Nachricht dauerhaft auf der Startseite angezeigt.

Wichtig: Wenn Änderungen an den Parametern der Locking-ID vorgenommen werden (IP-Adresse, Gateway-Adresse, DNS-Adresse, Hostname für S-Systeme, MAC-Adresse für X-Systeme), wird die Systemlizenz ungültig. Sie sollten sich an einen autorisierten Partner am Cental License Server wenden, um eine neue Lizenzdatei zu erstellen, und die neue Lizenzdatei muss im System installiert sein.

Wichtig: Wenn ein Benutzer auf die Bestätigungsschaltfläche klickt, wird anschließend keine E-Mail gesendet. Eine E-Mail wird nur gesendet, wenn der Benutzer die Änderungen nicht über die Startseite bestätigt hat. Der E-Mail-Mechanismus wird jeden Tag mit einem 24-Stunden-Intervall ausgelöst, beginnend mit dem letzten Neustart des Systems.

8.10.1 Wie Sie die Locking ID des Kommunikationssystems abfragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Inventory**. Es wird Ihnen eine Übersicht der Komponenten angezeigt, die zum Kommunikationssystem gehören.
3) Klicken Sie auf **OK & Weiter**. Es werden Ihnen Informationen über die Hardware und die Software angezeigt. Unter **MAC-ID für Lizenz** finden Sie die Locking ID des Kommunikationssystems.

8.10.2 Wie Sie die Locking ID des Soft Switches abfragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Inventory**. Es werden Ihnen Informationen über die Software des Soft Switches, über den verfügbaren und den belegten Speicher der Festplatten und über den Applikationsstatus angezeigt. Unter **MAC-ID für Lizenz** finden Sie die Locking ID des Soft Switches.

8.10.3 Wie Sie die Advanced Locking ID des Soft Switches abfragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**. Es werden Ihnen alle vorhandenen Lizenzen angezeigt. Unter **Locking ID** finden Sie die Advanced Locking ID des Soft Switches, wenn der Soft Switch in einer virtualisierten Umgebung betrieben wird.

8.11 So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System)

Voraussetzungen

- Aktualisieren Sie auf die neueste Systemversion.
- Stecken Sie die IVM-Karten ab, reinigen Sie die Kartensteckplätze und entfernen Sie die IVM-Konfiguration vom System.
- Achten Sie darauf, dass die Anschlüsse im Bereich 511-532 nicht konfiguriert sind. Diese Anschlüsse werden von SmartVM auf V3-Mainboard

reserviert. Dies ist nur für Systeme erforderlich, die im UC Smart-Modus arbeiten.

Um Probleme mit der UC Fax-Funktionalität während der Migration auf das V3-Mainboard-System zu vermeiden, wird empfohlen, den Betriebsmodus des Systems vor der Migration zu konfigurieren. Wenn das System im UC Smart-Modus betrieben wird, sollte der Administrator die Konfiguration der Ports 511-532 löschen, bevor die Migration stattfindet. Wenn das System im UC Suite-Modus betrieben wird, werden die zusätzlichen SmartVM-Ports nicht erstellt und die Faxkonfiguration wird nicht beeinträchtigt. Wenn das Backup-Set beispielsweise von einem UC Suite-System stammt, sollte der Betriebsmodus des V3-Mainboards auf den UC Suite-Modus umgestellt werden, bevor das Backup-Set migriert wird.

Anmerkung: Wenn Sie ein OpenScape Business PAYGO-System aktualisieren, aktualisieren Sie zuerst das OpenScape Business System auf die V3 Software und verwenden Sie dann auf der CLS die Funktion **Lizenzschlüssel erneut generieren**, um eine gültige Lizenzdatei für V3 zu erhalten, die dann über die Lizenz „OpenScape Business Info Ready for V3 SW F31505-K158-D129“ verfügt. Danach muss die neu generierte Lizenzdatei in OpenScape Business System WBM unter **Lizenzverwaltung** manuell aktiviert werden.

Anmerkung: Wenn Sie ein OpenScape Business PAYGO-System aktualisieren, aktualisieren Sie zuerst das OpenScape Business System auf die V3 Software und verwenden Sie dann auf der CLS die Funktion **Lizenzschlüssel erneut generieren**, um eine gültige Lizenzdatei für V3 zu erhalten, die dann über die Lizenz „OpenScape Business Info Ready for V3 SW F31505-K158-D129“ verfügt. Danach muss die neu generierte Lizenzdatei in OpenScape Business System WBM unter **Lizenzverwaltung** manuell aktiviert werden.

Schritt für Schritt

1) Wechseln Sie zum entsprechen Systembetriebsmodus.

Sicherungen des Systems in einem Betriebsmodus können nicht in einem anderen verwendet werden. Wenn Sie beispielsweise eine Sicherung Ihres Systems im UC Suite-Modus erstellen, müssen Sie das aktualisierte System zuerst in den UC Suite-Modus bringen, bevor Sie die Sicherung wiederherstellen können. Die Wiederherstellung einer Sicherung im UC Smart-Modus ist nicht möglich.

Das V3-Mainboard-System wird im UC Smart-Modus betrieben:

Die zusätzlichen Smart VM-Ports werden ab heute erstellt; der Administrator sollte die Konfiguration aus dem oben genannten Portbereich auf dem OCC-System löschen, bevor die Migration stattfindet.

Das V3-Mainboard-System wird im UC Suite-Modus betrieben:

Die zusätzlichen SmartVM-Ports werden nicht erstellt, sodass die Faxkonfiguration nicht beeinträchtigt wird.

2) Aktivieren Sie die Lizenz des Systems.

CLS Connect	Aktion
Aktiviert	Generieren Sie die Lizenz für die V3-MAC-Adresse auf CLS erneut.
Nicht aktiviert	Importieren Sie die neue Lizenz und aktivieren Sie sie auf dem OpenScape Business V2 System. Die Bestätigungscodeforderung wird ausgelöst und zeigt den Bestätigungscode auf der Startseite von WBM.

3) Erstellen Sie eine Sicherung des V2-Systems einschließlich der Systemkonfiguration.

Wenn das OCC mit einem Booster Server verbunden ist, muss ein kompletter Sicherungssatz des Booster Servers heruntergeladen und gespeichert werden.

4) Tauschen Sie das Mainboard aus.

5) Importieren der neuen Lizenz

CLS Connect	Aktion
Aktiviert	Importieren Sie die V3-Lizenzdatei aus CLS in OpenScape Business, um **CLS Connect** auf dem V3-Mainboard zu aktivieren.
Nicht aktiviert	Generieren Sie eine neue V3-Lizenz unter Verwendung des Bestätigungscodes auf CLS mit der V3-Mainboard MAC-Adresse und importieren Sie die neue V3-Lizenzdatei in OpenScape Business.

6) Stellen Sie die V2-Sicherung auf dem V3-Mainboard wieder her.

7) Ändern Sie die IP-Adresskonfiguration der UC-Clients.

Verwenden Sie bei der ersten Verbindung der UC-Clients (nach der Migration) die neuen IP-Adressen des V3-Mainboards.

Mit V3-Mainboard wird nur der Vollduplex-Modus unterstützt.

OptiPoint 4xx/5xx-Geräte werden mit V3-Mainboard nicht mehr unterstützt.

8.12 So migrieren Sie den Master-Knoten eines vernetzten Systems von V2-Mainboard zu V3-Mainboard

Voraussetzungen

Das System hat eine Networking-Lizenz.

Schritt für Schritt

1) Aktualisieren Sie alle OpenScape Business-Slave-Knoten auf V3.

Szenario	Zu befolgende Vorgehensweise
Upgrade mit CLS Connect	Aktualisierung von V2 auf V3 mit CLS Connect auf Seite 350
Upgrade ohne CLS Connect	Aktualisierung von V2 auf V3 ohne CLS Connect auf Seite 350

2) Migrieren des Master-Knoten des Systems.
   Befolgen Sie weiter die Anweisung So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346

Bis der Master-Knoten migriert ist, befinden sich die Slave-Knoten im Failover-Modus. Nach der Migration des Master-Knoten steht wieder ihre volle Funktion zur Verfügung.

8.13 So migrieren Sie den Slave-Knoten eines vernetzten Systems von V2-Mainboard zu V3-Mainboard

Voraussetzungen

Das System hat eine Networking-Lizenz.

Anmerkung: Wenn CLS Connect nicht aktiviert ist, entfernen Sie das Slave-System auf dem Netzwerk auf CLS.

Schritt für Schritt

1) Migrieren Sie das Slave-System
   Befolgen Sie weiter die Anweisung So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346
2) Aktualisieren oder migrieren Sie den Master-Knoten.

Szenario	Zu befolgende Vorgehensweise
Migration von V2-Mainboard auf V3-Mainboard	So migrieren Sie von V2-Mainboard zu V3-Mainboard (Standalone-System) auf Seite 346
Softwareupgrade mit CLS Connect	Aktualisierung von V2 auf V3 mit CLS Connect auf Seite 350
Softwareupgrade ohne CLS Connect	Aktualisierung von V2 auf V3 ohne CLS Connect auf Seite 350

8.14 Migration von HiPath 3000 Systemen auf OSBiz V3 Software mit V3 Mainboard

Die Software-Migration erfolgt über den normalen HiPath 3000-zu-OSBiz-Migrationsprozess mit dem Manager E-Tool. Bestehende HiPath 3000 ComScendo und S2m-Lizenzen werden auf die MAC-Adresse des OCCe-

Mainboards aktualisiert. TDM-Lizenzen und V3-Software-Indikatoren werden vom CLS auf der Grundlage der XML-Datei-Informationen generiert, die während dieses Vorgangs von ManagerE erstellt werden.

Im Falle eines wiederverwendeten OCC-Mainboards aus einer früheren Migration von OSBiz auf OCCe ist keine Lizenzmigration möglich. Alle Lizenzen müssen erworben werden.

Bei einem OCC aus dem Ersatzteillager oder einem neu erworbenen OCC (MAC-Adresse ist im CLS nicht gesperrt) ist ein Upgrade der HiPath 3000 auf diese MAC-Adresse möglich und es wird eine neue Lizenzdatei erzeugt (wie bei der Migration auf OSBiz V2).

8.15 Aktualisierung von V2 auf V3 mit CLS Connect

Die neueste Version V2R7 ist für die Aktualisierung erforderlich und **CLS Connect** muss aktiv sein. Bestehende OpenScape Business V2 Lizenzen, die an die MAC-Adresse des OCC Mainboard gebunden sind, sind auch für V3 gültig.

Nach der Softwareaktualisierung gibt die OpenScape Business V3 Software beim Starten auf CLS an, dass die Lizenzen in Verbindung mit der V3-Software funktionieren. V3-Informationen werden zur Lizenzdatei hinzugefügt und beim Starten automatisch über die CLS-Verbindung zurück zum System übertragen. Manuelle Aktionen sind nicht erforderlich.

Bei einer Softwareaktualisierung ohne Migration von Slave-Systemen mit einer Networking-Lizenz ist keine Aktion erforderlich. In diesem Fall können die Slave-Systeme aktualisiert werden und ihre Lizenz wird nach der Aktualisierung/Migration des Master-Systems automatisch aktualisiert.

8.16 Aktualisierung von V2 auf V3 ohne CLS Connect

Voraussetzungen

- CLS Connect ist nicht aktiv
- OpenScape Business S benötigt einen Internetzugang
- Entfernen Sie bei der Aktualisierung eines Slave-Knotens in einem vernetzten System zuerst den Slave vom CLS.

Schritt für Schritt

1) Aktivieren Sie die Softwareaktualisierungslizenz auf CLS als normale Lizenz für das OpenScape Business System. Die Aktivierung der Softwareaktualisierungslizenz auf CLS generiert eine neue Lizenzdatei mit folgenden Inhalten:

- Neue V3-Lizenz
- Neue (erhöhte) Lizenzdatei-ID
- Wenn das System OSBiz S ist, wird CLS Connect Start zum Zertifikat hinzugefügt.

2) Importieren Sie diese neue Lizenzdatei und aktivieren Sie sie auf OpenScape Business V2 System.

3) Führen Sie die Softwareaktualisierung von V2 auf V3 durch.

Nach der Softwareaktualisierung auf V3 prüft das OpenScape Business System beim Start die Lizenz und erlaubt die Lizenzierungsfunktionalität nur, wenn die V3-Lizenzkomponente in der Lizenzdatei vorhanden ist.

9 Integration ins interne Datennetz (LAN)

Die Integration des Kommunikationssystems in das bestehende interne Datennetz (LAN) ermöglicht die Nutzung der UC-Lösungen und der Administration des Kommunikationssystems über PCs im internen Netz.

Folgende Netzwerkparameter sind im WBM einzurichten:

- Hardware-Plattform OpenScape Business X: IP-Adresse und Netzmaske des Mainboards und der UC Booster Card (falls vorhanden). Diese Einstellungen werden während der Erstinstallation getroffen, können aber nachträglich geändert werden.

  Softswitch OpenScape Business S: IP-Adresse und Netzmaske des Linux-Servers, auf dem die Kommunikationssoftware läuft. Diese Einstellungen werden während der Linux-Installation getroffen, können aber nachträglich geändert werden.
- Das Kommunikationssystem kann optional als DHCP-Server (mit Versorgung von netzwerkspezifischen Parametern wie Netzmaske, Default Gateway, DNS-Server) oder als DHCP Relay Agent eingerichtet werden. Die Einrichtung als DHCP-Server wird während der Erstinstallation getroffen, kann aber nachträglich geändert werden. Die Einrichtung als DHCP Relay Agent erfolgt über den Experten-Modus.
- IP-Adresse des Default Routers und des (externen) DNS-Servers für den Zugang zu anderen IP-Netzen (z.B. Internet). Diese Einstellungen werden während der Erstinstallation getroffen, können aber nachträglich geändert werden.

9.1 LAN-Schnittstelle

Um das Kommunikationssystem in die LAN-Infrastruktur einzubinden, müssen die IP-Adresse und der interne IP-Adressbereich des Kommunikationssystems an das IP-Adressen-Schema des internen Netzes (LAN) angepasst werden.

9.1.1 IP-Adresse und Netzmaske der LAN-Schnittstelle

IP-Adresse und Netzmaske des Kommunikationssystems werden bei der Erstinstallation definiert, können aber auch nachträglich geändert werden. Eventuell müssen IP-Adresse und/oder Netzmaske an den IP-Adressbereich des LAN angepasst werden.

Hardware-Plattform

Der Hardware-Plattform ist standardmäßig eine IP-Adresse und eine Subnetzmaske zugewiesen. Die UC Booster Card benötigt ebenfalls eine IP-Adresse. Unabhängig davon, ob sie gesteckt ist oder nicht, kann die IP-Adresse der UC Booster Card eingerichtet werden.

Die Hardware-Plattform verwendet für die Integration in das LAN die Schnittstelle "LAN" des Mainboards. Ist die UC Booster Card gesteckt, muss zusätzlich die Schnittstelle "LAN" der UC Booster Card an das LAN angeschlossen werden. Hardware-Plattform und UC Booster Card müssen sich in dem selben Subnetz befinden.

Um die Änderungen von IP-Adresse oder Netzmaske zu aktivieren, ist bei der Hardware-Plattform ein Neustart notwendig.

Die Änderungen der IP-Adresse und der Netzmaske bleiben bei einer Softwareaktualisierung erhalten, werden aber bei einem Reload der Hardware-Plattform wieder auf die Standardwerte zurückgesetzt. Diese Änderungen können nicht in einem Backup-Set gespeichert werden.

Softswitch

Beim Softswitch wird der Linux-Server, auf dem die Kommunikationssoftware läuft, über seine Netzwerkkarte in das LAN integriert.

Die Änderungen von IP-Adresse oder Netzmaske sind nach einem Restart der Applikation aktiv (siehe Restart, Reload, Shutdown).

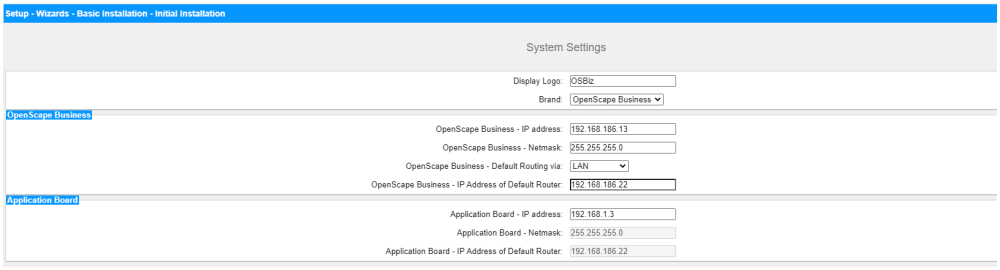
9.1.1.1 Wie Sie IP-Adresse und Netzmaske der Hardware-Plattform ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.



3) Ändern Sie unter **OpenScape Business - IP-Adresse** die IP-Adresse der Hardware-Plattform. Die IP-Adresse muss zu dem IP-Adressen-Schema des internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt. Standardmäßig ist die IP-Adresse `192.168.1.2` eingetragen.
4) Ändern Sie unter **OpenScape Business - Netzmaske** die Netzmaske der Hardware-Plattform. Die Netzmaske muss zu dem IP-Adressen-Schema des internen Netzes passen. Standardmäßig ist die Netzmaske `255.255.255.0` eingetragen.
5) Klicken Sie auf **OK & Weiter**.
6) Klicken Sie so oft auf **OK & Weiter**, bis Sie die Meldung erhalten, dass das Leistungsmerkmal eingerichtet wurde.
7) Klicken Sie auf **Beenden**. Die Hardware-Plattform führt automatisch einen Neustart durch.

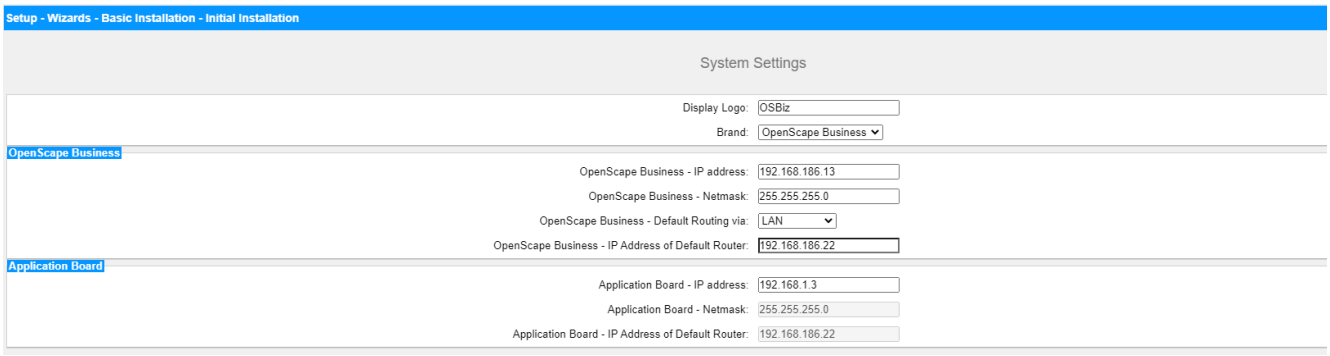
9.1.1.2 Wie Sie IP-Adresse der UC Booster Card ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.



3) Ändern Sie unter **UC Booster Card - IP-Adresse** die IP-Adresse der UC Booster Card. Die IP-Adresse muss zu dem IP-Adressen-Schema des internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt. Standardmäßig ist die IP-Adresse `192.168.1.3` eingetragen.
4) Klicken Sie auf **OK & Weiter**.
5) Klicken Sie so oft auf **OK & Weiter**, bis Sie die Meldung erhalten, dass das Leistungsmerkmal eingerichtet wurde.
6) Klicken Sie auf **Beenden**. Die Hardware-Plattform führt automatisch einen Neustart durch.

9.1.1.3 Wie Sie IP-Adresse und Netzmaske des Softswitches ändern

Schritt für Schritt

1) Klicken Sie in der Taskleiste auf **Computer**.
2) Klicken Sie im Menübaum auf **System** > **YaST**.
3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Es öffnet sich das YaST Control Center.
4) Klicken Sie im Menübaum auf **Network Devices**.
5) Klicken Sie im Bereich **Network Devices** auf **Network Settings**.
6) Markieren Sie im Register **Overview** die gewünschte Netzwerkkarte und klicken Sie auf **Edit**.
7) Aktivieren Sie das Optionsfeld **Statically assigned IP Address**.
8) Ändern Sie unter **IP Address** die IP-Adresse des Linux-Servers, auf dem die Software des Softswitches läuft. Die IP-Adresse muss zu dem IP-Adressen-Schema des internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt.

9) Ändern Sie unter **Subnet Mask** die Subnetzmaske des Linux-Servers. Die Subnetzmaske muss zu dem IP-Adressen-Schema des internen Netzes passen.

10) Klicken Sie auf **Weiter** und anschließend auf **OK**.

11) Schließen Sie das **YaST Control Center**.

9.1.2 Interner IP-Adressbereich der LAN-Schnittstelle

Der interne IP-Adressbereich der LAN-Schnittstelle, den die Hardware-Plattform für die interne Kommunikation ihrer Module verwendet, kann bei Bedarf geändert werden.

Die Hardware-Plattform nutzt standardmäßig den internen IP-Adressbereich 192.168.3.xxx. Dieser kann auch auf den gewünschten IP-Adressbereich geändert werden. Die interne Subnetzmaske ist 255.255.255.0 und kann nicht geändert werden.

Um die Änderungen des internen IP-Adressbereichs zu aktivieren, ist ein Neustart der Hardware-Plattform notwendig.

Die Änderungen des internen IP-Adressbereichs bleiben bei einer Softwareaktualisierung erhalten, werden aber bei einem Reload wieder auf die Standardwerte zurückgesetzt. Diese Änderungen können nicht in einem Backup-Set gespeichert werden.

9.1.2.1 Wie Sie den internen IP-Adressbereich der Hardware-Plattform ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

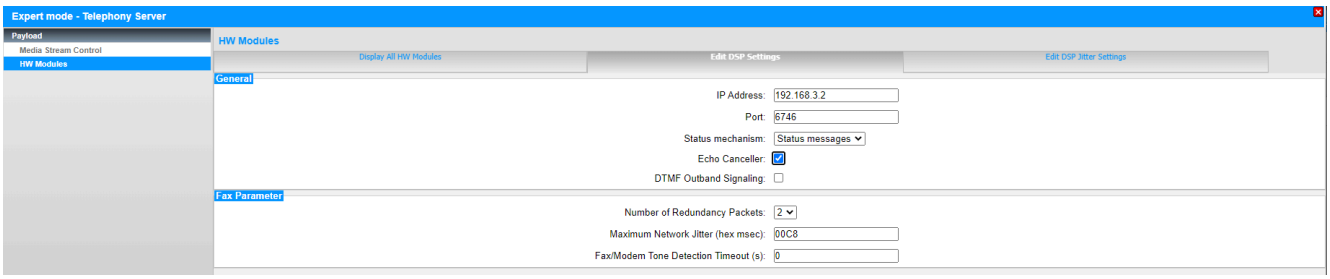
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Payload**.

3) Klicken Sie im Menübaum auf **Hardware-Module**.

4) Klicken Sie auf die Registerkarte **DSP-Einstellungen ändern**.



5) Geben Sie im Bereich **Allgemein** unter **IP-Adresse** eine IP-Adresse für das Kommunikationssystem ein, die im gewünschten neuen internen Bereich liegt, z. B. `192.168.40.2`. Der gesamte IP-Adressbereich (im Beispiel `192.168.40.xxx`) ist nun für andere Clients im LAN gesperrt.

6) Klicken Sie auf **Übernehmen** und bestätigen Sie mit **OK**.

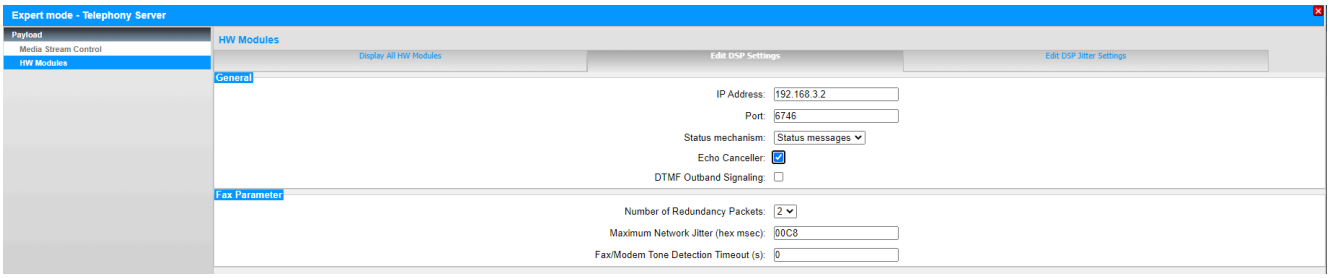
9.1.2.2 Wie Sie den internen IP-Adressbereich der Hardware-Plattform zurücksetzen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Payload**.
3) Klicken Sie im Menübaum auf **Hardware-Module**.
4) Klicken Sie auf die Registerkarte **DSP-Einstellungen ändern**.



5) Geben Sie im Bereich **Allgemein** unter **IP-Adresse** die IP-Adresse `192.168.3.2` ein. Der gesamte IP-Adressbereich (`192.168.3.xxx`) ist nun für andere Clients im LAN gesperrt.
6) Klicken Sie auf **Übernehmen** und bestätigen Sie mit **OK**.

9.2 DHCP

DHCP (Dynamic Host Configuration Protocol) ermöglicht mit Hilfe eines DHCP-Servers die dynamische Zuweisung von netzwerkspezifischen Daten an die IP-Teilnehmer eines Netzes (z.B. LAN).

Durch DHCP wird die automatische Integration eines IP-Teilnehmers (z.B. IP-Telefone oder PCs) in ein bestehendes LAN ermöglicht. Der IP-Teilnehmer muss für den automatischen Empfang der netzwerkspezifischen Daten eingerichtet sein und ist damit ein DHCP-Client. Der DHCP-Server versorgt den IP-Teilnehmer auf Anfrage mit den netzwerkspezifischen Daten.

9.2.1 DHCP-Relay-Agent

Bei Verwendung des internen DHCP-Servers der Hardware-Plattform müssen sich der interne DHCP-Server und die DHCP-Clients im selben Netzsegment befinden. Ist das nicht der Fall, muss die Hardware-Plattform als DHCP-Relay-Agent konfiguriert werden. Die DHCP-Anfragen der IP-Teilnehmer werden dann von der Hardware-Plattform an den eigentlichen DHCP-Server weitergeleitet.

9.2.1.1 So konfigurieren Sie die Hardwareplattform als DHCP-Relay-Agent

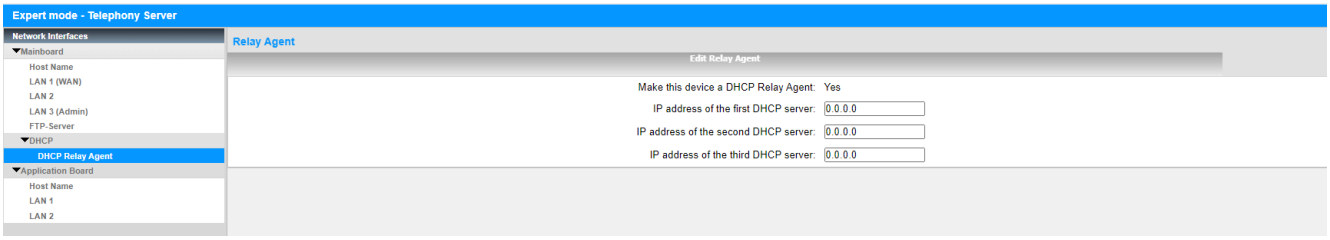
Wenn die Hardwareplattform als DHCP-Relay-Agent konfiguriert ist, leitet sie DHCP-Anforderungen an den externen DHCP-Server weiter.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie-Server** > **Netzwerkschnittstellens**.
3) Klicken Sie im Menübaum auf **Hauptplatine** > **DHCP**.
4) Aktivieren Sie das Optionsfeld **DHCP-Relay-Agent**.
5) Klicken Sie auf **Anwenden** und bestätigen Sie mit **OK**.
6) Klicken Sie in der Menüstruktur auf **DHCP-Relay-Agent**.



7) Geben Sie die **IP-Adresse des ersten DHCP-Servers**ein.
8) Geben Sie die **IP-Adresse des zweiten DHCP-Servers**ein.
9) Geben Sie die **IP-Adresse des dritten DHCP-Servers**ein.

Tipp: Sie können bis zu drei DHCP-Server eingeben. Der Eintrag des ersten DHCP-Servers ist obligatorisch.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.2.2 DHCP-Server

Der DHCP-Server weist den IP-Teilnehmern (IP-Telefone, SIP-Telefone, PCs, WLAN Access Points, usw.) dynamisch die netzwerkspezifischen Daten zu, wie z.B. die zu verwendende IP-Adresse und Netzmaske des IP-Teilnehmers, die IP-Adresse des Standard-Gateways, die IP-Adresse des SNTP-Servers, usw.

Als DHCP-Server kann der interne DHCP-Server des Kommunikationssystems oder ein externer DHCP-Server genutzt werden (z.B. der DHCP-Server des Internet-Routers).

Bei der Hardware-Plattform ist der integrierte DHCP-Server standardmäßig aktiviert. Soll ein externer DHCP-Server verwendet werden, muss der interne DHCP-Server deaktiviert werden. Andernfalls kommt es zu Konflikten mit dem externen DHCP-Server.

Bei dem Softswitch kann der Linux-Server als interner DHCP-Server konfiguriert werden.

Bei der Erstinbetriebnahme sollte entschieden werden, ob der interne DHCP-Server des Kommunikationssystems oder ein externer DHCP-Server genutzt werden soll. Der interne DHCP-Server kann auch nachträglich aktiviert oder deaktiviert werden. Auch die netzwerkspezifischen Daten können nachträglich konfiguriert werden.

Interner DHCP-Server

Wird der interne DHCP-Server genutzt, werden die IP-Teilnehmer automatisch mit folgenden netzwerkspezifischen Daten versorgt:

- IP-Adresse und Netzmaske des IP-Teilnehmers
- IP-Adresse des Kommunikationssystems (Default-Gateway)
- IP-Adresse des SNTP-Servers (für die Versorgung mit Datum & Uhrzeit)
- IP-Adresse des DNS-Servers (für die Namensauflösung)
- IP-Adresse des SIP-Servers (für die Authentifizierung von SIP-Teilnehmern)
- IP-Adresse des internen DLI oder des externen DLS-Servers (für die Softwareaktualisierung der IP-Systemtelefone)
- Routing-Regeln

Externer DHCP-Server

Wird ein externer DHCP-Server genutzt, muss dieser einen Vendor Specific Option Space unterstützen, der es ermöglicht, herstellerspezifische Parameter zu versorgen. Folgende netzwerkspezifischen Daten sollten im externen DHCP-Server eingegeben werden:

- IP-Adresse und Netzmaske des IP-Teilnehmers
- IP-Adresse des Default Routers = Option 3
- IP-Adresse des Kommunikationssystems (Default-Gateway) = Option 33
- IP-Adresse des DNS-Servers (für die Namensauflösung) = Option 6
- IP-Adresse des internen DLI oder des externen DLS-Servers (für die Softwareaktualisierung der IP-Systemtelefone) = Option 43
- Nur für SIP-Telefone: IP-Adresse des SIP-Servers (SIP-Registrar, für die Authentifizierung von SIP-Teilnehmern) = Option 120
- Nur für SIP-Telefone: IP-Adresse des SNTP-Servers (für die Versorgung der SIP-Telefone mit Datum & Uhrzeit) = Option 42

Anmerkung: Weitere Informationen zum DHCP-Server in einer Windows-Umgebung finden Sie hier: http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment.

Ist eine Eingabe am externen DHCP-Server nicht möglich, so müssen diese Daten direkt an den IP-Systemtelefonen eingegeben werden. Nur dann werden die IP-Systemtelefone automatisch z.B. mit dem aktuellen Datum und Uhrzeit und mit dem neuesten Software-Update versorgt.

Weitere Informationen finden Sie im folgenden Unify Experts Wiki unter: http://wiki.unify.com/wiki/DHCP

DHCP-Adress-Pool (IP-Adressbereiche)

Meldet sich ein IP-Teilnehmer am DHCP-Server an, bekommt er u.a. eine dynamische IP-Adresse zugewiesen. Der Administrator kann einen IP-Adressbereich festlegen, aus dem der DHCP-Server die IP-Adressen an die IP-Teilnehmer vergeben darf. Es sollen z.B. nicht alle IP-Adressen aus dem Band 192.168.1.x vergeben werden, sondern nur von 192.168.1.50 bis 192.168.1.254, da die unteren IP-Adressen bis 192.168.1.49 für IP-Teilnehmer mit statischen IP-Adressen reserviert sein sollen.

Im Experten-Modus lassen sind unter **Netzwerk-Schnittstellen** für den internen DHCP-Server sogar mehrere IP-Adressbereiche einrichten.

9.2.2.1 Aktivieren und Konfigurieren des DHCP-Servers der Hardwareplattform

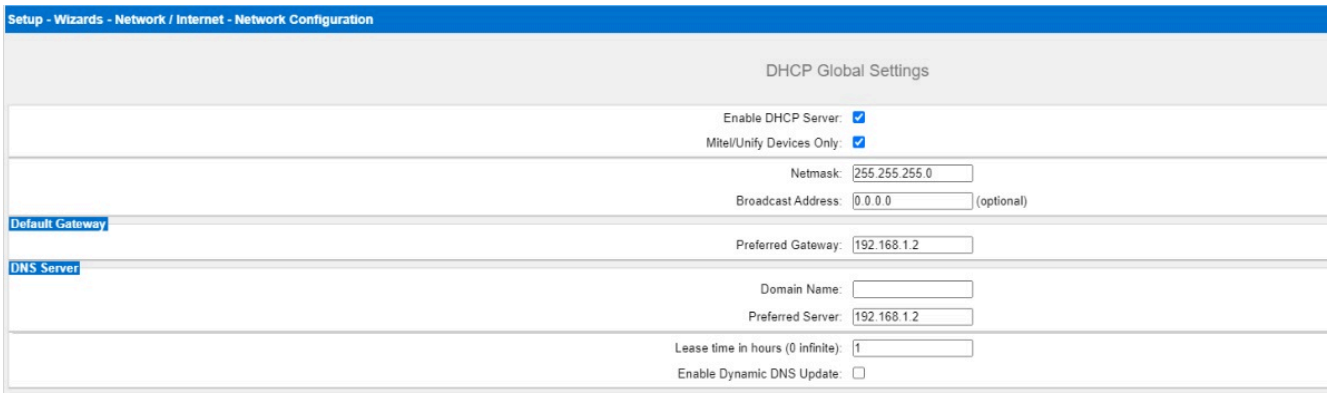
Der **Netzwerkkonfigurationsassistent** kann verwendet werden, um den DHCP-Server der Hardwareplattform zu aktivieren und zu konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Assistenten** > **Netzwerk/Internet**.
3) Klicken Sie auf **Bearbeiten**, um den **Netzwerkkonfigurationsassistenten** zu starten.



4) Aktivieren Sie das Kontrollkästchen **DHCP-Server aktivieren**.
5) Aktivieren Sie bei Bedarf das Kontrollkästchen **Nur Mitel-/Unify-Geräte** checkbox.

Anmerkung: Diese Option ist nur für V3-Hauptplatinen verfügbar.

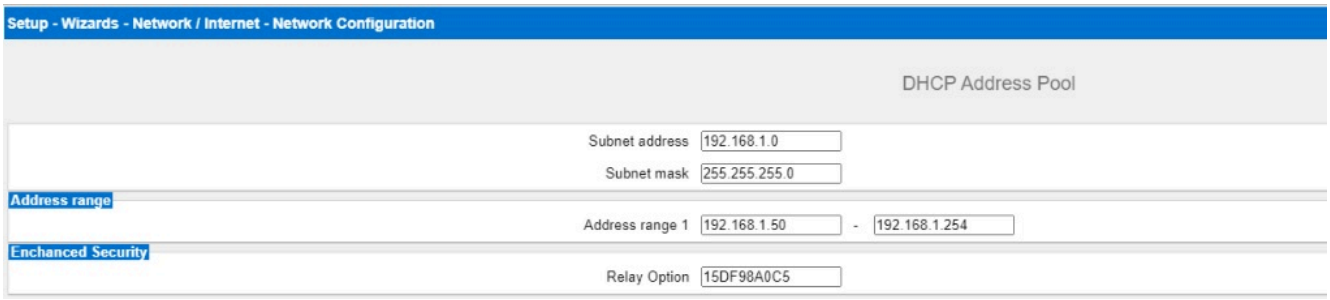
---

6) Geben Sie die Subnetzmaske Ihres Netzwerks in das Feld **Subnetzmaske** ein (z. B. `255.255.255.0`).
7) Geben Sie im Feld **Broadcast-Adresse** die Broadcast-Adresse ein ("letzte" IP-Adresse des Netzes oder Subnetzes, Standard: `0.0.0.0`) falls erforderlich.
8) Geben Sie im Feld **Bevorzugtes Gateway** die IP-Adresse des Standardgateways ein. In der Regel beträgt die IP-Adresse für den Internetrouter `192.168.1.1`.
9) Wenn Sie einen vollqualifizierten Domänennamen für den DHCP-Server benötigen, geben Sie diesen unter **Domänenname** ein (max. 80 zeichen).
10) Geben Sie im Feld **Bevorzugter Server** die IP-Adresse eines verfügbaren DNS-Servers ein, z.B. die IP-Adresse des Internetrouters `192.168.1.1`.
11) Geben Sie bei Bedarf die maximale Leasingzeit in Stunden ein (Standard: 1 h, 0 = unendliche Lease-Zeit) im Feld **Lease-Zeit in Stunden (0 = unendlich)**.

12) Wenn Sie dynamische Updates des DNS-Servers zulassen möchten, aktivieren Sie die Option **Dynamisches DNS-Update aktivieren** (Standard: deaktiviert).

> **Anmerkung:** Wenn die Option Dynamische DNS-Aktualisierung aktiviert ist, ist es zwingend erforderlich, den **Domänennamen** im entsprechenden Feld für den IP-Adresspool zu konfigurieren.

13) Klicken Sie auf **OK & Weiter**. Die Einstellungen für den DHCP-Adresspool werden angezeigt.



14) Geben Sie im Feld **Subnet Address** die niedrigste IP-Adresse des Subnetzes ein, in dem sich der gewünschte IP-Adressbereich befindet (in unserem Beispiel `192.168.1.0`).
15) Geben Sie die Subnetzmaske des gewünschten IP-Adressbereichs in das Feld **Subnetzmaske** ein (z. B. `255.255.255.0`).
16) Geben Sie im Feld **Adressbereich 1** den oberen und unteren Schwellenwert für den gewünschten IP-Adressbereich ein (z. B. `192.168.1.50` bis `192.168.1.254`).
17) Geben Sie bei Bedarf den Wert des Feldes **Relay-Option** ein.

> **Anmerkung:** Diese Option ist nur für V3-Hauptplatinen verfügbar.

18) Klicken Sie auf **OK & Weiter**. Das Fenster **Routing-Einstellungen** erscheint.
19) Geben Sie im Feld **IP-Adresse des DNS-Servers**die IP-Adresse eines verfügbaren DNS-Servers ein, z. B. die IP-Adresse des Internetrouters `192.168.1.1`ein.
20) Wählen Sie den Element **LAN** aus der Dropdown-Liste **Standard-Routing über** aus.
21) Wenn der Zugriff auf das Internet über einen Internetrouter erfolgt, geben Sie die IP-Adresse des Internetrouters (z. B.`192.168.1.1`) in das Feld **IP-Adresse des Standardrouters** ein.
22) Klicken Sie auf **OK & Weiter** gefolgt von **Fertigstellen**.

9.2.2.2 So deaktivieren Sie den DHCP-Server der Hardwareplattform

Der **Netzwerkkonfigurationsassistent** kann verwendet werden, um den DHCP-Server der Hardwareplattform zu deaktivieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Assistenten** > **Netzwerk/Internet**.
3) Klicken Sie auf **Bearbeiten**, um den **Netzwerkkonfigurationsassistenten** zu starten.
4) Deaktivieren Sie das Kontrollkästchen **DHCP-Server aktivieren**.
5) Klicken Sie weiter auf **OK & Weiter**, bis Sie eine Meldung erhalten, dass die Funktion installiert wurde.
6) Klicken Sie auf **Fertigstellen**.

9.2.2.3 Wie Sie den DHCP-Server des Softswitches aktivieren und konfigurieren

Schritt für Schritt

1) Klicken Sie in der Taskleiste auf **Computer**.
2) Klicken Sie im Menübaum auf **System** > **YaST**.
3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Es öffnet sich das YaST Control Center.
4) Klicken Sie im Menübaum auf **Network Services**.
5) Klicken Sie im Bereich **Network Services** auf **DHCP Server**.
6) Markieren Sie die gewünschte Netzwerkkarte und klicken Sie auf **Select**.
7) Aktivieren Sie das Kontrollkästchen **Open Firewall for Selected Interfaces**.
8) Klicken Sie auf **Weiter**.
9) Wenn Sie einen vollqualifizierten Domänennamen für den DHCP-Server benötigen, geben Sie diesen unter **Domänen-Name** ein (max. 80 Zeichen).
10) Geben Sie im Feld **Primary Name Server IP** die IP-Adresse eines verfügbaren DNS-Servers ein, z.B. die IP-Adresse des Internet-Routers, `192.168.1.1`.
11) Geben Sie im Feld **Default Gateway (Router)** die IP-Adresse des Standardgateways ein. In der Regel ist das die IP-Adresse des Internet-Routers, z.B. `192.168.1.1`.
12) Geben Sie im Feld **NTP Time Server** den bei der Erstinbetriebnahme festgelegten SNTP-Server ein.
13) Klicken Sie auf **Weiter**.
14) Geben Sie im Feld **First IP Address** die untere Grenze und im Feld **Last IP Address** die obere Grenze des gewünschten IP-Adressbereichs ein (z.B. `192.168.1.50` bis `192.168.1.254`).
15) Aktivieren Sie das Kontrollkästchen **Allow Dynamic BOOTP**.
16) Klicken Sie auf **Weiter**.
17) Aktivieren Sie das Optionsfeld **When Booting**.
18) Klicken Sie auf **Beenden**.
19) Schließen Sie das **YaST Control Center**.

9.2.2.4 Wie Sie den DHCP-Server des Softswitches deaktivieren

Schritt für Schritt

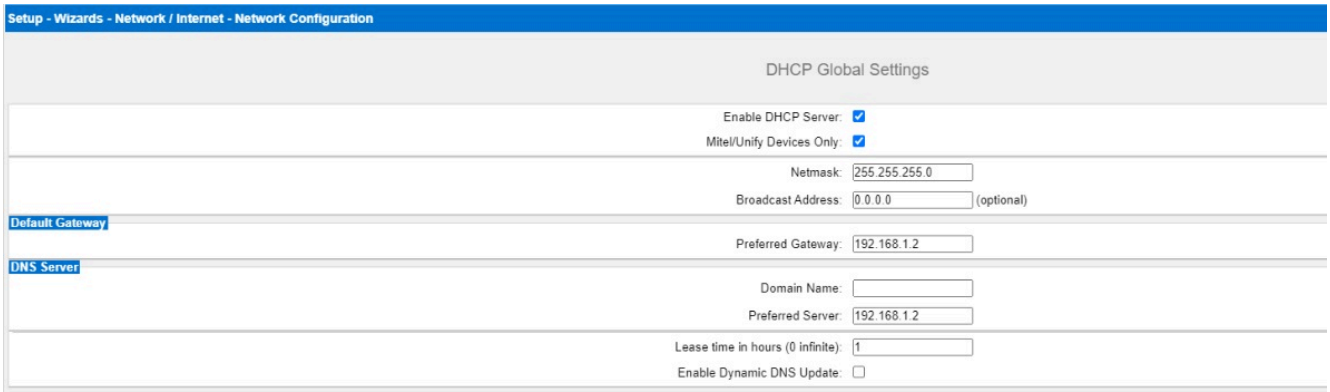
1) Klicken Sie in der Taskleiste auf **Computer**.
2) Klicken Sie im Menübaum auf **System** > **YaST**.
3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Es öffnet sich das YaST Control Center.
4) Klicken Sie im Menübaum auf **Network Services**.
5) Klicken Sie im Bereich **Network Services** auf **DHCP Server**.
6) Deaktivieren Sie das Kontrollkästchen **Start DHCP Server**.
7) Klicken Sie auf **Beenden**.
8) Schließen Sie das **YaST Control Center**.

9.2.2.5 So aktivieren Sie DHCP nur für Mitel/Unify Geräte

Mit dieser Option kann der Systemadministrator den OpenScape Business DHCP-Dienst ausschließlich für Mitel- und Unify-Geräte aktivieren.

Voraussetzungen

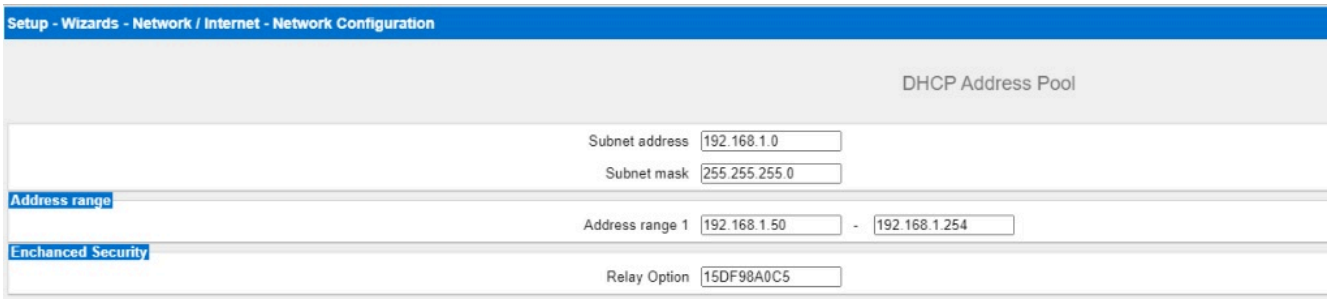
Sie befinden sich im Fenster **Globale DHCP-Einstellungen**.



Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **DHCP-Server aktivieren** aktiviert.
2) Klicken Sie, um das Kontrollkästchen **Nur Mitel-/Unify-Geräte** zu aktivieren. Weitere Informationen zu dieser Option finden Sie unter DHCP-Server > Globale Parameter.
3) Gehen Sie zum Feld **Netmaske** und passen Sie die Subnetzmaske an Ihren IP-Adressbereich an (z. B. `255.255.255.0`).
4) Geben Sie im Feld **Bevorzugtes Gateway** die IP-Adresse des Internetrouters ein (z. B. `192.168.1.1`).
5) Geben Sie im Feld **Bevorzugter Server** die IP-Adresse des DNS-Servers ein (z.B. die IP-Adresse des Internet-Routers `192.168.1.1` ein.

6) Klicken Sie auf **OK & Weiter**. Das **DHCP-Adresspool** erscheint.



7) Geben Sie die Werte für **Subnetzadresse**, **Subnetzmaske** und **Adressbereich 1** an, um den IP-Adressbereich zu definieren, der vom internen DHCP-Server verwaltet werden soll.

   Wenn das interne Netzwerk statische IP-Adressen verwendet (z.B. für einen Drucker-Server), muss der IP-Adressbereich (DHCP-Adresspool) ausgewählt werden, damit die festen IP-Adressen nicht in diesen Bereich einbezogen werden.

   Beispiel:

   Internetrouter: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Subnetzadresse: `192.168.1.0`

   Subnetzmaske: `255.255.255.0`

   Drucker-Server: `192.168.1.10`

   DHCP-Adresspool: `192.168.1.50` zu `192.168.1.254`
8) Geben Sie den Wert des Feldes **Relais-Option** an.
9) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

Land- und Zeiteinstellungen konfigurieren.

9.3 DNS - Namensauflösung

Der Domain Name Service (DNS) dient der Umsetzung von Namen in numerische Adressen. Damit können Rechnernamen oder Domänen-Namen in IP-Adressen übersetzt werden und umgekehrt.

DNS nutzt eine weltweit auf Servern verteilte hierarchische Datenbank, die den Namensraum des Internets verwaltet. Dieser Namensraum ist in so genannte Zonen (Domänen) unterteilt. Für lokale Anforderungen – etwa innerhalb eines Firmennetzes – werden in der Regel eigene DNS-Server betrieben, die vom Internet unabhängig sind.

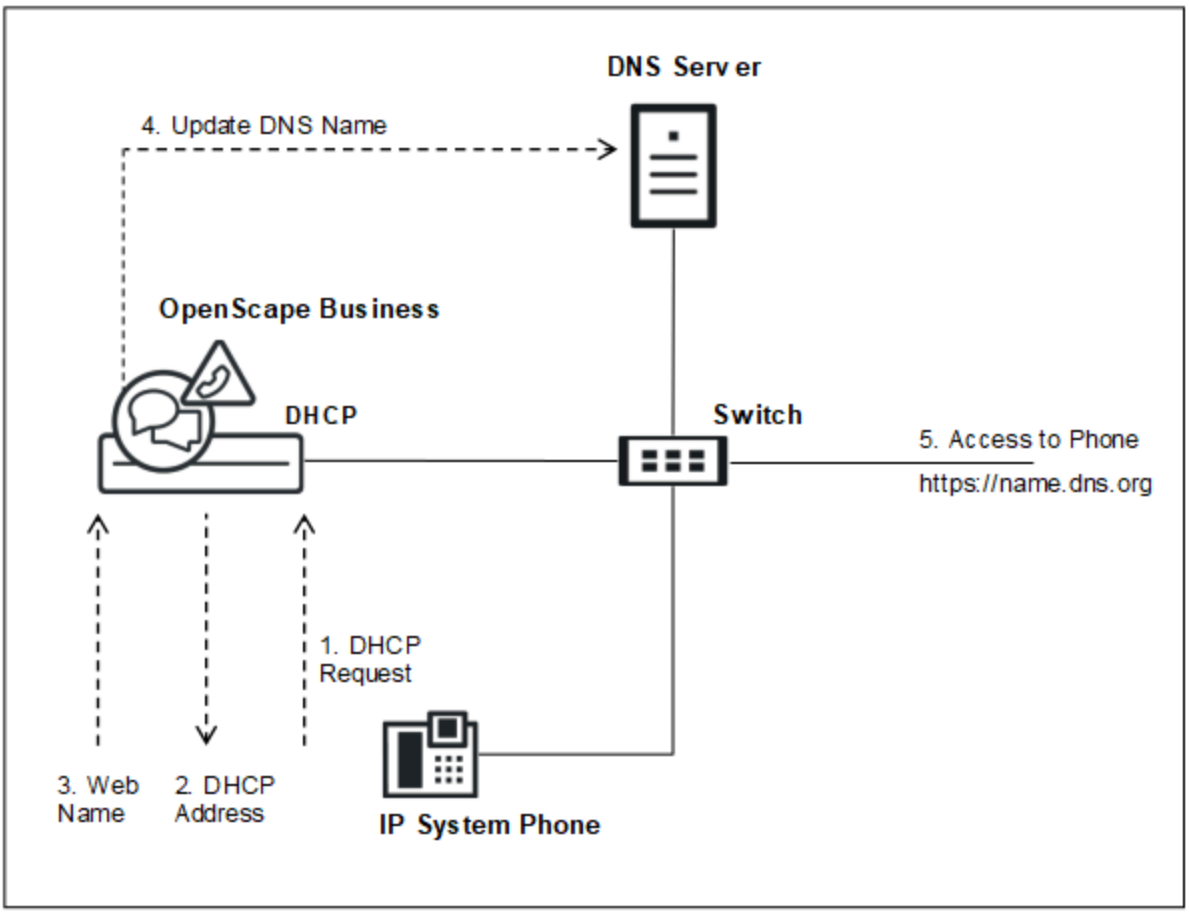
Namensauflösung bei IP-Systemtelefonen

Folgende Voraussetzungen müssen erfüllt sein:

- Windows 2008 DNS-Server (mit aktuellem Patchstand und die Einstellung "unsicheren Update zulassen" muss aktiviert werden)

- Interner DHCP-Server ist aktiviert
- Die Funktionalität "Dynamisch DNS aktualisieren" ist im internen DHCP-Server aktiviert (siehe DHCP-Server)
- Im IP-Systemtelefon ist der Web-Name eingetragen.

Das IP-Systemtelefon sendet einen DHCP-Request (1) und erhält vom internen DHCP-Server eine gültige IP-Adresse und die weiteren netzwerkspezifischen Daten (2). Nach dem Erhalt dieser Daten sendet das IP-Systemtelefon den eingestellten Web-Namen an den internen DHCP-Server (3), der den Namen automatisch an den konfigurierten DNS-Server weiterleitet (4). Der DNS-Server kennt nun den zur IP-Adresse des IP-Systemtelefons gehörenden Namen. Das IP-Systemtelefon kann nun z.B. über das WBM mit seinem Web-Namen angesprochen werden (5).



DNS Server

Der DNS-Server, auch Nameserver genannt, ist ein Programm, das Anfragen zu Domänen-Namen oder Rechnernamen beantwortet. Auch der PC, auf dem dieses Programm läuft, kann als DNS-Server bezeichnet werden.

Bei Anfragen nach einem Domänen-Namen oder einem Rechnernamen sendet der DNS-Server die zugehörige IP-Adresse.

Beispiel: Für `www.wikipedia.org` geben die DNS-Server im Internet die IP-Adresse `91.198.174.2` zurück.

Kann der bevorzugte DNS-Server die Anfrage nicht beantworten, leitet er diese an einen anderen DNS-Server weiter.

Beim Softswitch kann der Linux-Server, auf dem die Kommunikationssoftware läuft, als DNS-Server konfiguriert werden. Die Hardware-Plattform kann nicht als DNS-Server eingesetzt werden. Sowohl beim Softswitch als auch bei der Hardware.Plattform kann ein externer DNS-Server angegeben werden.

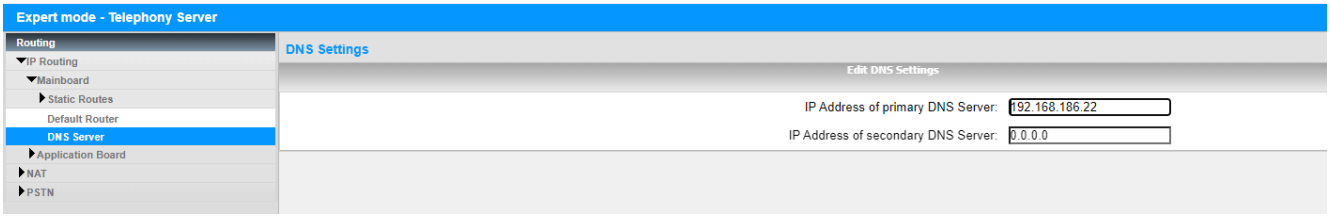
9.3.1 Externen DNS-Server festlegen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Routing**.
3) Navigieren Sie im Menübaum zu **IP-Routing** > **Mainboard** > **DNS-Server**. Das Fenster **DNS-Einstellungen ändern** erscheint.



4) Geben Sie im Feld **IP-Adresse des DNS-Servers** die IP-Adresse des gewünschten externen DNS-Servers ein.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Anmerkung: Im Falle eines OpenScape Business S-Systems ist ein Systemneustart erforderlich, damit die Änderungen wirksam werden.

9.4 IP-Routing

IP-Routing bezeichnet in der Datentechnik das Festlegen von Wegen (Routen) für Datenströme innerhalb von Netzwerken. IP-Routing ist dann erforderlich, wenn Absender und Empfänger in verschiedenen Netzen liegen.

Default-Router

Um sicherzustellen, dass IP-Teilnehmer auch Ziele erreichen, die außerhalb des eigenen Netzwerks liegen und die nicht explizit in einer Routingtabelle aufgeführt sind, muss ein Gateway für die Weiterleitung solcher Pakete angegeben werden (Default Router). Der Default Router wird die Daten dann an das übergeordnete Netzwerk weiterleiten.

Sie können IP-Routing über einen Default Router sowohl für das Mainboard als auch für das Application Board aktivieren oder deaktivieren.

Statische Routen

Statische Routen werden benutzt, um Daten den Weg zu einem Netzwerk zu benennen, das nicht über den Default Router erreicht werden kann.

Sie können statische Routen sowohl für das Mainboard als auch für das Application Board anlegen.

9.4.1 Wie Sie den Default Router aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Routing**.
3) Navigieren Sie im Menübaum zu **IP-Routing** > **Mainboard / Application Board** > **Default Router**. Das Fenster **Default-Router ändern** wird angezeigt.

4) Wenn Sie IP-Routing über einen Default Router aktivieren möchten, wählen Sie in der Auswahlliste **Default-Routing über** den Eintrag **LAN** aus und geben Sie unter `IP-Adresse des Default Routers` die IP-Adresse des Default Routers an, z. B. die IP-Adresse des Internet-Routers: **192.168.1.1**.
5) Wenn Sie IP-Routing über einen Default Router deaktivieren möchten, wählen Sie in der Auswahlliste **Default-Routing über** den Eintrag **Keine Schnittstelle** aus.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.4.2 Wie Sie eine statische Route hinzufügen

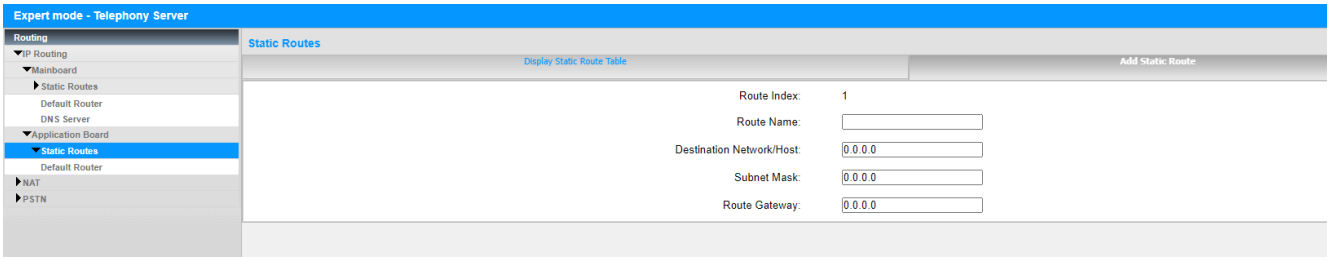
Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Routing**.
3) Navigieren Sie im Menübaum zu **IP-Routing** > **Mainboard / Application Board** > **Statische Routen**. Das Fenster **Statische Routen** wird angezeigt.

4) Klicken Sie auf die Registerkarte **Statische Route hinzufügen**. Der **Route-Index** zeigt an, welche Route hinzugefügt wird.



5) Im Feld **Route-Name** geben Sie den gewünschten Namen für diese Route an.
6) Geben Sie die IP-Adresse des **Ziel-Netzwerk/Host** ein.
7) Geben Sie die IP-Adresse der **Ziel-Netzmaske** (Subnetzmaske) ein.
8) Geben Sie im Feld **Route-Gateway** die IP-Adresse des Routers ein, über den das gewünschte Zielnetzwerk erreicht werden soll.
9) Wenn Sie eine oder mehrere statische Routen für das Mainboard angelegt haben, können Sie alle statische Routen des Mainboards mit der Schaltfläche **Nach OCAB kopieren** zum Application Board kopieren.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.4.3 Wie Sie statische Routen löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Routing**.
3) Navigieren Sie im Menübaum zu **IP-Routing** > **Mainboard / Application Board** > **Statische Routen**.
4) Markieren Sie die zu löschende Route.
5) Wechseln Sie auf die Registerkarte **Statische Route löschen**.
6) Klicken Sie auf **Löschen**.
7) Bestätigen sie die Hinweismeldung und klicken Sie anschließend auf **OK**.

9.5 Deployment Service (DLI und DLS)

Mithilfe von DLI und DLS können IP-Komponenten zentral administriert und mit Software versorgt werden. Die DLI ist im Kommunikationssystem integriert. Der DLS eine eigenständige Applikation, die auf einem externen Server-PC installiert werden muss.

DLI (Deployment Server Integrated)

Der DLI ist eine im Kommunikationssystem integrierte Komponente, die eingeschränkte DLS-Funktionalität zur Verfügung stellt. Mit dem internen DLI lassen sich alle am Kommunikationssystem angeschlossenen IP-Systemtelefone zentral konfigurieren und automatisch mit der

aktuellsten Telefon-Software versehen. Wenn DLI für DeskPhone CP 400/600/600E/700/700X/710 aktiviert ist, werden die folgenden UC-Server-Parameter automatisch konfiguriert: UC-Protokoll, UC-Server-Adresse, UC-Server-Port.

Das interne DLI arbeitet mit dem ebenfalls integrierten FTP-Server zusammen, auf dem die aktuellste Telefon-Software gespeichert ist.

Ist dem DHCP-Server die IP-Adresse des DLI bekannt, sendet der DHCP-Server diese Daten an das IP-Systemtelefon (HFA, SIP), sobald es sich im internen Netz anmeldet. Somit kann sich das Telefon die aktuelle Software vom FTP-Server des Kommunikationssystems holen. Im internen DHCP-Server ist standardmäßig der DLI konfiguriert. Soll stattdessen ein externer DLS-Server genutzt werden, muss seine IP-Adresse im internen DHCP-Server konfiguriert werden.

DLS (Deployment Service)

Der DLS ist eine Client/Server-Applikation zur zentralen Administration der IP-Komponenten. Der DLS-Server ist nicht im Kommunikationssystem intergriert und muss separat auf einem Server-PC installiert werden. Der DLS-Client läuft auf den IP-Komponenten. Die Administration erfolgt über einen Web-Browser.

IP-Komponenten sind IP-Systemtelefone, SIP-Telefone, SIP-Clients und IP-Gateways.

Anmerkung: Die Eigenschaften und Leistungsmerkmale des DLS sind in der Produktbeschreibung des DLS zu finden und werden nicht in dieser Dokumentation beschrieben.

DLI oder DLS mit externem DHCP-Server

Damit auch bei Nutzung eines externen DHCP-Servers die Software der IP-Systemtelefone (HFA, SIP) automatisch aktualisiert werden kann, haben Sie folgende Alternativen:

- IP-Adresse des DLI oder DLS im externen DHCP-Server konfigurieren

  Beim externen DHCP-Server müssen die netzwerkspezifischen Daten eingetragen werden und die IP-Adresse des verwendeten Deployment-Servers (DLI oder externer DLS-Servers). Zusätzlich muss auf dem externen DLS-Server die aktuelle Telefon-Software gespeichert sein.
- Alle IP-Systemtelefone konfigurieren

  Bei jedem IP-Systemtelefon muss als DLS-Adresse die IP-Adresse des verwendeten Deployment-Servers eingetragen werden (IP-Adresse des Kommunikationssystems für den internen DLI oder IP-Adresse des externen DLS-Servers).

Funktionen und Einschränkungen

Funktion	DLI	DLS
Zentrale Konfiguration der Parameter der IP-Komponenten Die Parameter der IP-Komponenten sind über anpassbare XML-Templates konfigurierbar.	Ja	Ja

Funktion	DLI	DLS
Plug-and-Play-Inbetriebnahme der IP-Komponenten Über einen DHCP-Server können sich die IP-Komponenten automatisch am System anmelden, z.B. bei einem Neuanschluss oder einem Austausch einer IP-Komponente.	Ja	Ja
Zentrale & automatische Softwareaktualisierung der IP-Komponenten Die IP-Komponenten werden automatisch beim ersten Anmelden mit der aktuellsten Software-Version versorgt oder wenn eine neue Software-Version zur Verfügung steht. In der IP-Komponente muss die IP-Adresse des DLI/DLS konfiguriert sein.	Ja	Ja Auf dem DLS muss die aktuellste Telefon-Software gespeichert sein.
Zentrales Inventory-Management der IP-Komponenten Die Daten zu den Hardware-Konfigurationen der IP-Komponenten können zentral abgerufen werden.	Nein	Ja
Unterstützung von IP Mobility (DeskSharing) Telefonie-Daten eines Benutzers werden zentral abgespeichert und können an anderen Telefonen wieder abgerufen werden (z.B. Tastenprogrammierungen, Telefonbucheinträge, Journale).	Ja Nicht für SIP-Telefone, Nicht im Netzverbund möglich.	Ja Nicht für SIP-Telefone, In homogenen Netzen (nur OpenScape Business Systeme) nur bei geschlossener Nummerierung, Nicht in inhomogenen Netzen (mit OpenScape 4000 oder OpenScape Voice).
Unterstützung von SPE in Netzen	Die Verwendung von SPE in Netzwerken ist möglich. DLS muss verwendet werden (DLI nicht zulässig).	Ja Die bereitzustellenden Schlüssel und Zertifikate müssen auf dem DLS verfügbar sein.
Zentrale Versorgung mehrerer unterschiedlicher Plattformen	Nein	Ja
Freischaltung der 2. LAN-Schnittstelle der IP-Systemtelefone (PC Ethernet Mode). Siehe Grundeinstellungen > Telefonparameter-Bereitstellung	Ja	Ja

Deployment- und Licensing-Client (DLSC) (Menü)

Um DLS-Funktionen, wie z.B. den Element-Manager, nutzen zu können, muss das Kommunikationssystem dem externen DLS den Zugriff auf die Konfigurationsdaten gewähren. Das Kommunikationssystem wird dann als Deployment und Licensing Client betrieben.

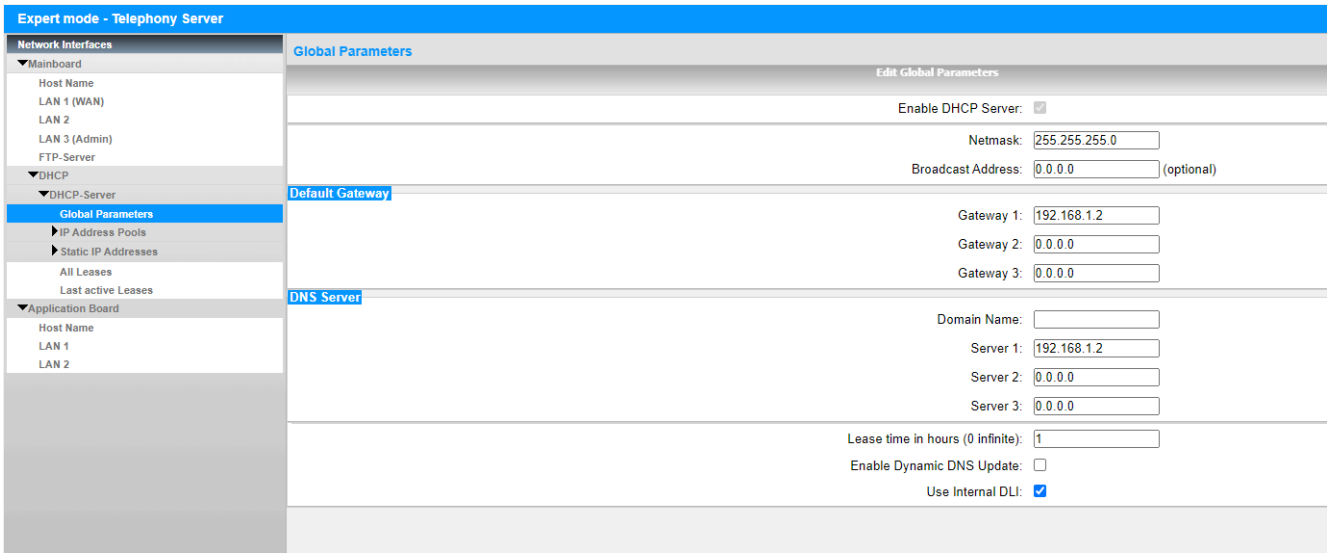
9.5.1 Wie Sie einen externen DLS-Server im internen DHCP-Server konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Netzwerkschnittstellen**.
3) Navigieren Sie im Menübaum zu **Mainboard** > **DHCP** > **DHCP-Server** > **Globale Einstellungen**. Das Fenster **Globale Parameter ändern** wird angezeigt.



4) Deaktivieren Sie das Kontrollkästchen **Internes DLI verwenden**.
5) Geben Sie im Feld **IP-Adresse** die IP-Adresse ein, unter der der externe DLS-Server zu erreichen ist.
6) Geben Sie im Feld **Port** den Port ein, den der DLS-Server nutzt. Dieser Port muss in der Firewall freigegeben sein.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.5.2 Wie Sie den internen DLI aktivieren

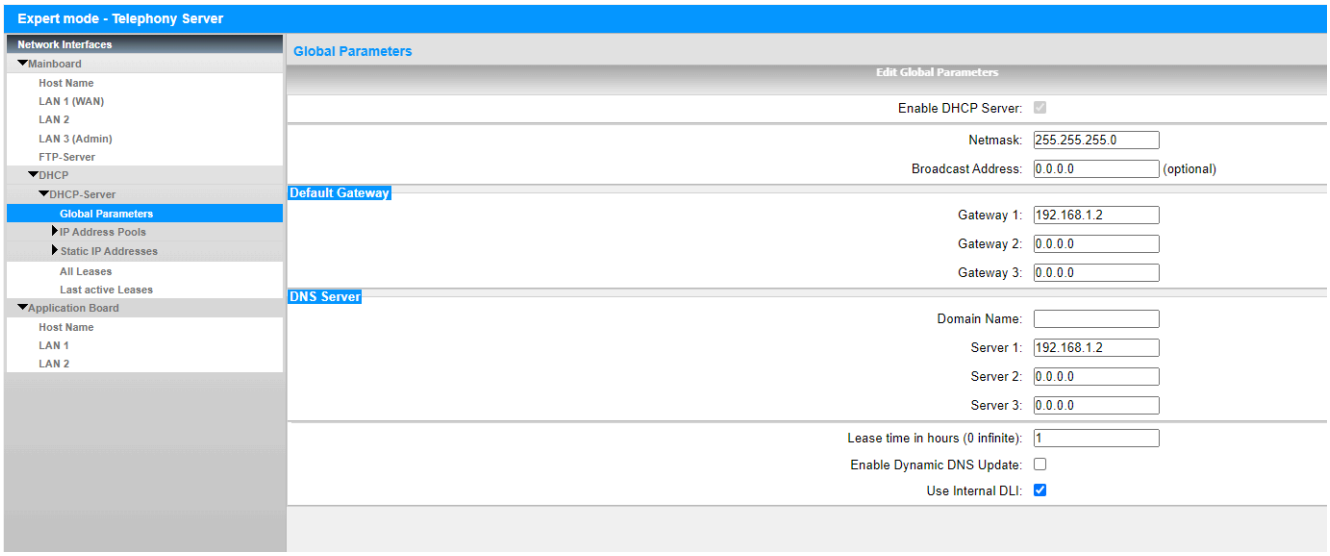
Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Netzwerkschnittstellen**.

3) Navigieren Sie im Menübaum zu **Mainboard** > **DHCP** > **DHCP-Server** > **Globale Einstellungen**. Das Fenster **Globale Parameter ändern** wird angezeigt.



4) Aktivieren Sie das Kontrollkästchen **Internes DLI verwenden**. Das Kontrollkästchen ist standardmäßig aktiviert.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

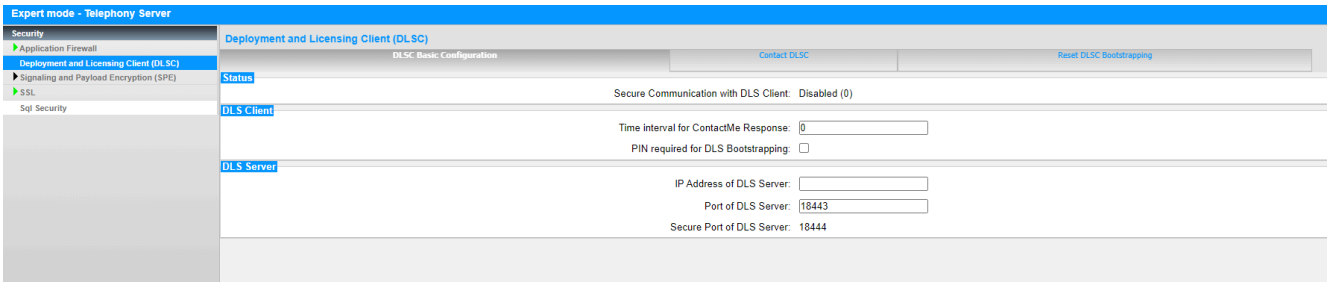
9.5.3 Wie Sie das Kommunikationssystem als Deployment und Licensing Client konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Klicken Sie im Menübaum auf **Deployment- und Licensing-Client (DLSC)**.



4) Geben Sie in der Registerkarte **DLSC Grundeinstellung** im Bereich **DLS-Server** im Feld **IP-Adresse des DLS-Servers** die IP-Adresse ein, unter der der externe DLS-Server zu erreichen ist.
5) Ändern Sie falls nötig unter **Port des DLS-Servers** den Port, den der DLS-Server nutzt. Die beiden angezeigten Ports müssen in der Firewall freigegeben sein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10 Anbindung an Service-Provider

Das Kommunikationssystem unterstützt die Anbindung an öffentliche Kommunikationsnetze. Die Anbindung an das IP-Netz bietet den Zugang zum Internet und zur Internet-Telefonie, der Amtszugang bietet Zugang zum ISDN-Netz und zum analogen Netz.

Der Zugang zum Internet erfolgt entweder über ein Internet-Modem oder über einen Internet-Router.

Der ISDN-Amtszugang erfolgt bei den Hardware-Plattformen über das Mainboard oder über zusätzlich steckbare Baugruppen. Beim Softswitch ist ein ISDN-Amtszugang nicht möglich.

Der analoge Amtszugang benötigt bei den Hardware-Plattformen eine zusätzlich steckbare Baugruppe. Beim Softswitch ist ein analoger Amtszugang nicht möglich.

10.1 Internetzugang

Für den Zugang zum Internet ist eine Breitbandverbindung (DSL-Anschluss oder Kabelanschluss) nötig. Damit ist eine schnelle Datenübertragung im Rahmen der verfügbaren Bandbreite möglich.

Internet-Zugang über DSL-Anschluss

Die Breitbandverbindung zum Internet über DSL (Digital Subscriber Line) erfolgt über die herkömmliche Telefonleitung. Der Internet-Zugang kann parallel zum normalen Telefon genutzt werden. Fax, analoges Telefon oder ISDN stehen auch während der DSL-Verbindung zur Verfügung. Somit lässt sich ein Internet-Zugang realisieren, der wie bei einer Standleitung ständig verfügbar ist (Flatrate).

Für einen Internet-Zugang über DSL benötigen Sie einen Telefonanschluss (analog oder ISDN) und einen Internet-Service-Provider (ISP). Der ISP stellt einen Splitter und ein Internet-Modem (DSL-Modem) bzw. einen Internet-Router mit eingebautem Internet-Modem zur Verfügung. Der Splitter teilt das Signal in die DSL- und Telefonie-Anteile auf und gibt die DSL-Signale an das Internet-Modem weiter.

Das Kommunikationssystem kann direkt an das Internet-Modem oder an den Internet-Router mit integriertem Internet-Modem angeschlossen werden. Im ersten Fall müssen die Zugangsdaten des ISP im Kommunikationssystem eingegeben werden, im zweiten Fall muss dem Kommunikationssystem der Internet-Router bekannt gegeben werden. Die Zugangsdaten des ISP sind im Internet-Router gespeichert.

Um Internet-Telefonie nutzen zu können, benötigen Sie zusätzlich einen Internet-Telefonie-Service-Provider (ITSP, SIP-Provider).

Internet-Zugang über Kabel-Anschluss

Die Breitbandverbindung zum Internet über Kabel erfolgt über den TV-Kabelanschluss. Zusätzlich zur Übertragung der TV-Signale kann der TV-Kabelanschluss für den Zugang zum Internet und zum Telefonieren genutzt werden. Somit ist Surfen und Telefonieren ohne Telefonleitung möglich.

Für einen Internet-Zugang über Kabel benötigen Sie einen Kabelbetreiber, der dieses Leistungsmerkmal anbietet. Er ist zugleich auch Ihr Internet-Service-Provider (ISP). Dieser Kabelbetreiber stellt Ihnen einen Kabelanschluss mit einem Rückkanal und ein Kabelmodem zur Verfügung, das die Daten über das TV-Kabelnetz überträgt. An das Kabelmodem wird der Kabelanschluss und das Kommunikationssystem über Ethernet angeschlossen. Das Herausfiltern der Internetdaten wird im Kabelmodem selbst vorgenommen.

Das Kommunikationssystem kann direkt an das Kabel-Modem angeschlossen werden oder an einen Internet-Router, der wiederum an das Kabelmodem angeschlossen ist. In beiden Fällen muss dem Kommunikationssystem das Kabelmodem oder der Internet-Router bekannt gegeben werden.

Um Internet-Telefonie nutzen zu können, benötigen Sie zusätzlich einen Internet-Telefonie-Service-Provider (ITSP, SIP-Provider).

Konfiguration des Internet-Zugangs

Die Konfiguration des Internet-Zugangs im WBM ist davon abhängig, ob der Internet-Zugang bereits in einem externen Router eingerichtet ist oder ob er über ein Internet-Modem erfolgt und somit im WBM eingerichtet werden muss.

- **Internet-Zugang über ein Internet-Modem** (**DSL am WAN Port direkt**)

  Sie wollen das Kommunikationssystem direkt an einem Internet-Modem (DSL, Kabel, UMTS ...) betreiben. OpenScape Business hat den Internet-Router integriert. Geben Sie die Zugangsdaten des Internet-Service-Providers (ISP) direkt im Kommunikationssystem ein und nutzen den WAN-Anschluss des Kommunikationssystems. Diese Möglichkeit besteht nicht beim Softswitch.

  Sie haben folgende Möglichkeiten:

  – Internet-Zugang über vorkonfigurierten ISP
  – Internet-Zugang über Standard-ISP PPPoE
  – Internet-Zugang über Standard-ISP PPTP

  Ist Ihr ISP nicht unter den vorkonfigurierten ISP, verwenden Sie den Standard-ISP PPPoE oder PPTP.

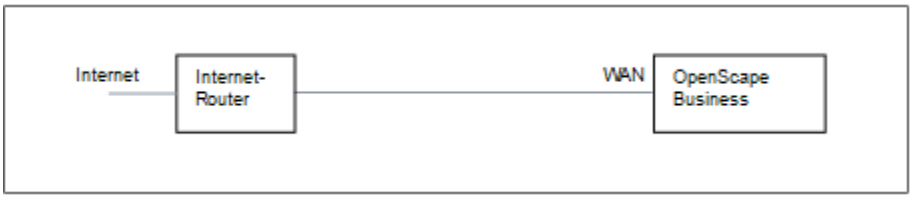
- **Internet-Zugang über einen externen Internet-Router**

  Sie wollen das Kommunikationssystem an einem externen Internet-Router betreiben. Der Internet-Service-Provider ist bereits im Internet-Router konfiguriert.

  Sie haben folgende Möglichkeiten:

  – **Internet-Zugang über externen Internet-Router am WAN-Anschluss**

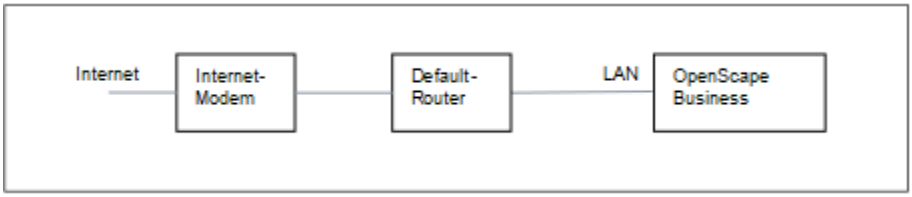
    (**TCP/IP am WAN Port über einen externen Router**)



    Dazu nutzen Sie den WAN-Anschluss des Kommunikationssystems. OpenScape Business kennt entweder den Internet-Router oder arbeitet als DHCP-Client. Diese Möglichkeit kann verwendet werden, wenn der Internet-Router in einem anderen Netzsegment liegt und einen eigenen DHCP-Server hat.

  – **Internet-Zugang über externen Internet-Router am LAN-Anschluss**

    (**TCP/IP am LAN Port über einen externen Router**)



    Dazu nutzen Sie den LAN-Anschluss des Kommunikationssystems. OpenScape Business kennt nur den Default-Router und nicht die dahinterliegende Infrastruktur. Um die Verbindung zum Internet-Router zu aktivieren, muss dem Kommunikationssystem die IP-Adresse des Default-Routers und des DNS-Servers bekannt gegeben werden.

- **Internet-Zugang deaktivieren** (Standardeinstellung)

  Sie wollen das Internet nicht nutzen. Dann lassen Sie den Internet-Zugang deaktiviert.

10.1.1 Internet-Zugang über einen externen Internet-Router

Mit dem Wizard **Internet-Konfiguration** richten Sie Ihren Internet-Zugang über einen zusätzlichen Internet-Router ein.

Um den Internet-Zugang einzurichten, haben Sie folgende Möglichkeiten:

- **Internet-Zugang über externen Internet-Router am LAN-Anschluss**

  Dazu nutzen Sie den LAN-Anschluss des Kommunikationssystems.
  Um die Verbindung zum Internet-Router zu aktivieren, muss dem Kommunikationssystem die IP-Adresse des Default-Routers und des DNS-Servers bekannt gegeben werden.

- **Internet-Zugang über externen Internet-Router am WAN-Anschluss**

  Dazu nutzen Sie den WAN-Anschluss des Kommunikationssystems. Diese Möglichkeit kann verwendet werden, wenn der Internet-Router in einem anderen Netzsegment liegt und einen eigenen DHCP-Server hat.

10.1.1.1 Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie den Internet-Zugang konfigurieren, wenn das Kommunikationssystem hinter einem zusätzlichen Internet-Router betrieben wird. Kommunikationssystem und der Internet-Router befinden sich im gleichen LAN-Segment. Dazu müssen Sie die IP-Adresse des Internet-Routers und des DNS-Servers eingeben.

Voraussetzungen

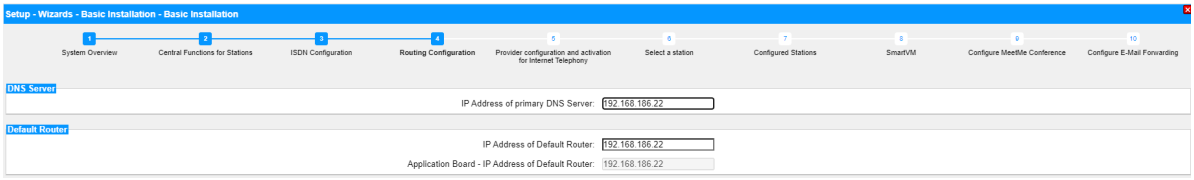
Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Für OpenScape Business X: das Kommunikationssystem ist über die Schnittstelle "LAN" mit dem Kunden-Netz verbunden. Die Verbindung darf nicht über die Schnittstelle "WAN" erfolgen.

Für OpenScape Business S: der Linux-Server ist über die LAN-Schnittstelle der Netzwerkkarte mit dem Kunden-Netz verbunden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.
4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
5) Aktivieren Sie das Optionsfeld **TCP/IP am LAN Port über einen externen Router** und klicken Sie auf **OK & Weiter**.



6) Geben Sie im Feld **IP-Adresse des DNS-Servers** die IP-Adresse des lokalen DNS-Servers (z.B. Internet-Router) oder des Internet-DNS-Servers (z.B. für Internet-Telefonie) ein.
7) Geben Sie im Feld **IP-Adresse des Default Routers** die IP-Adresse des externen Internet-Routers ein.
8) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.1.1.2 Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie den Internet-Zugang konfigurieren, wenn das Kommunikationssystem hinter einem zusätzlichen Internet-Router betrieben wird. Kommunikationssystem und Internet-Router müssen sich nicht im gleichen LAN-Segment befinden.

Voraussetzungen

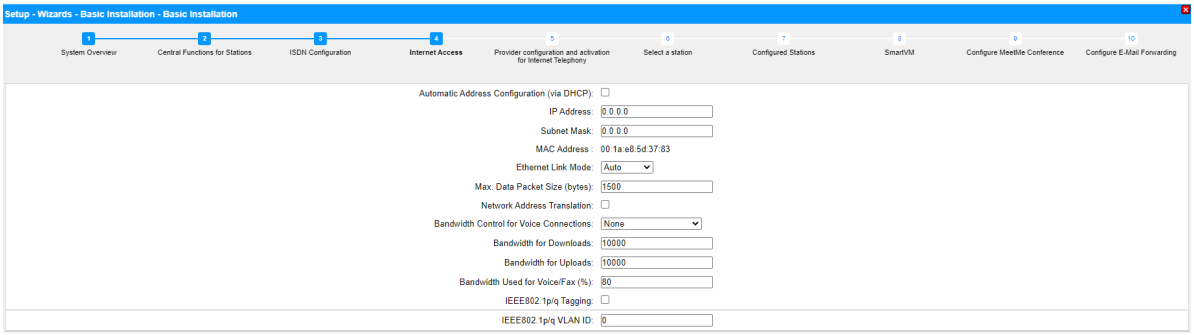
Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Das Kommunikationssystem muss über die Schnittstelle "WAN" mit dem LAN-Segment des Kundennetzes verbunden sein, indem sich der Internet-Router befindet.

Sie befinden sich im Fenster **Konfiguration des Internetzugangs**.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.
4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
5) Aktivieren Sie das Optionsfeld **TCP/IP am WAN Port über einen externen Router** und klicken Sie auf **OK & Weiter**.



6) Wenn für die WAN-Schnittstelle die netzwerkspezifischen Daten von einem bereits aktiven DHCP-Server bezogen werden sollen:
   a) Aktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.
   b) Aktivieren Sie das Kontrollkästchen **IP-Adresse des Default Routers übernehmen**.
   c) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des DNS-Servers übernehmen**.
   d) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des SNTP-Servers übernehmen**.
7) Wenn der WAN-Schnittstelle eine feste IP-Adresse zugeordnet werden soll:
   a) Deaktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.
   b) Geben Sie die gewünschte **IP-Adresse** und **Netzmaske** der WAN-Schnittstelle ein.
8) Aktivieren Sie das Kontrollkästchen **Netzwerkaddressübersetzung (NAT)**.

9) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Bei einer hohen Download-Bandbreite und zugleich niedrigen Upload-Bandbreite sollte die Bandbreitensteuerung nur für den Upload aktiviert werden, damit nicht unnötig viel Download-Bandbreite für die Sprachübertragung reserviert wird.

10) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download und Upload ein, die Ihnen Ihr Internet-Service-Provider zur Verfügung stellt.

11) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.1.1.3 Konfigurieren des Internetzugriffs über einen externen Internetrouter über das LAN mit dem für ITSP dedizierten WAN-Port

Voraussetzungen

Sie haben im SLES eine neue Netzwerkschnittstelle erstellt.

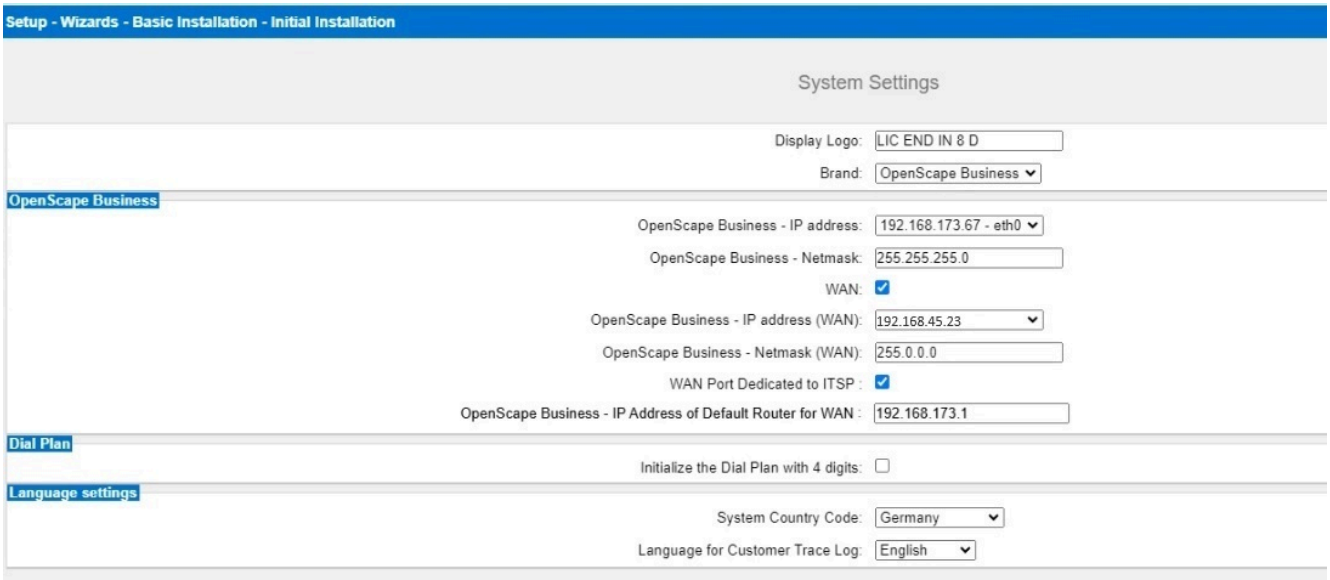
Sie befinden sich im Fenster **Systemeinstellungen** des Assistenten für die **Erstinstallation**.

Bitte beachten Sie, dass diese Funktion nur für ITSPs, die in den Anbieter-Einstellungen nicht STUN verwenden müssen, gilt.

Schritt für Schritt

1) Aktivieren Sie das Kontrollkästchen **WAN** und wählen Sie die entsprechende Netzwerkschnittstelle aus.
   Die Option **WAN-Schnittstelle für ITSP** wird verfügbar.

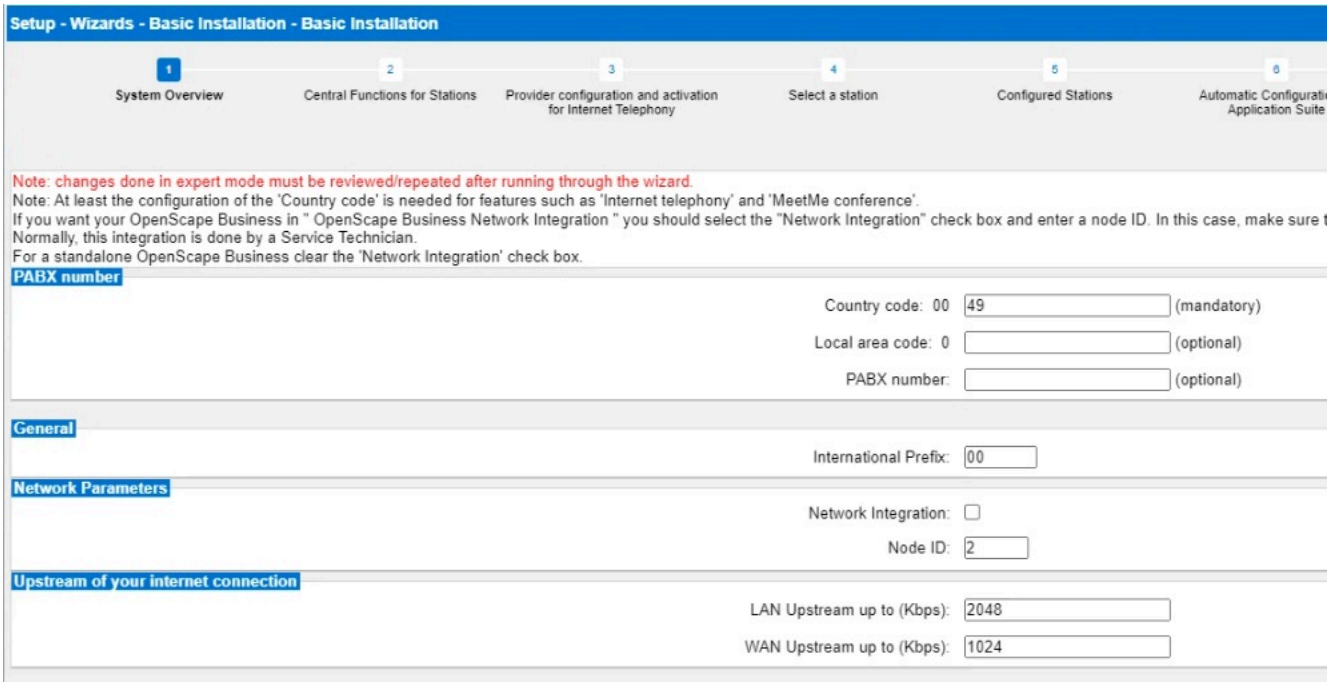
2) Klicken Sie, um die **WAN-Schnittstelle für ITSP** zu aktivieren.



3) Klicken Sie auf **OK & Weiter**.

4) Navigieren Sie zu **Setup > Basisinstallation** und führen Sie den Assistenten für **Basisinstallation** aus.

5) Konfigurieren Sie die maximalen Upstream-Werte in den entsprechenden Feldern **LAN Upstream bis zu (Kbps)** und **WAN Upstream bis zu (Kbps)**.



6) Klicken Sie auf **OK & Weiter**.

7) Nach dem Anwenden der Konfiguration ist ein Neustart des Systems erforderlich.

10.1.2 Internet-Zugang über Internet-Modem

Mit dem Wizard **Internet-Konfiguration** richten Sie Ihren Internet-Zugang über ein Internet-Modem ein. Dazu wird der WAN-Anschluss des Kommunikationssystems direkt an ein Internet-Modem angeschlossen. Sie können einen im Kommunikationssystem vorkonfigurierten ISP oder einen Standard-ISP-Typ (Typ ist vom ISP zu erfragen) verwenden.

Um den Internet-Zugang einzurichten, haben Sie folgende Möglichkeiten:

- **Internet-Zugang über vorkonfigurierten ISP einrichten**

  Sie nutzen einen im Kommunikationssystem vorkonfigurierten ISP. Dann können Sie aus einer Liste Ihren vorkonfigurierten ISP auswählen.
- **Internet-Zugang über Standard-ISP PPPoE einrichten**

  Sie nutzen den Standard-ISP-Typ **Provider PPPoE**. Erfragen Sie die notwendigen Einstellungen von Ihrem ISP.
- **Internet-Zugang über Standard-ISP PPTP einrichten**

  Sie nutzen den Standard-ISP-Typ Provider **Provider PPTP**. Erfragen Sie die notwendigen Einstellungen von Ihrem ISP.

Verbindungstrennung in Abhängigkeit vom Tarifmodell

Abhängig vom Tarifmodell kann definiert werden, ob die Verbindung zum ISP bei Inaktivität aufrechterhalten werden soll oder nicht.

- Bei dem Tarifmodell Flatrate muss bei Inaktivität keine Trennung der Internet-Verbindung erfolgen. Viele ISP fordern alle 24 Stunden eine Zwangstrennung. Der Zeitpunkt, zu der die Verbindung getrennt werden soll, kann angegeben werden.
- Bei dem Tarifmodell Zeittarif soll die Internet-Verbindung bei Inaktivität getrennt werden. Die Zeitdauer der Inaktivität, nach der die Verbindung getrennt werden soll (z.B. 60 Sekunden) kann angegeben werden. Bei der nächsten Internet-Anforderung wird die Verbindung automatisch wieder aufgebaut. Ist VPN konfiguriert, darf die Verbindung nicht bei Inaktivität getrennt werden - hier sollte das Tarifmodell Flatrate gewählt werden.

Anmerkung: Programme oder Dienste im Netzwerk können automatisch eine Internet-Verbindung aufbauen und Ihnen dadurch bei einem Zeittarif zusätzliche Verbindungskosten verursachen.

Bandbreite

Der ISP stellt für den Download und den Upload von Daten unterschiedliche Bandbreiten zur Verfügung. Die Bandbreite wird in kbit/s angegeben. Wird zusätzlich Internet-Telefonie genutzt, teilen sich Sprachübertragung und Datenübertragung die Bandbreite. Deshalb ist es sinnvoll, für eine gute Sprachqualität der Sprachübertragung eine ausreichend hohe Bandbreite zu reservieren. Allerdings kann dies bei intensiver Sprachübertragung zu Engpässen bei der Datenübertragung (z.B. langsamere Downloads) führen.

Sie können wählen, ob die Bandbreitensteuerung für Sprachverbindungen nur für den Upload aktiv sein soll oder für Upload und Download zusammen. Bei einer hohen Download-Bandbreite und zugleich niedrigen Upload-Bandbreite sollte die Bandbreitensteuerung nur für den Upload aktiviert werden, damit nicht unnötig viel Download-Bandbreite für die Sprachübertragung reserviert wird.

Anmerkung: Für ein Internet-Gespräch werden ca. 128 kbit/s Bandbreite reserviert.

10.1.2.1 Wie Sie den Internet-Zugang über einen vorkonfigurierten ISP konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie Ihren Internet-Zugang über einen im Kommunikationssystem vorkonfigurierten Internet-Service-Provider (ISP) konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Internet-Zugangsdaten Ihres ISP liegen Ihnen vor (z.B. Benutzerkennung, Passwort).

Schritt für Schritt

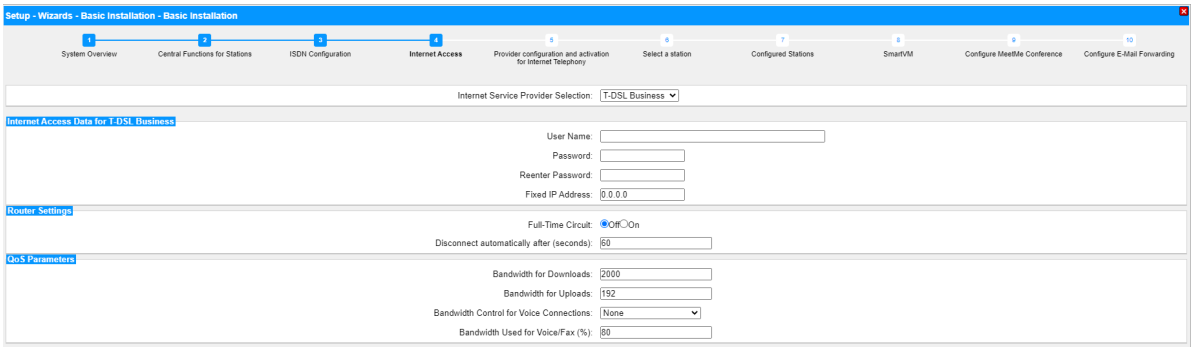
1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

5) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.



6) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** Ihren ISP aus.

7) Geben Sie im Bereich **Internet-Zugangsdaten für...** die Zugangsdaten ein, die Sie von ihrem ISP bekommen haben. Die Felder in diesem Bereich sind providerabhängig. Achten Sie bei der Eingabe der Daten auf korrekte Groß- und Kleinschreibung.

8) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:

   - Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z.B. 04:59).
   - Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z.B. 60 Sekunden).

9) Stellen Sie im Bereich **QoS-Parameter** die folgenden Werte ein:

   a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

   b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

10) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

11) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.

   a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).

   b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist

abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.
d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z.B. myhost. Ihr vollständiger Domänenname lautet dann z.B. myhost.dyndns.org.
e) Testen Sie den DynDNS-Account mit **Verbindung testen**.
f) Klicken Sie nach erfolgreichem Test auf **OK**.
g) Klicken Sie auf **OK & Weiter**.

12) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

13) Klicken Sie auf **Beenden**. Das Kommunikationssystem führt einen Neustart durch.

10.1.2.2 Wie Sie den Internet-Zugang über einen Standard-ISP PPPoE konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie Ihren Internet-Zugang über den Standard-Internet-Service-Provider PPPoE konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feldname	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmode	Authentifizierungsmodus für die PPP-Verbindung über PAP: **PAP-Client**, **PAP-Host** oder **Nicht verwendet**.	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmode	Authentifizierungsmodus für PPP-Verbindung über CHAP: **CHAP-Client**, **CHAP-Host**, **CHAP-Client und -Host** oder **Nicht verwendet**.	

Feldname	Beschreibung	Wert vom ISP
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.
4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
5) Aktivieren Sie das Optionsfeld **DSL am WAN-Port direkt** und klicken Sie auf **OK & Weiter**.
6) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPPoE** aus.
7) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.
8) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:
   - Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).
   - Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).
9) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.
   - Authentifizierung durch den ISP erforderlich: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Der gebräuchliche Standard ist der Authentifizierungsmode **CHAP-Client**.
   - Keine Authentifizierung durch den ISP erforderlich: Stellen Sie sicher, dass das Kontrollkästchen PPP-Authentifizierung deaktiviert ist.
10) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

11) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:
   a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.
   b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)**in Prozent an, wie viel Bandbreite für Sprach- und Faxverbindungen als Prozentwert reserviert werden soll (Standardwert: 80%).
12) Klicken Sie auf **OK& Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.
13) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.
   a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).
   b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

      `http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
   c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.
   d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z.B. myhost.dyndns.org.
   e) Testen Sie den DynDNS-Account mit **Verbindung testen**.
   f) Klicken Sie nach erfolgreichem Test auf **OK**.
   g) Klicken Sie auf **OK& Weiter**.
14) Wenn Sie eine statische öffentliche IP-Adresse haben oder kein VPN oder keinen Fernzugriff verwenden möchten, klicken Sie auf **Kein DynDNS**.
15) Klicken Sie auf **Fertig**.

10.1.2.3 Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie Ihren Internet-Zugang über den Standard-Internet-Service-Provider PPTP konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feldname	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		

Feldname	Beschreibung	Wert vom ISP
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
PPTP-Parameter		
Lokale IP-Adresse der Kontrollverbindung	IP-Adresse, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 10.0.0.140.	
Partner-IP-Adresse der Kontrollverbindung	IP-Adresse des ISP-Servers für die PPTP-Verbindung. Der voreingestellte Wert lautet 10.0.0.138.	
Partner-Netzmaske für die Kontrollverbindung	Netzmaske, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 255.255.255.248.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über PAP: **PAP-Client**, **PAP-Host** oder **nicht benutzt**.	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über CHAP: **CHAP-Client**, **CHAP-Host**, **CHAP-Client und -Host** oder **nicht benutzt**.	
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

5) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.

6) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPTP** aus.

7) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.

8) Geben Sie in dem Bereich **PPTP-Parameter** die Werte ein, die Sie von Ihrem ISP bekommen haben.

9) Wenn Sie als Tarifmodell einen Zeittarif haben, aktivieren Sie das Kontrollkästchen **Short-Hold-Modus**. Geben Sie im Feld **Short-Hold-Zeit (s)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z.B. 60 Sekunden).

10) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.

- Authentifizierung wird vom ISP gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Treffen Sie die PAP- und CHAP-Einstellungen, wie Sie sie von Ihrem ISP zugeteilt bekommen haben.
- Authentifizierung wird vom ISP nicht gefordert: Stellen Sie sicher, dass das Kontrollkästchen PPP-Authentifizierung deaktiviert ist.

11) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

12) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:

a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

13) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

14) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.

a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).

b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen

Benutzerdefinierte Domäne. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.
d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z.B. myhost.dyndns.org.
e) Testen Sie den DynDNS-Account mit **Verbindung testen**.
f) Klicken Sie nach erfolgreichem Test auf **OK**.
g) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

16) Klicken Sie auf **Fertig**. Das Kommunikationssystem führt einen Neustart durch.

10.1.3 WAN-Schnittstelle

WANs (**W**ide **A**rea **N**etwork) werden benutzt, um verschiedene LANs (**L**ocal **A**rea **N**etwork), aber auch einzelne PC miteinander zu vernetzen. An die WAN-Schnittstelle kann ein Internet-Modem für den Zugang zum Internet angeschlossen werden.

Die WAN-Schnittstelle darf nicht für die Vernetzung von Netzwerk-Knoten und zum Anschluss von IP-Teilnehmern oder IP-Clients benutzt werden.

10.1.4 DynDNS

DynDNS (Dynamic Domain Name Service) ist ein Internetdienst, der einer sich dynamisch ändernde IP-Adresse einen festen DNS-Namen zuordnet.

OpenScape Business X stellt den DynDNS Service zur Verfügung, wenn ein Internet-Modem am WAN-Port von OpenScape Business X angeschlossen ist und das Kommunikationssystem als Internet-Router genutzt wird. Ist dies nicht der Fall, wird DynDNS im externen Internet-Router in der Infrastruktur des Kunden eingerichtet.

DNS-Name

Ein Client, der mit einer dynamischen IP-Adresse am Internet angeschlossen ist, kann mit Hilfe von DynDNS immer mit demselben Namen, dem DNS-Namen, angesprochen werden. Dazu ist ein DynDNS-Account bei einem DynDNS-Anbieter (z.B. www.dyndns.org) nötig. Wird dem Kommunikationssystem eine neue IP-Adresse zugewiesen (z.B. vom Internet-Service-Provider), wird diese IP-Adresse automatisch an den DynDNS-Anbieter gesendet und im DynDNS-Account gespeichert. Das Zeitintervall, in der diese Aktualisierung erfolgt, ist einstellbar. Wird ein DNS-Name angesprochen, wird er über eine Anfrage beim DynDNS-Anbieter in die momentan gültige IP-Adresse aufgelöst. Der komplette DNS-Name (auch Domänenname

genannt) setzt sich aus dem frei wählbaren Hostnamen (z.B. myhost) und dem ausgewählten DynDNS-Anbieter (z.B. dyndns.org) zusammen, z.B. myhost.dyndns.org. Nähere Informationen finden Sie z.B. unter der Internet-Adresse:

`http://www.dyndns.org/services/dyndns`

Mit DynDNS ist es auch möglich, ein virtuelles privates Netzwerk (VPN) über einen Internet-Service-Provider aufzubauen, der dynamische IP-Adressen liefert. So können z.B. Teleworker über das Internet auf das interne Netz zugreifen. Weitere Informationen finden Sie unter Virtual Private Network VPN .

Mail Exchanger

Der Mail-Exchange-Eintrag (MX-Record) gibt innerhalb des Domain Name Service (DNS) an, zu welcher IP-Adresse E-Mails für den eingerichteten Domänennamen (z.B. myhost.dyndns.org) zu schicken sind. Hinter der angegebenen IP-Adresse muss sich ein Mail-Server (Mail-Exchanger) befinden. Eine E-Mail-Adresse für diesen Domänennamen könnte z.B. folgendermaßen aussehen: mymail@myhost.dyndns.org.

Mit der Funktion Backup MX werden E-Mails, die nicht an den oben eingetragenen Mail-Exchanger zugestellt werden können (weil dieser z.B. temporär nicht verfügbar ist), zwischengespeichert und zugestellt, sobald der Mail-Exchanger wieder verfügbar ist.

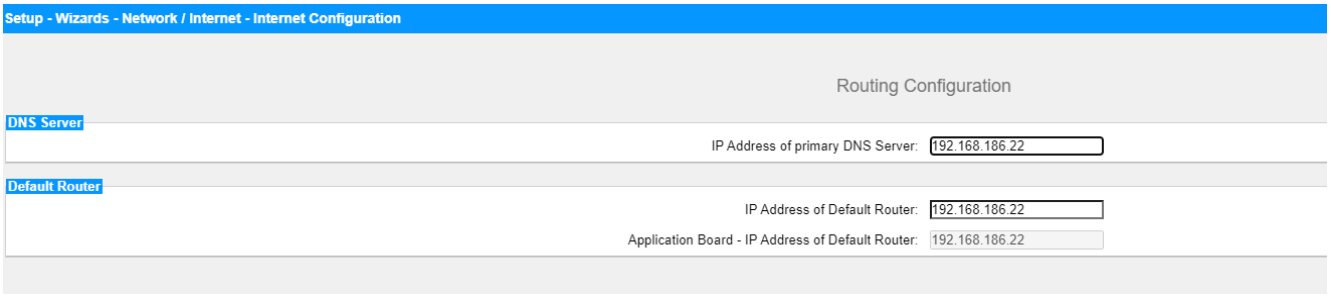
10.1.4.1 Wie Sie den DynDNS-Service konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **DynDNS**.
4) Klicken Sie auf **Aktualisierungszeit der DNS-Namen**.



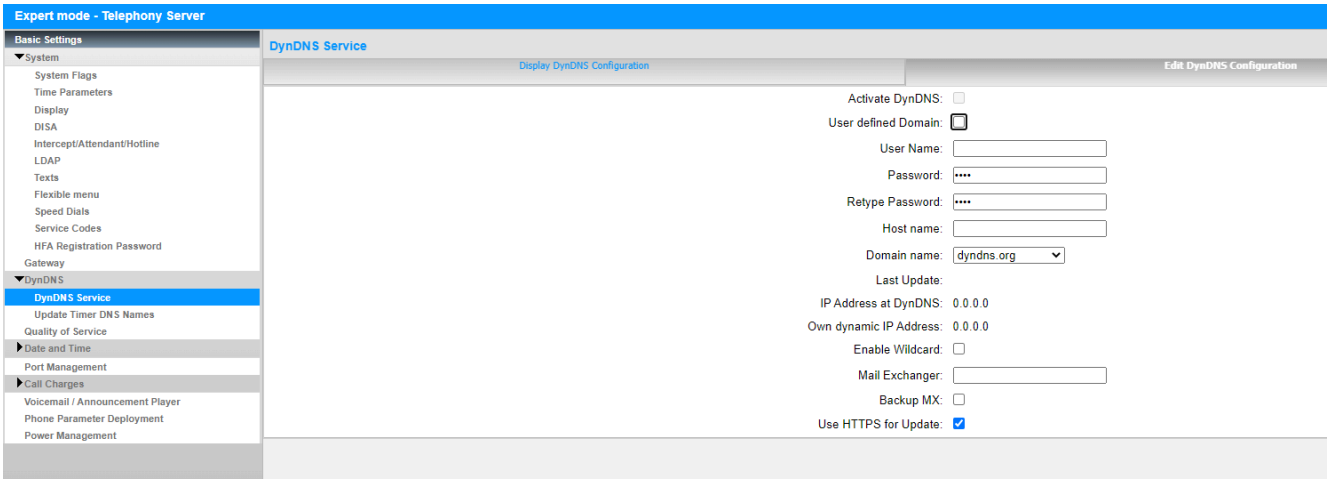
5) Aktivieren Sie das Optionsfeld **DNS-Namen aktualisieren**.
6) Dieser Timer-Wert gilt nur für VPN: Geben Sie im Feld **Timer-Wert für Aktualisierung der DNS-Namen** (s) die Zeit in Sekunden ein, nach der die VPN-Komponente überprüft, ob sich eventuell verwendete DNS-Namen in der VPN-Konfiguration zu neuen IP-Adressen auflösen (VPN

mit dynamischen IP-Adressen). In dem Fall wird VPN mit den neuen IP-Adressen rekonfiguriert.

Das Feld ist mit `180` vorbelegt, was einem Aktualisierungsintervall von 3 Minuten entspricht.

7) Klicken Sie im Menübaum auf **DynDNS Service**.

8) Klicken Sie auf die Registerkarte **DynDNS Konfiguration ändern**.



9) Aktivieren Sie das Kontrollkästchen **DynDNS aktivieren**.

10) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).

11) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

Beispiel einer Update-URL mit Base64 verschlüsselter Authentifizierung:

`https://<b64><`*`username`*`>:<`*`pass`*`></b64>@members.dyndns.org/nic/update?hostname=<`*`domain`*`>&myip=<`*`ipaddr`*`>&wildcard=NOCHG&mx=NOCHG&backmx=NOC`

<b64>...</b64> für Base64 codierte Parameter

12) Geben Sie im Feld **Benutzername** den Benutzernamen für Ihren DynDNS-Account beim DynDNS-Anbieter ein.

13) Geben Sie in den Feldern **Kennwort** und **Kennwort wiederholen** das Kennwort Ihres DynDNS-Accounts beim DynDNS-Anbieter ein.

14) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z.B. myhost.dyndns.org.

15) Nur sichtbar für DynDNS-Anbieter, die in der Aufklappliste **Domänenname** enthalten sind: Aktivieren Sie das Optionsfeld **Wildcard aktivieren**, wenn Sie möchten, dass auch Abfragen zu einem untergeordneten Domänennamen wie any.myhost.dyndns.org akzeptiert werden.

16) Nur sichtbar für DynDNS-Anbieter, die in der Aufklappliste **Domänenname** enthalten sind: Aktivieren Sie das Optionsfeld **HTTPS für die Aktualisierung verwenden**, wenn Sie eine sichere Verbindung zum DynDNS-Anbieter für die Aktualisierung der IP-Adresse verwenden möchten.
17) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

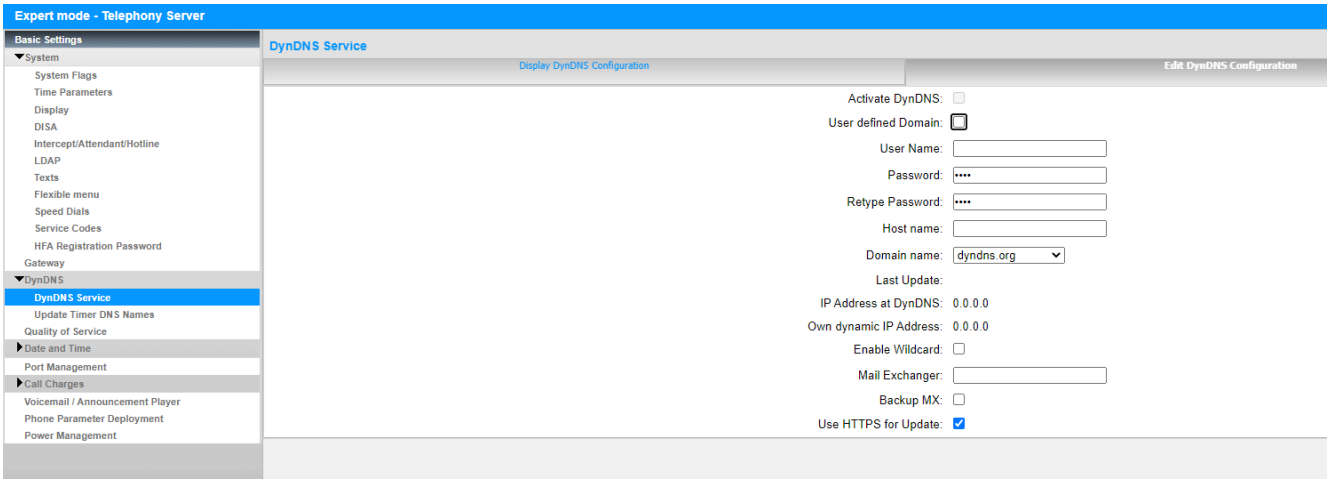
10.1.4.2 Wie Sie den Mail-Exchanger definieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **DynDNS**.
4) Klicken Sie auf **DynDNS Service**.
5) Klicken Sie auf die Registerkarte **DynDNS Konfiguration ändern**.



6) Geben Sie im Feld **Mail Exchanger** die IP-Adresse des Mail-Servers (Mail-Exchange-Eintrag bzw. MX-Record) ein.
7) Aktivieren Sie bei Bedarf das Optionsfeld **Backup MX**.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.2 Amtszugang über ITSP

Um über das Internet zu telefonieren zu können, benötigen Sie einen Zugang zu einem Internet-Telefonie-Service-Provider (ITSP, SIP-Provider). Dazu muss beim ITSP ein Internet-Telefonie-Anschluss und ein Benutzerkonto beantragt werden.

Verbindung zum ITSP

Das Kommunikationssystem nutzt die im Kapitel "Internet-Zugang" beschriebenen Möglichkeiten, den ITSP zu erreichen (OpenScape Business X: über LAN oder WAN / OpenScape Business S: ausschließlich über LAN).

Der ITSP-Zugang basiert auf SIP (Session Initiation Protocol) für die Signalisierung und auf RTP (Realtime Transport Protocol) für Sprache und Daten.

Internet-Telefonie-Service-Provider bieten nicht alle den gleichen Umfang von SIP-Leistungsmerkmalen. Daher sollten nur für das Kommunikationssystem zertifizierte ITSPs genutzt werden. Eine Liste mit den zertifizierten ITSPs sowie den Zertifizierungsprozess finden Sie unter folgendem Link:

`http://wiki.unify.com/wiki/Collaboration_with_VoIP_Providers`

Anmerkung: Sonderrufnummern und Notrufnummern, die vom ITSP nicht unterstützt werden, sollten über die Festnetzanschlüsse geführt werden.

Bei Ausfall des ITSP ist über Least Cost Routing (LCR) eine Rückfalllösung über die Festnetzanschlüsse möglich.

ITSP-Benutzerkonto

Das ITSP-Benutzerkonto (SIP User Account) wird beim ITSP beantragt. Der ITSP stellt dafür einen SIP-Registrar-Server zur Verfügung, an dem sich das Kommunikationssystem vorher anmelden muss (providerabhängig).

Anmerkung: Eine Registrierung ist nicht notwendig, wenn der ITSP statische IP-Authentifizierung oder VPN-Tunnels verwendet.

Mobile Extension (MEX)

Dieses Leistungsmerkmal wird von einigen Mobilfunkbetreibern in Verbindung mit dem Service MDA (Mobile Direct Access) angeboten. Damit können Mobiltelefone/Smartphones als interne Teilnehmer in ein Kommunikationssystem integriert werden.

Dieses Leistungsmerkmal ist nur mit einem Internet-Telefonie-Durchwahlanschluss nutzbar. Dafür muss bei der Konfiguration des ITSP die vom ITSP zur Verfügung gestellte MEX-Nummer eingetragen werden. Beim ITSP ist die Rufnummer des Mobiltelefons mit der MEX-Nummer verknüpft. Zusätzlich muss das Mobiltelefon/Smartphone im Kommunikationssystem als Mobility-Teilnehmer konfiguriert sein (siehe Konfiguration von myPortal to go und Mobility Entrys).

Kurzbeschreibung:

- Der Mobilfunkbetreiber bietet ein Flatrate-Angebot für das Mobiltelefon an.
- One Number Service: das Mobiltelefon ist unter einer einzigen Festnetzrufnummer erreichbar, die auch dem Gesprächspartner übermittelt wird.
- Der Anwesenheitsstatus und der Verbindungsstatus von Mobiltelefonen ist genauso wie für interne Teilnehmer sichtbar.
- Jedes Telefonat vom/zum Mobiltelefon wird ausschließlich über OpenScape Business in Kombination mit einem zertifizierten ITSP geführt.

- Die mobile Rufnummer des Mobiltelefons ist nach außen nicht bekannt, d.h. das Mobiltelefon kann nicht direkt angerufen werden. Es kann ebenfalls keine abgehenden, direkten Anrufe tätigen. Alle Rufe führen über OpenScape Business.
- Das Mobiltelefon kann in systeminterne Teams eingebunden werden.
- UC-Anwendungen, wie z. B. myPortal for Desktop und myPortal for Outlook, können wie für interne Teilnehmer genutzt werden.
- myPortal to go ist unterwegs nutzbar.
- Eingebundene Mobiltelefone identifizieren sich bei Anruf eines internen Teilnehmers mit ihrem Namen.
- Die Wahlbewertung und das Call-Routing im System bzw. im Netz erfolgt wie für jeden anderen internen Teilnehmer (z.B. erlaubte Rufnummern, verbotene Rufnummern, LCR-Regeln)
- Der ITSP nutzt eine spezielle Anrufsignalisierung von/zur OpenScape Business, die entspr. administriert werden muss.
- Jedes integrierte Mobiltelefon benötigt eine Mobility User Lizenz.
- Um UC-Anwendungen zu nutzen, ist zusätzlich eine UC Client Lizenz erforderlich.

10.2.1 Konfiguration eines ITSP

Es können vordefinierte und neue Internet-Telefonie-Service-Provider (ITSP) konfiguriert werden. Für jeden ITSP können Sie einen oder mehrere Accounts konfigurieren. Es können bis zu 8 ITSP gleichzeitig aktiv sein.

Weiterführende Informationen zu ITSP und deren Leistungsmerkmalen finden Sie hier:

`http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#Overview`

Anmerkung: Einrichtebeispiele finden Sie im Internet im **Unify Experts Wiki** unter *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Zuordnung der ITSP-Rufnummern

- Bei einem **Internet-Telefonie-Teilnehmeranschluss** stellt der ITSP Einzelrufnummern zur Verfügung, z.B. 70005555, 70005556, ... Diese Einzelrufnummern werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.
- Bei einem **Internet-Telefonie-Anlagenanschluss** stellt der ITSP ein Rufnummernband (Rufnummernbereich) zur Verfügung, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Bereich werden dann manuell als interne Rufnummern der Teilnehmer vergeben.

Die beiden Anschlussarten können kombiniert werden.

Alternativ können für beide Anschlussarten die ITSP-Rufnummern bei der Teilnehmer-Konfiguration als Durchwahlrufnummern der Teilnehmer eingetragen werden.

Interne Rufnummer	Name	Durchwahl
100	Andreas Richter	897007100

Interne Rufnummer	Name	Durchwahl
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Somit ergeben sich die ITSP-Rufnummern aus der eingerichteten Anlagenrufnummer (z.B. Länderkennzahl 49) und den eingetragenen Durchwahlnummern im Langformat. Das hat Vorteile bei der Wahlbewertung und dem Call-Management, auch in einem Netzverbund. So ist der ITSP-Anschluss z. B. durchwahlfähig zu einem anderen Knoten.

Ein weiterer Amtsanschluss über ISDN ist in diesem Fall nur eingeschränkt möglich.

Multisite-Management

Die Teilnehmer des Kommunikationssystems können unterschiedlichen Standorten (z.B. mit unterschiedlichen Ortsvorwahlen) zugewiesen werden. Jedem Standort ist eine Richtung und jeder Richtung ist eine ITSP-Registrierung zugeordnet. Es können max. 8 ITSP-Registrierungen verwaltet werden. Dabei ist eine Registrierung pro ITSP möglich oder auch mehrere Registrierungen an einem ITSP. Jeder ITSP-Registrierung kann eine Ortsvorwahl und anschließend mehrere Teilnehmer zugeordnet werden. Der Anschluss der Teilnehmer an den verschiedenen Standorten an das Kommunikationssystem erfolgt über VPN. Alle Standorte müssen sich innerhalb eines Landes befinden und die gleiche Amtskennzahl nutzen (siehe auch *Vernetzung von OpenScape Business in Hosting-Umgebungen*, Szenario 1b).

Verwenden von ITSP-Vorlagen

Standard ist es, eine vorkonfigurierte ITSP-Vorlage zu verwenden. Dazu werden in diese Vorlage die eigenen Zugangsdaten und Rufnummern eingetragen und diese anschließend aktiviert.

Im Experten-Modus können Sie auch eine vorkonfigurierte ITSP-Vorlage ändern und als neue Vorlage abspeichern.

Aktualisieren von ITSP-Vorlagen

Die vorkonfigurierten ITSP-Vorlagen werden nach einem Software-Update des Systems automatisch aktualisiert, sofern es in diesem Update neue vorkonfigurierte ITSP-Vorlagen gibt oder aktuellere Standard-Werte für bereits vorhandene vorkonfigurierte Vorlagen.

Ist der ITSP einer Vorlage bereits aktiviert, wird die Aktualisierung nicht automatisch durchgeführt, da bei der Aktualisierung der Standard-Werte wichtige Anpassungen überschrieben werden könnten. Deshalb kann die Aktualisierung bei Bedarf manuell über den Experten-Modus durchgeführt werden. Anschließend müssen die Standard-Werte wieder an die eigenen Belange angepasst werden.

Leitungsrichtung-Modus

Einzelne Leitungen einer ITSP-Leitung können für ausgehenden und/oder eingehenden Verkehr gesperrt werden. Die folgenden Leitungsrichtung-Modi sind möglich:

- nur gehend
- nur kommend
- Ausgehend und eingehend (Standard)

Die Leitungsrichtung wird ausgewertet, wenn das Kommunikationssystem eine ITSP-Leitung für einen ankommenden oder abgehenden Anruf reservieren muss.

10.2.1.1 Vordefinierten ITSP konfigurieren

Mit dem **Internettelefonie-Assistenten** können Sie einen vordefinierten Internet-Telefonie-Dienstanbieter (ITSP) konfigurieren und aktivieren. Die können für jedes ITSP ein oder mehrere Konten konfigurieren.

Voraussetzungen

Die Verbindung zum Internet ist betriebsbereit.

Die Zugangsdaten Ihres ITSP zur Internettelefonie sind verfügbar (z.B. Benutzerkonto, Passwort und Internettelefonnummer).

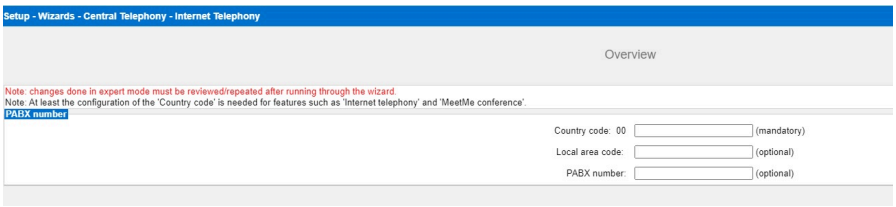
Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

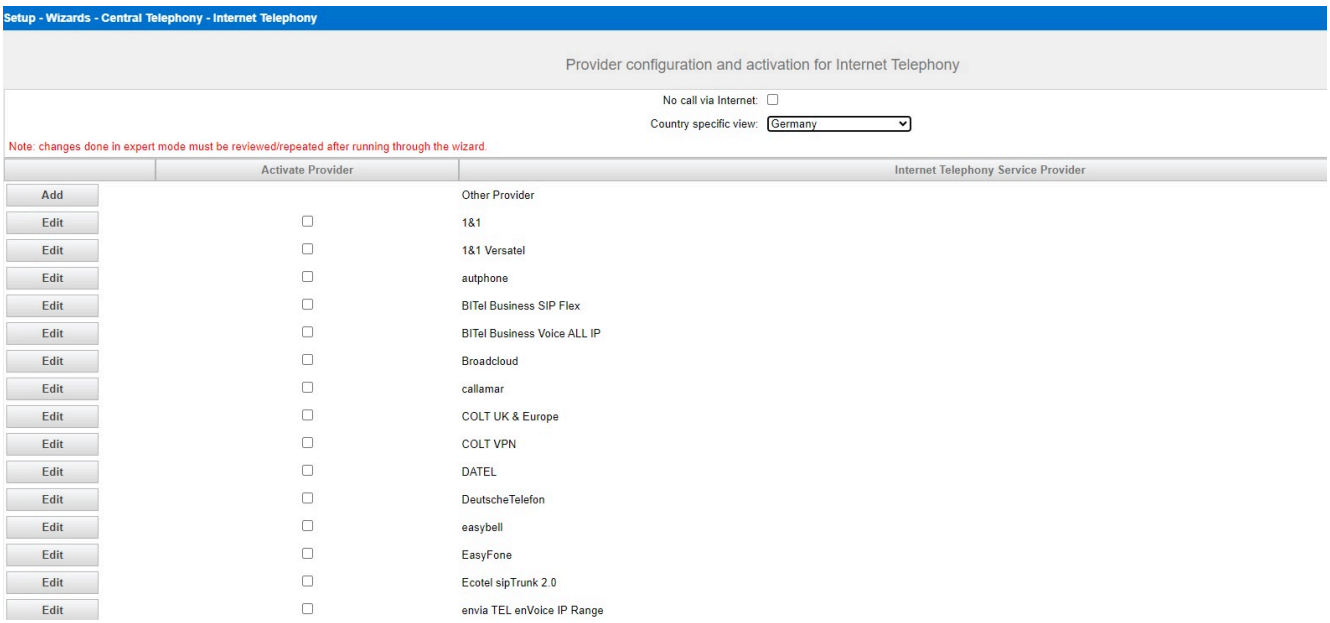
2) Klicken Sie im Navigationsbaum auf **Assistenten** > **Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um die **Internettelefonie-Assistenten** zu starten.



4) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt. Die

Liste enthält die vordefinierten ITSPs für das ausgewählte Land und die von Ihnen erstellten ITSPs.



5) Wenn Sie das voreingestellte Land ändern möchten, wählen Sie aus der Aufklappliste **Länderspezifische Ansicht** das gewünschte Land aus. Es werden die für das gewählte Land möglichen ITSP angezeigt.

6) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie 8 ITSP aktivieren. Klicken Sie anschließend auf **OK**.

7) Um den vordefinierten ITSP zu konfigurieren, klicken Sie in der mit dem gewünschten ITSP verbundenen Zeile auf **Bearbeiten**.

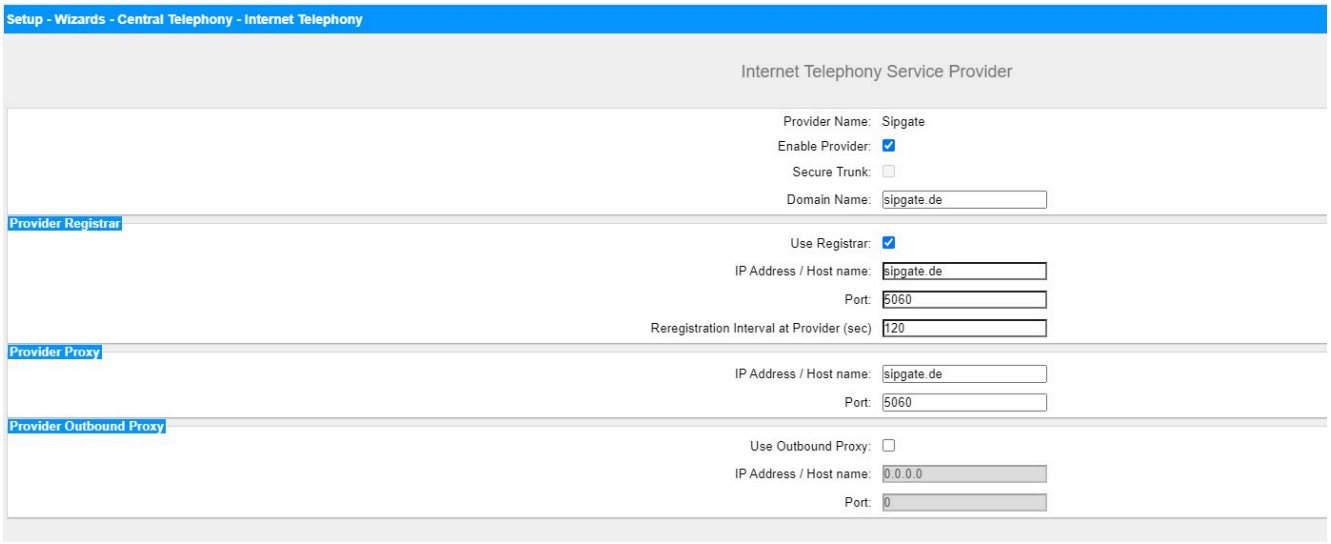
8) Aktivieren Sie das Kontrollkästchen **Provider aktivieren**.

9) Wenn der Anbieter eine sichere Verbindung unterstützt, kann das Kontrollkästchen **Secure Trunk** aktiviert werden.

10) Die Werte für "**Anbieter-Registrar**", "**Anbieter-Proxy**", "**Ausgehender Anbieter-Proxy**" und "**Anbieter-Merkmal**" (falls aktiviert) sind entsprechend den Anforderungen der meisten ITSPs vordefiniert. Für einige ITSPs werden kundenspezifische Server-Adressen verwendet. In diesem Fall müssen die nicht ausgegrauten Felder entsprechend der vom ITSP erhaltenen Dokumentation ausgefüllt werden.

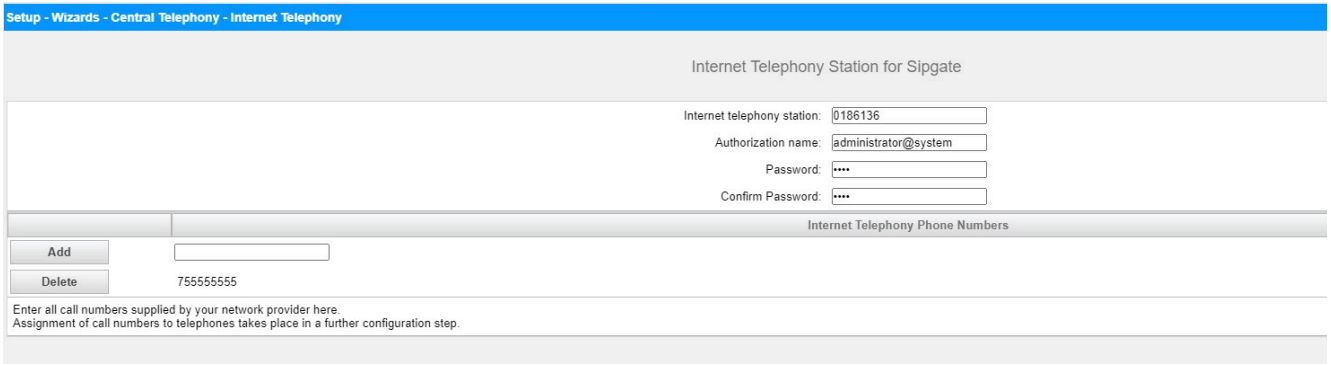
11) Wenn der Anbieter die Anrufumleitung unterstützt, wird der Abschnitt Anbieter-Merkmal angezeigt und Sie können die Anrufumleitung aktivieren. Wenn die Anrufumlenkung aktiviert ist, wird eine Anrufweiterleitung im

Anbieternetzwerk durchgeführt und die Anrufverwaltung im System ist nicht wirksam.



12) Klicken Sie auf **OK & Weiter**.

13) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.



14) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: SIP-Benutzer, SIP-ID usw.

    Weitere Details finden Sie unter http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

15) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen Autorisierungsnamen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

    Anmerkung: Wenn keine Registrierung verwendet ist, wird der **Autorisierungsname** ausgegraut und kann nicht konfiguriert werden.

16) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, dass Sie vom ITSP erhalten haben. Je nach ITSP

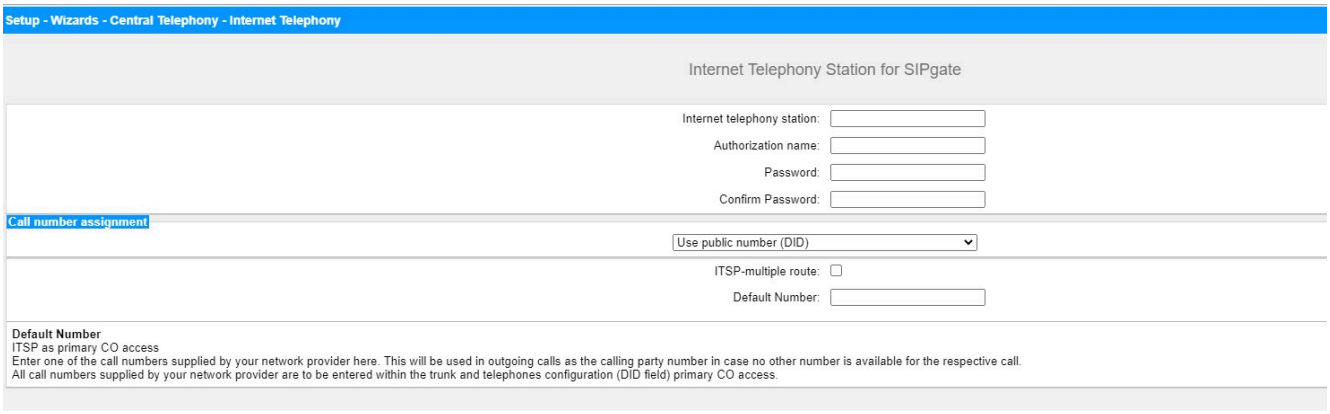
werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: Kennwort, SIP-Kennwort usw.

Anmerkung: Wenn keine Registrierung verwendet ist, wird das **Passwort** ausgegraut und kann nicht konfiguriert werden.

---

17) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

Öffentliche Nummer (DID) verwenden: Die Internettelefonie-Telefonnummern (DID) Ihrer Internettelefonie-Verbindung werden im Stationen-Setup (in den **DID-** Feldern) konfiguriert. Während der ITSP-Konfiguration ist keine Zuordnungskonfiguration erforderlich.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.

b) Unter **Standardnummer**, geben Sie die Telefonnummer, die für ausgehende Anrufe verwendet werden soll, wenn keine DID-Nummer des Anrufers verfügbar ist, ein.

c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern). Wenn Ihr ITSP das Merkmal "Mobile Extension (MEX)" nicht unterstützt, wird das Feld **MEX-Nummer** nicht angezeigt.

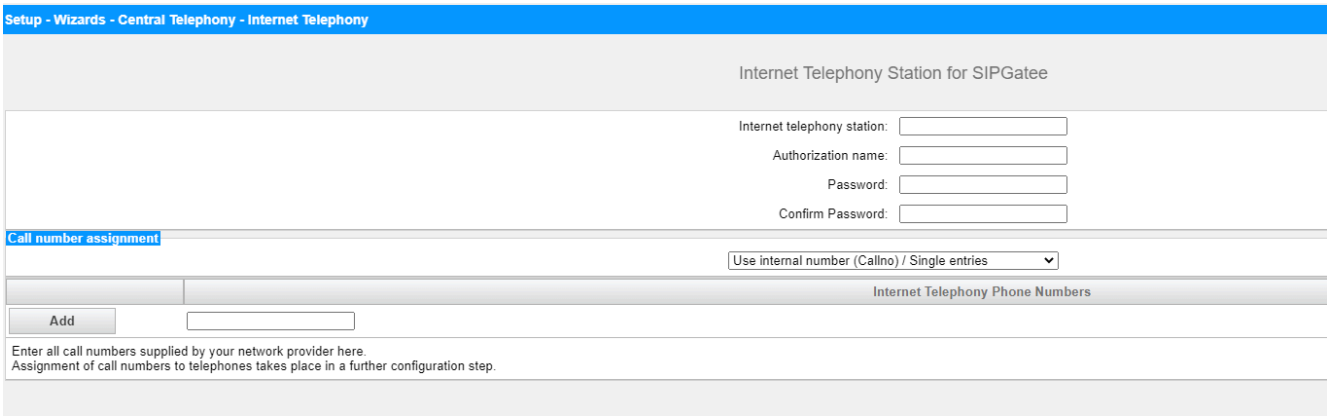
d) Wenn mehrere Routen konfiguriert werden müssen, aktivieren Sie das Kontrollkästchen **ITSP-mehrere Routen**.

e) Geben Sie die der Route zugewiesen **ITSP-Routenpräfixe** ein und klicken Sie auf **Hinzufügen**.

18) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

Interne Nummer (Rufnr.) verwenden / Einzeleinträge: Sie haben einen ITSP, der für jede Rufnummer SIP-Registrierung benötigt (z.B. 70005555, 70005556,...). Für jede Rufnummer muss eine Internettelefonie-Station erstellt und eine einzelne Rufnummer zugewiesen werden. Wenn Ihr ITSP

mehrere Rufnummern mit einer Registrierungsoption zulässt, sollte 1 verwendet werden.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.

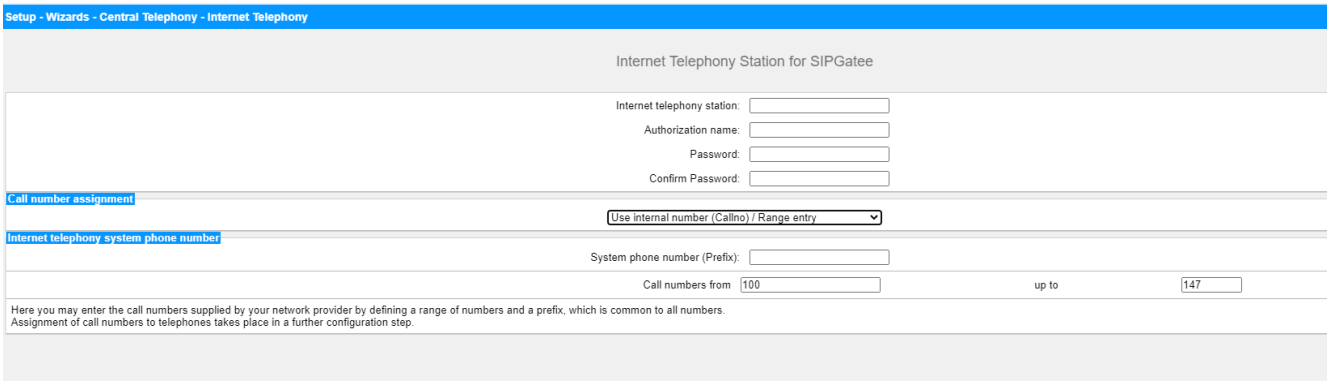
b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP mitgeteilten Internet-Telefonie-Teilnehmerrufnummern ein und klicken Sie auf **Hinzufügen**.

c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).

19) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:

Interne Rufnummer (Rufnummer) / Bereichseintrag verwenden: die Verwendung dieser Option ist veraltet, für die DID-Konfiguration sollte Option 1 verwendet werden.

Sie besitzen einen Internet-Telefonie-Anlagenanschluss und haben als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z.B. (+49) 89 7007-100 bis (+49) 89 7007-147. Sie weisen dann die Rufnummern aus dem Rufnummernbereich den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.

b) Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.

c) Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.

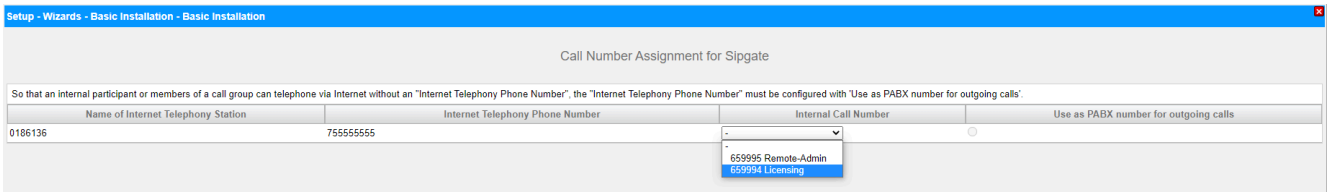
20) Klicken Sie auf **OK & Weiter**.

21) Wenn Sie zusätzliche Konten konfigurieren möchten, wiederholen Sie die Schritte 13 bis 20.

22) Klicken Sie auf **OK & Weiter**. Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.

23) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.

    Dieser Schritt entfällt, wenn Sie für die Zuordnung der Internet-Telefonie-Rufnummern die Möglichkeit 1 gewählt haben. Die Zuordnung treffen Sie in diesem Fall bei der Teilnehmer-Konfiguration im Feld **DuWa**. Der Bildschirm ist auch in diesem Fall sichtbar, aber nicht editierbar.



a) Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.

b) Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.

24) Klicken Sie auf **OK & Weiter**. Hier sehen Sie noch einmal eine Übersicht der möglichen ITSPs. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit Status anzeigen können Sie den Verbindungsstatus überprüfen. Wenn Sie Verbindungsprobleme mit einem bereits aktivierten ITSP haben, können Sie ihn mit **ITSP neu starten** auf dieser Seite erneut registrieren.

25) Klicken Sie auf **OK & Weiter**.

26) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!

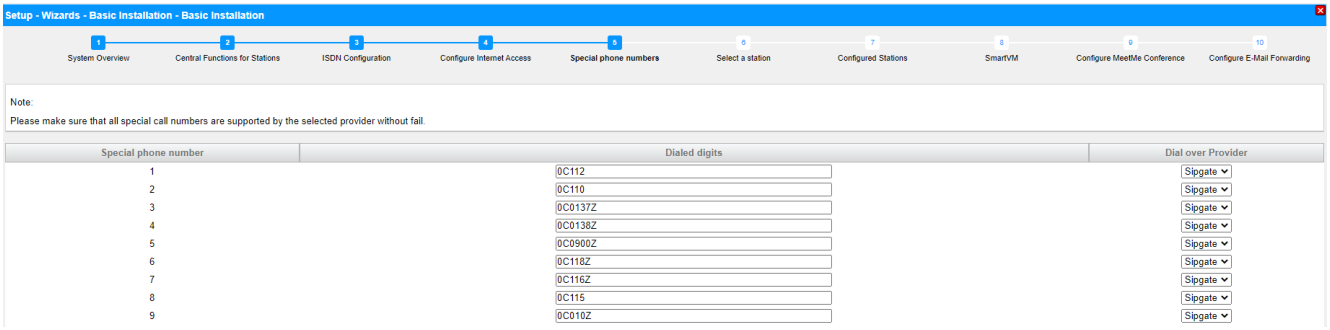
Anmerkung: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig zu führenden Internet-Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

Weitere Informationen über die Anzahl der gleichzeitigen Internetanrufe finden Sie unter Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP auf Seite 827.

---

27) Klicken Sie auf **OK & Weiter**.

28) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.



Folgende Rufnummerneinträge sind gültig:

- 0 bis 9: Zulässige Ziffern
- -: Feldtrennzeichen
- X: beliebige Ziffer von 0 bis 9
- N: beliebige Ziffer von 2 bis 9
- Z: Eine oder mehrere Ziffern folgen bis Wahlende
- C: Simulierter Wählton (kann max. dreimal eingetragen werden)

29) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

Anmerkung: Stellen Sie sicher, dass Notrufnummern immer gewählt werden können. Falls Notrufnummern über einen Internet-Telefonie-Service-Provider gewählt werden sollen, muss der ITSP dies unterstützen.

---

30) Klicken Sie auf **OK & Weiter**. Der Status Ihres ITSP wird angezeigt.

31) Klicken Sie auf **Weiter** und anschließend auf **Beenden**. Nach diesem Schritt führen Sie bitte den **CO Trunk ISDN / Analog / ITSP** Assistenten aus, um die Priorisierung für die Amtsleitungsbelegung festzulegen (zum Beispiel: Amtsleitungsbelegung Zuerst über ITSP und dann über ISDN).

10.2.1.2 So fügen Sie ein neues ITSP hinzu

Mit dem **Internettelefonie-Assistenten** können Sie einen neuen Internet-Telefonie-Dienstanbieter (ITSP) konfigurieren und aktivieren. Die können für jedes ITSP ein oder mehrere Konten konfigurieren.

Voraussetzungen

Die Verbindung zum Internet ist betriebsbereit.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Folgende Internet-Zugangsdaten Ihres ITSP liegen Ihnen vor:

Feldname	Beschreibung	Wert vom ISP
Gateway-Domänenname	Gateway-Domänenname des ITSP In der Regel identisch mit dem Hostnamen (z. B., sip-voice.de)	

Feldname	Beschreibung	Wert vom ISP
Anbieter-Registrar		
Registrar verwenden	Vordefiniert vom ITSP und in der Regel immer gesetzt (nicht erforderlich für ITSPs, die statische IP-Authentifizierung verwenden).	
IP-Adresse/Hostname	Hostname oder IP-Adresse des Registrar-Servers (z. B. sip-voice.de).	
Port	Portnummer des Registrar-Servers (z. B. 5060).	
Neuregistrierungsintervall beim Anbieter (Sek.)	Intervall (in Sekunden), in dem die ITSP-Registrierung wiederholt wird. Der Wert des Intervalls darf nicht 0 betragen und darf nicht zu hoch eingestellt werden, da bei Wiederholung der Registrierung am ITSP auch ein Verbindungsabbruch erkannt und bei Bedarf eine alternative Route (über ISDN oder einen alternativen Anbieter) ausgewählt werden kann. Standardwert: 120 Sekunden.	
Anbieter-Proxy		
IP-Adresse/Hostname	Hostname oder IP-Adresse des Proxy-Servers (z. B., sip-voice.de). Dieser ist in der Regel identisch mit dem Anbieter-Registrar-Eintrag.	
Port	Portnummer des Proxy-Servers (z. B. 5060). Diese ist in der Regel identisch mit der Portnummer des Anbieter-Registrars.	
Anbieter-Funktion		
Rufumlenkung	Nur sichtbar, wenn die ausgewählte Basisvorlage Anrufumlenkung unterstützt	
Ausgehender Anbieter-Proxy		
Ausgehenden Proxy verwenden	Nur gesetzt, wenn der ITSP einen ausgehenden Proxy verwendet.	
IP-Adresse/Hostname	Hostname oder IP-Adresse des ausgehenden Proxys	
Port	Portnummer des ausgehenden Proxys	
Eingehender Anbieter-Proxy		
Eingehenden Proxy verwenden	Nur gesetzt, wenn der ITSP einen zweiten Proxy verwendet.	

Feldname	Beschreibung	Wert vom ISP
IP-Adresse/Hostname	Hostname oder IP-Adresse des zweiten Proxys	
Port	Portnummer des zweiten Proxys	
Anbieter-STUN		
STUN verwenden	Wird nur verwendet, wenn STUN-Funktionalität erforderlich ist. Aktiviert auch den globalen STUN-Modus.	
IP-Adresse/Hostname	STUN-IP-Adresse, wenn der ITSP einen STUN Server verwendet.	
Port	STUN-Portnummer, wenn der ITSP einen STUN-Server verwendet.	

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Assistenten** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um die **Internettelefonie-Assistenten** zu starten.
4) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt. Die Liste enthält die für das gewählte Land vordefinierten ITSP und die eventuell bereits angelegten ITSP.
5) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie 8 ITSP aktivieren. Klicken Sie anschließend auf **OK**.
6) Klicken Sie auf **Hinzufügen**, um ein neues ITSP einzurichten. Es erscheint ein Konfigurationsfenster für das neue ITSP.
7) Wählen Sie eine **Basisvorlage** aus der Dropdown-Liste aus. Diese Option ermöglicht es, dasselbe ITSP in mehreren Routen konfiguriert zu haben.
8) Weisen Sie dem ITSP im Feld **Anbieter-Name** einen Namen Ihrer Wahl zu.

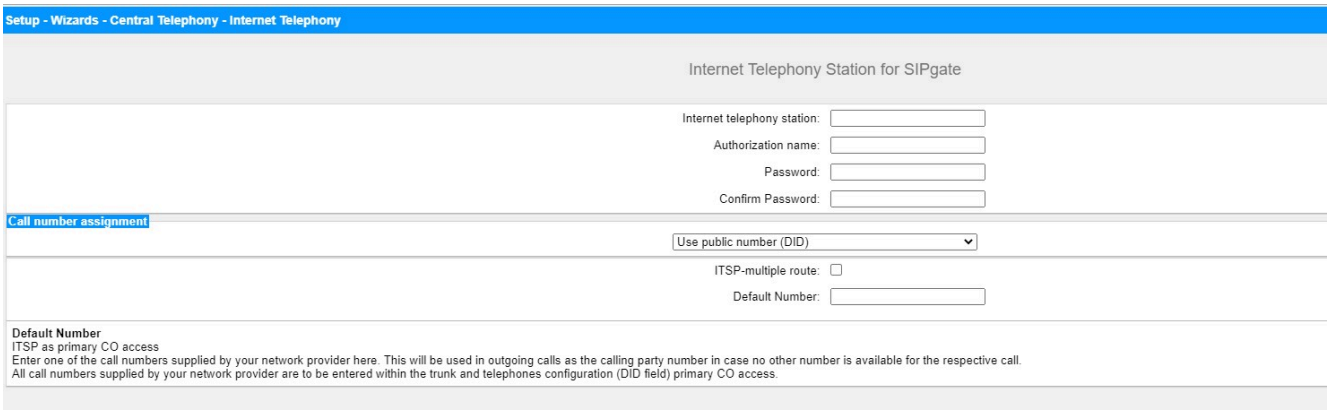
   Anmerkung: Die maximale Zeichengrenze beträgt 10.

9) Aktivieren Sie das Kontrollkästchen **Provider aktivieren**.
10) Geben Sie in den übrigen Bereichen die von Ihrem ITSP angegebenen Werte ein (siehe Tabelle unmittelbar nach den Voraussetzungen).

    Anmerkung: Die Werte unter den "Erweiterten SIP-Anbieterdaten" dürfen nur von autorisiertem Servicepersonal in Zusammenarbeit mit der Entwicklung geändert werden!

11) Klicken Sie auf **OK & Weiter**.

12) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.



13) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: SIP-Benutzer, SIP-ID usw.

    Weitere Details finden Sie unter http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

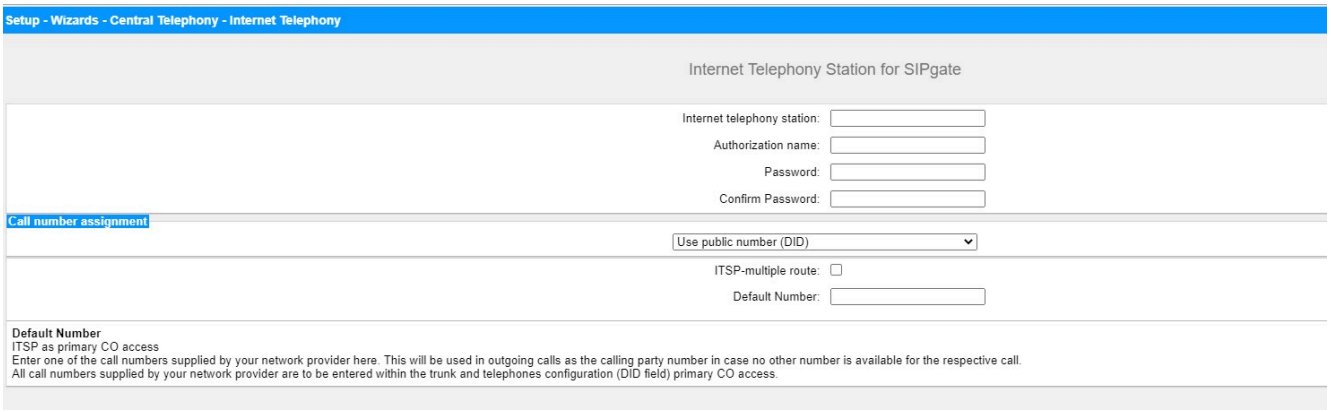
14) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen Autorisierungsnamen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

15) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, dass Sie vom ITSP erhalten haben. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: Kennwort, SIP-Kennwort usw.

16) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

    Öffentliche Nummer (DID) verwenden: Die Internettelefonie-Telefonnummern (DID) Ihrer Internettelefonie-Verbindung werden im

Stationen-Setup (in den **DID-** Feldern) konfiguriert. Während der ITSP-Konfiguration ist keine Zuordnungskonfiguration erforderlich.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.
b) Unter **Standardnummer**, geben Sie die Telefonnummer, die für ausgehende Anrufe verwendet werden soll, wenn keine DID-Nummer des Anrufers verfügbar ist, ein.
c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern).
d) Aktivieren Sie das Kontrollkästchen **ITSP-mehrere Routen**.
e) Geben Sie die der Route zugewiesen **ITSP-Routenpräfixe** ein und klicken Sie auf **Hinzufügen**.

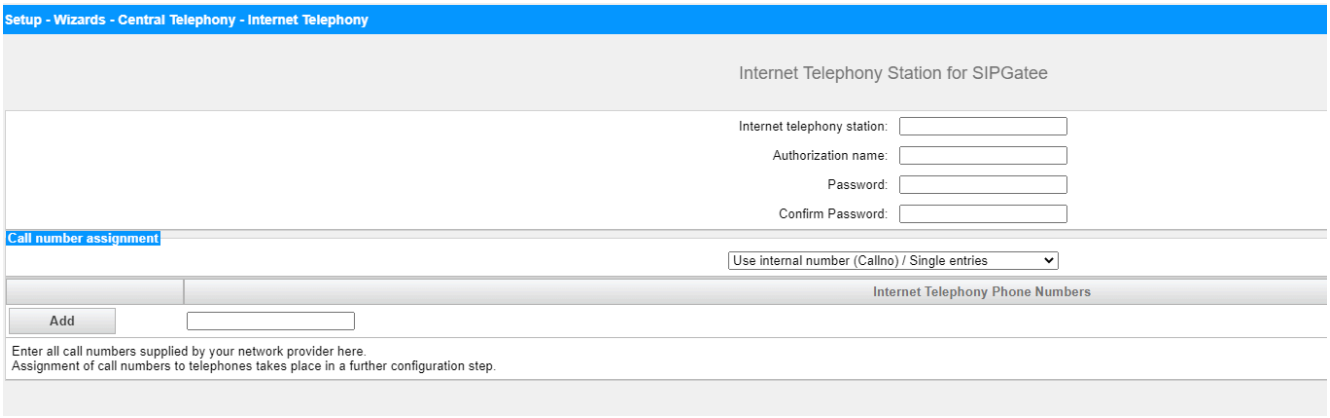
Anmerkung: Um mehrere Routen konfigurieren zu können, müssen die oben genannten Schritte wiederholt werden. Weitere Informationen finden Sie im Unify Wiki unter: http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#General_Configuration_guides

---

17) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

Interne Nummer (Rufnr.) verwenden / Einzeleinträge: Sie haben einen ITSP, der für jede Rufnummer SIP-Registrierung benötigt (z.B. 70005555, 70005556,...). Für jede Rufnummer muss eine Internettelefonie-Station erstellt und eine einzelne Rufnummer zugewiesen werden. Wenn Ihr ITSP

mehrere Rufnummern mit einer Registrierungsoption zulässt, sollte 1 verwendet werden.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.

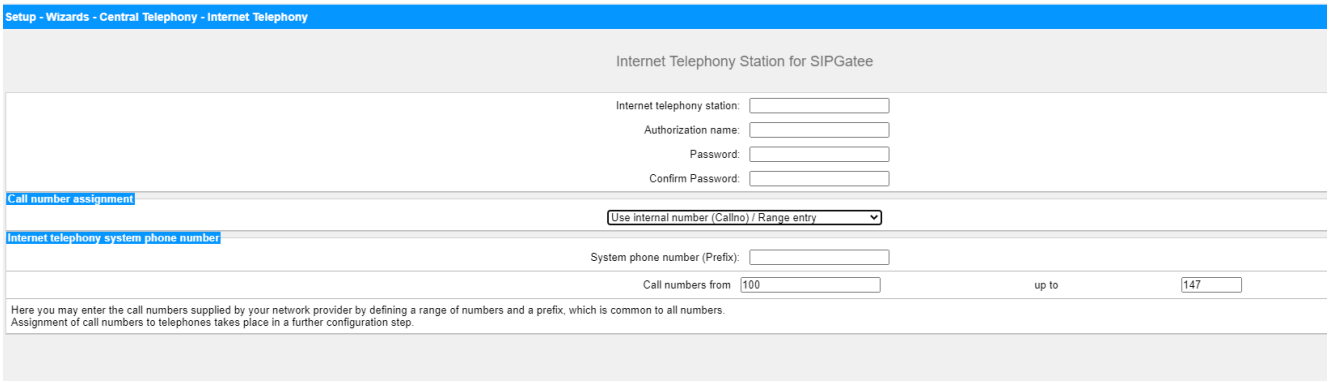
b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP mitgeteilten Internet-Telefonie-Teilnehmerrufnummern ein und klicken Sie auf **Hinzufügen**.

c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).

18) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:

Interne Rufnummer (Rufnummer) / Bereichseintrag verwenden: die Verwendung dieser Option ist veraltet, für die DID-Konfiguration sollte Option 1 verwendet werden.

Sie besitzen einen Internet-Telefonie-Anlagenanschluss und haben als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z.B. (+49) 89 7007-100 bis (+49) 89 7007-147. Sie weisen dann die Rufnummern aus dem Rufnummernbereich den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.

b) Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.

c) Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.

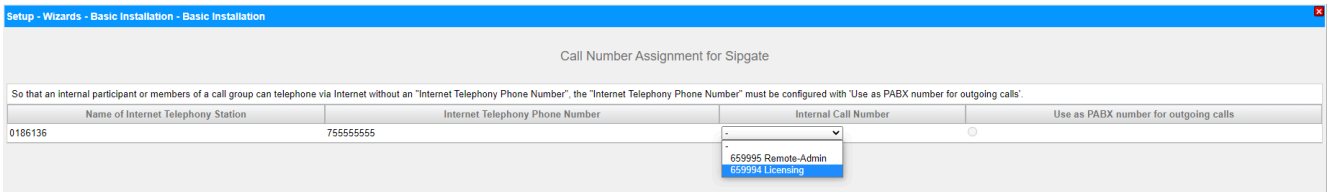
19) Klicken Sie auf **OK & Weiter**.

20) Wenn Sie zusätzliche Konten konfigurieren möchten, wiederholen Sie die Schritte 12 bis 19.

21) Klicken Sie auf **OK & Weiter**. Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.

22) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.

Dieser Schritt entfällt, wenn Sie für die Zuordnung der Internet-Telefonie-Rufnummern die Möglichkeit 1 gewählt haben. Die Zuordnung treffen Sie in diesem Fall bei der Teilnehmer-Konfiguration im Feld **DuWa**. Der Bildschirm ist auch in diesem Fall sichtbar, aber nicht editierbar.



a) Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.

b) Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.

23) Klicken Sie auf **OK & Weiter**. Hier sehen Sie noch einmal eine Übersicht der möglichen ITSPs. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit Status anzeigen können Sie den Verbindungsstatus überprüfen. Wenn Sie Verbindungsprobleme mit einem bereits aktivierten ITSP haben, können Sie ihn mit **ITSP neu starten** auf dieser Seite erneut registrieren.

24) Klicken Sie auf **OK & Weiter**.

25) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!

Anmerkung: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig zu führenden Internet-Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

Weitere Informationen über die Anzahl der gleichzeitigen Internetanrufe finden Sie unter Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP auf Seite 827.

---

26) Klicken Sie auf **OK & Weiter**.

27) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.

Folgende Rufnummerneinträge sind gültig:

- 0 bis 9: Zulässige Ziffern
- -: Feldtrennzeichen
- X: beliebige Ziffer von 0 bis 9
- N: beliebige Ziffer von 2 bis 9
- Z: Eine oder mehrere Ziffern folgen bis Wahlende
- C: Simulierter Wählton (kann max. dreimal eingetragen werden)

28) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

Anmerkung: Stellen Sie sicher, dass Notrufnummern immer gewählt werden können. Falls Notrufnummern über einen Internet-Telefonie-Service-Provider gewählt werden sollen, muss der ITSP dies unterstützen.

---

29) Klicken Sie auf **OK & Weiter**. Der Status Ihres ITSP wird angezeigt.

30) Klicken Sie auf **Weiter** und anschließend auf **Beenden**. Nach diesem Schritt führen Sie bitte den **CO Trunk ISDN / Analog / ITSP** Assistenten aus, um die Priorisierung für die Amtsleitungsbelegung festzulegen (zum Beispiel: Amtsleitungsbelegung Zuerst über ITSP und dann über ISDN).

10.2.1.3 Wie Sie Multisite über ITSP konfigurieren

Mit dem Wizard **Multisite Management** können Sie für das Kommunikationssystem bis zu 8 Standorte definieren, denen Sie jeweils eine ITSP-Registrierung und mehrere Teilnehmer zuordnen können.

Voraussetzungen

Es sind so viele Registrierungen bei einem oder mehreren ITSP angelegt, wie Standorte eingerichtet werden sollen.

Alle Standorte befinden sich innerhalb eines Landes.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Multisite Management** zu starten.

4) Geben Sie unter **Ortskennzahl** für jeden Standort eine Ortsvorwahl an (inkl. führender Null, z.B. `069` für Frankfurt und `030` für Berlin). Es können unterschiedliche oder auch gleiche Ortsvorwahlen eingetragen werden.

5) Geben Sie unter **Bereich** einen Namen für jeden Standort ein (z.B. die zu den Ortsvorwahlen passenden Städte, `Frankfurt` und `Berlin`, oder bei gleichen Ortsvorwahlen die Abteilungsbezeichnungen `Service` und `Vertrieb`).

6) Ordnen Sie in der Auswahlliste **Dedizierte Richtung** jedem Standort eine Richtung zu. Für jede ITSP-Registrierung ist automatisch eine Richtung reserviert (bis zu 8 möglich).

7) Wenn Sie einen oder mehrere Standorte löschen wollen, markieren Sie die Standorte in der Spalte **Löschen** und klicken Sie auf **Speichern**.

8) Klicken Sie auf **OK & Weiter**.

9) Ordnen Sie den Standorten die Teilnehmer und Gruppen zu:

a) Markieren Sie die gewünschten Teilnehmer und Gruppen.

Anmerkung:

Sie können auch nach Teilnehmern und Gruppen suchen, indem Sie in die Suchfelder **Rufnr.**, **DuWa** oder **Name** den Suchbegriff eingeben und anschließend auf das Lupen-Symbol klicken. Alle Teilnehmer und Gruppen werden aufgelistet, wenn alle Suchfelder leer sind und Sie anschließend auf das Lupen-Symbol klicken.

Über die Auswahl **Typ** lassen sich alle Teilnehmer-Typen anzeigen (z.B. **SIP Clients** oder **System Clients**).

Gefundene Teilnehmer und Gruppen können Sie entweder einzeln in der Spalte **Auswahl** markieren oder alle mit dem Kontrollkästchen **Alle** auswählen.

---

b) Wählen Sie unter **nach Bereich** den gewünschten Standort aus.

c) Klicken Sie auf **Speichern**.

d) Wiederholen Sie die vorangegangenen Schritte für weitere Standorte.

10) Bei Bedarf können Sie auch Teilnehmer und Gruppen eines Standorts einem anderen Standort zuordnen:

a) Wählen Sie unter **Verschiebe Auswahl von Bereich** den Standort aus, dessen Teilnehmer und Gruppen Sie einem anderen Standort zuordnen wollen. Es werden alle Teilnehmer und Gruppen des Standorts angezeigt.

b) Markieren Sie die gewünschten Teilnehmer entweder einzeln in der Spalte **Auswahl** oder alle mit dem Kontrollkästchen **Alle auswählen**.

c) Wählen Sie unter nach Bereich den neuen Standort aus.

d) Klicken Sie auf **Speichern**.

e) Wiederholen Sie die vorangegangenen Schritte für weitere Standorte.

11) Klicken Sie auf **OK & Weiter**.

10.2.1.4 So speichern Sie eine vorkonfigurierte ITSP-Vorlage als neue Vorlage

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Voice Gateway**.

3) Klicken Sie im Menübaum auf **Internettelefonie-Dienstanbieter**.

4) Klicken Sie auf die Registerkarte **Internet Telefonie Dienstanbieter hinzufügen**.
5) Wählen Sie die gewünschte ITSP-Vorlage aus der Liste **Basisvorlage** aus.
6) Geben Sie im Feld **Anbieter-Name** den gewünschten Namen für die neue ITSP-Vorlage ein.
7) Bearbeiten Sie die Werte der Vorlage nach Ihren Bedürfnissen. Eine Erklärung der Werte finden Sie unter Voice Gateway>Internet Telefonie Dienstleister.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.2.1.5 Wie Sie eine vorkonfigurierte ITSP-Vorlage anpassen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.
3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.
4) Klicken Sie im Menübaum auf die gewünschte ITSP-Vorlage.
5) Klicken Sie auf die Registerkarte **Internet-Telefonie Service Provider ändern**.
6) Passen Sie die Werte der Vorlage an Ihre Belange an. Die Erklärung der Werte finden Sie unter Sprachgateway>Internet-Telefonie Service Provider.

Anmerkung: Mit der Schaltfläche **Default-Werte zurücksetzen** können Sie Ihre geänderten Werte auf die Standard-Werte der Vorlage zurücksetzen. Ist der ITSP der Vorlage bereits aktiviert, werden alle Accounts des ITSP sofort abgemeldet und mit den Standard-Werten neu registriert.

Anmerkung: Mit der Schaltfläche **Aktualisieren** können Sie die Standard-Werte auf den neuesten Stand bringen, sofern ein Software-Update durchgeführt wurde und es in diesem Update aktuellere Standard-Werte für diese Vorlage gibt.

---

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.2.1.6 Wie Sie eine vorkonfigurierte ITSP-Vorlage manuell aktualisieren

Voraussetzungen

Der ITSP dieser Vorlage ist aktiviert.

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.
3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.
4) Klicken Sie im Menübaum auf die gewünschte ITSP-Vorlage.
5) Klicken Sie auf die Registerkarte **Internet-Telefonie Service Provider ändern**.
6) Notieren Sie sich die Werte der Vorlage, die Sie gegenüber den Standard-Werten geändert haben (z.B. mit Hilfe eines Screenshots).
7) Klicken Sie auf **Aktualisieren**. Die Standard-Werte der Vorlage werden aktualisiert, sofern ein Software-Update des Systems durchgeführt wurde und es in diesem Update aktuellere Standard-Werte für diese Vorlage gibt.
8) Passen Sie die Werte der Vorlage wieder an Ihre Belange an. Die Erklärung der Werte finden Sie unter Sprachgateway>Internet-Telefonie Service Provider.

Anmerkung: Mit der Schaltfläche **Default-Werte zurücksetzen** können Sie Ihre geänderten Werte auf die Standard-Werte der Vorlage zurücksetzen. Dabei werden alle Accounts des ITSP sofort abgemeldet und mit den Standard-Werten neu registriert.

---

9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.2.2 STUN (Simple Traversal of UDP over NAT)

STUN ermittelt beim Betrieb des Kommunikationssystems hinter einem NAT-Router die eigene öffentliche IP-Adresse/Port, die für einige ITSP erforderlich ist. Die Funktionalität wird im Internet auf STUN-Servern bereitgestellt, deren Adressen entsprechend in der Konfiguration des Kommunikationssystems hinterlegt sein müssen.

Der benötigte STUN-Modus ist abhängig von der ITSP-Infrastruktur und dem verwendeten Internet-Router. STUN wird nicht benötigt, wenn der ITSP NAT Traversal auflöst, indem er Infrastruktur-Komponenten im Provider-Netzwerk verwendet wie den Session Border Controller (SBC).

Folgende STUN-Modi können am Kommunikationssystem eingestellt werden:

- **Automatisch (Standard)**

  Ist kein ITSP aktiv, ist STUN in diesem Modus komplett ausgeschaltet. Ist ein ITSP aktiv, bestimmt STUN den verwendeten Firewall-Typ (NAT-Typ) beim Systemstart und kann während des Betriebs Änderungen an den IP-Adressen erkennen. Abhängig vom festgestellten NAT-Typ ändert STUN bestimmte Parameter in den SIP-Nachrichten.

  Anmerkung: Symmetric NAT wird nicht unterstützt.

- **Immer**

  STUN ist immer aktiv. Abhängig vom festgestellten NAT-Typ sind einige Parameter in den SIP-Nachrichten angepasst.
- **Statische IP verwenden**

  DSL-Modem oder Internet-Router nutzen eine statische IP-Adresse (öffentliche IP-Adresse) und der ITSP fordert eine statische IP-

Authentifizierung. Die vom Modem oder Router verwendete statische IP-Adresse und Port müssen zusätzlich angegeben werden.

- **Router behält Port bei**

  Die öffentliche IP-Adresse wird über STUN ermittelt. Der Port wird unverändert in die SIP-Nachrichten eingetragen.

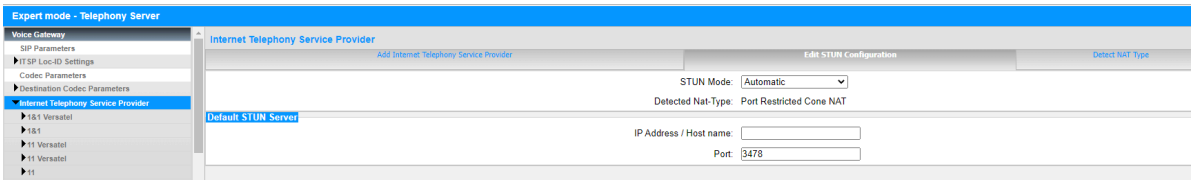
10.2.2.1 Wie Sie den STUN-Modus festlegen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.
3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.
4) Klicken Sie auf die Registerkarte **STUN-Konfiguration ändern**.



5) Wählen Sie aus der Aufklappliste **STUN-Modus** den gewünschten STUN-Modus aus.
6) Wenn Sie den STUN-Modus **Statische IP verwenden** ausgewählt haben, geben Sie unter **öffentliche IP-Adresse** und **öffentlicher SIP-Port** die statische IP-Adresse und den Port des DSL-Modems oder des Internet-Routers ein.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3 Amtszugang über digitale und analoge Leitungen

Der Amtszugang über ISDN-Leitungen oder analoge Leitungen verbindet die Hardwareplattformen mit dem öffentlichen Netz (PSTN).

Wizards erleichtern die Konfiguration eines ISDN-Amtszugangs oder eines analogen Amtszugangs.

10.3.1 Leitungen

Leitungen verbinden die Hardwareplattformen mit dem öffentlichen Netz (PSTN). Jeder Leitung muss eine Richtung zugewiesen sein, über die man der Leitung verschiedene Eigenschaften zuordnen kann.

Standardmäßig sind allen Leitungen eine Leitungskennzahl und eine Richtung zugewiesen. Diese Zuordnungen können vom Administrator geändert werden.

Bei einem ISDN-Amtsanschluss spricht man bei Leitungen auch von B-Kanälen.

Leitungskennzahl

Anhand der Leitungskennzahl wird vom Kommunikationssystem die der Leitungskennzahl zugeordnete Leitung belegt. Die Leitungskennzahl dient auch zum Programmieren einer Leitungstaste oder zum Prüfen einer Leitung.

MSN-Zuordnung

Der Service Provider vergibt zu jedem ISDN-Mehrgeräteanschluss (PMP, Point-to-Multipoint) eine oder mehrere MSN (Multiple Subscriber Number). Diese können direkt einer Leitung zugeordnet werden.

Systemrufnummern

Systemrufnummern beinhalten das internationale Präfix, die Länder- und Ortsvorwahl und die Anlagenrufnummer bzw. eine oder mehrere MSN.

ISDN-Protokoll

Das verwendete ISDN-Protokoll richtet sich nach der Länderkennzahl. Es sollte nur geändert werden, falls die PSTN-Anbindung ausdrücklich ein bestimmtes, abweichendes Protokoll erfordert. Es steht eine große Anzahl von Protokoll-Templates zur Verfügung, die an die eigenen Belange angepasst werden können. Die dafür notwendigen Informationen erhalten Sie von Ihrem Service Provider.

B-Kanal-Belegungsmodus

Einzelne B-Kanäle einer ISDN-Leitung lassen sich für gehenden und/oder kommenden Verkehr sperren.

Es sind folgende B-Kanal-Belegungsmodi möglich:

- nur gehend
- nur kommend
- Ausgehend und eingehend (Standard)

Der B-Kanal-Belegungsmodus wird nur dann ausgewertet, wenn das Kommunikationssystem einen B-Kanal vorschlagen muss. Dies gilt in folgenden Situationen:

S_2 gehend:	Hierbei muss das Kommunikationssystem einen B-Kanal vorschlagen.
S_2 kommend:	Die Gegenstelle ist verpflichtet, einen B-Kanal vorzuschlagen. Dieser B-Kanal wird vom Kommunikationssystem ohne Prüfung der Einstellung übernommen. Die Einstellung hat somit keinen Einfluss.
S_0 gehend:	Da das Kommunikationssystem keinen B-Kanal vorgibt (any channel), hat die Einstellung keinen Einfluss.
S_0 kommend:	Wenn die Gegenstelle das Gespräch ohne B-Kanal-Vorgabe aufbaut, so wird vom Kommunikationssystem ein B-Kanal vorgeschlagen. Für diesen Vorschlag wird der eingestellte B-Kanal-Belegungsmodus beachtet.

Wahlverfahren für analoge Amtsleitungen (HKZ)

Das Wahlverfahren wird vom Kommunikationssystem automatisch bei jeder Leitungsbelegung erkannt. Für spezielle Fälle kann das Wahlverfahren auch direkt auf das Mehrfrequenzwahlverfahren (MFV) oder das Impulswahlverfahren (IWV) eingestellt werden.

10.3.1.1 Wie Sie den ISDN-Amtszugang konfigurieren

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** konfigurieren Sie den ISDN-Amtszugang. Je nach den im Kommunikationssystem vorhandenen Ports für Amtsleitungen (ISDN oder analog) durchläuft der Wizard unterschiedliche Schritte.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Das Kommunikationssystem ist an eine ISDN-Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Amtsleitung ISDN / Analog / ITSP** zu starten. Der Wizard zeigt eine Übersicht der Box(en), Slots und S_0-Ports.
4) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. `49` für Deutschland oder `1` für USA.
5) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z.B. 89 für München.
6) Wenn es sich um einen Anlagenanschluss handelt, geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z.B. 7007 (Ihre Anschlussnummer).
7) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

   Bei Telefonaten ins Ausland wird der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z.B. von Deutschland nach USA `00-1` und von USA nach Deutschland `011-49`.
8) Klicken Sie auf **OK & Weiter**.
9) Wählen Sie für den betreffenden Anschluss (Box, Slot und S_0-Port) eine der folgenden Anschlussarten:
   - Wenn Sie einen Anlagenanschluss konfigurieren möchten, aktivieren Sie das Optionsfeld **Anlagenanschluss**.
   - Wenn Sie einen Mehrgeräteanschluss konfigurieren möchten, aktivieren Sie das Optionsfeld **Mehrgeräteanschluss**.
10) Klicken Sie auf **OK & Weiter**.
11) Wenn es sich um einen Mehrgeräteanschluss handelt, geben Sie für den betreffenden Anschluss (Box, Slot und S_0-Port) die MSN ein und klicken Sie auf **OK & Weiter**.
12) Belassen Sie die Einstellung des Kontrollkästchens **Keine Telefonie über Internet** und klicken Sie auf **Überspringen**.

13) Wählen Sie in der Aufklappliste **Zuerst über** den bevorzugten Amtszugang und klicken Sie auf **OK & Weiter**.
14) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.3.1.2 Wie Sie einen analogen Amtszugang konfigurieren

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** konfigurieren Sie den analogen Amtszugang.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Das Kommunikationssystem ist an eine analoge Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Amtsleitung ISDN / Analog / ITSP** zu starten. Der Wizard zeigt eine Übersicht der Box(en), Slots und analogen Ports.
4) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. `49` für Deutschland oder `1` für USA.
5) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z.B. 89 für München.
6) Wenn es sich um einen Anlagenanschluss handelt, geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z.B. 7007 (Ihre Anschlussnummer).
7) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

   Bei Telefonaten ins Ausland wird der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z.B. von Deutschland nach USA `00-1` und von USA nach Deutschland `011-49`.
8) Klicken Sie auf **OK & Weiter**.
9) Klicken Sie auf **ISDN überspringen**.
10) Belassen Sie die Einstellung des Kontrollkästchens **Keine Telefonie über Internet** und klicken Sie auf **Überspringen**.
11) Wählen Sie aus der Aufklappliste **Protokoll** das Protokoll für die Anzeige der Rufnummer (Service-Provider-abhängig) aus:
    - Wenn Sie Frequency Shift Keying verwenden möchten, wählen Sie **FSK**.
    - Wenn Sie das Mehrfrequenzwahlverfahren verwenden möchten, wählen Sie **MFW**.
    - Wenn Sie keine Rufnummernanzeige verwenden möchten, wählen Sie **keine**.
12) Klicken Sie auf **OK & Weiter**.
13) Klicken Sie auf **Bearbeiten**, um Eigenschaften der betreffenden Leitung zu konfigurieren. Ändern Sie bei Bedarf **Wahlverfahren**, **Amtsruferkennung**, **Flash**, **Leitungslänge** und **Flags** und klicken Sie auf **OK**.
14) Klicken Sie auf **OK & Weiter**.

15) Klicken Sie auf **Überspringen** und auf **OK & Weiter**.
16) Wählen Sie in der Aufklappliste **Zuerst über** den bevorzugten Amtszugang und klicken Sie auf **OK & Weiter**.
17) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.3.1.3 Wie Sie alle Leitungen anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Leitungen**. Ihnen werden abhängig vom Ausbau des Kommunikationssystems alle möglichen Leitungen inkl. Leitungskennzahl und Richtung angezeigt.

10.3.1.4 Wie Sie eine einzelne Leitung anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung** > **Leitungen** > **...** zur gewünschten Leitung. Ihnen wird die am Kommunikationssystem angeschlossene Leitung inkl. Leitungskennzahl und Richtung angezeigt.
4) Klicken Sie auf **OK**.

10.3.1.5 Wie Sie eine Leitungskennzahl ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung** > **Leitungen** > **...** zur gewünschten Leitung.
4) Klicken Sie auf die Registerkarte **Leitung ändern**.
5) Geben Sie im Feld **Kennzahl** den gewünschten Wert ein.

Anmerkung: Ist als Kennzahl kein Wert eingetragen, hat diese Leitung keine Leitungskennzahl.

---

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.1.6 Wie Sie eine MSN einer Leitung zuweisen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen / Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen / Vernetzung** > **MSN zuweisen**.
4) Klicken Sie im Menübaum unter **MSN zuweisen** auf den Eintrag, den Sie bearbeiten möchten.
5) Geben Sie die **MSN** ein.
6) Wählen Sie in der Aufklappliste die **Leitung**, die Sie zuweisen möchten.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.1.7 ISDN-Protokoll ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen / Vernetzung**.
3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung** > **Leitungen** > **...** zum gewünschten Port.
4) Klicken Sie auf die Registerkarte **ISDN-Flags ändern**.
5) Wählen Sie im Bereich **Protokoll: Beschreibung** in der Aufklappliste das gewünschte Protokoll aus.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.1.8 Wie Sie den B-Kanal-Belegungsmodus ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen / Vernetzung**.
3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung** > **Leitungen** > **...** zum gewünschten Port.
4) Klicken Sie auf die Registerkarte **B-Kanal ändern**.
5) Deaktivieren Sie pro Kanal die Kontrollkästchen in den Spalten **gehend** und **kommend** nach Ihren Wünschen.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.1.9 Wie Sie das Wahlverfahren ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung** > **Leitungen** > **...** zum gewünschten Port.
4) Klicken Sie auf die Registerkarte **HKZ-Flags ändern**.
5) Stellen Sie das Mehrfrequenzwahlverfahren (MFV) oder das Impulswahlverfahren (IWV) ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2 Richtungen

Über Richtungen können Leitungen (B-Kanäle) gebündelt werden. Für jedes Leitungsbündel (= Richtung) können eigene Parameter konfiguriert werden.

Jeder Leitung kann genau eine Richtung zugeordnet werden. Standardmäßig sind allen Leitungen die Richtung 1 zugewiesen.

Für jede Richtung kann ein Name und eine Richtungskennzahl vergeben werden.

Tipp: Richtungskennzahlen sind für gehende Amtsbelegungen nur wirksam, wenn LCR nicht aktiv ist.

B-Kanalaufteilung

Eine Teilung der B-Kanäle auf verschiedene Leitungsbündel nennt man auch B-Kanalaufteilung. Für ISDN-Amtsanschlüsse mit vielen B-Kanälen, wie z.B. S_{2M}-Anschlüsse, kann eine Aufteilung der B-Kanäle auf verschiedenen Leitungsbündel sinnvoll sein.

Bei gehenden Gesprächen werden nur B-Kanäle ausgewählt, die in dem Bündel enthalten sind (z.B. über Richtungskennzahl ausgewähltes Bündel, Überlaufbündel oder über LCR ausgewähltes Bündel).

Kommende Gespräche werden immer unabhängig vom Bündel akzeptiert. Im Regelfall wird der vom Partner angebotene B-Kanal belegt. Daher muss die im System konfigurierte B-Kanalaufteilung auch auf der Partner-Seite (Anlage oder öffentliches Netz) unterstützt werden. Ist das nicht der Fall, kann die korrekte Zuordnung des Rufes zum entsprechenden Leitungsbündel nicht garantiert werden.

Richtungstaste

Ein Teilnehmer kann am Telefon eine Richtungstaste programmieren. Eine Richtungstaste ist für gehende Anrufe reserviert. Über Richtungstasten getätigte Anrufe unterliegen den Stufen und Regeln der COS-Wahlkontrolle.

Nachdem der Teilnehmer eine Richtungstaste drückt (oder eine Richtungskennzahl wählt), belegt das Kommunikationssystem zum Verbindungsaufbau eine verfügbare Leitung, die der entsprechenden Richtung zugeordnet ist. Das Telefon zeigt die Leitungsnummer im Display an. Sind alle Leitungen der Richtung belegt, leuchtet die entsprechende LED, auch bei erfolgreichem Überlauf.

Überlaufrichtung bei deaktiviertem LCR

Der Administrator kann für jede Richtung eine Überlaufrichtung festlegen. Sind bei einem Belegungsversuch alle Leitungen einer Richtung belegt, so wird die Suche unter allen Leitungen dieser Überlaufrichtung fortgesetzt. Sind auch in der Überlaufrichtung alle Leitungen belegt, erfolgt kein weiterer Überlauf.

Überlaufrichtung bei aktiviertem LCR

Der Administrator kann im Rahmen der LCR-Konfiguration bis zu 16 Einträge je Wegetabelle konfigurieren, die im Sinne eines Überlaufes nacheinander abgearbeitet werden.

Belegungsart

Für gehende Richtungsbelegung kann der Administrator festlegen, nach welchem Kriterium das Kommunikationssystem eine verfügbare Leitung in der entsprechenden Richtung sucht. Die geschieht durch Definition der Belegungsart wie folgt:

- Zyklisch:

  Nach der zuletzt gehend belegten Leitung - die Suche beginnt bei der nächsthöheren Leitungsnummer, bezogen auf die zuletzt gehend belegte Leitung in dieser Richtung. Dadurch werden alle Leitungen etwa gleich häufig verwendet.
- Linear:

  Immer die erste freie Leitung - die Suche beginnt bei der niedrigsten Leitungsnummer, die dieser Richtung zugeordnet ist.

Anlagenrufnummer kommend und gehend

Der Administrator kann die Anlagenrufnummer kommend und die Anlagenrufnummer gehend getrennt festlegen. Damit kann die eigene Rufnummer bei gehenden Gesprächen anders darstellt werden als sie für die Erreichbarkeit bei kommenden Gesprächen benötigt wird. Die Anteile für Ländervorwahl, Ortsnetzkennzahl und Anlagenrufnummer sind dabei jeweils getrennt einzutragen. Unterschiedliche Einträge bei der Anlagenrufnummer kommend und gehend setzen die Verfügbarkeit des Leistungsmerkmal "CLIP no screening" im Amt voraus. Ist keine Anlagenrufnummer gehend konfiguriert, verwendet das Kommunikationssystem stets die Daten der Anlagenrufnummer kommend.

Bei einer kommenden Belegung auf einer ISDN-Leitung blendet das Kommunikationssystem aus der empfangenen Rufnummer die Anteile für die Anlagenrufnummer kommend entsprechend dem empfangenen Rufnummerntyp (Type Of Number = TON, siehe Tabelle unter

Rufnummernübermittlung) linksbündig aus und interpretiert den verbleibenden Teil als Durchwahlnummer. Bei Rufnummerninformationen an das PSTN setzt das Kommunikationssystem die Anteile der Anlagenrufnummer gehend entsprechend dem konfigurierten Rufnummerntyp gehend automatisch als führenden Teil der Rufnummer ein. Der Anteil der Anlagenrufnummer muss am Amtsanschluss in Deutschland ohne Ortsnetzkennzahl und ohne Abwurf-Kennziffer (0) angegeben werden.

Rufnummernübermittlung

Die Rufnummer, die zum PSTN und zum Empfänger gesendet wird, kann sich folgendermaßen zusammensetzen:

Type Of Number (TON), gehend	zum PSTN übermittelte Rufnummer
Unbekannt TON=Unknown	Nur Durchwahlnummer (Standardeinstellung)
Anlagenrufnummer TON=Subscriber	Anlagenrufnummer + Durchwahlnummer
Ortsnetzkennzahl TON=National	Ortsnetzkennzahl + Anlagenrufnummer + Durchwahlnummer
Ländervorwahl TON=International	Ländervorwahl + Ortsnetzkennzahl + Anlagenrufnummer + Durchwahlnummer
Intern TON=Intern	Nur für vernetzes System: bei einem geschlossenen Rufnummernplan darf kein Nummern-Präfix ergänzt werden. Hier wird eine Rufnummernergänzung unterdrückt.

Weiterhin besteht die Möglichkeit anzugeben, welche Rufnummerninformation von dem wählenden Teilnehmer an den Zielteilnehmer gesendet werden soll.

Rufnummerntyp	zum PSTN übermittelte Rufnummer
Intern	Hier wird nur eine Information über die interne Rufnummer gesendet. Ist der Zielteilnehmer Extern, wird entweder keine oder die Vermittlungsplatz-Rufnummer gesendet. Bei internen Zielteilnehmern kann die interne Rufnummer angezeigt werden.
Durchwahl	Hier wird nur eine Information über die DuWa-Nummer versendet. Bei internen Zielteilnehmern in einem anderen Knoten fehlt für eine Displayanzeige die interne Rufnummer. Für externe Ziele ist die Rufnummerninformation ausreichend.

Rufnummerntyp	zum PSTN übermittelte Rufnummer
Intern / DuWa	In einer Vernetzung ist es sinnvoll diese Einstellung zu wählen. Dem Zielteilnehmer werden sowohl die interne als auch die DuWa-Rufnummer gesendet. Wird in der Vernetzung ein interner Teilnehmer gerufen, kann diesem Teilnehmer die interne Rufnummer des Rufers angezeigt werden. Hat der interne Zielteilnehmer beispielsweise eine Anrufumleitung an ein externes Ziel aktiviert, so kann in diesem Fall eine DuWa-Rufnummer mitgesendet werden.

Zusätzlich kann die gewünschte Behandlung des Richtungspräfix konfiguriert werden:

- Kommender Ruf

  Die Anrufernummer wird bei der Weitergabe zum S0-Bus um die Richtungskennzahl ergänzt (-> wählbares Format für Rückruf) bzw. transparent durchgereicht. Standard: Aktiviert.
- Gehender Ruf

  Die Darstellung der gewählten Rufnummer am Systemtelefon erfolgt mit bzw. ohne Richtungspräfix. Standard: Aktiviert.

Zweite Amtskennziffer

Eine zweite Amtskennziffer wird dann definiert, wenn das Kommunikationssystem eine Unteranlage eines anderen Kommunikationssystems ist oder mit mehreren anderen Kommunikationssystemen vernetzt ist. Sie ist nur für Vernetzungs-Richtungen (Richtungsart=PABX) relevant. In diesem Fall dient die zweite Amtskennziffer als Belegungskennzahl für die Hauptanlage. Innerhalb einer Vernetzung sind die Kennzahlen für die Amtsbelegung, die Richtungskennzahl(en) und die zweite Amtskennziffer einheitlich zu konfigurieren. Standard in Deutschland ist 0.

10.3.2.1 Wie Sie die Richtungszuordnung ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.

3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung** > **Leitungen** > **...** zur gewünschten Leitung.

4) Klicken Sie auf die Registerkarte **Leitung ändern**.

5) Wählen Sie aus der Aufklappliste **Richtung** die Richtung aus, die Sie der Leitung zuweisen möchten.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.2 Wie Sie den Richtungsnamen ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.
5) Geben Sie im Feld **Richtungsname** den gewünschten Wert ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.3 Wie Sie die Richtungskennzahl ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Anmerkung: Richtungskennzahlen sind nur wirksam, wenn LCR nicht aktiv ist.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.
5) Geben Sie im Feld **Richtungskennzahlen** den gewünschten Wert ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.4 Wie Sie eine Überlaufrichtung bei deaktiviertem LCR konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen / Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen / Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.
5) Wählen Sie in der Aufklappliste **Überlaufrichtung** den gewünschten Eintrag.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.5 Wie Sie eine Überlaufrichtung bei aktiviertem LCR konfigurieren

Bei aktiviertem LCR erfolgt die Überlaufbehandlung durch sukzessive Abarbeitung der einzelnen Einträge einer LCR-Wegetabelle im Rahmen der LCR-Konfiguration (siehe LCR (Least Cost Routing, Leitweglenkung)).

10.3.2.6 Wie Sie die Belegungsart konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die Richtung, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.
6) Wählen Sie in der Aufklappliste **Belegungsart** entweder **zyklisch** oder **linear** aus.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.7 Wie Sie die Anlagenrufnummer kommend und gehend eintragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen / Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen / Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.
5) Geben Sie im Bereich **Anlagenrufnummer kommend** in die Felder **Ländervorwahl**, **Ortsnetzkennzahl** und **Anlagenrufnummer** die entsprechenden Werte ohne führende Nullen ein.
6) Geben Sie im Bereich **Anlagenrufnummer gehend** in die Felder **Ländervorwahl**, **Ortsnetzkennzahl** und **Anlagenrufnummer** die entsprechenden Werte ohne führende Nullen ein.
7) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Teilnehmer-Rufnummer unterdrücken möchten, aktivieren Sie das Kontrollkästchen **Tln.-Ruf Nr. unterdrücken**.
   - Wenn Sie die Teilnehmer-Rufnummer nicht unterdrücken möchten, deaktivieren Sie das Kontrollkästchen **Tln.-Ruf Nr. unterdrücken**.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.8 Wie Sie das Format der übermittelten Rufnummer konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die Richtung, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.
6) Wählen Sie in der Aufklappliste **Nr.-Typ, gehend** das gewünschte Format der übermittelten Rufnummer aus.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.9 Wie Sie die Art der übermittelten Rufnummer konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die Richtung, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.
6) Wählen Sie in der Aufklappliste **Rufnummer Typ** den Eintrag **Intern**, **Durchwahl** oder **Intern/DuWa**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.10 Wie Sie das Richtungs-Präfix konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die Richtung, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.

6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Rufnummernanzeige für kommende Gespräche um die Richtungskennzahl ergänzen möchten, aktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Rtg.-Präfix ergänzen kommend**.
   - Wenn Sie die Rufnummernanzeige für kommende Gespräche nicht um die Richtungskennzahl ergänzen möchten, deaktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Rtg.-Präfix ergänzen kommend**.
   - Wenn Sie die Rufnummernanzeige für gehende Gespräche um die Richtungskennzahl ergänzen möchten, aktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Rtg.-Präfix ergänzen gehend**.
   - Wenn Sie die Rufnummernanzeige für gehende Gespräche nicht um die Richtungskennzahl ergänzen möchten, deaktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Rtg.-Präfix ergänzen gehend**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.2.11 Wie Sie eine Richtung für die Vernetzung definieren und eine zweite Amtskennziffer eintragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.
5) Geben Sie im Feld **Amtskennziffer (2. AKZ)** den gewünschten Wert ein.
6) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.
7) Wählen Sie in der Aufklappliste **Richtungsart** den Eintrag **PABX** aus.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.3 Wähltonüberwachung

Beim Verbindungsaufbau über eine analoge Amtsleitung können die gewählten Ziffern erst zum Amt geschickt werden, wenn ein Wählton (Hörzeichen) erkannt wurde. Da die Zeit bis zum Eintreffen des Wählttons je nach Netzbetreiber und Netzzustand variiert, muss das Eintreffen des Wählttons überwacht werden.

Die Konfiguration der Wähltonüberwachungszeit und der Ziffernwahlzeit erfolgt mit dem Manager E.

Verzögerungszeit der Wähltonüberwachung

Die Überwachung des Wählttons kann sofort erfolgen oder erst nach einer Pause. In manchen Fällen müssen dem Teilnehmer nach Leitungsbelegung zusätzlich Töne eingespielt werden, z.B. um ihm mitzuteilen, dass eine Umleitung im Amt aktiv ist. Für diese Fälle kann eine Verzögerungszeit der Wähltonüberwachung (Pause vor Wahl, 1-9 Sekunden) programmiert

werden. Die gewählten Ziffern werden erst nach Ablauf dieser Pause zum Amt geschickt.

Anmerkung: Anmerkung für Brasilien:

Wird das MFV-Wahlverfahren von analogen Endgeräten aus verwendet in Verbindung mit analogen Amtsleitungen (TLAx und TML8W) und Impulswahlverfahren nach der Wähltonüberwachung, kann es Probleme mit der Wahlkontrolle geben, wenn die Ländervorwahl auf Brasilien eingestellt ist. In diesem Fall gehen die MFV-Signale von den analogen Endgeräten direkt zu den analogen Amtsleitungen. Alle MFV-Signale gehen verloren, die vor dem Empfang des Wähltons gewählt werden. Hier muss die automatische Wegesuche (LCR) für eine einwandfreie Funktion von Wahlverfahren und Wahlkontrolle des Endgeräts aktiviert sein.

Wähltonüberwachungszeit

Die Zeit, wie lange auf den Wählton gewartet werden soll, kann konfiguriert werden. Wird nach der konfigurierten Zeit kein Wählton erkannt, wird die Leitung außer Betrieb genommen. Das System überprüft in zyklischen Abständen, ob der Wählton erneut vorhanden ist. Ist dies der Fall, wird die betreffende Leitung wieder in Betrieb genommen.

Ziffernwahlzeit

Es kann eingestellt werden, wieviele Sekunden nach Erkennung des Wähltons die erste gewählte Ziffer zum Amt geschickt werden soll (Standard: 0 s).

Auswertung des zweiten Wähltons

Das Kommunikationssystem kann einen zusätzlichen Wählton (2. Hörzeichen) erkennen. Das ist relevant für öffentliche Netzbetreiber, die bei Auslandsgesprächen einen zweiten Wählton senden, z.B. für Belgien nach 00 und für Frankreich nach 16 bzw. 19. Für Deutschland ist diese Funktion nicht relevant.

10.3.3.1 Wie Sie die Verzögerungszeit der Wähltonüberwachung konfigurieren

Voraussetzungen

Ein analoger Port mit dem analogen Amtszugang ist vorhanden.

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die analoge Richtung, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.
6) Wenn die Wähltonüberwachung sofort erfolgen soll, aktivieren Sie im Bereich **Pause vor Wahl** das Optionsfeld **Hörtonauswertung**.

7) Wenn die Wähltonüberwachung erst nach einer Verzögerungszeit erfolgen soll, wählen Sie im Bereich **Pause vor Wahl** die Verzögerungszeit in Sekunden aus.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3.3.2 Wie Sie die Wähltonüberwachungszeit konfigurieren

Voraussetzungen

Es ist eine analoge Amtsbaugruppe gesteckt.

Schritt für Schritt

1) Melden Sie sich auf dem Admin-PC am Manager E an.
2) Klicken Sie in der Menüleiste auf **Datei | Übertragen**.
3) Wählen Sie das Register **Kommunikation**.
4) Aktivieren Sie im Bereich **Zugang** das Optionsfeld je nach Anschlussart des Admin-PC an das Kommunikationssystem.
5) Aktivieren Sie das Optionsfeld **KDS lesen/schreiben** und klicken Sie auf **Anlage -> PC**.
6) Klicken Sie auf **OK**. Klicken Sie auf OK und der KDS wird vom Kommunikationssystem zum Manager E übertragen.
7) Klicken Sie nach erfolgreicher Übertragung auf **OK** und anschließend auf **Schließen**.
8) Klicken Sie im Manager E im Menübaum der Anlagensicht auf **Einstellungen** > **Systemparameter** > **Zeitparameter**.
9) Stellen Sie in der Liste unter **Wähltonüberwachungszeit** mit **Basis** und **Faktor** die Zeit ein, wie lange max. auf den Wählton gewartet werden soll (Standard: Basis = `1s`, Faktor = `10`).
10) Klicken Sie auf **Übernehmen**.
11) Klicken Sie in der Menüleiste auf **Datei | Übertragen**.
12) Wählen Sie das Register **Kommunikation**.
13) Klicken Sie auf **PC -> Anlage** und anschließend auf **OK**. Die Einstellungen werden an das Kommunikationssystem übertragen.
14) Klicken Sie abschließend auf **OK** und **Schließen**.

10.3.3.3 Wie Sie die Ziffernwahlzeit konfigurieren

Voraussetzungen

Es ist eine analoge Amtsbaugruppe gesteckt.

Schritt für Schritt

1) Melden Sie sich auf dem Admin-PC am Manager E an.
2) Klicken Sie in der Menüleiste auf **Datei | Übertragen**.
3) Wählen Sie das Register **Kommunikation**.
4) Aktivieren Sie im Bereich **Zugang** das Optionsfeld je nach Anschlussart des Admin-PC an das Kommunikationssystem.

5) Aktivieren Sie das Optionsfeld **KDS lesen/schreiben** und klicken Sie auf **Anlage -> PC**.
6) Klicken Sie auf **OK**. Klicken Sie auf OK und der KDS wird vom Kommunikationssystem zum Manager E übertragen.
7) Klicken Sie nach erfolgreicher Übertragung auf **OK** und anschließend auf **Schließen**.
8) Klicken Sie im Manager E im Menübaum der Anlagensicht auf **Einstellungen** > **Systemparameter** > **Zeitparameter**.
9) Stellen Sie in der Liste unter **Zeit zur HT-Auswertung nach der Wahl Trunk-HKZ** mit **Basis** und **Faktor** die Zeit ein, nach wie vielen Sekunden nach Erkennung des Wähltons die erste gewählte Ziffer zum Amt geschickt werden soll (Standard: Basis = `10ms`, Faktor = `0`).
10) Klicken Sie auf **Übernehmen**.
11) Klicken Sie in der Menüleiste auf **Datei | Übertragen**.
12) Wählen Sie das Register **Kommunikation**.
13) Klicken Sie auf **PC -> Anlage** und anschließend auf **OK**. Die Einstellungen werden an das Kommunikationssystem übertragen.
14) Klicken Sie abschließend auf **OK** und **Schließen**.

10.3.3.4 Wie Sie die Auswertung des zweiten Wähltons aktivieren oder deaktivieren

Voraussetzungen

Ein analoger Port mit dem analogen Amtszugang ist vorhanden.

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die analoge Richtung, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.
6) Wenn die Auswertung des zweiten Wähltons aktiviert werden soll, aktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Auswertung 2. Hörzeichen**.
7) Wenn die Auswertung des zweiten Wähltons deaktiviert werden soll, deaktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Auswertung 2. Hörzeichen /Leitungsüberwachung**.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.4 Priorisierung der Amtsholung bei aktiviertem LCR

Bei der Priorisierung der Amtsholung wird festgelegt, in welcher Reihenfolge verschiedene Anbieter (ISDN/Analog oder ITSPs) ausgewählt werden.

Die Amtsholung geschieht normalerweise über die Vorwahl der Kennzahl "0". Innerhalb dieser Kennzahl werden (je nach Voreinstellung) verschiedene

Anbieter priorisiert. So kann ein gehendes Gespräch zuerst über einen ITSP und, bei erfolgloser Amtsholung, danach über ISDN abgesetzt werden.

10.4.1 Wie Sie die Amtsholung priorisieren

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** konfigurieren Sie die Reihenfolge der Amtsholung über ISDN/Analog und ITSPs.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet. Verschiedene ITSPs sind eingerichtet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Amtsleitung ISDN / Analog / ITSP** zu starten. Der Wizard zeigt eine Übersicht der Box(en), Slots und analogen Ports.
4) Klicken Sie auf **OK & Weiter**.
5) Klicken Sie so oft auf **OK & Weiter** bis Sie auf das Fenster **Priorisierung für die Amtsholung** kommen.
6) Wählen Sie im Bereich **Versuche Amtsholung** in der Aufklappliste **Zuerst über** den bevorzugten Anbieter, über den das Kommunikationssystem als Erstes versucht eine freie Amtsleitung zu bekommen.
7) Wählen Sie in der Aufklappliste **Dann über** einen zweiten Anbieter, über den der nächste Versuch einer Amtsholung gemacht wird.
8) Wählen Sie in der nächsten Aufklappliste **Dann über** den dritten Anbieter, über den der Versuch einer Amtsholung gemacht wird.
9) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11 Teilnehmer

Ein Abonnent oder ein Teilnehmer ist ein Kommunikationspartner, der an das Kommunikationssystem angeschlossen ist. In der Regel ist jedem Teilnehmer (abgesehen von virtuellen Teilnehmern) ein Endgerät zugeordnet. Ein Endgerät ist z.B. ein Telefon, ein PC oder ein Faxgerät. Die Teilnehmer können auch Benutzer der UC-Klienten sein.

Es gibt die folgenden Typen von Teilnehmern:

- IP-Teilnehmer (auch als IP-Klienten genannt)
- SIP-Teilnehmer (eine Untergruppe der IP-Teilnehmer)
- UP0-Teilnehmer
- DECT-Teilnehmer
- Mitel SIP-DECT-Teilnehmer
- ISDN-Teilnehmer
- Analoge Teilnehmer
- Mobility-Teilnehmer (mobile Teilnehmer, siehe Mobility)
- Virtuelle Teilnehmer

Die Daten der Abonnenten (Name, Teilnehmernummer, DuWa-Nummer, E-Mail-Adresse usw.) können bei der Erstinstallation als XML-Datei importiert werden (siehe Individueller Wahl-Plan). Darüber hinaus können die Teilnehmerdaten auch in eine XML-Datei exportiert werden (siehe Exportieren von Teilnehmerdaten).

Lizenzierungsverfahren für Teilnehmer

Alle Teilnehmer sind lizenzierungspflichtig. Die Teilnehmer können zunächst bei der Erstinstallation oder später mit Hilfe der Teilnehmer-Assistenten eingerichtet werden. Nach erfolgreicher Einrichtung können die Teilnehmer untereinander telefonieren. Im nächsten Schritt müssen die Teilnehmerlizenzen aktiviert und den Teilnehmern zugewiesen werden. Nach erfolgreicher Zuweisung der Lizenzen können die Teilnehmer auch extern telefonieren.

Zugehörige Konzepte

Lizenzierung auf Seite 297
Mobility auf Seite 955

11.1 Rufnummernplan

Ein Rufnummernplan ist eine Liste aller im Kommunikationssystem verfügbaren Rufnummern und Kennzahlen. Er beinhaltet u.a. interne Rufnummern, Durchwahlrufnummern und Gruppenrufnummern. Im Kommunikationssystem sind die Rufnummern und Kennzahlen mit Standardwerten vorbelegt. Diese Werte können aber bei Bedarf individuell angepasst werden.

Eventuell kann es beim Einrichten von Rufnummern oder Kennzahlen zu Fehlermeldungen kommen, wenn die gewünschte Nummer bereits belegt ist. Mit Hilfe des Rufnummernplans kann geprüft werden, welche Rufnummern noch zu vergeben sind.

11.1.1 Standard-Rufnummernplan

Der Standardrufnummernplan beinhaltet alle Rufnummern und Kennzahlen, die im Kommunikationssystem mit Standardwerten vorbelegt sind.

Die Standardwerte können bei Bedarf geändert werden. Einige Rufnummern können zusätzlich komplett gelöscht werden, so dass sie in einer Rufnummernplan-Übersicht nicht mehr angezeigt werden.

Standard-Rufnummernplan für die Hardware-Plattformen und den Softswitch:

Art der Rufnummern	X1	X3/X5/X8/S	Aktion
Interne Teilnehmer-Rufnummern	11-30	100-742	löschbar
Teilnehmer-Durchwahlnummern	11 -30	100-742	löschbar
Gruppenrufnummern 1-90 Gruppenrufnummern 91-800	31-40 -	350-439 Nicht vorbelegt	löschbar
Leitungsrufnummern	700-703	ab 7801	löschbar
Richtungskennzahlen (Externkennzahlen): Rtg. 1 (Amt ISDN, analog) Rtg. 8 (UC Suite) Rtg. 12-15 (Amt ITSP) Rtg. 16 (Vernetzung)	0 = Welt / 9 = USA - Nicht vorbelegt Nicht vorbelegt	0 = Welt / 9 = USA 851 855-858 859	Nur änderbar
Platzkennzahl (Abwurfplatz) Intern	9 = Welt 0 = USA	9 = Welt 0 = USA	Nur änderbar
Platzkennzahl (Abwurfplatz) Durchwahl	0 = Welt – = USA	0 = Welt – = USA	Nur änderbar
Rufnummer für Online User	Nicht vorbelegt	749	Nur änderbar
Rufnummer für den Remote-Zugang	Nicht vorbelegt	Nicht vorbelegt	Nur änderbar
Rufnummer für Sprachnachrichten UC Smart UC Suite	351 -	351 Nicht vorbelegt	Nur änderbar Nur änderbar
Konferenz-Rufnummern	-	Nicht vorbelegt	Nur änderbar
Rufnummer für Parken	-	Nicht vorbelegt	Nur änderbar

Art der Rufnummern	X1	X3/X5/X8/S	Aktion
AutoAttendant-Rufnummern	-	Nicht vorbelegt	Nur änderbar
Rufnummer für Vermittlungsplatz	9 = Welt 0 = USA	9 = Welt 0 = USA	Nur änderbar
Substitution für "#" (bei Servicekennzahlen)	75	75	löschbar
Substitution für "#" (bei Servicekennzahlen)	76	76	löschbar
Servicekennzahlen			Nur änderbar

11.1.2 Individueller Rufnummernplan

Das Kommunikationssystem ermöglicht das Einrichten eines individuellen Rufnummernplans. Dazu können die Standardwerte der Rufnummern und Kennzahlen geändert werden. Bei einem Reload des Kommunikationssystems werden die Werte auf den Standard zurückgesetzt.

Folgende Aktionen sind dabei hilfreich:

- Standard-Rufnummern löschen: bis auf einige Ausnahmen (spezielle Standard-Rufnummern) können Standard-Rufnummern zusammenhängend gelöscht werden. Diese Rufnummern sind in der Tabelle des Standardrufnummernplans in der Spalte "Aktion" mit "löschbar" gekennzeichnet.
- Spezielle Standard-Rufnummern ändern: diese Rufnummern dürfen nicht gelöscht werden. Allerdings lassen sich die Werte dieser Rufnummern ändern. Diese Rufnummern sind in der Tabelle des Standardrufnummernplans in der Spalte "Aktion" mit "nur änderbar " gekennzeichnet.
- Rufnummern und Teilnehmerdaten importieren: über eine XML-Datei können Teilnehmerdaten während der Erstinstallation importiert werden. Dabei werden auch Rufnummer und Durchwahlrufnummer der Teilnehmer importiert. In der Regel wird das während der Erstinstallation durchgeführt.

Teilnehmerdatenimport über XML-Datei

Ein individueller Rufnummernplan kann über eine XML-Datei im UTF-8-Format während der Erstinstallation in das Kommunikationssystem importiert werden.

Das Administrationsprogramm OpenScape Business Assistant stellt unter **Service-Center** > **Dokumente** > **CSV-Vorlagen** die Datei `csv-templates.zip` zur Verfügung. Diese Zip-Datei enthält u.a. die folgenden Dateien inkl. Beschreibung.

- `portdata_xml_import_empty.xml`

  Diese Vorlage enthält Register ohne Beispieldatensätze. Es können z.B. mit Microsoft Excel neue Datensätze eingetragen werden.

- `portdata_xml_import_example.xml`

  Diese Vorlage enthält Register mit Beispieldatensätzen. Diese können z.B. mit Microsoft Excel überschrieben werden. Nicht benötigte Datensätzen sollten gelöscht werden.
- `portdata_xml_import_syntax.txt`

  Beschreibung in Deutsch und Englisch zum korrekten Anlegen der Datensätze.

11.1.2.1 Wie Sie Standard-Rufnummern löschen oder ändern

Sie können einige der Standard-Rufnummern löschen und anschließend über die Wizards neu definieren. Für die nicht löschbaren speziellen Standard-Rufnummern können Sie die vorbelegten Werte ändern.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

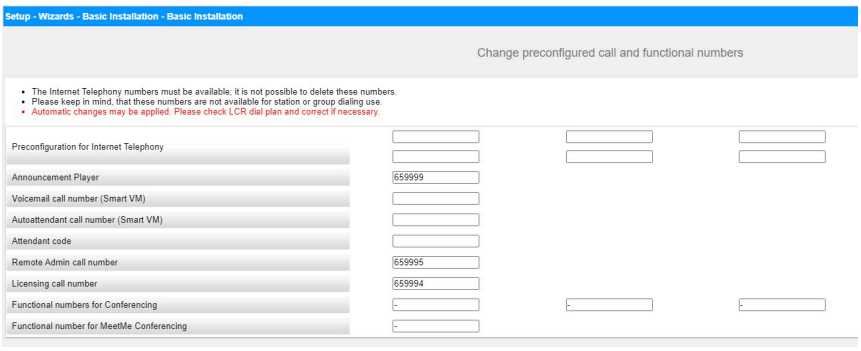
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.
3) Klicken Sie auf **Weiter**.

Anmerkung: Eine Übersicht über die aktuell konfigurierten Rufnummern können Sie sich anzeigen lassen, indem Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen** aktivieren und auf **Funktion ausführen** klicken.

---

4) Aktivieren Sie das Optionsfeld **Alle Rufnummern löschen**.
5) Aktivieren Sie in der Sicherheitsabfrage das Kontrollkästchen **Alle Rufnummern löschen**.
6) Klicken Sie auf **Funktion ausführen**.



7) Ändern Sie bei Bedarf in den Feldern die vorbelegten Werte der speziellen Standard-Rufnummern.
8) Klicken Sie auf **OK**. Die Rufnummern werden gelöscht und eventuelle Änderungen an den speziellen Standard-Rufnummern durchgeführt.
9) Klicken Sie auf **Abbrechen**, um den Wizard **Basisinstallation** zu beenden.

11.1.2.2 Wie Sie spezielle Standard-Rufnummern ändern

Sie können die für spezielle Funktionen vordefinierten Rufnummern ändern.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

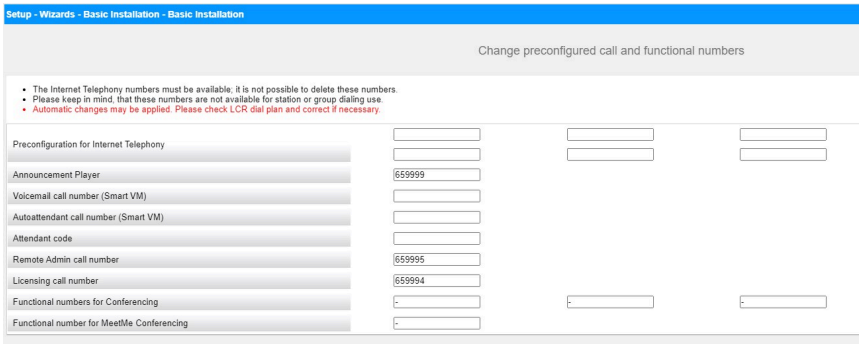
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.
3) Klicken Sie auf **Weiter**.

Anmerkung: Eine Übersicht über die aktuell konfigurierten Rufnummern können Sie sich anzeigen lassen, indem Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen** aktivieren und auf **Funktion ausführen** klicken.

---

4) Aktivieren Sie das Optionsfeld **Vorkonfigurierte Rufnummern ändern**.
5) Klicken Sie auf **Funktion ausführen**.



6) Geben Sie in den Feldern die gewünschten Rufnummern und Kennzahlen ein und klicken Sie auf **OK**. Die neuen Rufnummern und Kennzahlen sind gespeichert.

Anmerkung: Die hier konfigurierten Rufnummern können nicht als Teilnehmerrufnummern, Durchwahlrufnummern oder Gruppenrufnummern vergeben werden.

---

7) Klicken Sie auf **Abbrechen**, um den Wizard **Basisinstallation** zu beenden.

11.1.2.3 Wie Sie Rufnummern und Teilnehmerdaten importieren

Über eine XML-Datei können Sie vorab definierte Teilnehmerdaten importieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Eine XML-Datei im UTF-8-Format mit den eingetragenen Daten liegt vor. Eine XML-Vorlage finden Sie unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.
3) Klicken Sie auf **Weiter**.

Anmerkung: Eine Übersicht über die aktuell konfigurierten Rufnummern können Sie sich anzeigen lassen, indem Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen** aktivieren und auf **Funktion ausführen** klicken.

---

4) Aktivieren Sie das Optionsfeld **XML-Datei mit Teilnehmerdaten importieren**.
5) Klicken Sie auf **Funktion ausführen**.
6) Wählen Sie mit **Durchsuchen** die erstellte XML-Datei aus und klicken Sie auf **Öffnen**.
7) Klicken Sie anschließend auf **OK**. Die Teilnehmerdaten werden importiert.
8) Klicken Sie auf **Abbrechen**, um den Wizard **Basisinstallation** zu beenden.

11.2 Anforderungen an die LAN-Telefonie

Unter LAN-Telefonie versteht man das Kommunizieren von IP-Teilnehmern innerhalb des internen Netzes (LAN). Um die Qualität der Sprachübertragung bei der LAN-Telefonie sicherzustellen, müssen die verwendeten IP-Netze und das Kommunikationssystem bestimmte Anforderungen erfüllen. Die Sprachqualität und die Zuverlässigkeit der Sprachkommunikation hängen hierbei von der eingesetzten Netzwerktechnik ab.

Um eine verlustfreie Übertragung und eine gute Sprachqualität zu gewährleisten, werden die Sprachsignale mit Hilfe von Audio-Codecs digitalisiert und mit speziellen Verfahren (Quality of Service) so gekennzeichnet, dass die Sprachübertragung gegenüber der Datenübertragung vorrangig behandelt wird.

Anforderungen

- LAN mit mind. 100 Mbit/s und Full-Duplex
- Jede Komponente im IP-Netz muss an einem eigenen Port an einem Switch oder einem Router abgeschlossen sein; keinen HUB verwenden.
- Höchstens 50 ms Verzögerung in einer Richtung (One Way Delay); höchstens 150 ms Gesamtverzögerung
- Höchstens 3% Paketverlust; wird Fax/Modem über G.711 verwendet, darf der Paketverlust 0,05% nicht übersteigen.
- Höchstens 20 ms Jitter
- Unterstützung für Quality of Service (QoS): IEEE 802.p, DiffServ (RFC 2474) oder ToS (RFC 791)
- Höchstens 40% Netzwerkauslastung

11.2.1 Audio-Codecs

Als Audio-Codec bezeichnet man ein Programm, das Sprache in digitale Datenpakete (IP-Pakete) codiert und umgekehrt wieder decodiert. Abhängig vom verwendeten Audio-Codec können die Daten unterschiedlich stark komprimiert werden. Durch die Komprimierung wird bei der Übertragung des IP-Pakets weniger Bandbreite benötigt als ohne Komprimierung. Bei der Decodierung der Datenpakete kann es allerdings zu Einbußen der Sprachqualität und der Kontinuität der Wiedergabe kommen.

Damit die Daten nach dem Transport auch wieder korrekt in Sprache umgewandelt werden können, muss der Empfänger den gleichen Codec wie der Sender benutzen.

Unterstützte Audio-Codecs

Folgende Audio-Codecs werden unterstützt:

- G.729A, G.729AB: Sprachkodierung mit 8 Kbit/s - gute Sprachqualität.
- G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt.

Den Audio-Codecs können Prioritäten von 1 (hoch) bis 4 (niedrig) zugewiesen werden. Das Kommunikationssystem versucht automatisch, für jede Verbindung einen Audio-Codec mit einer möglichst hohen Priorität zu verwenden. Wird ein Audio-Codec mit geringer Sprachkomprimierung (guter Sprachqualität) verwendet, wird das Netz höher ausgelastet. Bei intensiver IP-Telefonie kann das bei einem durch Datentransfer bereits ausgelasteten Netz zu einer Verschlechterung der Sprachqualität führen.

Bei einigen Codecs kann das Kommunikationssystem eine Sprechpausenerkennung (VAD, Voice Activity Detection) aktivieren. Bei langen Sprechpausen kann somit die Last auf das Netz reduziert werden.

Für jeden Codec kann die Rahmengröße (Größe des IP-Pakets) von 10 bis zu 90 Millisekunden angegeben werden. Damit legen Sie die Abtastrate fest, mit der das Sprachsignal in IP-Pakete zerlegt wird. Ein höherer Wert (z. B. 90 ms) bedeutet einerseits ein besseres Verhältnis von Nutzdaten zum IP-Paket-Overhead, andererseits aber eine größere Verzögerung bei der Übertragung.

Es besteht die Möglichkeit, die ressourcen-hungrigen G.729-Codecs zu deaktivieren und nur die G.711-Codecs zu verwenden. Damit wird die Anzahl der möglichen, parallel geführten Gespräche optimiert. Wird diese Funktion aktiviert, ist ein Neustart des Systems nötig.

In OSBiz X-Systemen endet die Nutzlast im System, so dass die Benutzer mit einem vom System unterstützten Codec sprechen. Zum Beispiel hat das HFA-Telefon zunächst den Codec G.722 festgelegt. Das System unterstützt den G.722-Codec nicht und der G.711-Codec wurde als erste Option festgelegt. In diesem Fall sprechen beide Benutzer mit dem G.711-Codec. Bei OSBiz S-Systemen sprechen die Benutzer mit dem G.722-Codec, solange ein End-to-End Payload vorhanden ist.

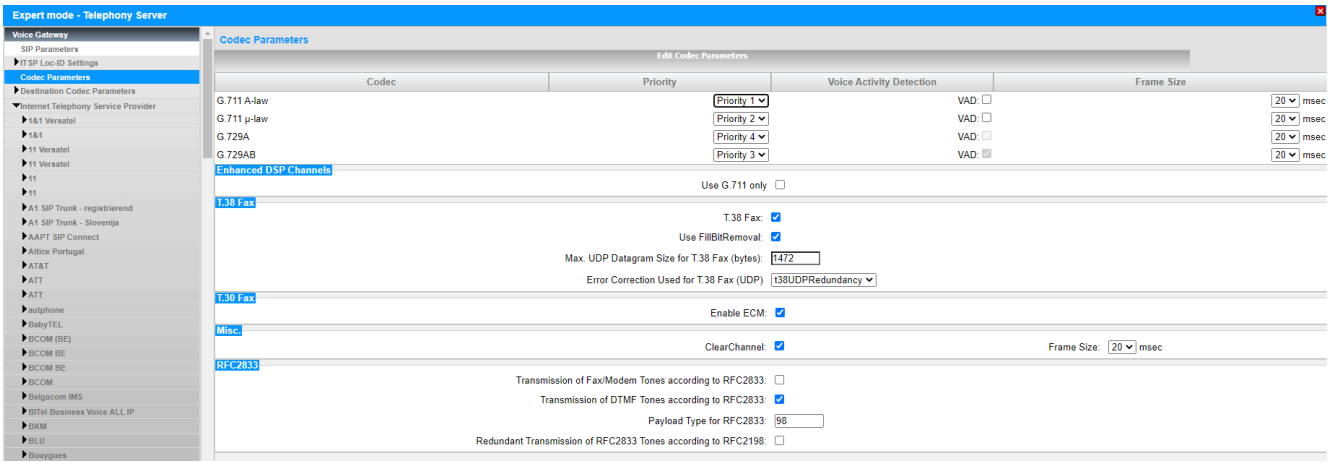
11.2.1.1 Wie Sie Audio-Codec-Parameter konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.
3) Klicken Sie im Menübaum auf **Codec-Parameter**.



4) Ordnen Sie den gewünschten Audio-Codecs über die Aufklappliste **Priorität** eine Priorität von 1 (hoch) bis 4 (niedrig) zu.
5) Aktivieren oder deaktivieren Sie bei den gewünschten Audio-Codecs das Optionsfeld **Sprechpausenerkennung (VAD)**.
6) Legen Sie bei den gewünschten Audio-Codecs im Feld **Rahmengröße** die Größe fest, in die der Audio-Codec die IP-Sprachpakete zerlegt.

Anmerkung: Sie müssen für alle Codecs den gleichen Wert eingeben, z. B. 20 msec. Es ist nicht möglich, für jeden Codec unterschiedliche Werte zu konfigurieren.

---

7) Wenn Sie nur die beiden G.711-Audio-Codecs verwenden wollen, aktivieren Sie im Bereich **Erweiterte DSP-Kanäle** das Kontrollkästchen **Nur G.711 verwenden**.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.2.1.2 Wie Sie Audio-Codec-Parameter einem Ziel zuordnen

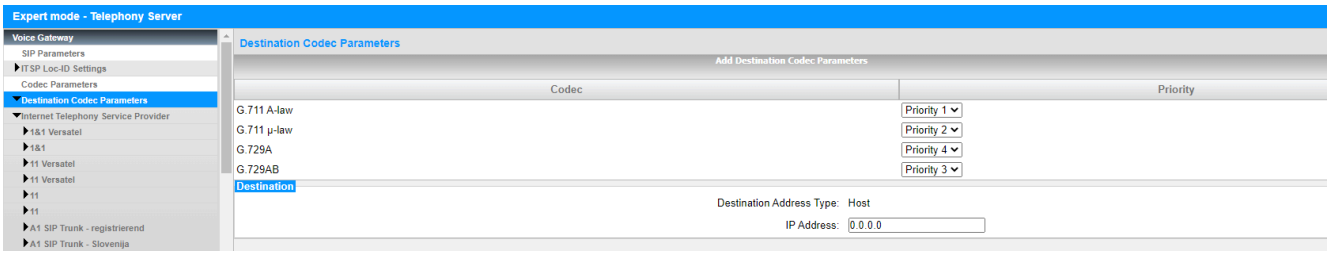
Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.

3) Klicken Sie im Menübaum auf **Ziel-Codec-Parameter**.



4) Ordnen Sie den gewünschten Audio-Codecs über die Aufklappliste **Priorität** eine Priorität von 1 (hoch) bis 4 (niedrig) zu.
5) Geben Sie unter **IP-Adresse** die IP-Adresse des Ziels ein, dem die zuvor eingestellten Prioritäten der Audio-Codec zugeordnet werden sollen (`z. B. 192.168.1.10`).
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.2.2 Übertragung von Tönen nach RFC2833

Die Übertragung von DTMF-Tönen und von Fax-/Modem-Tönen nach RFC2833 kann aktiviert oder deaktiviert werden.

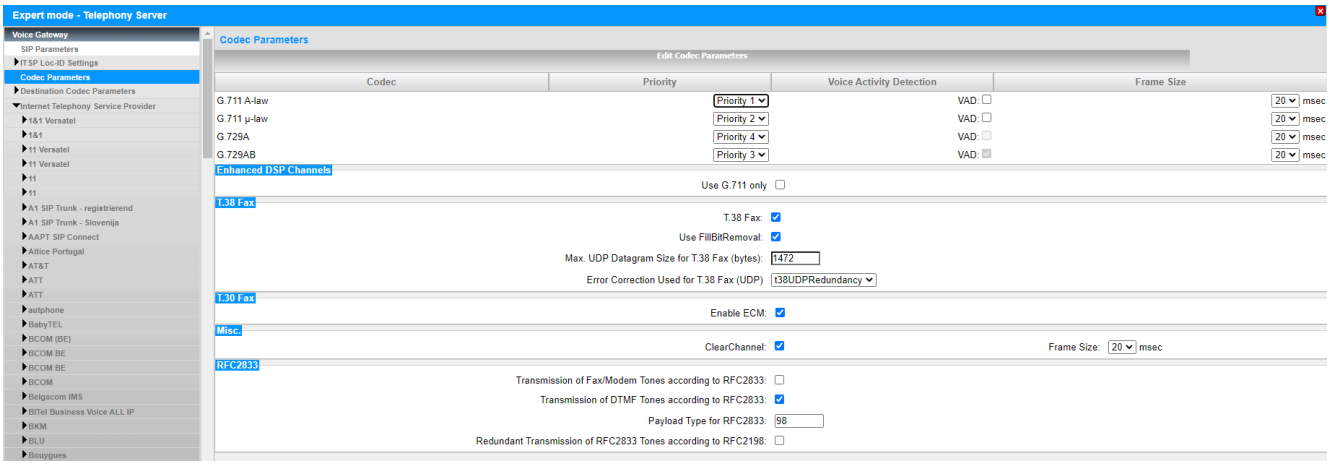
11.2.2.1 Wie Sie die Übertragung von Fax- und Modem-Tönen nach RFC2833 aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.
3) Klicken Sie im Menübaum auf **Codec-Parameter**.



4) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Übertragung von Fax/Modem Tönen nach RFC2833**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Übertragung von Fax/Modem Tönen nach RFC2833**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

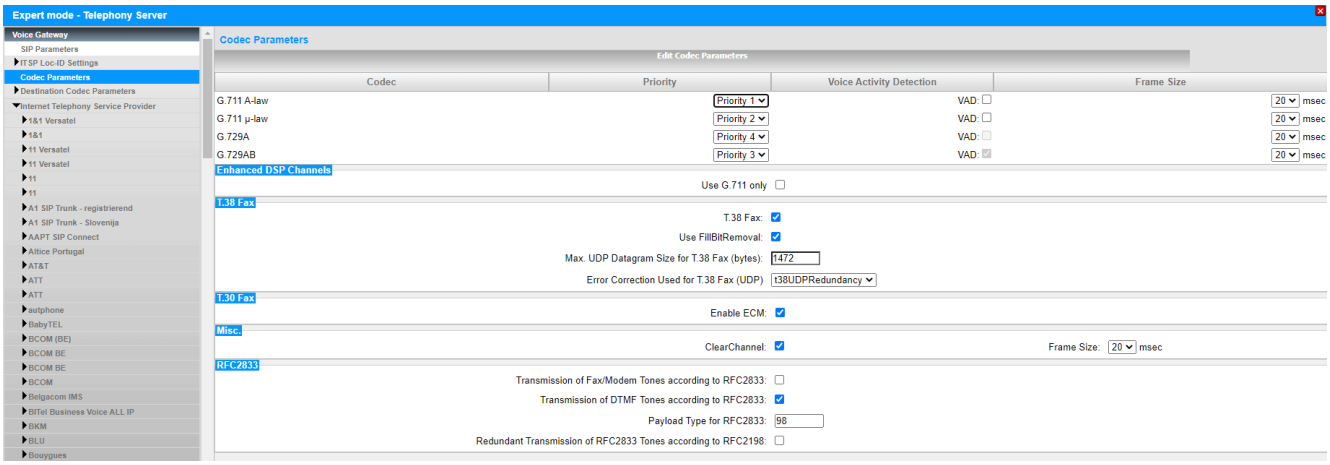
11.2.2.2 Wie Sie die Übertragung von DTMF-Tönen nach RFC2833 aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.
3) Klicken Sie im Menübaum auf **Codec-Parameter**.



4) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Übertragung von DTMF Tönen nach RFC2833**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Übertragung von DTMF Tönen nach RFC2833**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.2.3 Quality of Service

Quality of Service (QoS) umfasst unterschiedliche Verfahren, um die höchstmögliche Qualität und Verlustfreiheit bei der Übertragung von Datenpaketen (IP-Pakete) zu gewährleisten. Um bei der Sprachübertragung eine gute Sprachqualität zu erreichen, werden mit QoS im IP-Netz die IP-Sprachpakete vor den IP-Datenpaketen anderer Applikationen priorisiert.

Für die Priorisierung werden die IP-Pakete mit einer besonderen Markierung (Codepunkt) versehen. Die Priorisierungsinformation bewirkt eine Einstufung

in unterschiedliche Klassen. Wenn die im IP-Netz vorhandenen Komponenten (z.B. Kommunikationssystem, SIP-Teilnehmer und Internet-Router) QoS unterstützen, können sie diesen Klassen unterschiedliche Bandbreite zuordnen und somit die IP-Sprachpakete bevorzugt transportieren.

Prioritätsklassen nach DiffServ

Für die Priorisierung nach dem DiffServ-Verfahren werden verschiedene Codepunkte für das Type of Service (ToS)- Feld definiert, um die Übertragung von IP-Paketen in unterschiedliche Klassen einteilen zu können.

- Codepunkt Expedited Forwarding (EF): Garantiert eine konstante Bandbreite. Für IP-Pakete, die mit diesem Codepunkt markiert sind, steht immer die gleiche Bandbreite zur Verfügung. Wird der festgelegte Wert erreicht, werden alle Pakete verworfen, die diese Bandbreite überschreiten.
- Codepunkt Assured Forwarding (AF): Garantiert eine minimale Bandbreite. IP-Pakete, die mit diesem Codepunkt markiert sind, haben eine niedrigere Priorität als EF und müssen sich die von EF nicht genutzte Bandbreite teilen. Wird der festgelegte Wert erreicht, werden alle IP-Pakete, die diese Bandbreite überschreiten würden, verworfen.

  Für AF sind vier Klassen reserviert: AF1x (niedrige Priorität), AF2x, AF3x und AF4x (hohe Priorität), wobei x für einen von drei Dropping-Stufen steht: niedrig (1), mittel (2) und hoch (3). Bei niedrig werden Pakete lange zwischengespeichert, bei hoch werden Pakete früh verworfen, wenn sie nicht weitertransportiert werden können.
- Best Effort (BE): Unmarkierte IP-Pakete (Type of Service (ToS)-Feld=00) werden mit niedrigster Priorität behandelt.

Prioritätsklassen nach IP-Precedence

Neben dem DiffServ-Verfahren existieren verschiedene ältere Definitionen, die eine Priorisierung auf Basis des ToS-Feldes vornehmen. Für eine bestmögliche Anpassung des Kommunikationssystemes an die ggf. erforderlichen Einstellungen im Kundennetz können z.B. für IP-Precedence die Klassen 3 bis 7 (CS3-CS7) ausgewählt werden.

Individuelle Prioritätsklassen

Falls keine der voreingestellten Möglichkeiten im Kundennetz verwendet wird, kann der ToS-Wert auch direkt manuell eingestellt werden. Der eingestellte Wert wird dezimal 0-63 eingestellt und in die oberen 6 Bits des ToS-Bytes übernommen (z.B. 41 = 101-001-00 = 0xA4).

Tabelle der möglichen Prioritätsklassen

Prioritätsklasse	ToS-Wert Binär	ToS-Wert Hexadezimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58

Prioritätsklasse	ToS-Wert Binär	ToS-Wert Hexadezimal
AF31	011-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60
CS4	100-000-00	80
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Manuelle Eingabe	xxx-xxx-00	0-63 (dezimal)

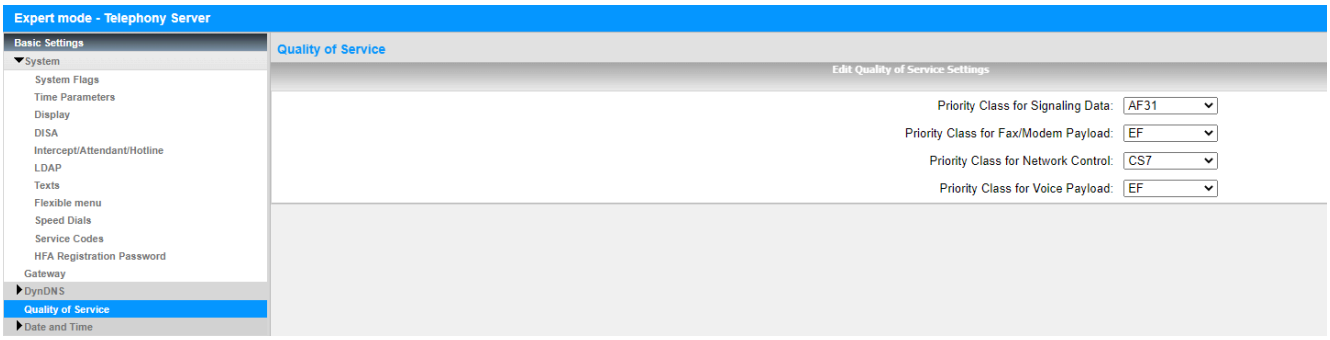
11.2.3.1 Wie Sie Quality of Service konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Quality of Service**.



4) Wählen Sie aus der Aufklappliste **Prioritätsklasse für Signalisierungsdaten** die gewünschte Prioritätsklasse aus.

5) Wählen Sie aus der Aufklappliste **Prioritätsklasse für Fax/Modem-Payload** die gewünschte Prioritätsklasse aus.
6) Wählen Sie aus der Aufklappliste **Prioritätsklasse für Netzwerksteuerung** die gewünschte Prioritätsklasse aus.
7) Wählen Sie aus der Aufklappliste **Prioritätsklasse für Sprach-Payload** die gewünschte Prioritätsklasse aus.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.3 IP-Teilnehmer

IP-Teilnehmer sind über das LAN mit dem Kommunikationssystem verbunden. In der Regel ist ein IP-Teilnehmer ein LAN- oder WLAN-Telefon.

Folgende IP-Protokolle werden unterstützt:

- Herstellerabhängiges Protokoll des Kommunikationssystems

  Das Kommunikationssystem verwendet das auf Basis von H.323 weiterentwickelte CorNet-IP (CorNet-Internet-Protokoll) für die LAN-Telefonie innerhalb des internen Netzes. Mit CorNet-IP können alle Telefonleistungsmerkmale des Kommunikationssystems genutzt werden.
- SIP (Session Initiation Protocol)

  SIP wird üblicherweise bei der Internet-Telefonie eingesetzt, ist aber nicht darauf beschränkt. Es kann z.B. auch bei der Telefonie in internen Netzen verwendet werden. Mit SIP können aber nicht alle Telefonleistungsmerkmale des Kommunikationssystems genutzt werden.

Es gibt folgenden Typen von IP-Teilnehmern:

- **System-Client**: Ein System-Client ist ein IP-Teilnehmer, der über CorNet-IP alle Leistungsmerkmale des Kommunikationssystems nutzen kann. Das kann ein IP-Systemtelefon sein, wie z.B. ein OpenStage 60 HFA oder ein PC mit CTI-Software, wie OpenScape Personal Edition.
- **SIP-Client**: Ein SIP-Client ist ein IP-Teilnehmer, der das Protokoll SIP nutzt. Er kann über SIP nur einen eingeschränkten Leistungsumfang des Kommunikationssystems nutzen. Ein SIP-Client ist z.B. ein SIP-Telefon wie das OpenStage 15 S.
- **Deskshare User**: Ein Deskshare User ist ein IP-Teilnehmer, der sich auf einem anderen IP-Systemtelefon anmelden kann (Mobile Login) und dieses Telefon wie sein eigenes Telefon nutzen kann (inkl. Rufnummer).
- **RAS User**: Einem RAS User (Remote Access Service User) wird über den ISDN-Anschluss der Zugang zum IP-Netz gewährt. Dadurch kann das Kommunikationssystem ferngewartet werden.

Für jeden angeschlossenen IP-Teilnehmer ist eine Teilnehmer-Lizenz "IP User" nötig.

Zwei IP-Teilnehmer sind reserviert für den Online User und für den Remote-Zugang über ISDN. Diese IP-Teilnehmer benötigen keine Teilnehmer-Lizenz. Falls einer oder mehrere dieser drei reservierten IP-Teilnehmer nicht benötigt werden, können diese Teilnehmer über den Experten-Modus zu normalen IP-Teilnehmern umkonfiguriert werden. Dann werden für diese IP-Teilnehmer allerdings Teilnehmer-Lizenzen gebraucht.

IP-Teilnehmer konfigurieren

Folgende Konfigurationen zu einem IP-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard **IP-Endgeräte** (siehe IP-Teilnehmer konfigurieren).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe >Station>Station>IP Clients).

OpenScape Desk Phone IP Systemtelefone werden standardmäßig mit der SIP-Software ausgeliefert. Sobald ein OpenScape Desk Phone IP Systemtelefon im WBM als **System Client** konfiguriert wird, wird automatisch die im Kommunikationssystem gespeicherte HFA-Software auf das IP-Systemtelefon geladen.

11.4 SIP-Stationen

SIP-Stationen sind IP-Stationen, die das Session Initiation Protocol (SIP) für die Kommunikation verwenden. SIP-Stationen können mit diesem Protokoll auf eine begrenzte Anzahl von Funktionen des Kommunikationssystems zugreifen. SIP-Stationen sind wie IP-Stationen über das LAN mit dem Kommunikationssystem verbunden.

Eine SIP-Station ist beispielsweise ein WLAN-Telefon oder ein LAN-Telefon wie das OpenStage 15 S.

Für jede angeschlossene SIP-Station ist eine "IP-Benutzer"-Stationslizenz erforderlich.

SIP-Authentifizierung

Um die Sicherheit des internen Netzwerks zu gewährleisten, ist es wichtig, dass SIP-Abonnenten am Kommunikationssystem mit den unten beschriebenen Werten authentifiziert werden. Diese Werte müssen im WBM des Kommunikationssystems für jeden SIP-Teilnehmer und auch an jedem SIP-Telefon selbst konfiguriert werden. Zum Schutz vor SIP-Angriffen wird eine Authentifizierung dringend empfohlen!

- Kennwort

  Passwort für die Authentifizierung: frei zugewiesen; mindestens 8 Zeichen bis maximal 20 Zeichen. Das Passwort sollte mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Für jeden SIP-Abonnenten sollte ein separates Passwort vergeben werden.
- SIP User ID / Benutzername

  Benutzername für die Authentifizierung: vorab zugewiesen; kann bei Bedarf geändert werden, maximal 20 Zeichen. Jeder SIP-Abonnent hat eine andere vorab zugewiesene SIP User ID.
- Realm

  Zone oder Domäne für Authentifizierung: frei zugewiesen; kann bei Bedarf geändert werden, max. 20 Zeichen. Der Realm für alle SIP-Abonnenten ist mit dem gleichen Wert vorbestimmt. Es kann beliebig geändert werden, z.B. im Hostnamen oder Domänennamen des Kommunikationssystems.

Konfiguration von SIP-Stationen im Kommunikationssystem

Die folgenden Konfigurationen können im WBM des Kommunikationssystems für eine IP-Station durchgeführt werden:

- Konfiguration von Standardparametern mit dem **IP-Telefonassistenten** (siehe So konfigurieren Sie SIP-Stationen).
- Konfiguration aller Parameter (Standard- und erweiterte Parameter im Expert-Modus (siehe Station>Station>IP-Clients).

Konfiguration des SIP-Telefons

Die zur Authentifizierung eines SIP-Abonnenten am Kommunikationssystem verwendeten Daten müssen zusätzlich direkt am SIP-Telefon eingegeben werden.

Konfiguration der Authentifizierungsdaten am SIP-Telefon (siehe Konfigurieren der Authentifizierungsdaten am SIP-Telefon).

Funktionen, die mit SIP Telefonen verwendet werden können

Die folgenden Funktionen können mit SIP-Telefonen verwendet werden:

- Ein- und ausgehende Anrufe mit Anzeige von Rufnummer und Name
- Halten, Umschalten/Verbinden, Beratung
- Anrufübertragung (gescreent/ungescreent)
- Anruf annehmen
- Sofortige Anrufweiterleitung, bei Besetzt und nach Timeout
- Dreiparteienkonferenz
- Anruflisten, Anzeige des Wartens von Nachrichten
- Klingel-Abschaltung am Telefon, Anruf ablehnen, Anrufweiterleitung
- Anklopfen
- Mitgliedschaft in Gruppen (ohne Anzeige der Gruppennummer)
- Verschiedene Anrufe für interne, externe und Rückrufe
- Mailbox LED - Anzeige der Warten-Meldung
- DTMF-Wählung, z.B. für den Betrieb von Voicemail-Boxen
- Verwendung der UC-Clients
- Automatische Software-Updates (bei Verwendung des DLI)

Anmerkung: Die Bereitstellung mit einem Multichannel Contact Center wurde nicht freigegeben (z.B. Übertragung in UCD-Gruppen).

Abhängig vom Telefon können die verfügbaren Funktionen eingeschränkt werden; siehe Wiki unter:

`http://wiki.unify.com/wiki/SIP_devices_configuration_examples`

Mit SIP-Telefonen können folgende Funktionen, die über Service-Codes mit * und oder # aktiviert werden, verwendet werden:

- Alle Dienste zurücksetzen: #0
- Anrufweiterleitung: *1xf (x = 1 - alle, 2 - intern, 3 - extern) (f = Weiterleitungsnummer)
- Anrufweiterleitung aus: #1

- Sammelanschluss verlassen/wieder beitreten: #85g/*85g (g = Gruppennummer, optionale Markierung erforderlich, wenn in mehreren Gruppen)
- Anruf-ID unterdrücken/aktivieren (CLIR): *86/#86
- Kurzwahl: * 7nnnn (nnnn = Kurzwahlnummer)
- Türöffner: *61

Tipp: Für die beste Kompatibilität mit SIP-Geräten von Drittanbietern wird empfohlen, * oder # Ersatz-Codes zu verwenden. Der SIP-Benutzer muss die vollständige Dienst-Codesequenz als Blockwahl senden.

Tipp: Im Gegensatz zu HFA-Geräten gibt es keine Benutzerinteraktion oder Anleitung für Dienst-Codesequenz auf SIP-Geräten. Die vollständige Dienst-Codesequenz muss sofort gewählt werden.

Funktionen, die mit SIP Telefonen und myPortal/myAttendant verwendet werden können

SIP-Telefone, die mit myPortal und myAttendant verwendet werden können, müssen folgende Anforderungen erfüllen:

- 3PCC gemäß RFC 3725 wird unterstützt.
- Die Funktion "Anklopfen" wird unterstützt.
- Die lokale Funktion Nicht stören ist deaktiviert.

Die vollständige Funktionalität der Funktionen hängt vom verwendeten SIP-Telefon ab und kann nicht garantiert werden. Ein erfolgreicher Test der unten aufgeführten Funktionen wurde mit den OpenStage SIP Telefonen durchgeführt.

Verbindungs-/ruforientierte Features:

- Anruf tätigen
- Anruf umleiten
- Anruf annehmen
- Anruf fortsetzen
- Anwendungsgesteuerte Konferenz
- Stellen Sie den Anruf auf Warteschleife
- Alternativ (Umschalten/Verbinden)
- Konsultation
- Trennen
- Übergeben

Telefonorientierte Funktionen:

- Anrufschutz
- Anrufumleitung

11.5 UP0-Teilnehmer

Ein UP0-Teilnehmer nutzt für die Übertragung der digitalen Signale eine $U_{P0/E}$-Leitung. UP0-Teilnehmer werden über UP0-Schnittstellen an das Kommunikationssystem angeschlossen und sind Systemtelefone, wie z.B. ein

OpenStage 60T. UP0-Teilnehmer können den kompletten Funktionsumfang des Kommunikationssystems nutzen.

Für einen UP0-Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1

  an die $U_{P0/E}$-Schnittstellen des Mainboards.
- OpenScape Business X3/X5

  an die $U_{P0/E}$-Schnittstellen des Mainboards oder bei vielen UP0-Teilnehmern an zusätzlich gesteckte $U_{P0/E}$-Baugruppen.
- OpenScape Business X8

  an zusätzlich gesteckte $U_{P0/E}$-Baugruppen.
- OpenScape Business S

  Kein Anschluss möglich.

Für jeden angeschlossenen UP0-Teilnehmer ist eine Teilnehmer-Lizenz "TDM User" nötig. Auch Systemtelefone, die im Slave-Modus angeschlossen sind, benötigen eine Teilnehmerlizenz.

Konfiguration der UP0-Teilnehmer

Folgende Konfigurationen zu einem UP0-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard **UP0-Endgeräte** (siehe UP0-Teilnehmer konfigurieren).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe Teilnehmer>Teilnehmer>UP0 Teilnehmer).

11.6 DECT-Teilnehmer

Ein DECT-Teilnehmer nutzt für die Übertragung der digitalen Signale eine Cordless-Basisstation. Ein DECT-Teilnehmer ist ein DECT-Telefon.

Für einen DECT-Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1W/X1R/X3W/X3R/X5R

  Cordless-Basisstation an eine $U_{P0/E}$-Schnittstelle des Mainboards.
- OpenScape Business X8

  Cordless-Basisstation an eine oder mehrere SLMUC-Baugruppen.
- OpenScape Business S

  DECT IP-Basisstation im LAN

Der Anschluss einer Cordless-Basisstation nennt sich integrierte Cordless-Lösung. Damit stehen fast alle Funktionen des Kommunikationssystems zur Verfügung.

Die Integration einer DECT IP-Basisstation in das interne Netz nennt sich Cordless IP. Da in diesem Fall nur das SIP-Protokoll genutzt werden kann, stehen nicht alle Funktionen des Kommunikationssystems zur Verfügung.

Für jeden angeschlossenen DECT-Teilnehmer ist eine Teilnehmer-Lizenz „TDM User“ nötig.

Für die Beschreibung und Konfiguration der integrierten Cordless-Lösung siehe Integrierte Cordless-Lösung.

Konfiguration der DECT-Teilnehmer

Folgende Konfigurationen zu einem DECT-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Assistenten **DECT-Endgeräte** (siehe Wie Sie DECT-Teilnehmer konfigurieren).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe Teilnehmer>Teilnehmer>DECTTeilnehmer>DECT-Teilnehmer).

DECT IP-Teilnehmer werden wie normale SIP-Teilnehmer konfiguriert.

11.7 Mitel SIP DECT-Teilnehmer

Für Mitel SIP DECT-Teilnehmer stehen die folgenden Anschlussmöglichkeiten zur Verfügung:

- OpenScape Business S-System
- OpenScape Business V3-Hardware (OCCe)

Bereitstellung von Mitel SIP DECT RFP-Teilnehmern

Der Prozess umfasst die folgenden allgemeinen Schritte:

1) Konfigurieren Sie den DHCP mit einer statischen IP-Adresse für die OMM-Basisstation.
2) Die Basisstation erhält dann eine IP-Adresse und startet die OMM-Anwendung.
3) Konfigurieren Sie die Basisstation über ihre Webschnittstelle.
4) Die Basisstation holt sich automatisch die Konfigurationsdateien von OpenScape Business.
5) Wenn sich ein Mobilteil anmeldet, ruft die Basisstation auch die Konfigurationsdatei des Benutzers ab und richtet das Mobilteil ein.

Konfiguration von Mitel SIP-DECT-Teilnehmern über WBM

Es sind folgende Konfigurationsschritte durchzuführen:

1) Aktivieren Sie den DHCP-Server und stellen Sie eine statische IP-Adresse für die OMM-Basisstation bereit (siehe Netzwerkschnittstellen > Hauptplatine > DHCP-Modus > DHCP-Server > Statische IP-Adressen).
2) Konfiguration der Standardparameter mit dem Assistenten für Mitel SIP-DECT-Geräte (siehe So konfigurieren Sie Mitel SIP-DECT-Teilnehmer).
3) Konfiguration von SIP-Teilnehmern und deren Parametern über den Expertenmodus (siehe So konfigurieren Sie SIP-Teilnehmern über den Expertenmodus).

11.8 ISDN-Teilnehmer

Ein ISDN-Teilnehmer nutzt für die Übertragung der digitalen Signale den S_0-Bus. Deshalb wird er auch oft S_0-Teilnehmer genannt. Mit dem

Kommunikationssystem wird der ISDN-Teilnehmer über die S_0-Schnittstellen verbunden.

Für einen S_0-Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1

  an eine S_0-Schnittstelle des Mainboards.
- OpenScape Business X3/X5

  an eine S_0-Schnittstelle des Mainboards oder an eine S_0-Baugruppe.
- OpenScape Business X8

  an eine oder mehrere S_0-Baugruppen.
- OpenScape Business S

  an zusätzlich benötigte Gateways oder Adapter

Folgende ISDN-Teilnehmer können angeschlossen werden:

- ISDN-Telefon
- Fax Gruppe 4
- ISDN-Modem
- PC mit ISDN-Karte

Folgende Typen von ISDN-Teilnehmern können definiert werden:

- Standard: für ISDN-Telefon, Fax Gruppe 4, ISDN-Modem oder PC mit ISDN-Karte
- Fax: Voraussetzung für die Einrichtung der Taste "Info von Fax/ Anrufbeantworter". Wird z.B. ein PC mit ISDN-Karte und Faxsoftware an den S_0-Bus angeschlossen und ihm der Typ "Fax" zugewiesen, kann auf jedem Endgerät eine Taste "Info von Fax/Anrufbeantworter" eingerichtet werden. Wenn diese Taste leuchtet, wird damit signalisiert, dass ein Fax empfangen wurde.
- Anrufbeantworter: Voraussetzung für die Übernahme eines Gespräches, wenn der Anrufbeantworter das Gespräch bereits angenommen hat. Wird z.B. ein Gigaset ISDN mit Anrufbeantworter angeschlossen und ihm der Typ "Anrufbeantworter" zugewiesen, kann man auf jedem Endgerät ein Gespräch übernehmen, das der Anrufbeantworter bereits angenommen hat. Dazu muss am Endgerät eine Taste mit der internen Rufnummer des Gigasets programmiert werden.

Für jeden angeschlossenen ISDN-Teilnehmer ist eine Teilnehmer-Lizenz "TDM User" nötig.

Anschluss von ISDN-Teilnehmern an die S_0-Schnittstelle

Um ISDN-Teilnehmer an das Kommunikationssystem anschließen zu können, muss mindestens eine der S_0-Schnittstellen, die für den ISDN-Teilnehmeranschluss oder den ISDN-Anlagenanschluss verwendet werden, als interner S_0-Bus (S_0-Euro-Bus) konfiguriert werden.

Anmerkung: Falls bei einem ISDN-Mehrgeräteanschluss mehrere ISDN-Teilnehmer an einer S_0-Schnittstelle angeschlossen werden (bis zu 8 ISDN-Teilnehmer möglich), muss jedem einzelnen ISDN-Teilnehmer eine eindeutige MSN

zugeordnet werden. Diese Zuordnung ist im Konfigurationsmenü des ISDN-Teilnehmers durchzuführen.

Konfiguration der ISDN-Teilnehmer

Folgende Konfigurationen zu einem ISDN-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard **ISDN-Endgeräte** (siehe ISDN-Teilnehmer konfigurieren).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter über den Experten-Modus (siehe Teilnehmer>Teilnehmer>ISDN Teilnehmer).

Nur eingerichtete Nummern für MSN zulassen

Der Administrator kann festlegen, dass weitere MSNs an einem S0-Bus nur für dort bereits vorhandene interne Rufnummern einrichtbar sind. In diesem Fall kann ein Teilnehmer nicht unberechtigt eine MSN hinzuzufügen, indem er den S0-Bus mit einer weiteren MSN gehend belegt und das Kommunikationssystem dem S0-Bus daraufhin eine freie interne Rufnummer für diese MSN zuordnet.

Umstecken am Bus

Das Kommunikationssystem unterstützt das Parken eines Gesprächs am S_0-Bus mit anschließendem Ausstecken und Anschließen des Endgeräts an einer anderen Stelle, um das Gespräch dann wieder aufzunehmen – Umstecken am Bus (Terminal Portability TP). Der geparkte Teilnehmer erhält eine Displaymeldung über den Umsteckvorgang. Für den gesamten Vorgang stehen drei Minuten zur Verfügung.

Für Dienste wie Telefax, Teletex oder Datenübermittlung wird das Leistungsmerkmal nicht unterstützt.

11.8.1 Wie Sie die S_0-Schnittstelle für ISDN-Teilnehmer konfigurieren

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** können Sie eine oder mehrere S_0-Schnittstellen so konfigurieren, dass ISDN-Telefone daran angeschlossen werden können.

Voraussetzungen

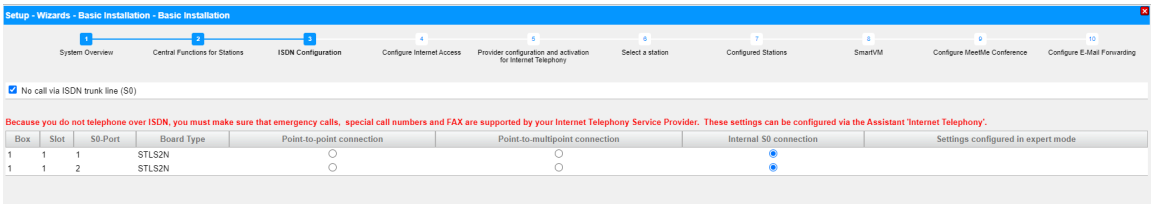
Es sind eine oder mehrere freie S_0-Schnittstellen vorhanden.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie bei dem Wizard **Amtsleitung ISDN / Analog / ITSP** auf **Bearbeiten**.

4) Klicken Sie auf **OK & Weiter**. Es werden Ihnen die vorhandenen S_0-Schnittstellen (S_0-Ports) angezeigt.



5) Lassen Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)** so wie eingestellt.
6) Aktivieren Sie bei den gewünschten S_0-Schnittstellen das Optionsfeld **interner S0-Anschluss**.

Anmerkung: Diese S_0-Schnittstellen können Sie nicht mehr für den ISDN-Amtszugang nutzen.

---

7) Klicken Sie so oft auf **OK & Weiter**, bis Sie die Meldung erhalten, dass die Änderung des Leistungsmerkmals abgeschlossen ist.
8) Klicken Sie auf **Beenden**.

11.8.2 Wie Sie nur eingerichtete Nummern für MSN zulassen

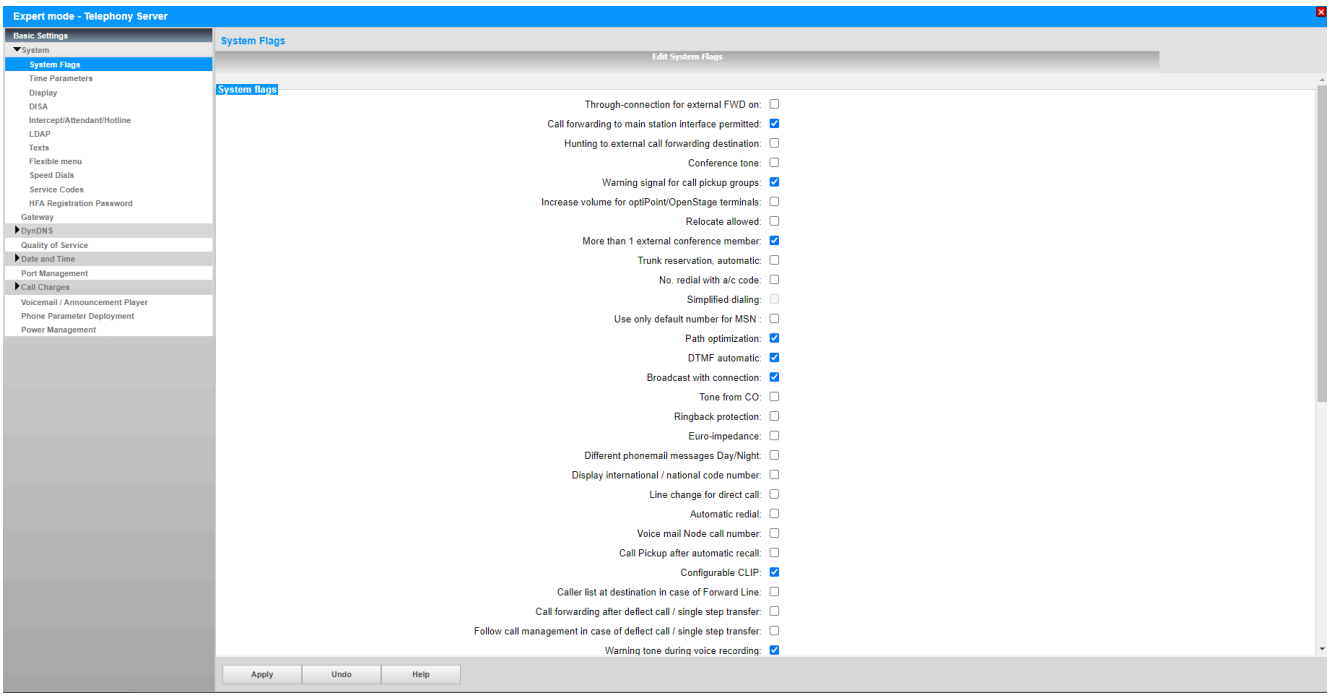
Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Systemflags**.



4) Wenn Sie nur eingerichtete Nummern für MSNs zulassen möchten, aktivieren Sie das Kontrollkästchen **Nur eingerichtete Nummer für MSN benutzen**.
5) Wenn Sie nicht nur eingerichtete Nummern für MSNs zulassen möchten, deaktivieren Sie das Kontrollkästchen **Nur eingerichtete Nummer für MSN benutzen**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.9 Analoge Teilnehmer

Ein analoger Teilnehmer (a/b-Teilnehmer) nutzt für die Übertragung der analogen Signale eine zweiadrige a/b-Leitung. Mit dem Kommunikationssystem wird der analoge Teilnehmer über die a/b-Anschlüsse verbunden.

Für einen analogen Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1

  an eine analoge Schnittstelle des Mainboards.
- OpenScape Business X3/X5

  an eine analoge Schnittstelle des Mainboards oder an eine analoge Baugruppe.
- OpenScape Business X8

  an eine oder mehrere analoge Baugruppen.
- OpenScape Business S

  an zusätzlich benötigte Gateways oder Adapter

Folgende analoge Teilnehmer können angeschlossen werden:

- Analoges Telefon
- Analoges Fax (Gruppe 3)
- Anrufbeantworter
- Modem ab 9600 bit/s
- Türsprechstelle
- Lautsprecher

Folgende Typen von analogen Teilnehmern können definiert werden:

- Standard: für analoges Telefon, Fax Gruppe 3, Anrufbeantworter oder Lautsprecher
- Fax: Voraussetzung für die Einrichtung der Taste "Info von Fax/ Anrufbeantworter". Wird z.B. ein Fax Gruppe 3 angeschlossen und ihm der Typ "Fax" zugewiesen, kann auf jedem Endgerät eine Taste "Info von Fax/ Anrufbeantworter" eingerichtet werden. Wenn diese Taste leuchtet, wird damit signalisiert, dass ein Fax empfangen wurde.
- Anrufbeantworter: Voraussetzung für die Übernahme eines Gespräches, wenn der Anrufbeantworter das Gespräch bereits angenommen hat. Wird z.B. ein Gigaset mit Anrufbeantworter angeschlossen und ihm der Typ "Anrufbeantworter" zugewiesen, kann man auf jedem Endgerät ein Gespräch übernehmen, das der Anrufbeantworter bereits angenommen hat. Dazu muss am Endgerät eine Taste mit der internen Rufnummer des Gigasets programmiert werden.
- Modem: Analoge Modems mit einer festen Geschwindigkeit von 56 kbit/s oder höher werden nicht unterstützt, da Geschwindigkeiten von 56 kbit/s oder höher nicht verarbeitet werden können.

Für jeden angeschlossenen analogen Teilnehmer ist eine Teilnehmer-Lizenz "TDM User" nötig.

Erreichbarkeit eines analogen Faxgeräts im System mit bisheriger Faxnummer

Da die Umleitung eines analogen Faxgerätes auf eine Faxnummer im System nicht möglich ist, besteht folgende Umgehungslösung: Die bisherige Faxnummer wird im System konfiguriert und erhält die ankommenden Faxnachrichten. Für das analoge Faxgerät wird ein Port konfiguriert mit der bisherigen Nummer als CLIP. Einstellbare CLIP muss aktiviert sein. Faxnachrichten nach extern zeigen die bisherige Nummer als Absender, interne Empfänger sehen die interne Nummer des Faxgerätes.

Konfiguration der analogen Teilnehmer

Folgende Konfigurationen zu einem analogen Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard **Analog-Endgeräte** (siehe Analoge Teilnehmer konfigurieren).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter über den Experten-Modus (siehe Teilnehmer>Teilnehmer>Analoge Teilnehmer).

11.10 Virtuelle Teilnehmer

Virtuelle Teilnehmer verhalten sich wie reale Teilnehmer, ihnen sind aber keine physikalischen Endgeräte zugeordnet.

Virtuelle Teilnehmer werden z.B. für die Mobiltelefon-Integration und für die Rufweiterschaltung benötigt. Diese sind wie reale Teilnehmer zu konfigurieren, um z.B. für die Signalisierung von Anrufen verwendet zu werden.

Konfiguration der virtuellen Teilnehmer

Die Konfiguration der Parameter eines virtuellen Teilnehmers wird mit dem Experten-Modus durchgeführt (siehe Teilnehmer>Teilnehmer>virtuelle Teilnehmer).

11.11 Tastenprogrammierung

Jedes Systemtelefon ist mit einer bestimmten Anzahl an Funktionstasten ausgestattet. Einige dieser Funktionstasten sind standardmäßig mit Funktionen vorbelegt. Diese Vorbelegung kann geändert und die restlichen nicht vorbelegten Funktionstasten können mit Funktionen programmiert werden.

Für die Tastenprogrammierung haben Sie folgende Möglichkeiten:

- Tastenprogrammierung über WBM

  Im WBM können über den Wizard **Tastenprogrammierung** die Tasten der angeschlossenen Systemtelefone programmiert werden.

  Über diesen Wizard kann auch für einen Teilnehmer eine Tastenbelegung programmiert werden, obwohl für diesen Teilnehmer noch kein Systemtelefon angeschlossen ist.
- Tastenprogrammierung über die UC Clients

  Nutzer der UC Clients **myPortal for Desktop**, **myPortal for Outlook** und **myAttendant** können die Tasten des Systemtelefons auch über die UC Clients programmieren (siehe Bedienungsanleitung der UC Clients).
- Tastenprogrammierung direkt am Systemtelefon

  Bei Systemtelefonen mit Display können bestimmte Funktionstasten auch direkt am Systemtelefon programmiert werden.

Mehrfachbelegung der Funktionstasten

Die Funktionstasten der Systemtelefone können zweifach belegt werden, nämlich auf der 1. Ebene und auf der 2. Ebene. Die 1. Ebene kann mit allen angebotenen Funktionen belegt werden. Die 2. Ebene kann mit externen Rufnummern belegt werden. Um die 2. Ebene verwenden zu können, muss am Systemtelefon die Ebenenumschaltetaste (Shift-key) eingerichtet sein. Die LEDs der Funktionstasten gehört dabei immer zur 1. Ebene.

Anmerkung: Bei einem **Benutzer kann die Tastenprogrammierung nicht kopiert werden, da die Funktion der automatischen Tastenbelegung MULAP-spezifisch ist und in keinem Fall kopiert werden sollte. Das Präfix ** sollte manuell von diesen Benutzern entfernt werden, damit das Kopieren der Tastenbelegung aktiviert werden kann.

11.11.1 Wie Sie die Funktionstasten der Systemtelefone programmieren

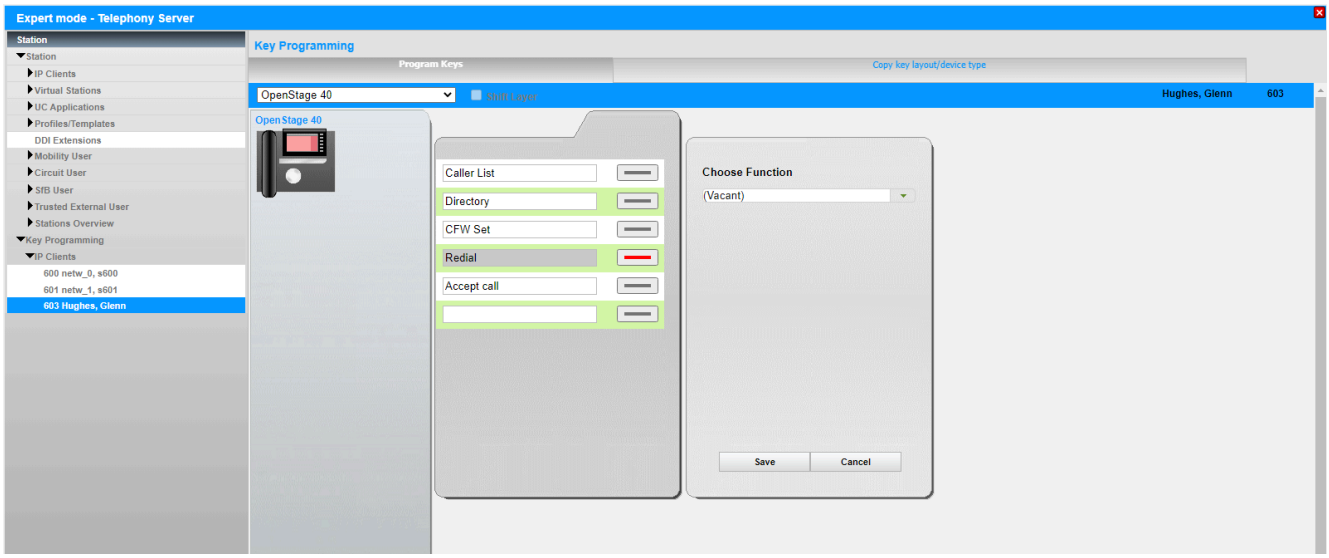
Mit dem Wizard **Tastenprogrammierung** können Sie die Funktionstasten der Systemtelefone konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Endgeräte / Teilnehmer**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Tastenprogrammierung** zu starten. Es wird die Liste aller Teilnehmer angezeigt.
4) Klicken Sie in der Zeile des gewünschten Teilnehmers auf **Bearbeiten**.
5) Ordnen Sie dem Teilnehmer das Systemtelefon zu:
   - Ist für den Teilnehmer bereits ein Systemtelefon angeschlossen, wird Ihnen eine vereinfachte Darstellung des Systemtelefons angezeigt.
   - Ist für den Teilnehmer noch kein Systemtelefon angeschlossen, wählen Sie in der Aufklappliste das anzuschließende Systemtelefon aus. Es wird Ihnen eine vereinfachte Darstellung des ausgewählten Systemtelefons angezeigt.
6) Klicken Sie in der vereinfachten Darstellung des Systemtelefons auf das gewünschte Tastenfeld. Es werden Ihnen die Funktionstasten des ausgewählten Tastenfelds angezeigt mit den momentan belegten Funktionen.



7) Belegen Sie die Funktionstasten:

a) Klicken Sie bei der zu belegenden Funktionstaste auf das Tastensymbol. Es wird Ihnen eine Aufklappliste mit den möglichen Funktionen angezeigt.

b) Wählen Sie in der Aufklappliste **Funktion auswählen** eine der angebotenen Möglichkeiten aus.

c) Einige Funktionen erfordern Zusatzinformationen. Wählen Sie diese falls erforderlich aus bzw. geben Sie die erforderlichen Daten ein.

d) Klicken Sie auf **Speichern**.

e) Ändern Sie im Feld **Neue Beschriftung eingeben** bei Bedarf die Beschriftung der Funktionstaste.

Anmerkung: Haben Sie ein Systemtelefon mit automatischer Tastenbeschriftung (z.B. OpenStage 60 HFA), wird dieser Text vom Systemtelefon übernommen.

---

f) Klicken Sie auf **Speichern**.

g) Wenn Sie weitere Funktionstasten belegen wollen, wiederholen Sie Schritt 7.

8) Haben Sie auf einer Funktionstaste die **Ebenenumschaltung** eingerichtet, aktivieren Sie das Kontrollkästchen **Ebenenumschaltung**. Belegen Sie die zweite Ebene der Funktionstasten mit den externen Rufnummern wie unter Schritt 7 beschrieben.

9) Klicken Sie auf **Tastenlayout übernehmen**.

10) Wenn Sie die soeben definierte Tastenbelegung für mehrere oder alle Systemtelefone übernehmen wollen, aktivieren Sie bei den gewünschten Systemtelefonen das Kontrollkästchen, klicken Sie anschließend auf **Übernehmen,** auf **OK** und auf **OK & Weiter**.

11) Wenn Sie die soeben definierte Tastenbelegung nur für das ausgewählte Systemtelefon übernehmen wollen, klicken Sie zur Sicherheit auf **Alle Teilnehmer deselektieren** und anschließend auf **OK & Weiter**.

12) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

11.12 Teilnehmer-Profile

In Profilen werden die Werte und Eigenschaften von Teilnehmern abgespeichert. Einem Profil können mehrere Mitglieder zugeordnet werden. Für alle Mitglieder dieses Profils gelten die gleichen Werte und Eigenschaften.

Teilnehmer-Profile können Teilnehmern mit Systemtelefonen zugeordnet werden. Es können bis zu 20 Teilnehmer-Profile angelegt werden. Die Teilnehmer-Profile können einzeln oder alle zusammen exportiert und importiert werden. Die Dateien sind vom Typ `xml`.

Jeder Teilnehmer kann Mitglied von genau einem Profil sein. Werden die Werte und Eigenschaften eines Teilnehmers, der Mitglied eines Profils ist, direkt - also nicht über das Profil - geändert, so wird der Teilnehmer aus dem Profil gelöscht.

11.13 Konfiguration der Teilnehmer

Für die Teilnehmer können bestimmte Werte (z.B. Rufnummer, Name und Durchwahlnummer) und Eigenschaften (z.B. Art der Rufsignalisierung) definiert werden.

Die Konfiguration der Teilnehmer ist unterteilt in eine Standard-Konfiguration und eine erweiterte Konfiguration. Die Standard-Einstellungen können über Wizards mit dem Profil **Advanced** konfiguriert werden. Die erweiterten Einstellungen können nur über den Experten-Modus mit dem Profil **Expert** konfiguriert werden.

Die Standard-Einstellungen lassen sich für alle Teilnehmer einer Teilnehmerart (z.B. IP-Teilnehmer oder analoge Teilnehmer) komfortabel in einer Liste ändern. Zusätzliche Einstellungen (wie z.B. die Rufsignalisierung oder die Teilnehmer-Flags) können für jeden Teilnehmer einzeln geändert werden.

Virtuelle Teilnehmer werden komplett über den Experten-Modus konfiguriert (sowohl die Standard-Einstellungen als auch die erweiterten Einstellungen).

Mit dem Profil **Basic** können die Teilnehmer zwar nicht konfiguriert werden, aber die Namen der Teilnehmer können geändert werden.

Für die am Kommunikationssystem angeschlossenen Teilnehmer sollte ein Rufnummernplan existieren. Rufnummern, Namen und Durchwahlnummern aller konfigurierten Teilnehmer können über den Experten-Modus unter **Teilnehmer** > **Durchwahl Rufnummern** angezeigt werden.

Durchwahlnummern, die nicht vom Service Provider zur Verfügung gestellt und nicht im System genutzt werden, sollten gelöscht werden, sonst kann es zu Konflikten mit MSN oder Internet-Telefonie-Teilnehmerrufnummern kommen. Durchwahlnummern, die von einem Internet-Telefonie-Service-Provider (ITSP) zur Verfügung gestellt werden, sind bei der Einrichtung des ITSP den Teilnehmern zuzuordnen (siehe Konfiguration eines ITSP).

Wichtig: Die Änderung einer Teilnehmerrufnummer setzt die für den Teilnehmer eventuell eingerichtete Smart VM (Voicemail) zurück. Alle persönlichen Sprachnachrichten, Begrüßungen und Ansagen gehen verloren und das Kennwort wird zurückgesetzt.

Standard-Einstellungen

Die Standard-Einstellungen sollten für jeden Teilnehmer kontrolliert und wenn nötig angepasst werden.

- **Rufnummer, Name, Durchwahlnummer**

  Standardmäßig ist jedem Teilnehmer eine Rufnummer zugeordnet (z.B. 101). Unter dieser Rufnummer ist der Teilnehmer intern erreichbar. Bei Systemtelefonen wird diese Rufnummer im eigenen Display und im Display des Kommunikationspartners angezeigt. Soll beim extern angerufenen Teilnehmer an Stelle der eigentlichen Rufnummer eine andere Rufnummer angezeigt werden, kann diese Rufnummer definiert werden.

  Jedem Teilnehmer kann zusätzlich eine Durchwahlnummer zugeordnet werden. Unter der Durchwahlnummer ist der Teilnehmer von extern direkt erreichbar. Der Teilnehmer kann z.B. intern über die Rufnummer 101 und extern über die Durchwahlnummer `3654321` (MSN bei Mehrgeräteanschluss) oder `<Anlagenrufnummer>-101` (bei

Anlagenanschluss) erreicht werden. Bei der Erstinstallation kann im Falle eines Anlagenanschlusses festgelegt werden, ob als Durchwahlnummer automatisch die interne Rufnummer eingetragen werden soll. Die Durchwahlnummer kann sich aber auch von der Rufnummer unterscheiden. Falls Internet-Telefonie genutzt wird, kann zusätzlich eine Durchwahlnummer festgelegt werden, mit der der Teilnehmer über die Internet-Telefonie erreichbar ist. Diese Rufnummer wird vom Internet-Telefonie-Service-Provider zur Verfügung gestellt.

Jedem Teilnehmer kann zusätzlich ein Name zugeordnet werden. Dieser Name erscheint beim Kommunikationspartner im Display (nur bei Systemtelefonen).

Existiert ein Rufnummernplan, so sollten die Rufnummern, die Durchwahlnummern und die Namen der Teilnehmer anhand des Rufnummernplans angepasst werden.

- **Typ**

  Für jeden Teilnehmer kann der Teilnehmertyp ausgewählt werden. Ein IP-Teilnehmer kann z.B. vom Teilnehmertyp **System Client** oder **SIP Client** sein, ein analoger Teilnehmer kann ein analoges Telefon oder ein analoges Faxgerät sein und ein ISDN-Teilnehmer kann ein ISDN-Telefon oder ein ISDN-Fax sein.

- **Fax-Rufnummer, Fax-Durchwahlnummer**

  Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B.mit den UC Clients myPortal for Desktop oder myPortal for Outlook) vergeben Sie eine Fax-Rufnummer (für den Empfang interner Faxnachrichten) und eine Fax-Durchwahlnummer (für den Empfang externer Faxnachrichten).

- **Berechtigungen (Classes of Service)**

  Einem Teilnehmer kann eine von 15 verschiedenen Berechtigungsklassen zugewiesen werden. Damit wird z.B. festgelegt, ob der Teilnehmer externe Gespräche annehmen und führen darf oder welche Rufnummern der Teilnehmer wählen darf und welche nicht (siehe Berechtigungen (Wahlkontrolle)).

- **Anrufübernahmegruppe**

  Jeder Teilnehmer kann einer Anrufübernahmegruppe zugeordnet werden.

- **Sprache, Rufsignalisierung**

  Die Sprache für die Menüsteuerung der angeschlossenen Systemtelefone kann einstellt werden.

  Der Klang des Ruftons eines externen und eines internen Anrufs kann ausgewählt werden.

- **Sprachbox (nur mit UC Smart)**

  Bei der UC-Lösung UC Smart kann man für jeden Teilnehmer eine Sprachbox einrichten und zwischen verschiedenen Begrüßungsansagen wählen. Für genauere Informationen zur Sprachbox siehe Sprachbox (SmartVM)

  Bei der UC-Lösung UC Suite wird jedem Teilnehmer automatisch eine Sprachbox zugewiesen. Somit fehlen in diesem Fall die Sprachbox-Einstellungen.

- **Teilnehmer-Flags**

  Die Teilnehmer-Flags eines jeden Teilnehmers können geändert werden. Für eine Beschreibung der Teilnehmer-Flags siehe >Teilnehmer>Teilnehmer>Teilnehmer-Parameter.

Erweiterte Einstellungen

Über den Experten-Modus können alle Einstellungen für alle Arten von Teilnehmern konfiguriert werden. Die erweiterten Einstellungen können für den Standard-Betrieb wie eingestellt belassen werden und müssen nur im Bedarfsfall angepasst werden. Informationen zu den erweiterten Einstellungen siehe Teilnehmer.

Zugehörige Konzepte

Berechtigungen (Wahlkontrolle) auf Seite 765
Mehrsprachige Textausgabe auf Seite 1243

11.13.1 IP-Teilnehmer konfigurieren

Mit dem Wizard **IP-Endgeräte** können Sie die IP-Teilnehmer (LAN-Telefone und WLAN-Telefone) konfigurieren.

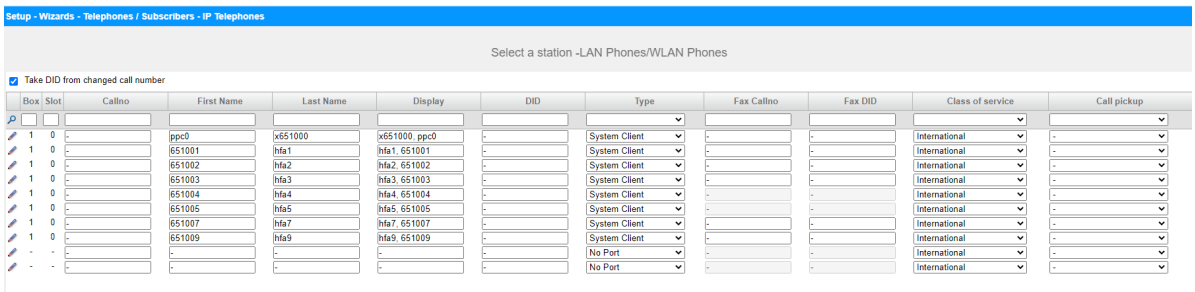
Voraussetzungen

Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless LAN-Netzwerk.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Endgeräte / Teilnehmer**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **IP-Endgeräte** zu starten. Es wird Ihnen eine Liste aller IP-Teilnehmer angezeigt.



4) Wenn der Teilnehmer automatisch als Durchwahlnummer die interne Rufnummer bekommen soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- Nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- Nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- Bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Wenn der Teilnehmer eine Internet-Telefonie-Teilnehmerrufnummer als Durchwahlnummer erhalten soll, lassen Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen** deaktiviert, wählen Sie aus der Liste neben diesem Optionsfeld den Internet-Telefonie-Service-Provider aus. und wählen in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **DuWa** die Internet-Telefonie-Teilnehmerrufnummer aus.

7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

8) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

9) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ des IP-Teilnehmers aus (z.B. **System Client** oder **Deskshare User**).

10) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

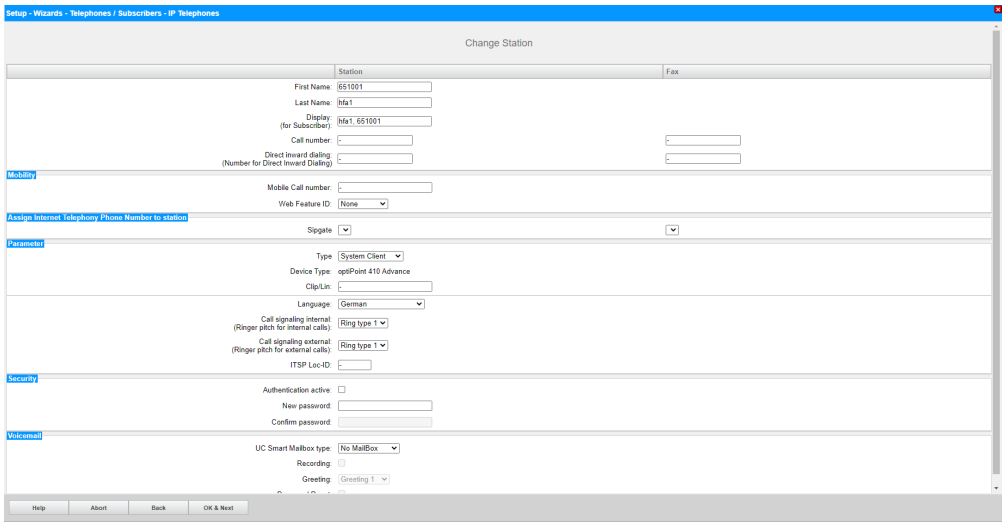
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

11) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

12) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

13) Führen Sie bei Bedarf weitere Einstellungen durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Weisen Sie eine **Mobile Rufnummer** zu und wählen Sie die **Web Feature ID** aus der Aufklappliste im Bereich **Mobility** aus.

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton,

durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Geben Sie im Feld **ITSP Loc-ID** die Indexnummer der ITSP Standort-ID ein.

h) Nur mit UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

i) Nur mit UC Smart und Standard-Mailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

j) Nur mit UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

k) Nur mit UC Smart: Wenn das Passwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

Anmerkung:

Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox deaktiviert werden. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

l) Wenn der Teilnehmer mit dem Internet verbunden ist, MUSS die Authentifizierung aktiviert sein und Sie MÜSSEN starke Kennwörter für alle IP-Stationen eingeben. Überprüfen Sie die Liste der Flags **Authentifizierung aktiv** und füllen Sie die Felder **Neues Kennwort** und **Kennwort bestätigen** aus.

m) Klicken Sie auf **OK & Weiter**.

n) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

o) Klicken Sie auf **OK & Weiter**.

14) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 13.

15) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten IP-Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der IP-Teilnehmer ausdrucken.

16) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11.13.2 Wie Sie SIP-Teilnehmer konfigurieren

Mit dem Wizard **IP-Endgeräte** können Sie die SIP-Teilnehmer (LAN-Telefone und WLAN-Telefone) konfigurieren.

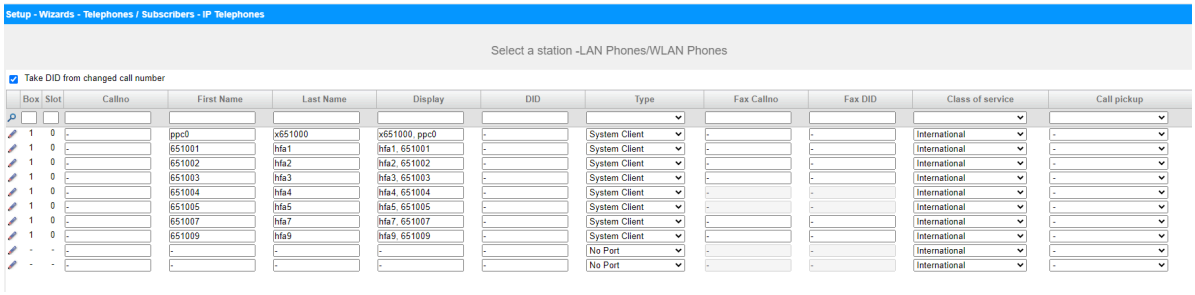
Voraussetzungen

Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless LAN-Netzwerk.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Endgeräte / Teilnehmer**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **IP-Endgeräte** zu starten. Es wird Ihnen eine Liste aller IP-Teilnehmer angezeigt. Diese Liste enthält auch alle SIP-Teilnehmer.



4) Wenn der Teilnehmer automatisch als Durchwahlnummer die interne Rufnummer bekommen soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.
5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:
   - Nur bei Anlagenanschluss:

     Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
   - Nur bei Mehrgeräteanschluss:

     Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
   - Bei Anlagenanschluss und Mehrgeräteanschluss:

     Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.
6) Wenn der Teilnehmer eine Internet-Telefonie-Teilnehmerrufnummer als Durchwahlnummer erhalten soll, lassen Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen** deaktiviert, wählen Sie aus der Liste neben diesem Optionsfeld den Internet-Telefonie-Service-Provider aus. und wählen in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **DuWa** die Internet-Telefonie-Teilnehmerrufnummer aus.
7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.
8) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.
9) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ **SIP Client** aus.

10) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

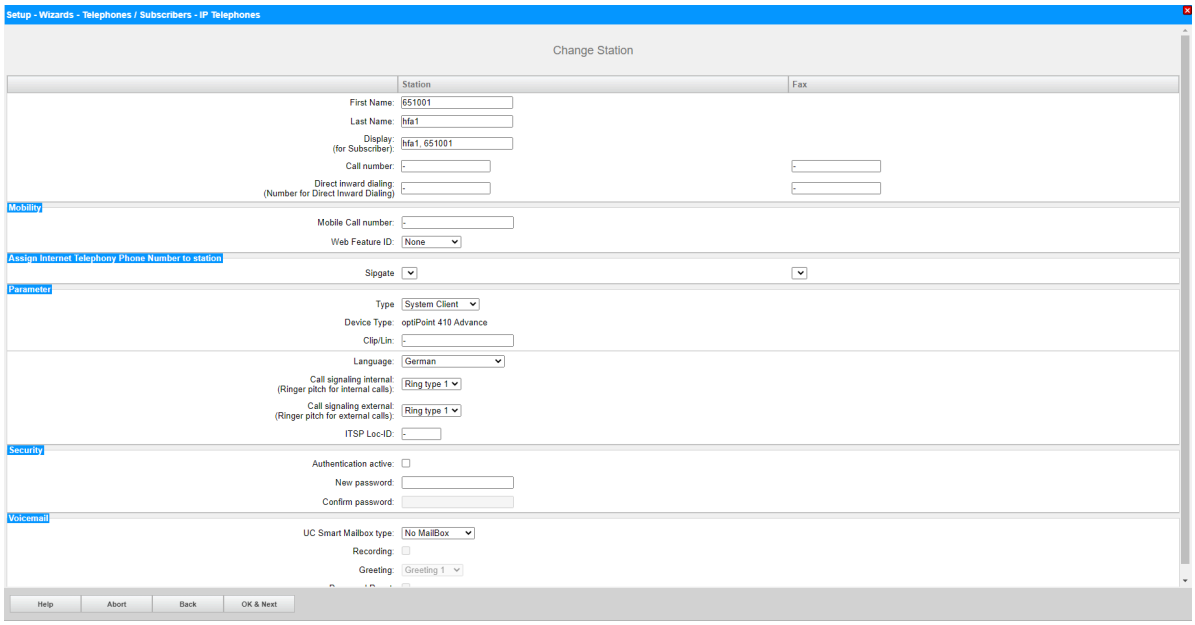
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

11) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

12) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

13) Konfigurieren Sie die Daten für die SIP-Registrierung:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Vergeben Sie im Bereich **Sicherheit** in den Feldern **Kennwort** und **Kennwort bestätigen** ein Kennwort für die Authentifizierung des SIP-Teilnehmers.

c) Vergeben Sie im Feld **SIP User ID / Benutzername** einen Benutzernamen Ihrer Wahl für die Authentifizierung des SIP-Teilnehmers, z.B. SIP-120.

d) Vergeben Sie unter **Realm** einen Namen Ihrer Wahl für die zugehörige Zone, z.B. OSBIZ-SIP. Dieser Wert sollte für alle SIP-Teilnehmer gleich sein.

Anmerkung: Die hier definierten Werte für Kennwort, SIP User ID und Realm müssen auch am SIP-Telefon eingegeben werden.

---

14) Führen Sie bei Bedarf weitere Einstellungen durch:

a) Wenn dieses SIP-Telefon zusammen mit einem Dual-Mode-Mobiltelefon betrieben werden soll, geben Sie im Bereich `Mobility` unter **mobile Rufnummer** die Amtskennziffer und gefolgt von der Rufnummer des Mobiltelefons ein (z.B. **0016012345678**). Wählen Sie zusätzlich aus der Aufklappliste **Web Feature ID** diesen SIP Client aus. (siehe Dual-Mode-Telefonie).

b) Ordnen Sie im Bereich **Durchwahl für Internet-Telefonie** dem Teilnehmer und falls gewünscht seiner Faxbox jeweils eine Durchwahlnummer für die Internet-Telefonie zu. Wählen Sie dazu aus den Aufklapplisten des gewünschten ITSP die Durchwahlnummern aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste für den Teilnehmer und eine Aufklappliste für seine Faxbox angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur mit UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

h) Nur mit UC Smart und Standard-Mailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

i) Nur mit UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

j) Nur mit UC Smart: Wenn das Passwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

Anmerkung: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox deaktiviert werden. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

k) Klicken Sie auf **OK & Weiter**.

l) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

m) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 14.

16) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten IP-Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der IP-Teilnehmer ausdrucken.

17) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11.13.3 UP0-Teilnehmer konfigurieren

Sie können den Assistenten für **UP0-Geräte** verwenden, um die UP0-Teilnehmer zu konfigurieren.

Voraussetzungen

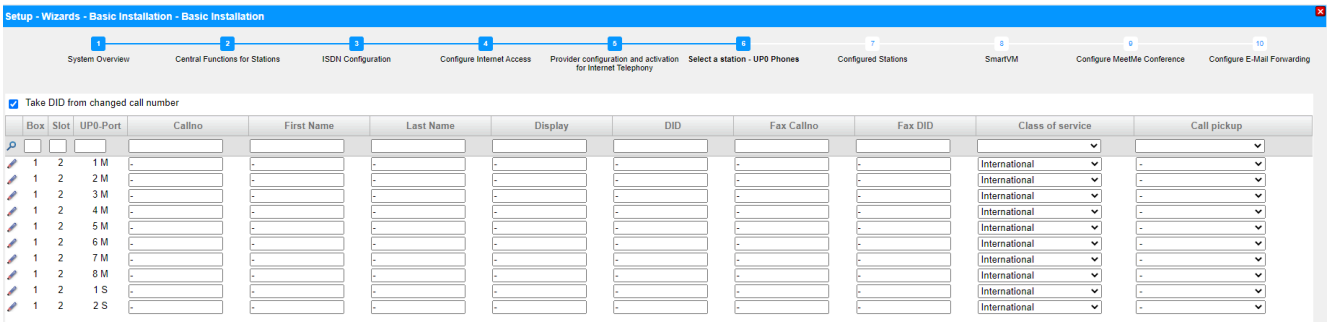
Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Assistenten** > **Telefone / Abonnenten**.

3) Klicken Sie auf **Bearbeiten**, um den Assistenten für **UP0-Geräte** zu starten. Sie sehen eine Liste aller UP0-Teilnehmer.



4) Wenn dem Teilnehmer automatisch die interne Rufnummer als Durchwahlnummer zugewiesen werden soll, aktivieren Sie die Optionsschaltfläche **DuWa von geänderter Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- Nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- Nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- Bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Wenn dem Teilnehmer eine Internet-Telefonie-Rufnummer als Durchwahlnummer zugewiesen werden soll, lassen Sie die Optionsschaltfläche **DuWa von geänderter Rufnummer übernehmen** deaktiviert und wählen stattdessen den Internet-Telefonie-Dienstanbieter aus der Liste neben der Optionsschaltfläche aus. Wählen Sie dann die Internet-Telefonie-Rufnummer aus der Dropdown-Liste **DuWa** in der Zeile des gewünschten Teilnehmers aus.

7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

8) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

9) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

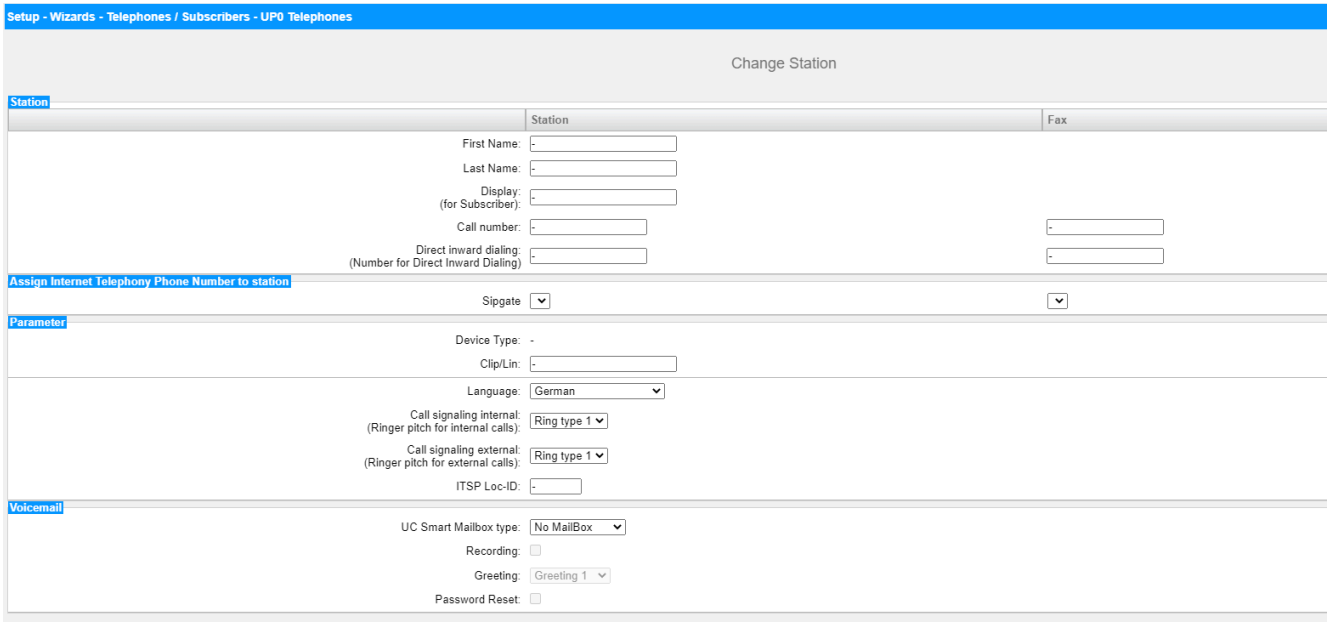
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

10) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

11) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

12) Nehmen Sie ggf. weitere Einstellungen vor:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht konfiguriert ist oder wenn kein Internet-Telefonie-Dienstanbieter aktiviert wurde.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Merkmal muss vom Netzbetreiber freigegeben werden.

Anmerkung: Es sollte mindestens eine DID-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton,

durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur bei UC Smart: Wählen Sie in der Dropdown-Liste **UC Smart Mailbox-Typ** , ob der Teilnehmer eine Standard-Mailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

h) Nur bei UC Smart und Standard-Mailbox: Wenn ein Anrufer eine Nachricht in der Sprachbox hinterlassen kann, aktivieren Sie das Kontrollkästchen **Aufnahme**.

i) Nur bei UC Smart: Wählen Sie eine Begrüßung aus der Dropdown-Liste **Begrüßung**.

j) Nur bei UC Smart: Wenn das Passwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort zurücksetzen**.

Anmerkung: Das Kontrollkästchen **Passwort zurücksetzen** muss beim Einrichten einer neuen Sprachbox deaktiviert werden. Es dient dazu, das Passwort der Sprachbox zurückzusetzen. Wenn eine neue Sprachbox eingerichtet wird, muss der Teilnehmer beim ersten Zugriff auf seine Sprachbox sowieso das Anfangspasswort ändern.

---

k) Klicken Sie auf **OK & Weiter**.

l) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

m) Klicken Sie auf **OK & Weiter**.

13) Wenn Sie einen weiteren Teilnehmer konfigurieren möchten, wiederholen Sie die Schritte 5 bis 12.

14) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten UP0-Teilnehmer. Bei Bedarf können Sie die Liste der UP0-Teilnehmer mit **Drucken** ausdrucken.

15) Klicken Sie auf **OK & Weiter** gefolgt von **Fertigstellen**.

11.13.4 Wie Sie DECT-Teilnehmer konfigurieren

Sie können den Assistenten für **DECT-Geräte** verwenden, um die DECT-Teilnehmer (DECT-Telefone) zu konfigurieren.

Voraussetzungen

Eine Basisstation wird an eine UP0-Schnittstelle oder an eine installierte SLC-Karte angeschlossen.

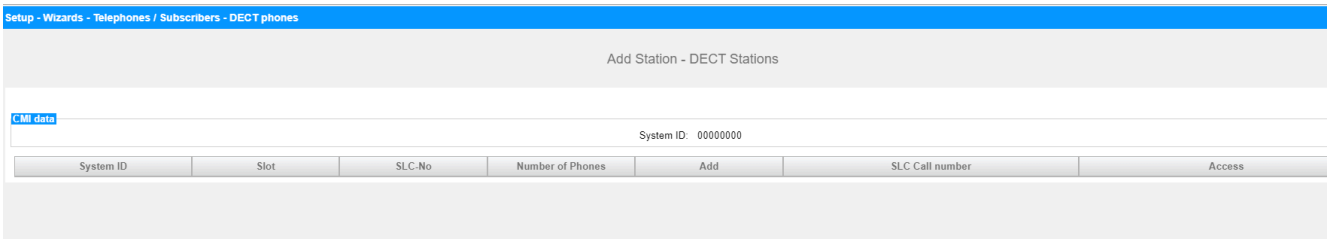
Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Assistenten** > **Telefone / Abonnenten**.

3) Klicken Sie auf **Bearbeiten**, um den Assistenten für **DECT-Telefone** zu starten. Sie sehen eine Liste aller DECT-Teilnehmer.



4) Wenn dem Teilnehmer automatisch die interne Rufnummer als Durchwahlnummer zugewiesen werden soll, aktivieren Sie die Optionsschaltfläche **DuWa von geänderter Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

   - Nur bei Anlagenanschluss:

     Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
   - Nur bei Mehrgeräteanschluss:

     Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
   - Bei Anlagenanschluss und Mehrgeräteanschluss:

     Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Wenn dem Teilnehmer eine Internet-Telefonie-Rufnummer als Durchwahlnummer zugewiesen werden soll, lassen Sie die Optionsschaltfläche **DuWa von geänderter Rufnummer übernehmen** deaktiviert und wählen stattdessen den Internet-Telefonie-Dienstanbieter aus der Liste neben der Optionsschaltfläche aus. Wählen Sie dann die Internet-Telefonie-Rufnummer aus der Dropdown-Liste **DuWa** in der Zeile des gewünschten Teilnehmers aus.

7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

8) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

9) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

   a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

   b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax**

Durchwahl die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

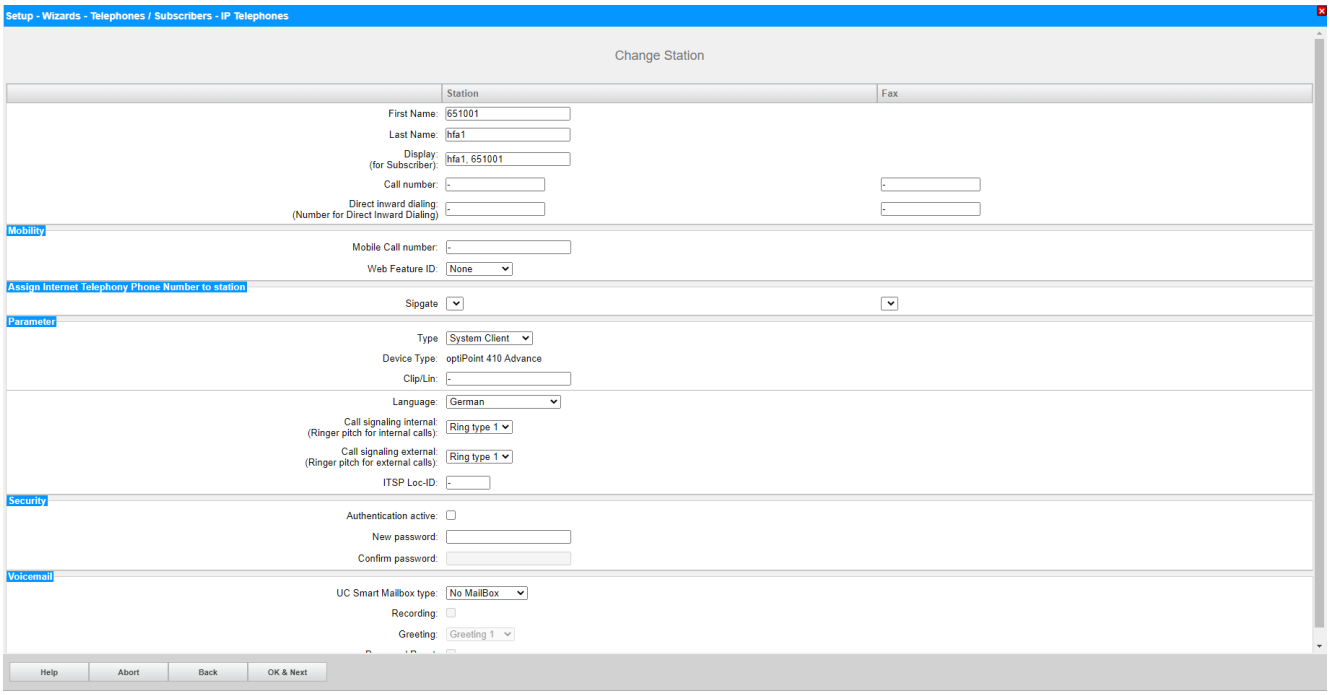
10) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

11) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

12) Falls Sie den DECT-Telefoncode (PIN) ändern wollen, geben Sie in der Zeile des gewünschten Teilnehmers unter **Mobilcode** den neuen Code ein. Der DECT-Teilnehmer muss sich mit diesem Code neu an der Basisstation anmelden.

13) Nehmen Sie ggf. weitere Einstellungen vor:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie

nicht konfiguriert ist oder wenn kein Internet-Telefonie-Dienstanbieter aktiviert wurde.

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Merkmal muss vom Netzbetreiber freigegeben werden.

Anmerkung: Es sollte mindestens eine DID-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur bei UC Smart: Wählen Sie in der Dropdown-Liste **UC Smart Mailbox-Typ** , ob der Teilnehmer eine Standard-Mailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

h) Nur bei UC Smart und Standard-Mailbox: Wenn ein Anrufer eine Nachricht in der Sprachbox hinterlassen kann, aktivieren Sie das Kontrollkästchen **Aufnahme**.

i) Nur bei UC Smart: Wählen Sie eine Begrüßung aus der Dropdown-Liste **Begrüßung**.

j) Nur bei UC Smart: Wenn das Passwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort zurücksetzen**.

Anmerkung: Das Kontrollkästchen **Passwort zurücksetzen** muss beim Einrichten einer neuen Sprachbox deaktiviert werden. Es dient dazu, das Passwort der Sprachbox zurückzusetzen. Wenn eine neue Sprachbox eingerichtet wird, muss der Teilnehmer beim ersten Zugriff auf seine Sprachbox sowieso das Anfangspasswort ändern.

k) Klicken Sie auf **OK & Weiter**.

l) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

m) Klicken Sie auf **OK & Weiter**.

14) Wenn Sie einen weiteren Teilnehmer konfigurieren möchten, wiederholen Sie die Schritte 5 bis 13.
15) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten DECT-Teilnehmer. Bei Bedarf können Sie die Liste der UP0-Teilnehmer mit **Drucken** ausdrucken.
16) Klicken Sie auf **OK & Weiter** gefolgt von **Fertigstellen**.

Zugehörige Tasks

Wie Sie DECT-Telefone erstmalig konfigurieren auf Seite 981

11.13.5 So konfigurieren Sie Mitel SIP-DECT-Teilnehmer über die Bereitstellung

Mithilfe des **Mitel SIP-DECT**-Assistenten können Sie die Mitel SIP-DECT-Geräte konfigurieren und mit dem Open Mobility Manager (OMM) verbinden.

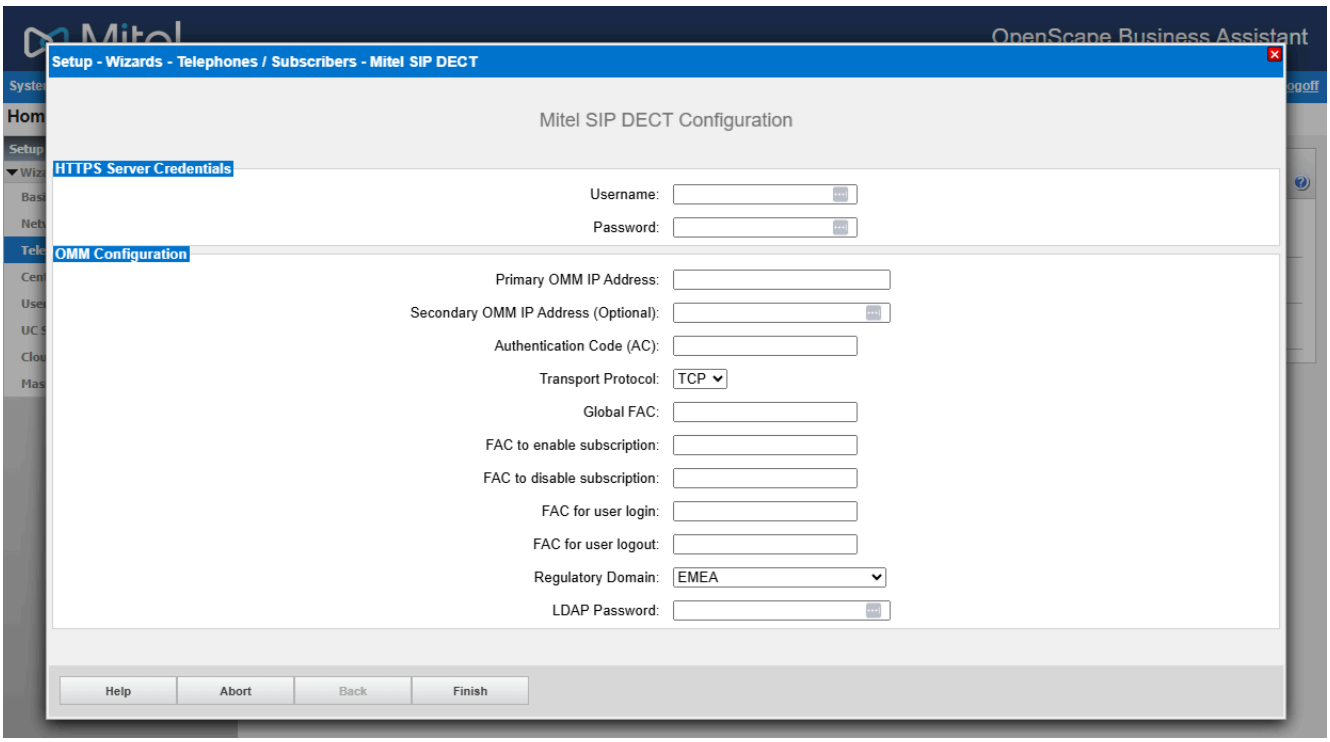
Voraussetzungen

Die MAC-Adresse für das SIP-DECT-RFP-Gerät ist bekannt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus > Netzwerkschnittstellen > DHCP**.
2) Klicken Sie darauf, um den **DHCP-Server** zu aktivieren.
3) Klicken Sie in der Navigationsleiste auf **DHCP-Server > Statische IP-Adressen**.
4) Klicken Sie im Fenster **Statische IP-Adressen** auf die Registerkarte **Statische IP-Adresse hinzufügen**.
5) Geben Sie die erforderlichen Informationen ein, wie unter Netzwerkschnittstellen > Hauptplatine > DHCP-Modus > DHCP-Server > Statische IP-Adressen beschrieben.
6) Klicken Sie auf **Anwenden**.
7) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
8) Klicken Sie im Navigationsbaum auf **Assistenten** > **Telefone / Abonnenten**.

9) Klicken Sie auf **Bearbeiten**, um den **Mitel SIP DECT**-Assistenten zu starten.



10) Geben Sie unter **HTTPS Server Credentials** die Zugangsdaten für den Server an.
    a) Stellen Sie den **Benutzernamen** und das **Passwort** ein.
11) Unter **OMM-Konfiguration**:
12) Geben Sie die **primäre OMM-IP-Adresse** und die **sekundäre OMM-IP-Adresse (optional)** IP-Adresse des OMM an.
13) Stellen Sie den **Authentifizierungscode (AC)** ein.
14) Wählen Sie unter **Transportprotokoll** einen der folgenden Werte aus dem Dropdown-Menü:
    - TCP
    - UDP
    - TLS
15) Stellen Sie die verschiedenen Feature Access Codes (FAC) in den folgenden Feldern ein:
    a) **Globale FAC**
    b) **FAC zum Aktivieren des Abonnements**
    c) **FAC für die Benutzeranmeldung**
    d) **FAC für die Benutzerabmeldung**
16) Wählen Sie unter **Regulierungsbereich** einen der folgenden Werte aus dem Dropdown-Menü:
    - EMEA
    - USA
    - Brasilien
    - Taiwan
    - Radio 1910 - 1927 MHz 250 Mw

17) Geben Sie das **LDAP-Passwort** für den Zugang zum internen Benutzerverzeichnis von OpenScape Business an.
18) Klicken Sie auf **Fertig**.
Die von der OMM-Anwendung benötigten Konfigurationsdateien werden generiert.
19) Konfigurieren Sie einen SIP-Teilnehmer, wie unter So konfigurieren Sie SIP-Teilnehmer über den Expertenmodus beschrieben.
20) Verbinden Sie das Mitel SIP DECT RFP-Gerät mit dem Netzwerk. Warten Sie einige Augenblicke, bis das Gerät eine IP-Adresse vom DHCP-Server erhalten hat.
21) Verbinden Sie sich mit der OMM-Anwendung und konfigurieren Sie die Basisstation, wie im „*Mitel SIP DECT -Telefonkonfigurationshandbuch*“ beschrieben.

11.13.5.1 So konfigurieren Sie SIP-Teilnehmer über den Expertenmodus

Sie können die SIP-Teilnehmer im **Expertenmodus** konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie im Navigationsbaum auf **Expertenmodus** > **Telefonie-Server** > **Teilnehmer**.
2) Erweitern Sie im neuen Fenster den Eintrag **Teilnehmer** und wählen Sie dann **IP-Klient**. Es wird Ihnen eine Liste alles IP/SIP-Teilnehmers angezeigt.
3) Wählen Sie in der Spalte **Typ** die Option **SIP-Klient**.
4) Klicken Sie auf **Anwenden**.
5) Klicken Sie auf den blauen Pfeil neben der Rufnummer des IP-Teilnehmers in der Spalte **Ruf-Nr.**.
6) Wählen Sie im Fenster **Teilnehmerparameter bearbeiten** die Option **Mitel SIP DECT-Gerät** aus dem Dropdown-Menü unter **Gerätebereitstellung**. Die Option **Mitel SIP DECT-Konfiguration** wird angezeigt.
7) Stellen Sie unter der Option **Mitel SIP DECT-Konfiguration** Folgendes ein:
   a) Geben Sie die **PIN** des Geräts ein.
   b) Aktivieren (Ja) oder deaktivieren (Nein) Sie unter **Tastensperre aktiviert** die Tastensperre des Geräts.
   c) Geben Sie unter **PIN für Tastensperre** die PIN für die Tastensperre ein.
   d) Geben Sie unter **Zeit für Tastensperre** die Zeit ein, nach der die PIN für die Tastensperre wirksam werden soll.
   e) Wählen Sie unter **Persönliches Verzeichnis anzeigen**, ob das persönliche Verzeichnis sichtbar (Ja) oder nicht sichtbar (Nein) ist.
8) Klicken Sie auf **Anwenden**.
9) Wechseln Sie auf die Registerkarte **Workpoint- Klientendaten bearbeiten**.
10) Konfigurieren Sie unter **Parameter** die Werte wie unter Teilnehmerparameter beschrieben.

11) Klicken Sie auf **Anwenden**.

11.13.6 ISDN-Teilnehmer konfigurieren

Mit dem Wizard **ISDN-Endgeräte** können Sie die ISDN-Teilnehmer (z.B. ISDN-Telefon oder ISDN-Fax) konfigurieren.

Voraussetzungen

Es ist mindestens eine freie S_0-Schnittstelle vorhanden. Wird einer der S_0-Ports einer Hardware-Plattform genutzt, muss dieser als interner S_0-Anschluss eingerichtet sein.

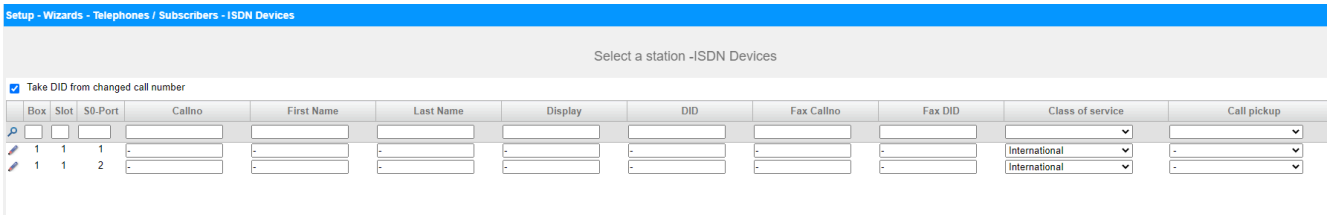
Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **Endgeräte / Teilnehmer**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **ISDN-Endgeräte** zu starten. Es wird Ihnen eine Liste aller ISDN-Teilnehmer angezeigt.



4) Wenn die Durchwahlnummer des Teilnehmers automatisch seiner Rufnummer angepasst werden soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- Nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- Nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- Bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

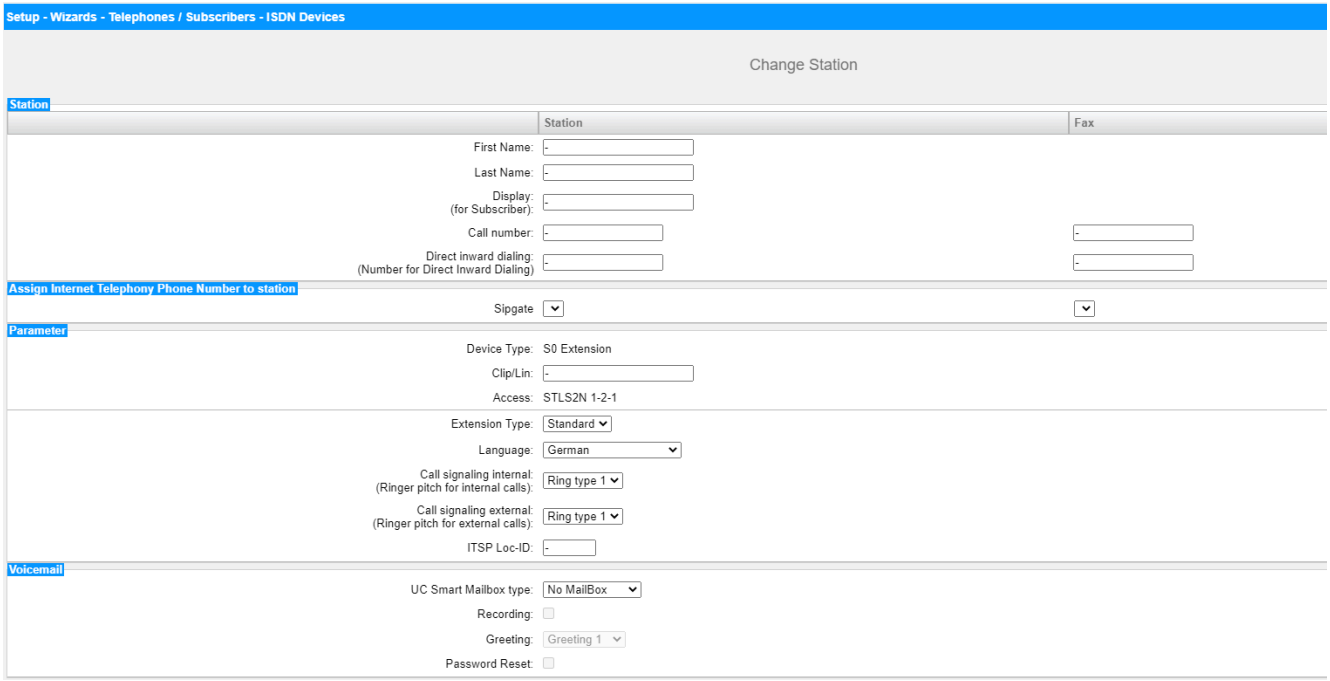
7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

8) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** eine der gewünschten Berechtigungsgruppen aus.

9) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

10) Führen Sie bei Bedarf weitere Einstellungen durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird

formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

d) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des ISDN-Endgeräts aus (`Standard` oder `Fax`).
e) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für ISDN-Endgeräte ist diese Einstellung ohne Bedeutung.
f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).
g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).
h) Nur mit UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.
i) Nur mit UC Smart und Standard-Mailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.
j) Nur mit UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.
k) Nur mit UC Smart: Wenn das Passwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

Anmerkung: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox deaktiviert werden. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

l) Klicken Sie auf **OK & Weiter**.
m) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.
n) Klicken Sie auf **OK & Weiter**.

11) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 10.
12) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten ISDN-Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der ISDN-Teilnehmer ausdrucken.
13) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11.13.7 Analoge Teilnehmer konfigurieren

Mit dem Wizard **Analog-Endgeräte** können Sie analoge Teilnehmer (z.B. analoges Telefon oder analoges Fax) einrichten.

Voraussetzungen

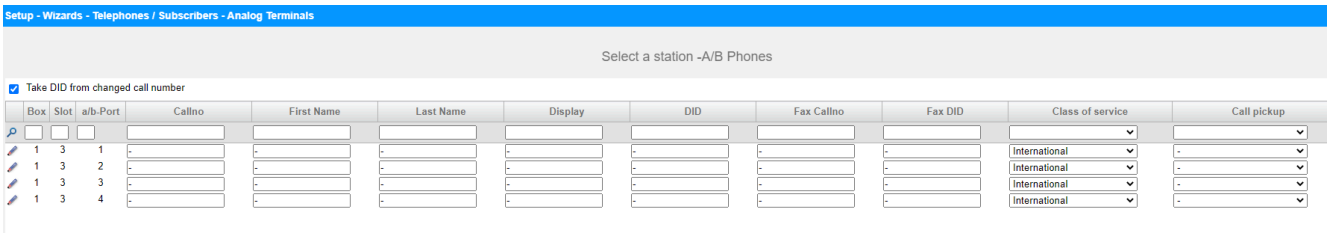
Es ist mindestens eine freie analoge Schnittstelle vorhanden.

An den analogen Geräten ist MFV aktiviert.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Endgeräte / Teilnehmer**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Analog-Endgeräte** zu starten. Es wird Ihnen eine Liste aller analogen Teilnehmer angezeigt.



4) Wenn die Durchwahlnummer des Teilnehmers automatisch seiner Rufnummer angepasst werden soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.
5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:
   - Nur bei Anlagenanschluss:

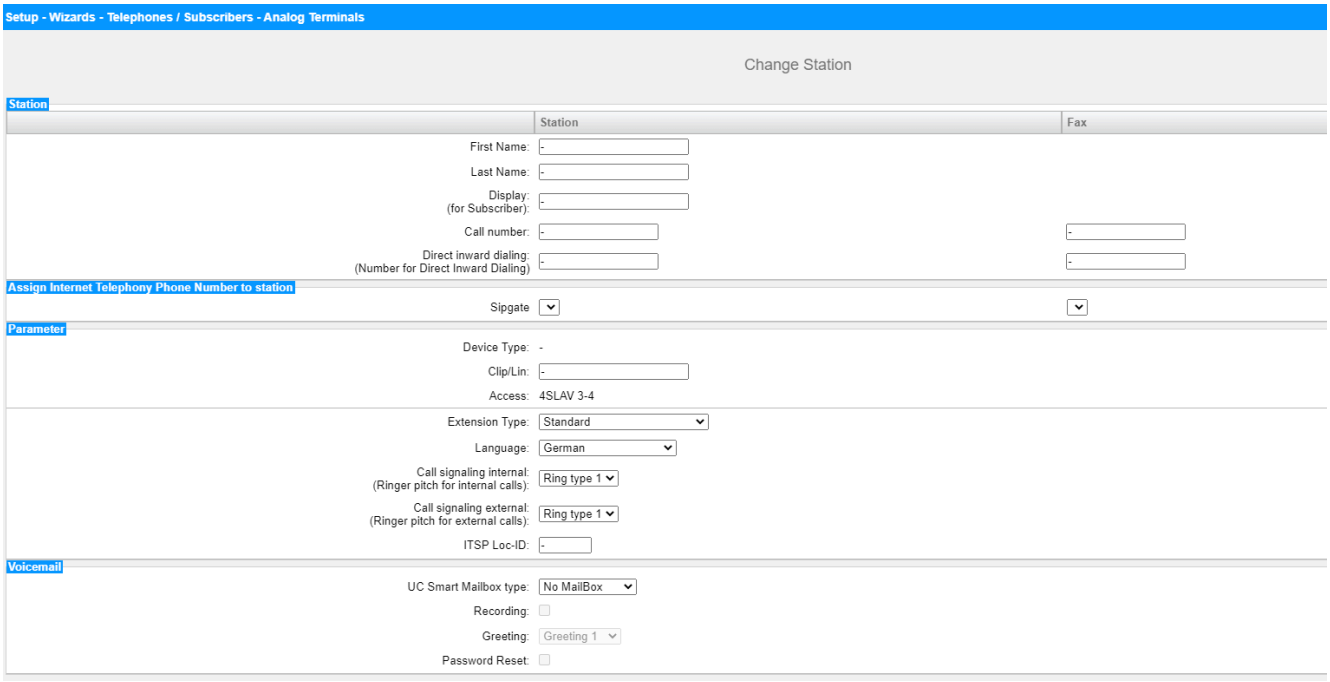
     Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
   - Nur bei Mehrgeräteanschluss:

     Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
   - Bei Anlagenanschluss und Mehrgeräteanschluss:

     Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.
6) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.
7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.
8) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** eine der gewünschten Berechtigungsgruppen aus.
9) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

10) Führen Sie bei Bedarf weitere Einstellungen durch: - Soll ein analoges Modem eingerichtet werden, ist hier der Stationstyp **Modem** auszuwählen.

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird

formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

d) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des analogen Endgeräts (z. B. **Fax**) aus.

   Soll ein analoges Modem eingerichtet werden, ist hier der Stationstyp **Modem** auszuwählen.

e) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für a/b-Endgeräte ist diese Einstellung ohne Bedeutung.

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

h) Nur mit UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

i) Nur mit UC Smart und Standard-Mailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

j) Nur mit UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

k) Nur mit UC Smart: Wenn das Passwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

   Anmerkung: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox deaktiviert werden. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

l) Klicken Sie auf **OK & Weiter**.

m) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter.

n) Klicken Sie auf **OK & Weiter**.

11) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 10.

12) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten analogen Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der analogen Teilnehmer ausdrucken.

13) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11.13.8 Wie Sie den Namen der Teilnehmer ändern

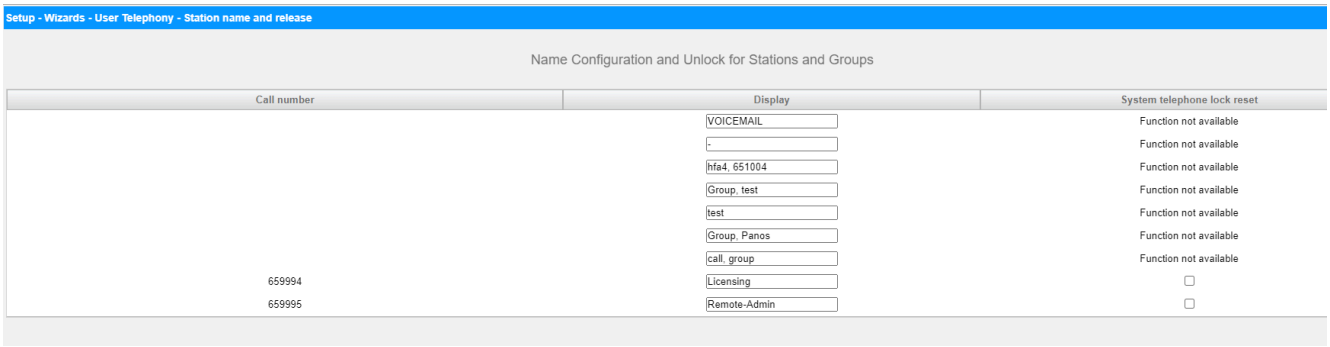
Mit dem Wizard **Teilnehmername und Freischaltung** können Sie die Namen der Teilnehmer ändern.

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmername und Freischaltung** zu starten.



4) Klicken Sie in der Spalte **`Display`** in das Feld des gewünschten Teilnehmers und ändern Sie den Namen des Teilnehmers in der Form `Nachname, Vorname` oder `Vorname Nachname`.
5) Wenn Sie die Namen weiterer Teilnehmer ändern wollen, wiederholen Sie den Schritt 4.
6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11.14 Konfiguration der Teilnehmer-Profile

In Teilnehmer-Profilen werden die Werte und Eigenschaften der IP-Teilnehmer abgespeichert.

Über den Wizard **Profile** kann ein Administrator mit dem Profil **Advanced** folgende Konfigurationen durchführen:

- Neues Profil anlegen
- Profile und deren Mitglieder anzeigen
- Mitglieder zu einem Profil hinzufügen
- Mitglieder aus einem Profil löschen
- Einzelnes Profil exportieren oder importieren

Über den Experten-Modus kann ein Administrator mit dem Profil **Expert** zusätzlich folgende Konfigurationen durchführen:

- Werte und Einstellungen eines bestehenden Profils ändern
- Alle Profile exportieren oder importieren

Bereits angelegte Teilnehmer-Profile können nicht gelöscht, aber überschrieben werden.

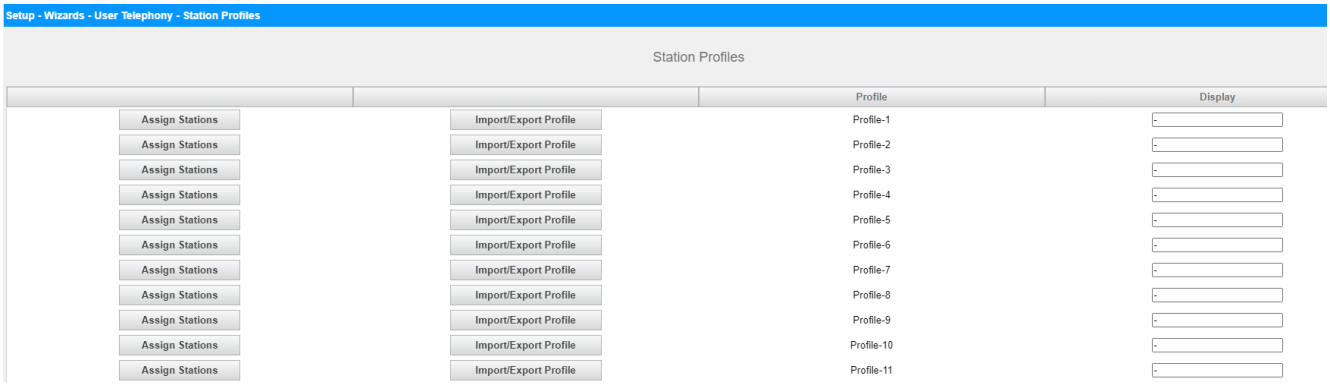
11.14.1 Wie Sie ein neues Teilnehmer-Profil anlegen

Voraussetzungen

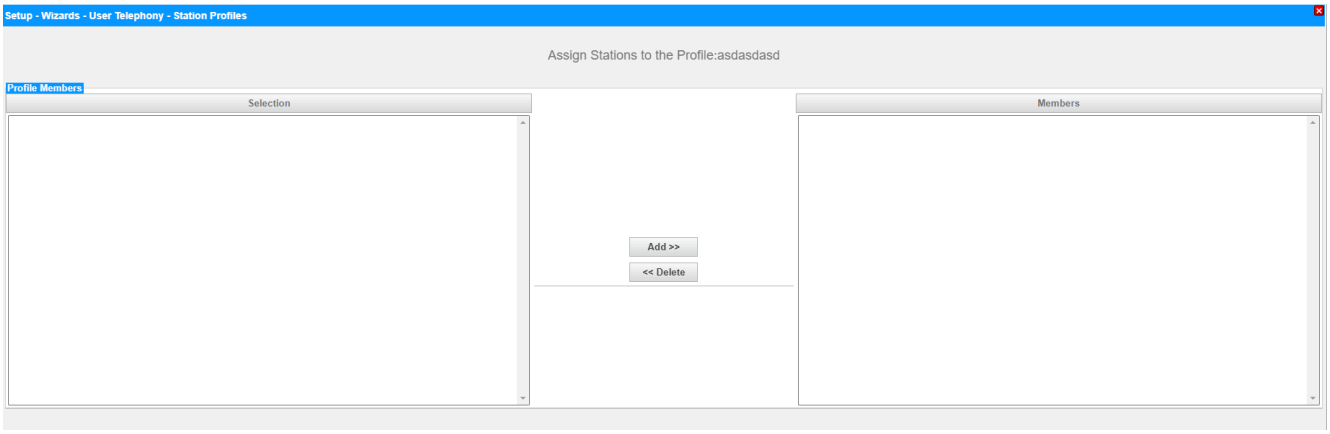
Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile angezeigt.



4) Geben Sie in der Zeile des gewünschten Teilnehmer-Profils in der Spalte **Display** einen frei wählbaren Namen für das Profil an (max. 16 Stellen möglich).
5) Klicken Sie in der Zeile des gewünschten Teilnehmer-Profils auf **Teilnehmer zuordnen**.



6) Wählen Sie aus der Tabelle **Profile Mitglieder** die gewünschten Mitglieder aus (Mehrfachauswahl ist möglich) und klicken Sie auf **Hinzufügen**. Diese Teilnehmer sind dem Teilnehmer-Profil zugeordnet und können keinem weiteren Teilnehmer-Profil zugewiesen werden.
7) Klicken Sie auf **OK**.
8) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.
9) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11.14.2 Wie Sie Teilnehmer-Profile und deren Mitglieder anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile angezeigt.
4) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

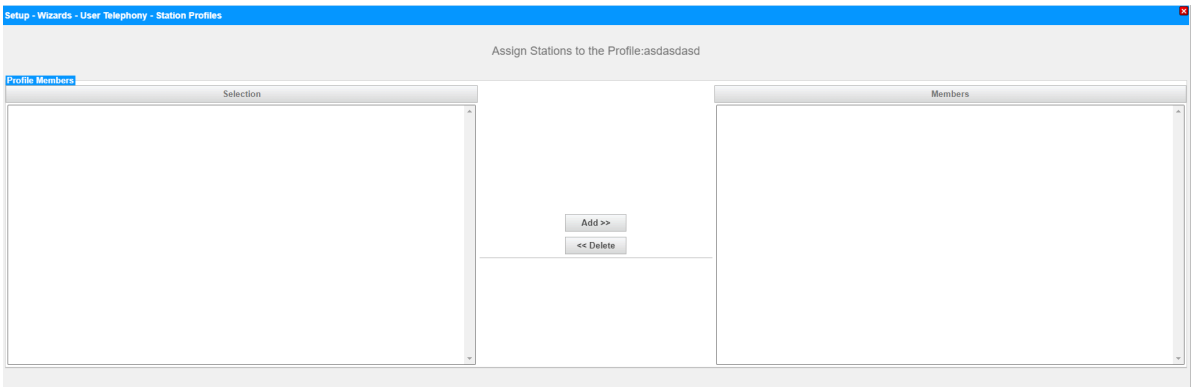
11.14.3 Wie Sie Mitglieder zu einem Teilnehmer-Profil hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.
4) Klicken Sie in der Zeile des gewünschten Teilnehmer-Profils auf **Teilnehmer zuordnen**.



5) Wählen Sie aus der Liste **Profile Mitglieder** die gewünschten Mitglieder aus (Mehrfachauswahl ist möglich) und klicken Sie auf **Hinzufügen**. Diese Teilnehmer sind dem Teilnehmer-Profil zugeordnet und können keinem weiteren Teilnehmer-Profil zugewiesen werden.
6) Klicken Sie auf **OK**.
7) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.
8) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

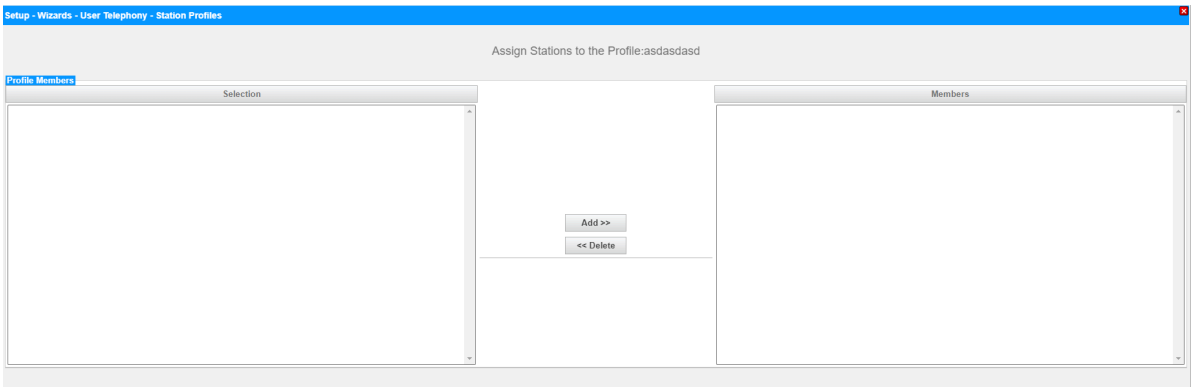
11.14.4 Wie Sie Mitglieder aus einem Teilnehmer-Profil löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.
4) Klicken Sie in der Zeile des gewünschten Teilnehmer-Profils auf **Teilnehmer zuordnen**.



5) Wählen Sie aus der Liste **Mitglieder** die gewünschten Mitglieder aus (Mehrfachauswahl ist möglich) und klicken Sie auf **Löschen**. Diese Teilnehmer können wieder einem anderen Teilnehmer-Profil zugewiesen werden.
6) Klicken Sie auf **OK**.
7) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.
8) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11.14.5 Wie Sie ein einzelnes Teilnehmer-Profil exportieren oder importieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

4) Klicken Sie in der Zeile des gewünschten Teilnehmer-Profils auf **Profil importieren/exportieren**.
5) Wenn Sie das Teilnehmer-Profil in eine Datei exportieren wollen, klicken Sie auf **Download** und speichern die Datei in einem Verzeichnis Ihrer Wahl.
6) Wenn Sie ein Teilnehmer-Profil aus einer Datei importieren wollen, klicken Sie auf **Durchsuchen**, navigieren Sie zum Ablageort der Datei und laden Sie die Datei in das Kommunikationssystem.
7) Klicken Sie auf **OK**.
8) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.
9) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

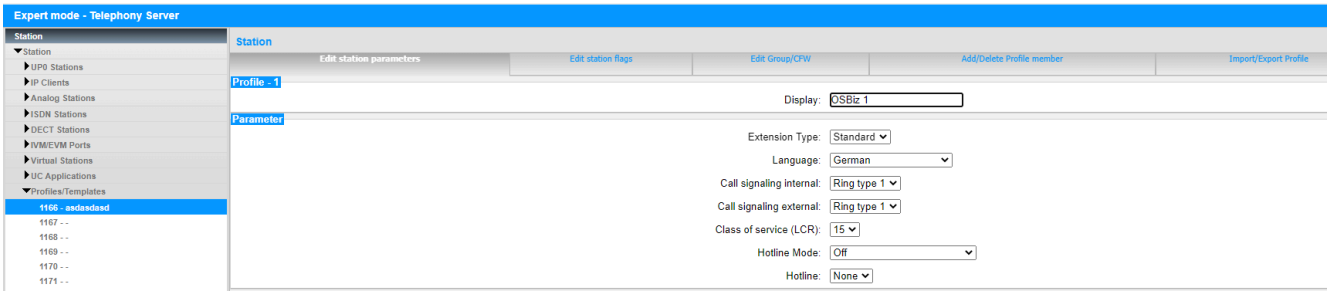
11.14.6 Wie Sie die Werte und Einstellungen eines Teilnehmer-Profils ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

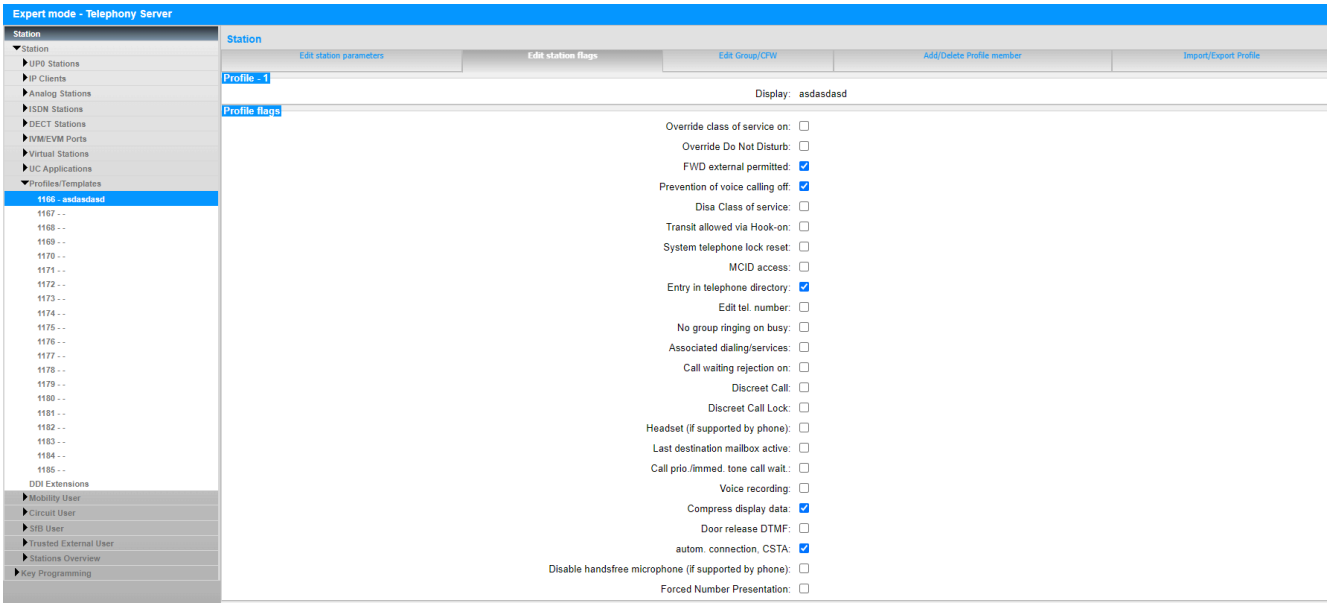
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer** > **Profile/Vorlagen**.
4) Klicken Sie im Menübaum auf eine Teilnehmer-Profilnummer.

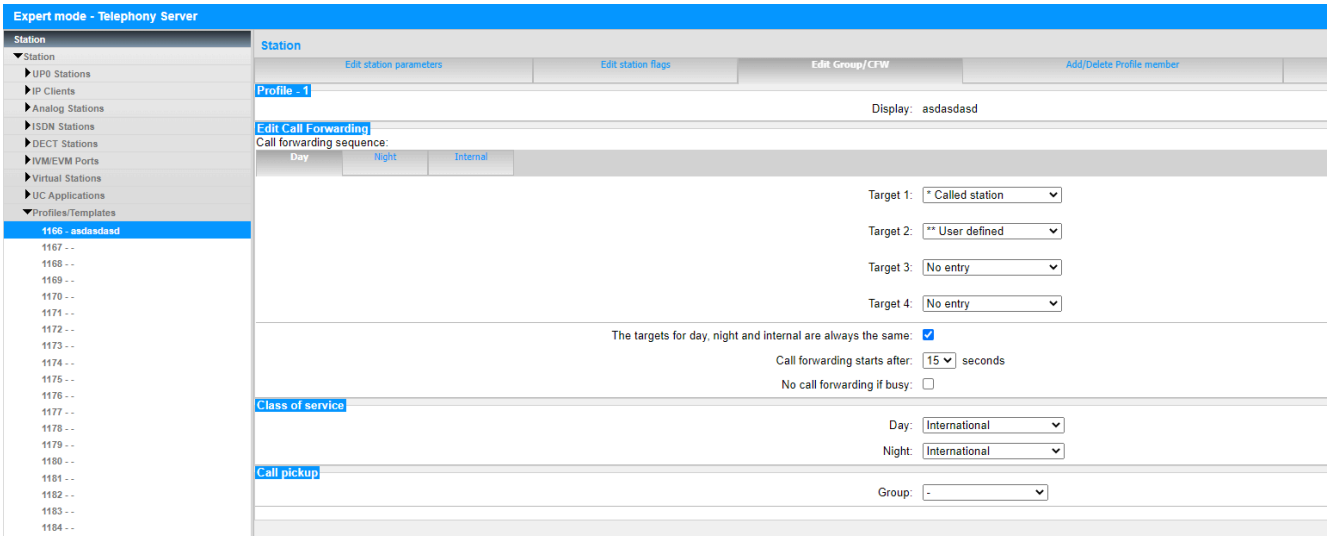


5) Ändern Sie bei Bedarf im Register **Teilnehmer-Parameter** im Feld **Name** den Namen des Teilnehmer-Profils (max. 16 Stellen möglich) und klicken Sie auf **Übernehmen**.

6) Ändern Sie bei Bedarf im Register **Teilnehmer-Parameter** die für das Teilnehmer-Profil gewünschten Teilnehmer-Parameter und klicken Sie auf **Übernehmen**.



7) Ändern Sie bei Bedarf im Register **Teilnehmer-Flags** die für das Teilnehmer-Profil gewünschten Teilnehmer-Flags und klicken Sie auf **Übernehmen**.



8) Ändern Sie bei Bedarf im Register **Gruppen/RWS ändern** die für das Teilnehmer-Profil gewünschten Rufweiterschaltungen und klicken Sie auf **Übernehmen**.

9) Klicken Sie auf **Übernehmen**.

11.14.7 Wie Sie alle Teilnehmer-Profile exportieren oder importieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer** > **Profile/Templates**.
4) Klicken Sie auf das Register **Import/Export alle Profile**.
5) Wenn Sie alle Teilnehmer-Profile in eine Datei exportieren wollen, klicken Sie auf **Download** und speichern die Datei in einem Verzeichnis Ihrer Wahl.
6) Wenn Sie alle Teilnehmer-Profile aus einer Datei importieren wollen, klicken Sie auf **Durchsuchen**, navigieren Sie zum Ablageort der Datei und laden Sie die Datei in das Kommunikationssystem.

11.15 Konfiguration der Authentifizierungsdaten am SIP-Telefon

Die Daten für die Authentifizierung eines SIP-Teilnehmers am Kommunikationssystem sind auch am SIP-Telefon direkt einzutragen. Dazu müssen die Daten verwendet werden, die im WBM bei jedem SIP-Teilnehmer eingetragen sind.

Folgende Daten müssen aus dem WBM übernommen und am SIP-Telefon eingetragen werden (für jedes SIP-Telefon extra):

- Passwort

  Kennwort für die Authentifizierung.
- SIP User ID / Benutzername

  Benutzername für die Authentifizierung.
- Realm

  Zone oder Domäne für die Authentifizierung.

Die Konfiguration kann über das WBM des SIP-Telefons durchgeführt werden oder direkt am Display des SIP-Telefons.

11.15.1 Wie Sie die Authentifizierungsdaten über das WBM des SIP-Telefons konfigurieren

Voraussetzungen

Das SIP-Telefon ist ins LAN integriert.

Der Admin-PC hat Zugang zum WBM des SIP-Telefons.

Sie kennen die IP-Adresse des SIP-Telefons.

Die Konfiguration ist am Beispiel eines OpenStage 60 SIP beschrieben.

Schritt für Schritt

1) Starten Sie auf dem Admin-PC den Webbrowser und rufen Sie die Anmeldeseite des WBM des SIP-Telefons auf unter folgender Adresse auf:

   `https://<IP-Adresse des SIP-Telefons>`

   Anmerkung: Lässt sich das WBM nicht starten, prüfen Sie die LAN-Verbindung und wiederholen Sie den Aufruf.

Lässt er sich noch immer nicht starten, prüfen Sie, ob die IP-Adresse durch Ihre Firewall geblockt wird. Genauere Informationen finden Sie in der Dokumentation Ihrer Firewall.

2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).

a) Schließen Sie den Webbrowser.

b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.

c) Erlauben Sie die Benutzerkontensteuerung.

d) Rufen Sie die Anmeldeseite des WBM des SIP-Telefons unter folgender Adresse auf:

`https://<IP-Adresse des SIP-Telefons>`

e) Klicken Sie auf **Laden dieser Website fortsetzen**.

f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.

g) Klicken Sie auf **Zertifikate anzeigen**.

h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).

i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.

j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.

k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.

l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.

m) Schließen Sie den Webbrowser.

n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie die Anmeldeseite des WBM des SIP-Telefons unter folgender Adresse auf:

`https://<IP-Adresse des SIP-Telefons>`

3) Bei der ersten Anmeldung werden aufgefordert, ein Passwort zu vergeben.

a) Geben Sie in den Feldern **Neues Passwort** und **Passwort bestätigen** ein neues Passwort ein, um das System gegen Missbrauch zu schützen. Berücksichtigen Sie Groß-/Kleinschreibung und den Zustand der Taste **Num**. Das Passwort erscheint verdeckt durch Sternchen (*).

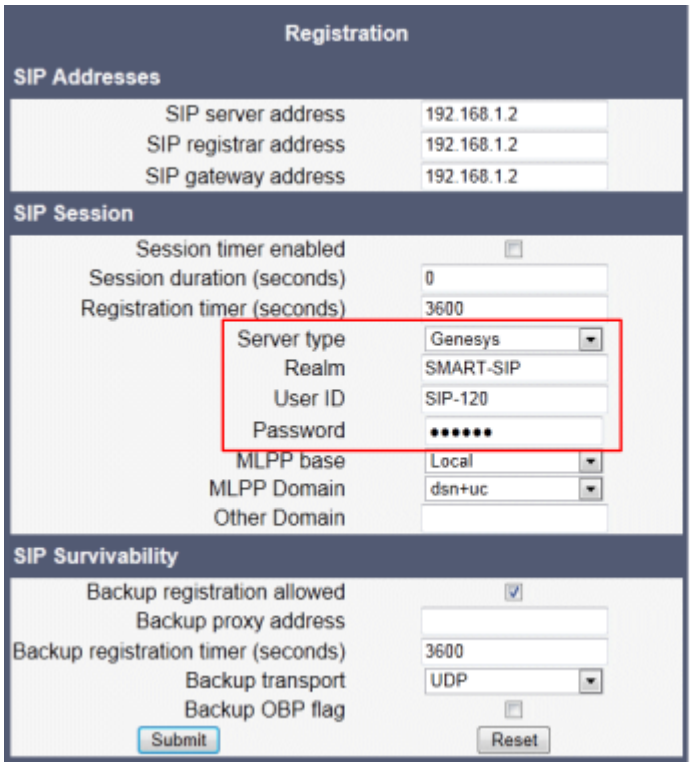
Anmerkung: Das Passwort muss mindestens 6 Zeichen lang sein und eine Ziffer enthalten. Bitte merken Sie sich Ihr neues Passwort genau.

4) Klicken Sie auf **OK**.

5) Klicken Sie auf die Registerkarte **Administratorseiten (Admin)**.

6) Geben Sie das Administrator-Passwort ein (Standard: 123456) und klicken Sie auf **Login**.

7) Navigieren Sie zu **System** > **Registration**.



8) Wählen Sie im Bereich **SIP Session** aus der Aufklappliste **Server type** den Eintrag **Genesys** aus.

9) Geben Sie im Feld **Realm** den Realm-Eintrag ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben (z.B. `SMART-SIP`).

10) Geben Sie im Feld **User ID** die User ID ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben (z.B. `SIP-120`).

11) Geben Sie im Feld **Password** das Kennwort ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben.

12) Klicken Sie auf **Submit**. Die Änderungen sind gespeichert.

13) Melden Sie sich am WBM ab mit der Schaltfläche **Abmeldung**.

11.15.2 Wie Sie die Authentifizierungsdaten am Display des SIP-Telefons konfigurieren

Voraussetzungen

Die Authentifizierungsdaten (User ID, Kennwort und Realm) sind Ihnen bekannt.

Die Konfiguration ist am Beispiel eines OpenStage 80 SIP beschrieben.

Schritt für Schritt

1) Um in den Administrationsmodus des Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.
2) Blättern Sie im Register `Einstellungen` bis `Admin` und bestätigen Sie mit der OK-Taste.
3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.
4) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
5) Blättern Sie bis `Registration` und bestätigen Sie mit der OK-Taste.
6) Blättern Sie bis `SIP session` und bestätigen Sie mit der OK-Taste.
7) Blättern Sie bis `Server type` und bestätigen Sie mit der OK-Taste.
8) Blättern Sie bis zum Eintrag `Genesys` und bestätigen Sie mit der OK-Taste.
9) Blättern Sie bis `Realm` und bestätigen Sie mit der OK-Taste.
10) Geben Sie den Realm-Eintrag ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben (z.B. `SMART-SIP`). Bestätigen Sie mit dem OK-Symbol.
11) Blättern Sie bis `User ID` und bestätigen Sie mit der OK-Taste.
12) Geben Sie die User ID ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben (z.B. `SIP-120`). Bestätigen Sie mit dem OK-Symbol.
13) Blättern Sie bis `Password` und bestätigen Sie mit der OK-Taste.
14) Geben Sie das Kennwort ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben. Bestätigen Sie mit dem OK-Symbol.
15) Bestätigen Sie die Abfrage nach der Speicherung der Änderungen, indem Sie `Save` auswählen und mit der OK-Taste bestätigen.
16) Navigieren Sie mit der Zurück-Taste zum Menü `Admin` zurück.
17) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

11.16 Export von Teilnehmerdaten

Wichtige Teilnehmerdaten können in eine XML-Datei exportiert werden.

Zusätzlich zu den Teilnehmerdaten, wie z.B. Namen und Rufnummern der Teilnehmer, E-Mail-Adressen und Telefontyp, kann die XML-Datei weitere Daten enthalten, wie z.B. Gruppenrufnummern und Lizenzzuordnungen.

Die XML-Datei können Sie mit einem Tabellenkalkulationsprogramm wie z.B. Microsoft Office Excel bearbeiten.

Eine Vorlage mit Beispieldatensätzen und Beschreibung finden Sie in der Datei `csv-templates.zip` unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**.

11.16.1 Wie Sie die Teilnehmerdaten exportieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Konfiguration**.
3) Klicken Sie im Menübaum auf **Konfiguration** > **Port-Konfiguration**.
4) Klicken Sie auf das Register **Konfiguration exportieren**.
5) Klicken Sie auf die Schaltfläche **Download**.
6) Bestätigen Sie die Abfrage mit **OK**.
7) Klicken Sie auf **Speichern** und wählen Sie den Ablageort der XML-Datei aus.
8) Klicken Sie anschließend auf **Speichern**.

12 UC Smart

UC Smart ist in allen OpenScape Business Modellen (mit und ohne UC Booster) integriert und bietet Unified Communications Leistungsmerkmale wie z.B. Anwesenheitsstatus und Sprachnachrichten sowie zusätzlich Konferenzen.

Clients für UC Smart

Die UC Smart Funktionen können mit folgenden Clients genutzt werden:

- myPortal @work
- myPortal to go (als Mobile UC App oder als Web Edition)
- Application Launcher
- OpenScape Business Attendant / BLF
- 3rd Party WSI Clients

Die Ausbaugrenzen sind abhängig vom genutzten OpenScape Business Modell und von den ggf. installierten OpenScape Business UC Booster Varianten.

Besonderheiten von UC Smart bei OpenScape Business S

Bedingt durch die Systemarchitektur gibt es bei OpenScape Business S folgende Einschränkungen:

- Die Anzahl der Voicemail-Nachrichten wird nicht im Display des Telefons angezeigt (MWI).
- Bei der Sprachbox (SmartVM) wird keine Fax,- Besetzt,- oder Ruheerkennung unterstützt. Kommende Fax-Verbindungen können nach Rufannahme durch die SmartVM nicht zu einem Standard-Fax-Gerät vermittelt werden. Die SmartVM zeichnet für 2 Minuten auf.
- Bei Vermittlung von Verbindungen durch den Company AutoAttendant auf besetzte Teilnehmer erhält der Anrufer Besetztton. Es besteht keine Möglichkeit eine Sprachnachricht zu hinterlassen.
- Soll bei der Abfrage einer Sprachnachricht auf die in der SmartVM hinterlegte Rufnummer weitergeleitet werden (Calling Party Number), muss diese Rufnummer identisch sein mit der für die SmartVM konfigurierten Rufnummer des Benutzers.
- Bei Verbindungen zur Sprachbox (SmartVM) werden beim UC Booster Server und bei OpenScape Business S SIPQ-Trunks belegt. Dafür werden keine Trunk-Lizenzen benötigt.
- Für gleichzeitige Ansagen werden MEB-Kanäle belegt.
- Für Sprachverbindungen zur Sprachbox (SmartVM) oder AutoAttendant stehen sechzig MEB-Kanäle zur Verfügung.

Anmerkung: Nach Änderungen in der Konfiguration von Stationen, Gruppen, Mobility oder anderen Systemparametern wie Trunk Access Codes müssen die UC-Daten für UC Smart oder UC Suite synchronisiert werden. Die Synchronisation erfolgt fünf Minuten nach der letzten Konfigurationsänderung. Wenn eine spätere Konfigurationsänderung vor dem 5-Minuten-Timer erfolgt, wird der Timer neu gestartet. UC-Daten können veraltet sein, bis die Synchronisation beginnt.

Zugehörige Konzepte

UC-Funktionen (Überblick) auf Seite 91

12.1 Grundeinstellungen für UC Smart

Grundlegende Einstellungen zu UC Smart können angepasst werden.

UC Smart kann aktiviert oder deaktiviert werden. Wenn UC Smart genutzt wird, muss UC Suite deaktiviert werden.

Kennwort-Einstellungen

Der Administrator muss für alle Benutzer von UC Smart ein Initial-Kennwort vergeben und dieses Kennwort den Benutzern mitteilen. Das Initial-Kennwort kann für alle Benutzer gleich sein oder für jeden Benutzer unterschiedlich. Das Initial-Kennwort muss der Benutzer bei seiner ersten Anmeldung an einem UC Smart Client ändern. Ohne die Vergabe eines Initial-Kennworts kann sich der Benutzer nicht an einem UC Smart Client anmelden.

Das vom Benutzer neu zu vergebende Kennwort sollte den strengen Kennwort-Richtlinien entsprechen.

Erweiterte Einstellungen für applikationsgesteuerte Konferenzen (optional)

Der Administrator muss im WBM während der Grundinstallation die **Funktionskennzahl für MeetMe Konferenz** (MeetMe-Einwahlnummer) und mindestens eine **Funktionskennzahl für Konferenz** (Konferenzraum) einrichten.

Für OpenScape Business X Systeme muss der MeetMe-Einwahlnummer eine Rufzielliste zugewiesen werden, in der der erste Eintrag leer ist und der zweite Eintrag der Rufnummer der Sprachbox (SmartVM) entspricht.

Für OpenScape Business S Systeme muss der MeetMe-Einwahlnummer eine Rufzielliste zugewiesen werden, in der der erste Eintrag der Rufnummer der Sprachbox (Richtung Anwendungssuite).

Zuletzt muss der MeetMe-Einwahlnummer noch eine Standardmailbox zugeordnet werden.

Die Beschreibung der Konfiguration finden Sie hier: Wie Sie die applikationsgesteuerten Konferenzen konfigurieren,

Lizenzzuweisungen

Der Administrator muss jedem UC Smart User eine UC User-Lizenz zuweisen.

Optional können zusätzliche Lizenzen zugewiesen werden für:

- Voicemail (auch ohne UC Smart nutzbar)
- Konferenz
- Application Launcher

12.1.1 Wie Sie UC Smart aktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Applikationsauswahl**.
3) Wenn Sie UC Smart ohne UC Booster Server nutzen möchten, klicken Sie auf **Paket mit UC Smart**.
4) Wenn UC Smart mit UC Booster Server nutzen möchten, klicken Sie auf **Paket mit UC Smart auf OSBiz UC Booster-Server** und geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers an.
5) Klicken Sie auf **Übernehmen**.

Nächste Schritte

Wie Sie UC Smart konfigurieren

12.1.2 Wie Sie UC Smart konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Smart**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.
4) Klicken Sie im Menübaum auf **Administration** > **Grundeinstellungen**.
5) Aktivieren Sie unter **UC Smart Aktivieren / Deaktivieren** das Kontrollkästchen **Aktiv**.
6) Initial-Kennwort unter **Passwort-Policy** vergeben:
   a) Klicken Sie bei **Systemweites initiales UC Smart Passwort** auf **Konfigurieren**.
   b) Geben Sie im Feld **Systemweites initiales UC Smart Passwort** das Initial-Kennwort für alle UC Smart Benutzer ein.
   c) Klicken Sie auf **Übernehmen**.
7) Kennwort-Richtlinien unter **Passwort-Policy** festlegen:

   Anmerkung: Für detaillierte Informationen zur den Kennwort-Richtlinien klicken Sie auf das Symbol **i**.

   - Wenn Sie möchten, dass Benutzer-Kennwörter den strengen Kennwort-Richtlinien entsprechen müssen (empfohlen), aktivieren Sie das Kontrollkästchen **Benutzer muss sicheres Passwort eingeben**.
   - Wenn Sie nicht möchten, dass Benutzer-Kennwörter den strengen Kennwort-Richtlinien entsprechen müssen (nicht empfohlen), deaktivieren Sie das Kontrollkästchen **Benutzer muss sicheres Passwort eingeben**.

8) Zugriff auf das System unter **Zugangseinstellungen** festlegen:
   - Wenn Sie verschlüsselten Zugriff von UC Smart Clients auf das System aktivieren möchten (bei Nutzung von myPortal to go via Internet empfohlen), aktivieren Sie das Kontrollkästchen **HTTPS**.
   - Wenn Sie unverschlüsselten Zugriff von UC Smart Clients auf das System aktivieren möchten (bei Nutzung von myPortal to go via Internet nicht empfohlen), aktivieren Sie das Kontrollkästchen **HTTP**.
9) Aktivieren Sie das Kontrollkästchen **Anmeldedaten im Endgerät speichern**, wenn die Anmeldedaten zusätzlich im Telefon gespeichert werden sollen.
10) Klicken Sie auf **Übernehmen**.

12.1.3 Wie Sie die applikationsgesteuerten Konferenzen konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.
3) Überspringen Sie das Fenster **Übersicht** mit **OK & Weiter**. Es erscheint das Fenster **Zentrale Teilnehmer-Funktionen**.
4) Aktivieren Sie das Optionsfeld **Vorkonfigurierte Rufnummern ändern**.
5) Klicken Sie auf **Funktion ausführen**. Es erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.
6) Passen Sie bei Bedarf die **Funktionskennzahl für MeetMe Konferenz** an Ihre Belange an.
7) Vergeben Sie mindestens eine **Funktionskennzahl für Konferenz** für den Konferenzraum.
8) Klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
9) Klicken Sie auf **OK & Weiter**.
10) Beenden Sie den Wizard, indem Sie alle weiteren Fenster mit **OK & Weiter** überspringen.
11) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
12) Klicken Sie im Navigationsbaum auf **Telephonie** > **Kommende Rufe**.
13) Klicken Sie im Menübaum auf **Kommende Rufe** > **Rufweiterschaltungen**.
14) Klicken Sie auf die Registerkarte **Rufzielliste - Definition**.
15) Für OpenScape Business X definieren Sie die Rufzielliste für die MeetMe-Einwahlnummer folgendermaßen:
    a) Wählen Sie unter **Rufzielliste** eine freie Rufzielliste aus, z.B. `500`.
    b) Wählen Sie als erstes Ziel **Kein Eintrag** aus und als zweites Ziel die Rufnummer der Sprachbox (z.B. `351 VOICEMAIL Gruppe`).

16) Für OpenScape Business S definieren Sie die Rufzielliste für die MeetMe-Einwahlnummer folgendermaßen:
    a) Wählen Sie unter **Rufzielliste** eine freie Rufzielliste aus, z.B. `500`.
    b) Wählen Sie das externe Ziel als erstes Ziel (Richtung Application Suite) und geben Sie die Rufnummer der Sprachbox in das Feld "Externes Ziel" ein.
17) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
18) Schließen Sie das Fenster.
19) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
20) Klicken Sie im Navigationsbaum auf **Telefonie** > **Anschaltungen**.
21) Klicken Sie im Menübaum auf **Anschaltungen** > **SmartVM**.
22) Klicken Sie auf die Registerkarte **SmartVM-Mailboxen bearbeiten**.
23) Geben Sie in der Spalte **Mailbox-Rufnummer** in einem freien Feld die MeetMe-Einwahlnummer ein, für die die Mailbox hinzugefügt werden soll.
24) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.1.4 Wie Sie die IP-Adressen von Komponenten des Systems ermitteln

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Applikationsauswahl**.

   Unter **Applikationsauswahl** werden die IP-Adressen verschiedener Komponenten des Systems angezeigt, z. B. von **UC Smart**, **Application Launcher**, **CSTA-Connector**, **Open Directory Service**, **UC Suite** und **Web Collaboration**.

Zugehörige Konzepte

Grundeinstellungen für UC Suite auf Seite 540

12.1.5 Wie Sie den Status von UC Smart ermitteln

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Smart**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.

4) Klicken Sie im Menübaum auf **Administration** > **Status**.

   Unter **Applikationsserver** werden Statusinformationen zu UC Smart angezeigt, z.B. **Status**, **Version**, **Telefonanlage**, **Datenbank**, **EVM**, **Fehlende Monitorpunkte**, **Aktive Benutzer**, **Aktive Verbindungen**, **Aktive HTTPS Verbindungen**, **Mobility Entry Benutzer**, **Benutzer ohne Endgerät** und **Gesperrte Benutzer**.

12.2 UC Smart Clients

UC Smart Clients bieten Teilnehmern Oberflächen für Unified Communications.

Das System bietet folgende UC Smart Clients für folgende Geräte:

Client-Typ	Client	Gerät
Communications Client	myPortal @work	PC
Mobile Client	myPortal to go (UC Smart) (siehe Mobility auf Seite 955)	Smartphone, Tablet-PC
Communications Client	OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA (in der Telefon-Software integrierter Client)	OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA

12.2.1 myPortal @work

myPortal @work ist eine Unified-Communication-Anwendung (Microsoft Windows und Mac OS X), die alle benötigten Funktionen und Services wie komfortables Wählen über Telefonverzeichnisse, Favoriten, Gespräche und Informationen zum Anwesenheitsstatus von Kollegen zu einem zentralen Lösungskonzept vereint, um die tägliche Kommunikation zu beschleunigen, die Teamarbeit zu verbessern sowie rasch mit Kollegen, Kunden und Partnern in Verbindung zu treten.

myPortal @work kann entweder im UC Smart oder im UC Suite Modus verwendet werden. Je nach Modus variieren die angebotenen Funktionen in der Benutzeroberfläche. Sie können die Betriebsart nicht ändern, da dies durch den Systemadministrator festgelegt ist. Wenn Sie Zweifel an der aktuellen Betriebsart Ihres myPortal @work-Clients haben, fragen Sie Ihren Systemadministrator um Rat.

myPortal @work bietet einen integrierten Voice over IP (VoIP) Telefonie-Client. Wenn die Option VoIP aktiviert ist, nutzen die sprachbezogenen Funktionen des myPortal @work-Clients die VoIP-Funktionen.

Anmerkung: Um die Voice over IP (VoIP)-Funktionen nutzen zu können, muss der Benutzer als System-Client konfiguriert sein.

Infos zur remoten Verwendung von VoIP über Device@Home, siehe 1 Konfiguration für System Device@Home

---

Die VoIP-Funktionen unterstützen eine Reihe von Funktionen, die über die UC-Funktionen hinausgehen:

- Anrufen
- Anruf annehmen
- Anruf beenden
- Rückfrage
- Übergeben nach Melden
- Übergabe ohne Rückfrage
- Ruf abweisen
- Zur Voicemail umleiten
- Wiederanruf (Benachrichtigung für einen Wiederanruf anzeigen wird noch nicht unterstützt)
- Makeln
- Stumm/Stummschalten aufheben(nur für VoIP-Funktionen)
- Systemkonferenz
- Anklopfschutz
- Sie klopfen an
- Anrufschutz (DND)
- DTMF
- Anrufübernahme

Anmerkung: Da der myPortal@Work-Client die Fähigkeit, DTMF-Töne an eine andere Station zu senden, nicht unterstützt, wird das Senden eines DTMF-Tons über den CSTA-Befehl „generateDigits“ ebenfalls nicht unterstützt, und eine solche Anfrage wird vom System abgelehnt und zurückgewiesen.

Arbeiten im Team:

myPortal @work VoIP-Client kann auch verwendet werden in:

- Gruppe (z. B. Linear, Anklopfen)
- MULAP als MULAP-Mitglied

Signaling- und Payload-Encryption (SPE) wird für das Kommunikationssystem ebenfalls unterstützt. Der VoIP-Client verwendet einen modernen WebRTC-Sicherheitsstapel und bietet somit auch einen sicheren Datentransfer mittels DTLS.

Anmerkung: Die Konfiguration von ITSP SDES wird ebenfalls unterstützt.

Servicecodes können über die Suchleiste verwendet werden, werden aber bei Problemen nicht unterstützt. Rückmeldungen über die erfolgreiche oder erfolglose Ausführung von Servicecodes werden nicht ausgegeben und es wird daher dringend empfohlen, die Eingabemöglichkeiten der Benutzeroberfläche myPortal @work zu nutzen, um die jeweiligen Funktionen zu steuern.

myPortal @work im UC Suite Modus kann nicht nur eigenständig, sondern auch in Verbindung mit dem bestehenden myPortal for Desktop/Outlook, myAgent, myAttendant Client (CTI, Favoriten und Gespräche) genutzt werden. Die vorhandenen UC User-Lizenzen können auch mit myPortal @work verwendet werden.

Die folgenden Abbildungen zeigen überwiegend myPortal @work im UC Smart Modus. Auf Abweichungen im UC Suite Modus wird ausdrücklich im Benutzerhandbuch für myPortal @work hingewiesen.

myPortal @work unterstützt allgemein folgende Leistungsmerkmale:

- Anwesenheitsstatus
- Statusbezogene Anrufumleitung
- Verzeichnisse einschließlich Suchen nach Namen
- Favoriten
- Konversationen: bis zu 25 Konversationen werden im Client angezeigt und jede Konversation hat bis zu 50 Einträge
- Konferenzschaltung
- Hotkey-Wahl/Hotkey-Suche/Telefonie-Hyperlinks
- Anruffunktionen über:
  1) Zugewiesenes Telefon
  2) Integrierten Voice over IP Telefonie-Client
- Voicemail-Steuerung
- Vergrößern/Verkleinern
- Bildschirmteilung mittels OpenScape Web Collaboration (optional)

Verwendung von myPortal @work in einer Microsoft Terminal Server-Umgebung

myPortal @work wurde für UC- und CTI-Funktionen in Microsoft Terminal Server-Umgebungen mit den folgenden Einschränkungen freigegeben:

- Telefonie-Hyperlinks und Click-to-Dial werden nicht unterstützt
- Anwendungsstart beim Hochfahren wird nicht unterstützt
- Hochladen von Benutzerbildern wird nicht unterstützt
- Die Funktionen für Andocken/Abdocken, Anheften/Loslösen und Minimieren auf der Taskleiste sind begrenzt
- Die Funktion VoIP wird nicht unterstützt

12.2.1.1 Voraussetzungen für myPortal @work

Um den UC Client zu nutzen, muss der Client-PC eine geeignete Hardware- und Softwareausstattung haben. Für die Installation und automatische Updates sind konfigurationsabhängig Administrationsrechte erforderlich. Der nutzbare Funktionsumfang ist abhängig von den verwendeten Lizenzen.

Die folgenden Voraussetzungen sind für die Installation von myPortal @work nötig:

- Administratorrechte
- myPortal @work Software-Einrichtungsprogramm
- IP-Adressen und Ports des Kommunikationssystems
- FQDN oder IP-Adresse, Port für WAN-Verbindung (Gerät@home)
- Zugangsdaten (Benutzer und Kennwort) für Ihr UC-Benutzerkonto im Kommunikationssystem
- Sprachbox-Kontoinformationen (optional)
- MULAP-Rufnummer bei mehrfacher Nummernvergabe (optional)
- Windows OS und Apple Mac OS X

Anmerkung: TLS 1.2 muss unter Internetoptionen (in der Systemsteuerung) aktiviert sein und die neuesten Patches von Microsoft müssen manuell installiert bzw. aktiviert werden.

Wenn die genannten Aktionen nicht ausgeführt werden, wird der HTTPS-Zugriff abgelehnt.

Telefone

myPortal @work kann in Verbindung mit folgenden Telefonen genutzt werden:

Anmerkung: myPortal @work kann auch einzeln mit VoIP-Funktionen verwendet werden, ohne ein physisches Gerät zu verwenden.

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- Analoge Telefone
- ISDN-Telefone
- OpenScape Personal Edition HFA
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)

Ältere Geräte (z. B. optiPoint 410/420/500 und Gigaset M2/SL3/S4/SL4/S5) werden unterstützt. Optiset E-Geräte können nicht betrieben werden. Getestete und freigegebene Geräte entnehmen Sie bitte der Freigabemitteilung.

Anmerkung: Für den OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA integrierten Client sind neben der Standard-Client-Konfiguration und -Lizenz keine besonderen Voraussetzungen erforderlich.

"Favoriten" im Telefonmenü enthält frei programmierbare Tasten und bezieht sich nicht auf UC-Favoriten. Details zu diesen Schlüsseln und eine Anleitung dazu finden Sie in der Gerätedokumentation.

Anmerkung: Bei analogen Telefonen und DECT-Telefonen wird die Message Waiting Indication (MWI) nicht unterstützt, die Anzeige von Informationen im Display wird nur eingeschränkt unterstützt.

Webbrowser

Für die Tastenprogrammierung der Telefone über den UC Client sind folgende Webbrowser freigegeben:

- Microsoft Internet Explorer Version 10 (oder neuer)
- Mozilla Firefox Version 19 (oder neuer)
- Google Chrome

Installationsdateien

Der Administrator kann die Installationsdateien aus dem **Service-Center** > **Software** herunterladen und diese den Benutzern bereitstellen, z. B. über ein Netzlaufwerk.

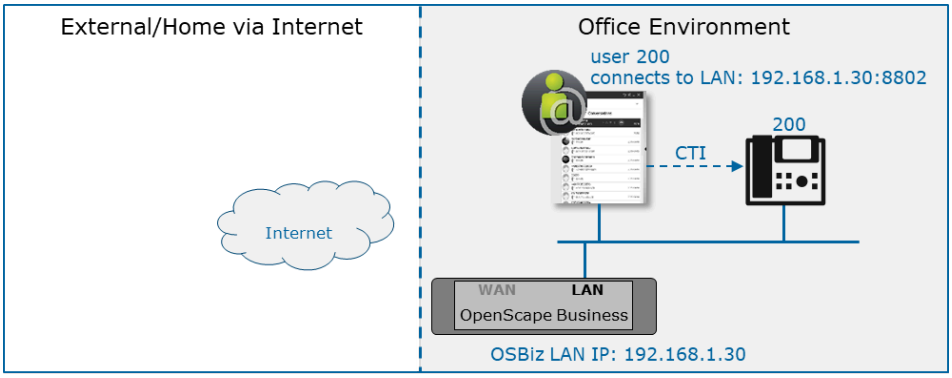
12.2.1.2 Benutzerkonfiguration für myPortal@work

myPortal @work ist eine Kombination aus einem UC- und einem VoIP-Client, und diese beiden Funktionalitäten erfordern die folgenden Konfigurationen/ Lizenzen für verschiedene UC-Modi (Smart/UC Suite) und Anwendungsfälle.

Anmerkung: Wenn ein myPortal @work-Benutzerkonto nach mehreren fehlerhaften Anmeldeversuchen im UC Suite-Modus gesperrt wird, ist es im UC Suite-Benutzerverzeichnis nicht sichtbar. Sie können die gesperrten myPortal @work-Benutzer unter**Expertenmodus > Web Services > Web Services Assistant > Benutzerverwaltung** einsehen. Unter **Expertenmodus > OpenScape Business UC Suite > Benutzerverzeichnis** können Sie diese Konten wieder entsperren.

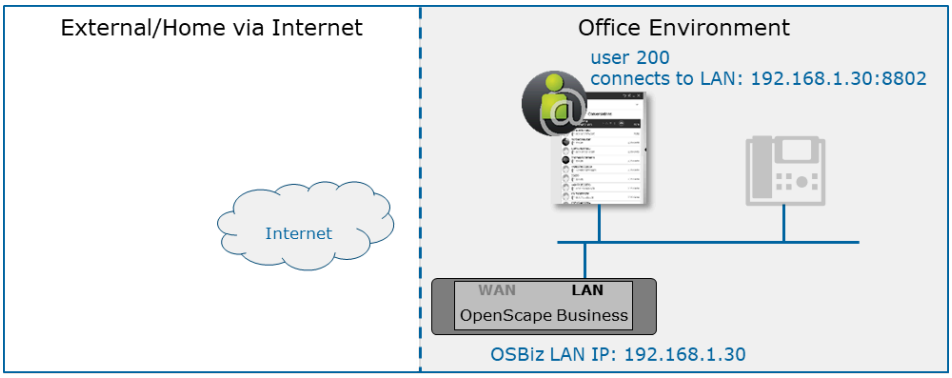
Lokale LAN-Konfiguration – nur UC- und CTI-Client

myPortal @work wird als UC- und CTI-Client für ein angeschlossenes Tischtelefon ohne VoIP verwendet.



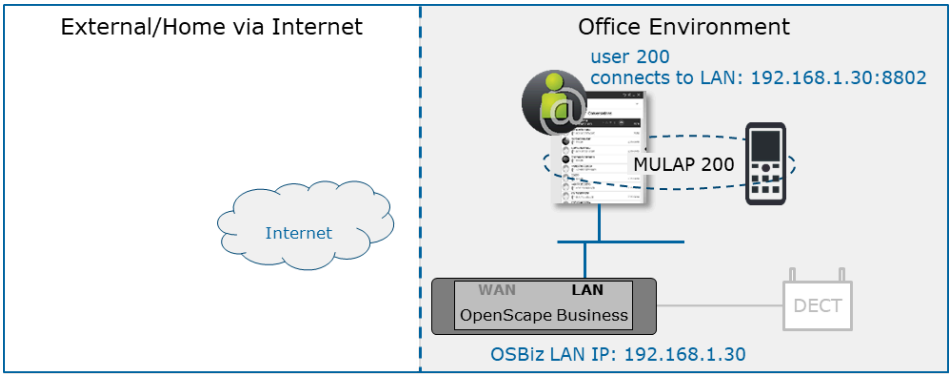
- Lizenzen: UC-Benutzer oder Groupware-Benutzer
- myPortal @work-Login: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Passwort ein sowie die LAN IP-Adresse:8802

Lokale LAN-Konfiguration – UC- und VoIP-Client



- Lizenzen: IP- und UC-Benutzer oder Groupware-Lizenz
- myPortal @work-Login: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Passwort ein sowie die LAN IP-Adresse:8802
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen
- STUN-Anbindung im Client ist für rein firmeninterne Verbindungen nicht erforderlich. Dies ist jedoch in einigen hybriden Szenarien mit anderen Benutzern erforderlich, die myPortal @work VoIP über das öffentliche Internet nutzen. Um die STUN-Anbindung zu prüfen, gehen Sie zu Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen.

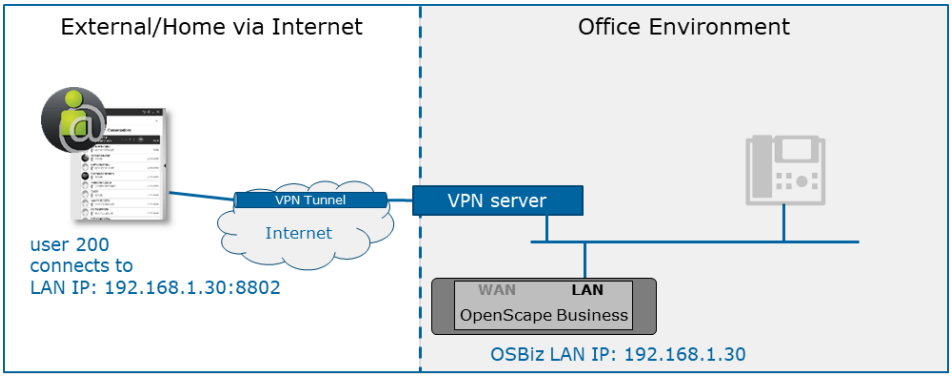
MULAP-Benutzerkonfiguration (Lokales LAN)



- Lizenzen:
  - myPortal @work: IP- und UC-Benutzer oder Groupware-Lizenz
  - ein anderes Mulap-Gerät – in diesem Beispiel DECT: TDM-Benutzerlizenz oder IP-Benutzer (Die Mulap-Konfiguration wird für die Kombination mit TDM- oder DECT-Geräten empfohlen, kann aber auch mit einem IP-Gerät verwendet werden. Im Falle eines IP-Geräts siehe auch Abschnitt Deskshare-Benutzer über lokales LAN auf Seite 504 und Remote-Deskshare-Benutzer über VPN auf Seite 504).
- myPortal @work-Login: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und das Passwort der MULAP-Nummer ein sowie die LAN-IP-Adresse:8802
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > das zugeordnete Telefon auswählen gehen und dann VoIP aktivieren

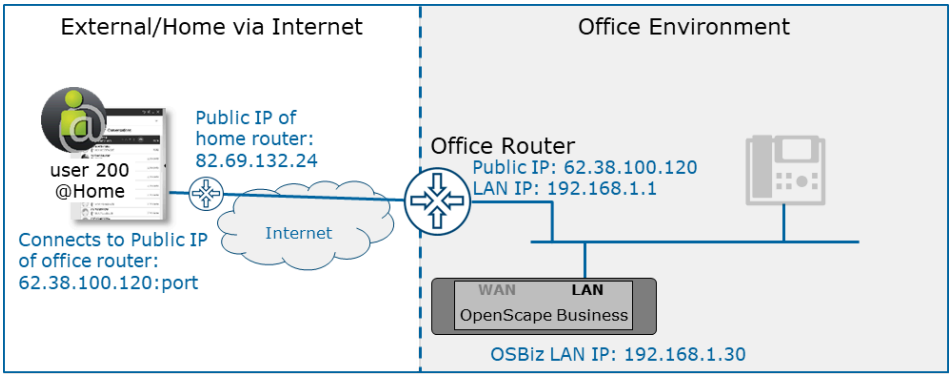
- STUN-Anbindung im Client ist für rein firmeninterne Verbindungen nicht erforderlich. Dennoch ist dies in einigen hybriden Szenarien mit anderen Benutzern erforderlich, die myPortal @work VoIP über das öffentliche Internet nutzen. Um die STUN-Anbindung zu prüfen, gehen Sie zu **Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen**.

Heimanwender mit VPN-Verbindungskonfiguration



- Lizenzen: IP- und UC-Benutzer oder Groupware-Lizenz
- myPortal @work-Login: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Passwort ein sowie die LAN IP-Adresse:8802
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen
- STUN-Anbindung ist obligatorisch. Um die STUN-Anbindung zu prüfen, gehen Sie zu Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen.

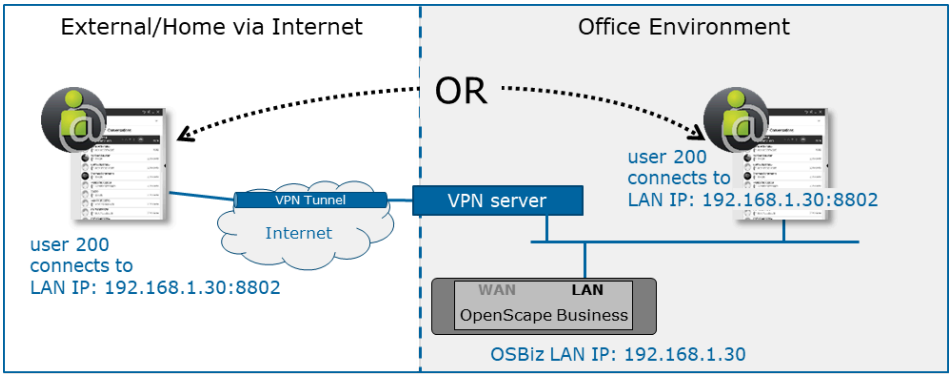
myPortal @work über das öffentliche Internet



- Lizenzen: IP- und UC-Benutzer oder Groupware-Lizenz
- myPortal @work-Login: Geben Sie im Login-Bildschirm Ihren Login-Benutzernamen und Ihr Passwort ein sowie die öffentliche IP-Adresse:Port, die vom Administrator konfiguriert wurde.
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen
- Bereiten Sie die Netzwerkumgebung vor wie beschrieben in Kapitel Konfigurationsschritte zur Nutzung von myPortal @work über das Internet auf Seite 506

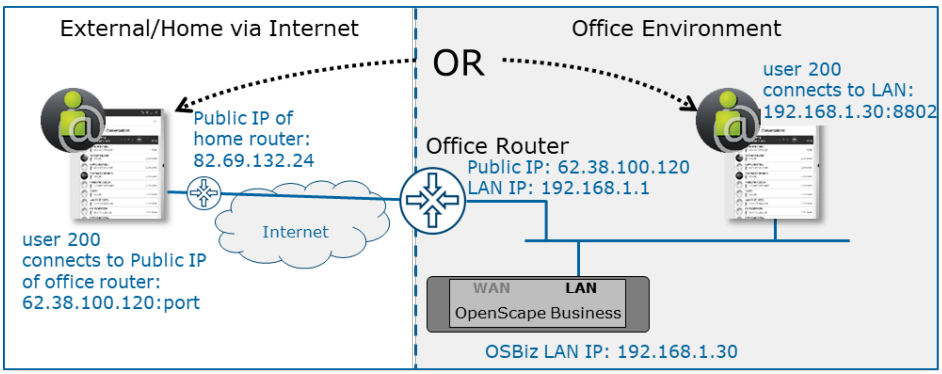
- Das SBC-Flag ist für myPortal @work nicht erforderlich. Es wird nur benötigt, wenn Sie ein Hardware-Gerät verwenden.
- Bitte verwenden Sie nicht die OSBiz WAN-Schnittstelle für die Verbindung zum Internet, wenn Sie myPortal @work über eine öffentliche IP nutzen. In diesem Fall erkennt der interne SBC die öffentliche IP-Adresse der WAN-Schnittstelle und verwendet diese bei der Kommunikation zwischen dem Client und dem OSBiz, was zu Problemen mit den Nutzdaten führt. Vorgeschlagene Konfiguration: Schließen Sie den ITSP über die LAN-Schnittstelle an. Dies kann über den normalen ISP-Router oder über einen zweiten Router und statische Routen erfolgen.
- STUN-Anbindung ist erforderlich. Um die STUN-Anbindung zu prüfen, gehen Sie zu Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen.

Heimanwender mit VPN und lokaler LAN-Konfiguration (z. B. Umzug vom Büro nach Hause und zurück)



- Lizenzen: IP- und UC-Benutzer oder Groupware-Lizenz
- myPortal @work-Login: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Passwort ein sowie die LAN-IP-Adresse:8802
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen
- myPortal @work kann in beiden Umgebungen ohne Änderung der Einstellungen verwendet werden.
- STUN-Anbindung ist zwingend erforderlich. Um die STUN-Anbindung zu prüfen, gehen Sie zu Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen.

myPortal @work über das öffentliche Internet und die lokale LAN-Konfiguration (z. B. beim Wechsel vom Büro nach Hause und zurück)



- Lizenzen: IP- und UC-Benutzer oder Groupware-Lizenz
- myPortal @work-Login: Geben Sie auf dem Anmeldebildschirm Ihren Benutzernamen, Ihr Passwort, dieLAN IP-Adresse:8802 und die öffentliche IP-Adresse:Port ein, die vom Administrator konfiguriert wurden. Wenn Sie beide Adressen konfigurieren, müssen Sie kein zweites Profil verwenden, wenn Sie vom Büro nach Hause und zurück wechseln.
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen
- Bereiten Sie die Netzwerkumgebung vor wie beschrieben in Kapitel Konfigurationsschritte zur Nutzung von myPortal @work über das Internet auf Seite 506
- Das SBC-Flag ist für myPortal @work nicht erforderlich. Es wird nur benötigt, wenn Sie ein Hardware-Gerät verwenden.

Für die VoIP-Registrierung

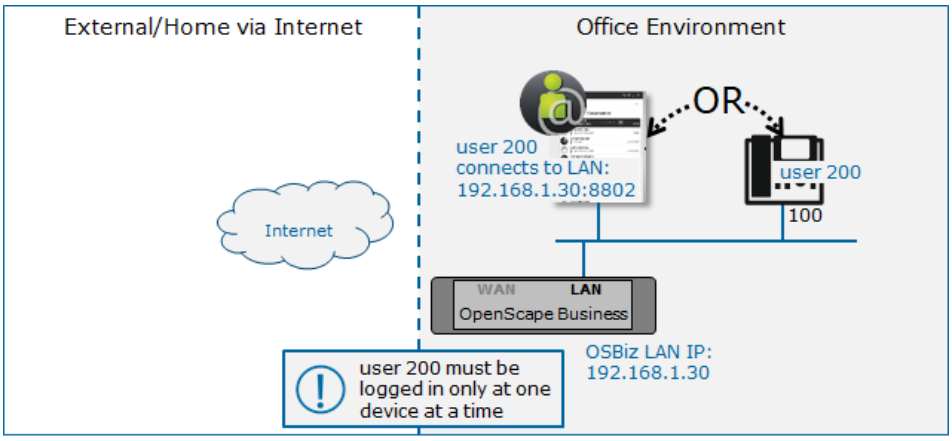
Wenn sowohl lokale als auch Heimanwender verwendet werden, sollte der Anwender nur einen VoIP-Anschluss entweder zu Hause oder im Büro haben.

Für UC

Wenn der Benutzer an mehreren Orten gleichzeitig mit UC verbunden sein möchte:

- UC Smart Modus: UC-Clients können gleichzeitig von zu Hause und vom Büro aus verbunden sein, aber in diesem Szenario wird nur ein VoIP-Client unterstützt, und die VoIP-Funktionalität des anderen Clients sollte unregistriert bleiben.
- UC Suite Modus: Bitte prüfen Sie den Abschnitt "Kombination von myPortal @work mit anderen UC Suite-Clients und Lizenzkonfiguration". Es ist nur ein myPortal @work-Client erlaubt.

Deskshare-Benutzer über lokales LAN



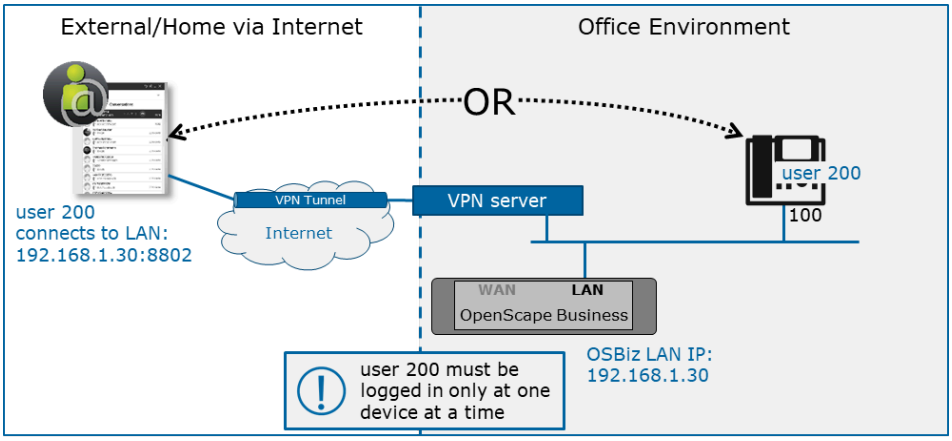
- Lizenzen: Deskshare-Lizenz und UC-Benutzer- oder Groupware-Lizenz
- myPortal @work-Login: Geben Sie im Anmeldebildschirm die Anmeldedaten der Deskshare-Erweiterung, Ihren Benutzername, Ihr Passwort und die LAN IP-Adresse:8802 ein
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen

Beispiel: Gerät verwendet Dummy-Nummer = "100" Verbinden Sie sich mit "100" mit Ihrem Tischtelefon als Deskshare z. B. 200 mit Servicecode *9419.

Um myPortal @work mit Benutzer 200 zu nutzen, wird das Tischtelefon automatisch abgemeldet und kehrt zur Dummy-Nummer "100" zurück. Wenn Sie wieder zum Tischtelefon wechseln, stellen Sie bitte sicher, dass myPortal @work nicht registriert ist (der Benutzer muss die Anwendung beenden oder sich abmelden).

Remote-Deskshare-Benutzer über VPN

Die gleiche Konfiguration wie in Kapitel Deskshare-Benutzer über lokales LAN auf Seite 504 beschrieben, wird auch für Heimanwender über VPN unterstützt.



- Lizenzen: Deskshare-Lizenz und UC-Benutzer- oder Groupware-Lizenz
- myPortal @work-Login: Geben Sie im Anmeldebildschirm die Anmeldedaten der Deskshare-Erweiterung, Ihren Benutzername, Ihr Passwort und die LAN IP-Adresse:8802 ein

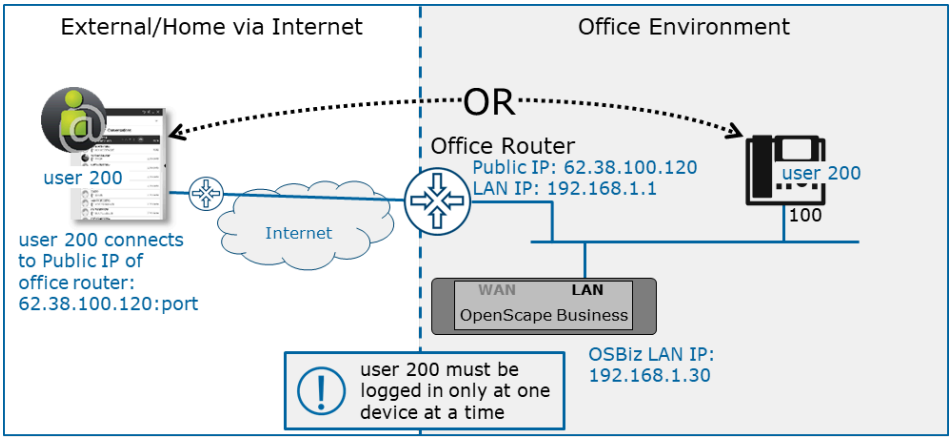
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen

Beispiel: Gerät verwendet Dummy-Nummer = "100" Verbinden Sie sich mit "100" mit Ihrem Tischtelefon als Deskshare z. B. 200 mit Servicecode *9419.

Um myPortal @work mit Benutzer 200 zu nutzen, wird das Tischtelefon automatisch abgemeldet und kehrt zur Dummy-Nummer "100" zurück. Wenn Sie wieder zum Tischtelefon wechseln, stellen Sie bitte sicher, dass myPortal @work nicht registriert ist (der Benutzer muss die Anwendung beenden oder sich abmelden).

Remote-Deskshare-Benutzer über das öffentliche Internet

Die gleiche Konfiguration wie in Kapitel Deskshare-Benutzer über lokales LAN auf Seite 504 beschrieben ist technisch auch bei Heimanwendern über das öffentliche Internet möglich. Dies ist jedoch noch nicht vollständig getestet und daher in dieser Version des Dokuments nur vorläufig beschrieben.



- Lizenzen: Deskshare-Lizenz und UC-Benutzer- oder Groupware-Lizenz
- myPortal @work-Login: Geben Sie im Anmeldebildschirm die Anmeldedaten der Deskshare-Erweiterung, Ihren Benutzername, Ihr Passwort und die LAN IP-Adresse:8802 ein
- Registrierung von myPortal @work VoIP: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen

Beispiel: Gerät verwendet Dummy-Nummer = "100" Verbinden Sie sich mit "100" mit Ihrem Tischtelefon als Deskshare z. B. 200 mit Servicecode *9419.

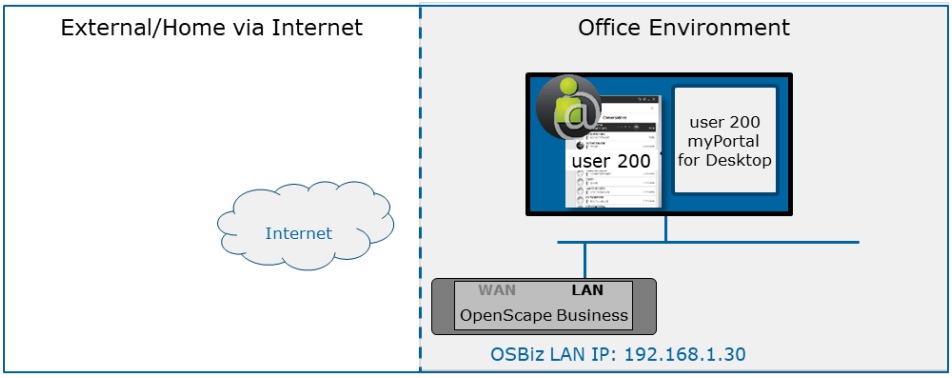
Um myPortal @work mit Benutzer 200 zu nutzen, wird das Tischtelefon automatisch abgemeldet und kehrt zur Dummy-Nummer "100" zurück. Wenn Sie wieder zum Tischtelefon wechseln, stellen Sie bitte sicher, dass myPortal @work nicht registriert ist (der Benutzer muss die Anwendung beenden oder sich abmelden).

Kombination von myPortal @work mit anderen UC Suite-Clients und Lizenzkonfiguration

Anmerkung: Die in diesem Kapitel beschriebenen Konfigurationen werden auch für Heimanwender über VPN unterstützt.

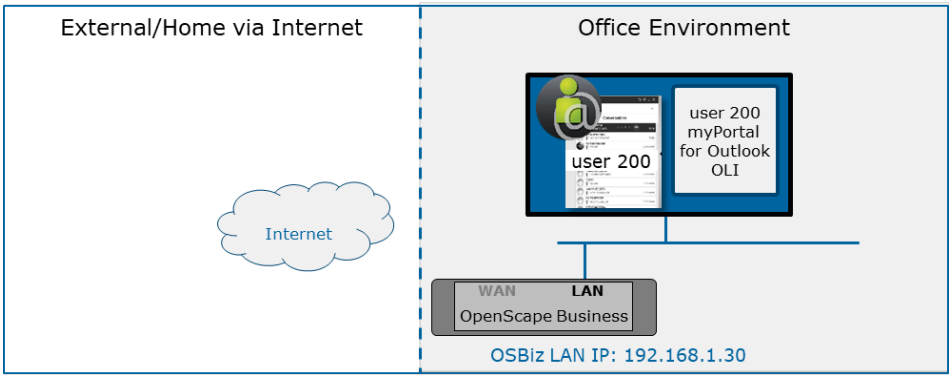
UC-Benutzerlizenz

Derselbe Benutzer kann parallel mit myPortal @work und myPortal for Desktop verbunden sein.



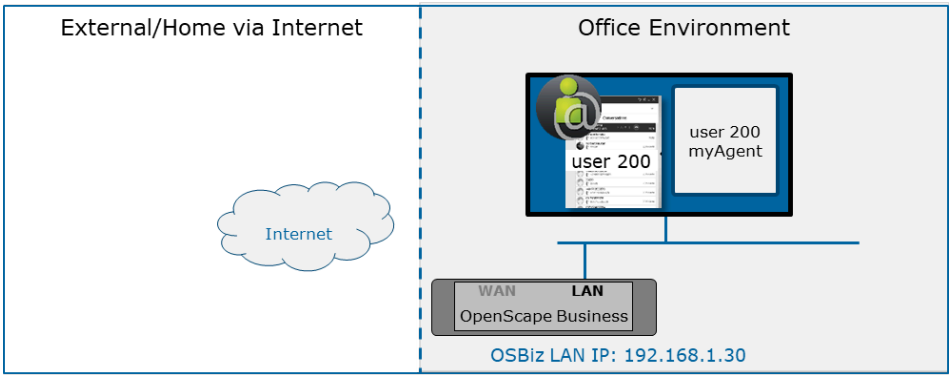
Groupware-Lizenz

Derselbe Benutzer kann parallel mit myPortal @work und OLI verbunden sein.



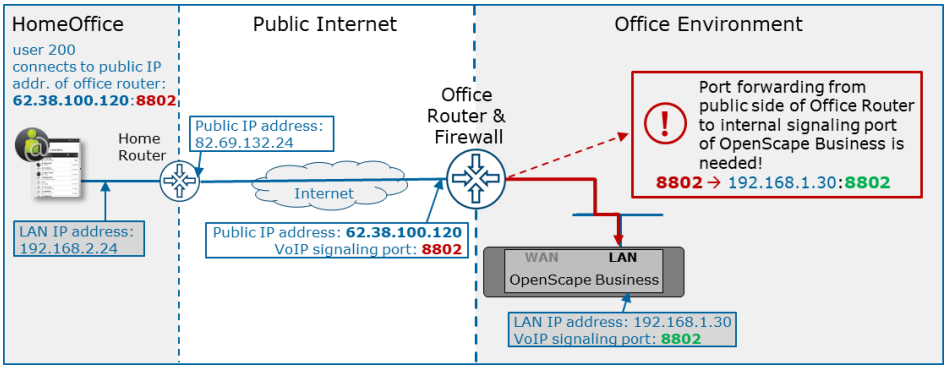
Kombination aus IP-, UC-Benutzer- und myAgent-Lizenz

myAgent und myPortal @work VoIP können parallel als Softphone genutzt werden.



12.2.1.3 Konfigurationsschritte zur Nutzung von myPortal @work über das Internet

Um myPortal @work über das Internet nutzen zu können, muss OpenScape Business auch über das Internet erreichbar sein. Für alle Beispiele in diesem Kapitel wird das folgende grundlegende Netzwerkszenario angenommen.



Beschreibung des Netzwerkszenarios

OpenScape Business befindet sich in der Büroumgebung, die über den Bürorouter mit dem Internet verbunden ist. Dieser Router ist vom Internet aus entweder über die öffentliche IP-Adresse "62.38.100.120" oder über einen DNS-Namen erreichbar.

Der myPortal @work-Client ist mit dem LAN innerhalb eines Heim- oder externen Netzwerks verbunden, das über einen separaten Router mit dem Internet verbunden ist. Der externe Router ist aus dem Internet mit der öffentlichen IP-Adresse "82.69.132.24" erreichbar.

Konfigurationsschritte

Um den myPortal @work-Client auf dem OpenScape Business über das Internet nutzen zu können, müssen die folgenden Komponenten entsprechend konfiguriert werden.

OpenScape Business im Büro

Aktive STUN-Unterstützung auf dem System, falls nicht bereits für einen ITSP geschehen.

Konfigurieren Sie den myPortal @work-Benutzer (SBC-Flag ist für VoIP nicht erforderlich)

Büro-Router

Damit der myPortal @work-Client OpenScape Business vom Internet aus erreichen kann und umgekehrt, muss die folgende Konfiguration auf dem Router im Büro vorgenommen werden:

- HTTPS-Port-Weiterleitung vom externen Port (Standard ist 8802) auf den internen Port 8802 des Systems
  - Externer Port (Standard ist 8802) -> Büro-Router -> 192.168.1.30:8802

Für weitere Informationen siehe auch Kapitel Ports und Firewall-Einstellungen auf Seite 508

myPortal @work / externer Router

Der myPortal @work-Client muss sich mit der öffentlichen IP-Adresse oder dem DNS des Internet-Routers im Büro auf dem externen Port verbinden, der standardmäßig 8802 ist (aufgrund der zuvor konfigurierten Port-Weiterleitung zeigt dieser auf OpenScape Business im Büronetzwerk).

In den meisten Fällen muss auf dem externen Router nichts zusätzlich konfiguriert werden. Sollte dennoch ein Problem auftreten, siehe Kapitel Ports und Firewall-Einstellungen auf Seite 508.

12.2.1.4 Weitere Konfigurationshinweise & Einstellungen

Einstellungen des STUN-Servers

Weitere Informationen zur Konfiguration des STUN-Servers finden Sie im Kapitel "STUN konfigurieren" in der Anleitung "So konfigurieren Sie das Systemgerät@home" und im OpenScape Business V3, my Portal @work, Benutzerhandbuch im Abschnitt "So fügen Sie einen STUN-Server hinzu".

Headsets

Jedes erkannte Audiogerät/Mikrofon des Betriebssystems kann verwendet werden.

Integration von Jabra/Plantronics-Headsets

Führen Sie bei Problemen mit der Integration von Jabra-Headsets die Anwendung mit Administratorrechten aus.

Um die Jabra-Headset-Integration nutzen zu können, muss das Jabra-Gerät in myPortal @work als Hauptmikrofon eingestellt werden.

Für die Integration von Plantronics muss der Plantronics-Hub installiert sein.

Ports und Firewall-Einstellungen

Grundsätzlich müssen die folgenden Ports für die Signalisierung von myPortal @work konfiguriert werden:

- UC-Funktionalität & WebRTC / VoIP-Signalisierung: 8802
- Standard-Port des STUN-Servers: 3478. Wenn ein benutzerdefinierter STUN-Server konfiguriert ist, ist möglicherweise ein anderer Port erforderlich.

Die Konfiguration der Ports für WebRTC/VoIP-Nutzdaten hängt von der Art der in der Kundenumgebung verwendeten Firewall ab. Um myPortal @work in einer Kundennetzwerkumgebung zu betreiben, muss unbedingt der Typ der verwendeten Firewall erfasst und überprüft werden, ob sie zustandsbehaftet oder zustandslos ist, und die Firewall-Einstellungen müssen zusammen mit dem zuständigen IT-Administrator konfiguriert werden.

Zum besseren Verständnis der Unterschiede zwischen den beiden Arten von Firewalls lesen Sie bitte die folgenden Ausführungen:

- Zustandslose Firewalls sind so konzipiert, dass sie Netze auf der Grundlage statischer Informationen wie Quelle und Ziel schützen.
- Bei einer zustandsbehafteten Firewall wird der vollständige Status aktiver Netzwerkverbindungen überwacht. Das bedeutet, dass zustandsbehaftete Firewalls ständig den gesamten Kontext des Datenverkehrs und der Datenpakete analysieren.

Weitere Informationen zu diesen Firewall-Typen finden Sie im Internet oder in einschlägiger Fachliteratur.

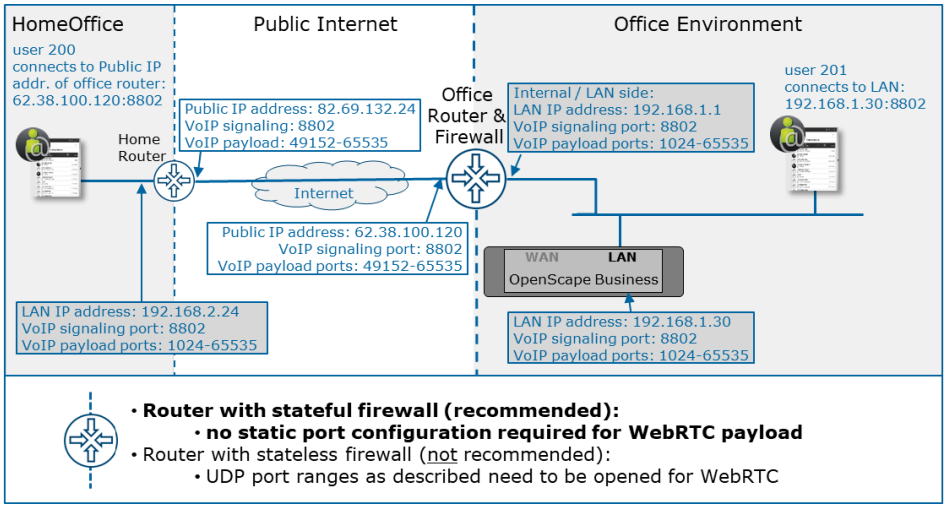
Es wird davon ausgegangen, dass ein Stateful-Firewall/NAT-Gerät verwendet wird, um private Kundennetzwerke besser zu schützen, was bedeutet, dass dieses Gerät interne ausgehende Verbindungen zu ihrem Ziel zulassen muss.

Die Firewall bzw. das NAT-Gerät blockiert alle Pakete in eingehender Richtung, es sei denn, sie gehören zu einer bereits aufgebauten Sitzung (an einem

ephemeren/dynamischen Port), die zuvor in ausgehender Richtung aufgebaut wurde.

In Bezug auf die Portnutzung muss in der Firewall/dem NAT-Gerät nichts konfiguriert werden, da dies bei Verwendung einer zustandsbehafteten Firewall automatisch erfolgt und abgewickelt wird.

Zur Ausführung sicherer WebRTC-basierter VoIP-Lösungen ist eine zustandsbehaftete Firewall zu empfehlen.



Im Rahmen einer zustandslosen Firewall (die für VoIP nicht empfohlen wird) muss der folgende Bereich von UDP-Quellports für Geräte innerhalb des Kundennetzes für den internen Nutzdatenverkehr geöffnet werden: 1024-65535.

Für den gesamten Nutzdatenverkehr, der über das Internet ausgetauscht wird, verwendet die WebRTC-Technologie Ports aus dem UDP-Portbereich von 49152-65535. Für weitere Informationen verweisen wir auf einschlägige Fachliteratur als Informationsquelle.

Jedes Netzwerkgerät auf dem Pfad zwischen den beteiligten Nutzdatenendpunkten muss entsprechend konfiguriert werden (z. B. Router, Firewall, NAT, Proxy usw.).

Aufgrund des breiten Portbereichs, der geöffnet werden muss, ist eine zustandslose Firewall für VoIP nicht zu empfehlen.

Tabelle 4:

	Zustandsbehaftete Firewall	**Zustandslose Firewall, die statisch geöffnet wird**
WebRTC-/VoIP-Signalisierungsport	8802	8802
WebRTC/VoIP-Nutzdaten UDP-Portbereich im lokalen LAN, d. h. in der Kundenumgebung	dynamisch[4]	1024-65535

	Zustandsbehaftete Firewall	Zustandslose Firewall, die statisch geöffnet wird
WebRTC/VoIP-Nutzdaten Über das öffentliche Internet verwendeter UDP-Portbereich	dynamisch[4]	49152-65535

Einschränkungen für VoIP

- In Szenarien mit mehreren Anrufen (z. B. Vermittlung, Konferenz, Anklopfen) empfehlen wir, die Headset-Integration im Fehlerfall zu deaktivieren. Durch die Deaktivierung der Headset-Integration in myPortal @work kann nur die Verbindungssteuerungsfunktion des Headsets nicht genutzt werden, das Headset kann aber weiterhin als Audiogerät verwendet werden.
- Die Funktion "Freie Platzwahl" von myAgent (der Agent kann das zu verwendende Telefon während des Anmeldevorgangs über ein Dropdown-Menü auswählen), d. h. die freie Auswahl eines physischen Geräts durch einen Agenten, wird in Kombination mit myPortal @work nicht unterstützt.
- Die symmetrische NAT-Konfiguration wird nicht unterstützt.
- Strenge Firewalls werden nicht unterstützt.

12.2.1.5 Leitfaden zur Fehlerbehebung

Zeitüberschreitung der Verbindung

- Als Heimanwender mit VPN-Verbindung sollten Sie sicherstellen, dass der Anwender auf die LAN-Adresse des Systems zugreifen und sich mit der LAN-Adresse: 8802-Port verbinden kann. Meldung zur Fehlerbehebung: Fehlermeldung "Time-out der Verbindung", Aktion: Prüfen Sie, ob der Benutzer bei der Verbindung über VPN eine lokale IP aus dem VPN-Netzwerk hat.
- Stellen Sie als Einzelbenutzer sicher, dass kein anderes Gerät und kein VoIP myPortal @work-Client mit derselben Rufnummer registriert ist. Prüfen Sie auch unter **WBM > Expertenmodus > Web Services Assistant** die offenen Verbindungen.

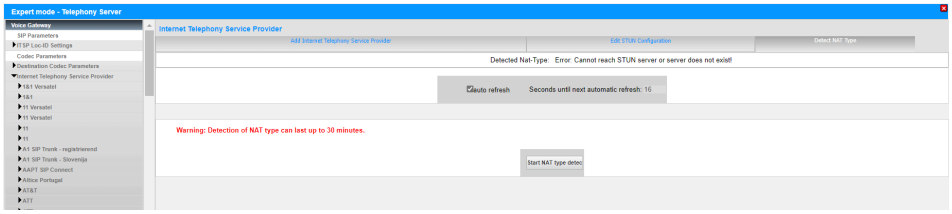
Keine Nutzdaten

Falls dauerhaft keine Nutzdaten ausgegeben werden:

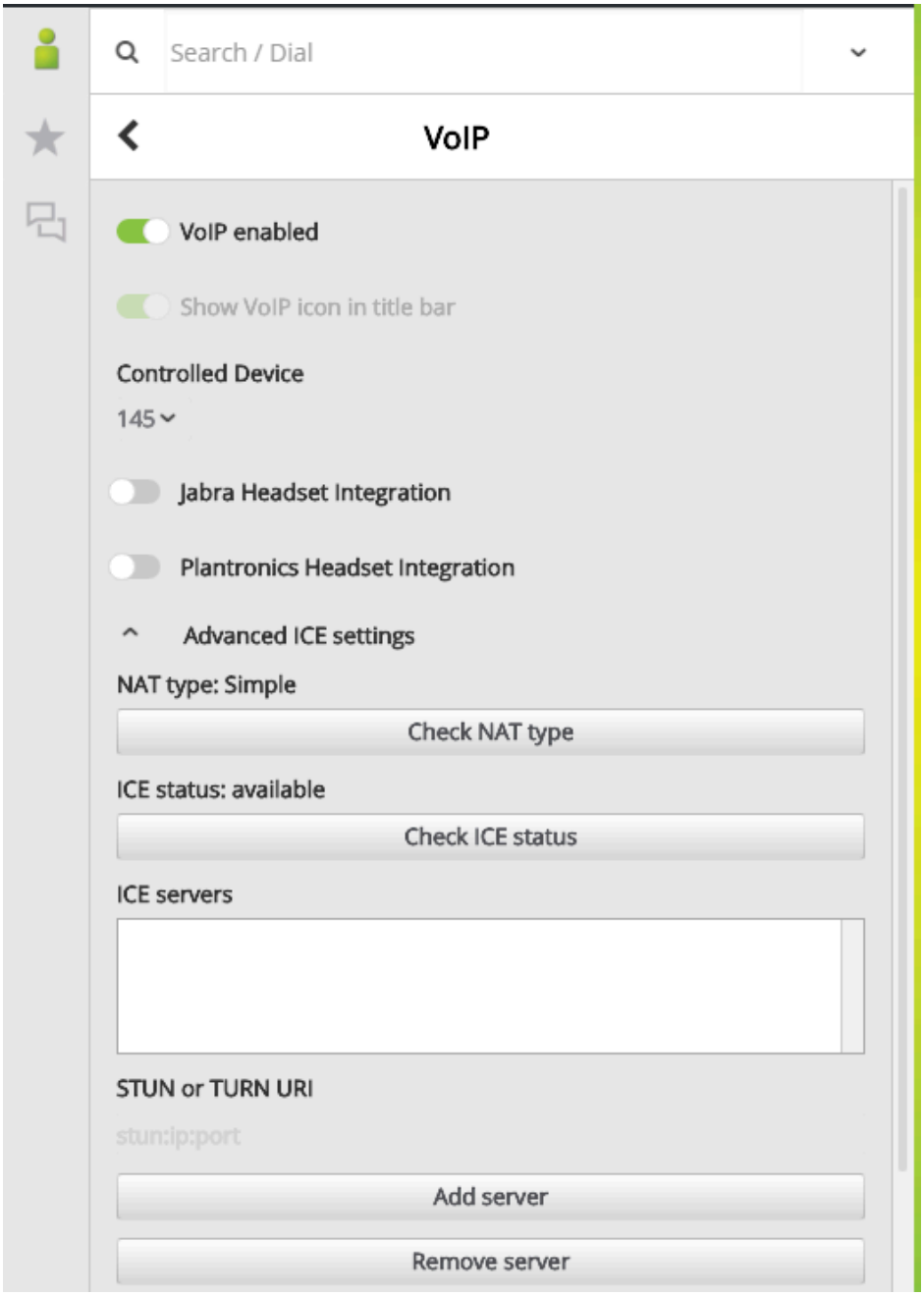
- Vergewissern Sie sich, dass die zulässigen Ports an der Firewall geöffnet sind. Für weitere Informationen siehe auch Kapitel Ports und Firewall-Einstellungen auf Seite 508.
- Überprüfen Sie die NAT-Firewall-Konfiguration. Die symmetrische NAT-Konfiguration wird nicht unterstützt.
- Sie können den NAT-Typ vom System aus unter **WBM > Expertenmodus > Sprachgateway > NAT-Typ erkennen** ermitteln.

[4] Keine Konfiguration erforderlich; die Ports werden dynamisch aus demselben UDP-Portbereich wie bei der zustandslosen Firewall genommen

- Überprüfen Sie die Anbindung des STUN-Servers im System.



- Prüfen Sie die ICE-Anbindung in myPortal @work: **Einstellungen > VoIP > Erweiterte ICE-Einstellungen**. Falls "NAT-Typ" und/oder "ICE-Status" nicht wie unten dargestellt sind, müssen die Netzwerk-/Firewall-Einstellungen von Ihrem Administrator überprüft werden.



Führen Sie "NAT-Typ prüfen" > NAT-Typ aus: Einfach

Führen Sie "ICE-Status prüfen" > ICE-Status aus: verfügbar

- Deaktivieren Sie die Headset-Integration in myPortal @work und führen Sie das Szenario erneut durch.
- Wählen Sie in den VoIP-Einstellungen erneut Audiogeräte aus.

12.2.1.6 Weitere Hinweise

SIP ALG (Application Layer Gateway)

Wenn eines der folgenden Probleme auftritt, überprüfen Sie bitte, ob ein SIP ALG auf einem der beteiligten Router aktiviert ist. Es gibt einige Kategorien von Symptomen, die SIP ALG VoIP-Verbindungen beeinflussen könnte. Es ist nicht immer offensichtlich, zumal diese Probleme oft still passieren, ohne dass Benutzer es wissen.

- Einweg-Audio (nur eine Person kann die andere hören)
- Client klingelt nicht, wenn er aufgerufen wird
- Anrufe werden nach dem Verbinden abgebrochen
- Anrufe gehen ohne bekannten Grund direkt zur Voicemail

12.3 Benutzer von UC Smart

Benutzer von UC Smart sind Teilnehmer, welche UC Clients von UC Smart nutzen.

Folgende Einstellungen für UC Smart Clients sind in UC Smart Assistant verfügbar:

Einstellungen	Erklärung
Einstellungen	
Benutzer	Einstellung wird hier nur angezeigt.
Name	Einstellung wird hier nur angezeigt.
Passwort	Kennwort für UC Smart Clients und UC Smart Assistant.
Sprache	Sprache der Benutzeroberfläche.
Anwender muss neues Passwort vergeben	Einstellung wird hier nur angezeigt.
Zugriff auf UC Smart Assistant	Erlaubnis für die Nutzung von UC Smart Assistant im Webbrowser durch den Benutzer für Konfigurationsaufgaben.
Konfiguriert als Mobility-Teilnehmer	Einstellung wird hier nur angezeigt.
Voicemail-Lizenz	Einstellung wird hier nur angezeigt.
Assoziierte Dienste	Einstellung wird hier nur angezeigt.
Profildetails	

Einstellungen	Erklärung
Mobile Rufnummer	Mobile Rufnummer des Teilnehmers im kanonischen Format (z.B. `+49 173 1234567`).
Private/Externe Rufnummer	Zusätzliche Rufnummer des Teilnehmers im kanonischen Format (z.B. `+49 89 987654321`).
E-Mail-Adresse	E-Mail-Adresse des Teilnehmers.
Voicemail an E-Mail	Aktivierung/Deaktivierung der Email-Benachrichtigung beim Eingang einer neuen Sprachnachricht.
Sichtbarkeit des Anwesenheitsstatus	Einstellung, ob der Anwesenheitsstatus für interne und externe Teilnehmer sichtbar sein soll oder nur für interne Teilnehmer oder ob er überhaupt nicht sichtbar sein soll.
Lizenzierungsinformationen	
Anzeige der dem Benutzer zugewiesenen Lizenzen	

12.3.1 Wie Sie Benutzer von UC Smart konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Smart**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.
4) Klicken Sie im Menübaum auf **Administration** > **Benutzerverwaltung**.
5) Wählen Sie in der Liste **Benutzer** den gewünschten Benutzer aus.
6) Geben Sie im Bereich **Einstellungen** und im Bereich **Profildetails** die Daten des Benutzers ein.
7) Klicken Sie auf **Übernehmen**.
8) Wenn Sie einen weiteren Benutzer konfigurieren möchten, wiederholen Sie die Schritte 5 bis 7.

12.3.2 Wie Sie für einen Benutzer von UC Smart das Kennwort ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Anmerkung: Bitte beachten Sie, dass UC Smart Benutzer standardmäßig ihr Passwort erneut ändern müssen, wenn der Administrator dieses geädert hat. Wenn das nicht gewünscht ist, bitte nach Ändern des Passworts das Flag "Anwender muss neues Passwort vergeben" deaktivieren.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Smart**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.
4) Klicken Sie im Menübaum auf **Administration** > **Benutzerverwaltung**.
5) Wählen Sie im Bereich **Benutzer** den betreffenden Benutzer aus.

   Anmerkung: Ein Passwort, das aus 5 Sternen (*****) besteht, wird aus Sicherheitsgründen vom System nicht akzeptiert.

6) Geben Sie im Bereich **Einstellungen** unter **Passwort** das neue Kennwort ein.
7) Klicken Sie auf **Übernehmen**.
8) Wenn Sie das Kennwort eines weiteren Benutzers zurücksetzen möchten, wiederholen Sie die Schritte 5 bis 7.

Nächste Schritte

Informieren Sie den bzw. die betroffenen Benutzer über das neue Kennwort.

12.4 Anwesenheitsstatus (Präsenz)

Der Anwesenheitsstatus (Präsenz, Presence) informiert im internen Verzeichnis über die Verfügbarkeit interner Teilnehmer (auch Mobility-Entry-Teilnehmer). Darüber hinaus steuert der Anwesenheitsstatus die Erreichbarkeit interner Teilnehmer mit der statusbezogenen Anrufumleitung.

Sie können als Teilnehmer Ihren Anwesenheitsstatus in myPortal @work oder myPortal to go ändern. Bei jeder Änderung des Anwesenheitsstatus außer für **Büro** können Sie bei Bedarf den Zeitpunkt der geplanten Rückkehr zu **Büro** festlegen.

Als Teilnehmer können Sie folgende Status auswählen:

- **Büro**
- **Besprechung**
- **Krank**
- **Pause**
- **Außer Haus**
- **Urlaub**
- **Mittagspause**
- **Zu Hause**
- **Anrufschutz**

Anmerkung: Der Systemadministrator kann die Sichtbarkeit des Status „krank“ innerhalb der Systemadministration ein- und ausschalten. Siehe OpenScape Business UC Suite > Server

Anrufe können über die statusbezogenen Anrufumleitung unter anderem zur persönlichen Sprachbox umgeleitet werden. Hat ein Teilnehmer keine persönliche Sprachbox, kann er Anrufe auf eine Gruppenmailbox oder eine Systemmailbox weiterleiten.

12.5 Verzeichnisse und Journal

Verzeichnisse und das Journal organisieren Kontakte und Anrufe.

12.5.1 Verzeichnisse

Verzeichnisse organisieren die Kontakte der Teilnehmer. Teilnehmer können mit UC Smart Clients auf Kontakte zugreifen.

Das System stellt folgende Verzeichnisse mit den folgenden Funktionen und folgender Prioritätsreihenfolge für die Rufnummernsuche bereit (Nummernsuche wird nur für externe Anrufe unterstützt, und für den Fall, dass Amt bzw. ITSP den Namen nicht bereitstellen):

Verzeichnis	UC Smart Clients	Systemtelefon mit Display
Persönliches Verzeichnis	Über den persönlichen Assistenten importierte Outlook-Kontakte.	
Internes Verzeichnis	Enthält alle internen Teilnehmer und Gruppen mit ihren eventuellen zusätzlichen Rufnummern, für welche das Anzeigen im System aktiviert ist. Interne Teilnehmer mit Systemtelefon werden mit Anwesenheitsstatus dargestellt. Voraussetzung für die Anzeige des Anwesenheitsstatus eines Teilnehmers ist, dass der betreffende Teilnehmer dies zulässt.	Enthält alle internen Teilnehmer und Gruppen, für die das Anzeigen im System aktiviert ist.
Favoritenliste	Enthält vom Teilnehmer ausgewählte Kontakte aus dem persönlichen und internen Verzeichnis. Interne Teilnehmer mit Systemtelefon werden mit Anwesenheitsstatus dargestellt. Interne Teilnehmer mit Systemtelefon werden mit Anwesenheitsstatus dargestellt. Voraussetzung für die Anzeige des Anwesenheitsstatus eines Teilnehmers ist, dass der betreffende Teilnehmer dies zulässt.	
System-Verzeichnis	Enthält alle zentralen Kurzwahlnummern.	

Anmerkung: Geben Sie Rufnummern in Verzeichnissen nach Möglichkeit stets im kanonischen Format ein.

Anmerkung: Beim Hinzufügen oder Entfernen eines UC-Kontakts kann es aufgrund der verwendeten Caching-Mechanismen mehrere Minuten**(und** bis zu 30 Min.) dauern, bis die Änderungen auf allen Clients und Geräten übernommen werden. Alternativ kann auch ein Neustart des Systems durchgeführt werden, damit die Änderungen **sofort** wirksam werden.

12.5.1.1 Verzeichnisse für Systemtelefone konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Sie können wählen, welche Verzeichnisse an Systemtelefonen mit Display zur Verfügung stehen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **Display**.
4) Wählen Sie in der Aufklappliste **Telefonbuch** eine der folgenden Möglichkeiten:
   - Wenn jedes persönliche/interne/externe/Netzwerk-Verzeichnis als auch das LDAP-Verzeichnis zur Verfügung stehen soll, wählen Sie **Alle**.
   - Wenn nur das persönliche/interne/externe/Netzwerk-Verzeichnis zur Verfügung stehen soll, wählen Sie **Intern**.
   - Wenn nur das LDAP-Verzeichnis zur Verfügung stehen soll, wählen Sie **LDAP**.
   - Wenn kein Verzeichnis zur Verfügung stehen soll, wählen Sie **Nein**.

   Anmerkung: Der Benutzer kann die Suchanfragen aktivieren, die als Anforderungen an das Unified-Verzeichnis behandelt werden sollen, indem **Internes Telefonbuch über Unified Directory** ausgewählt wird. Wenn das Flag deaktiviert ist und kein Zugriff auf das Unified Directory besteht, ist die Listenansicht im Telefonbuchmenü für das OpenScape Desk Phone CP 200/205/210 nicht verfügbar.
5) Klicken Sie auf **Übernehmen**.

Nächste Schritte

Wenn Sie **Alle** oder **LDAP** gewählt haben, sorgen Sie dafür, dass ein entsprechendes LDAP-Verzeichnis (z.B. Open Directory Service) für Systemtelefone zur Verfügung steht.

12.5.2 Internes Verzeichnis

Das interne Verzeichnis enthält die Kontaktdetails der internen Teilnehmer und der MULAP-Gruppen des Kommunikationssystems. UC Smart Clients haben Zugriff auf das interne Verzeichnis.

Als Administrator haben Sie uneingeschränkten Zugriff auf alle Daten im internen Verzeichnis. Als Teilnehmer können Sie aus dem internen Verzeichnis wählen.

Ob interne Teilnehmer und Gruppen im internen Verzeichnis angezeigt werden, ist abhängig von dem Teilnehmer-Parameter **Eintrag im Telefonbuch** (einstellbar im WBM über die Teilnehmer-Wizards).

Im Netzverbund gilt das interne Verzeichnis knotenübergreifend.

Zugehörige Konzepte

Gruppenruf auf Seite 691

12.5.2.1 Wie Sie die Anzeige eines Teilnehmers im internen Verzeichnis aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Navigieren Sie im Menübaum unter **Teilnehmer** > **Teilnehmer** > **...** zum gewünschten Teilnehmer (Index-Rufnummer-Name).
4) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn der Name des Teilnehmers im internen Verzeichnis angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Eintrag in Telefonbuch**.
   - Wenn der Name des Teilnehmers nicht im internen Verzeichnis angezeigt werden soll, deaktivieren Sie das Kontrollkästchen **Eintrag in Telefonbuch**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.5.3 Favoritenliste

Die Favoritenliste enthält die vom Teilnehmer ausgewählten Kontakte aus dem persönlichen und internen Verzeichnis. UC Smart Clients haben Zugriff auf die Favoritenliste.

Ein UC Smart Benutzer kann aus der Favoritenliste direkt einen Kontakt anrufen. Erhält ein interner Teilnehmer einen Anruf, wird der Rufzustand des Teilnehmers angezeigt. Der UC Smart Benutzer kann diesen Anruf übernehmen. Zusätzlich wird der Anwesenheitsstatus für interne Teilnehmer angezeigt.

12.5.4 Systemverzeichnis

Das Systemtelefonbuch enthält alle zentralen Kurzwahlnummern für welche jeweils ein Name vergeben wurde. UC Smart Clients haben Zugriff auf das Systemtelefonbuch.

Der Administrator kann die Anzeige für jeden Teilnehmer bzw. jede Kurzwahlnummer mit Namen individuell deaktivieren.

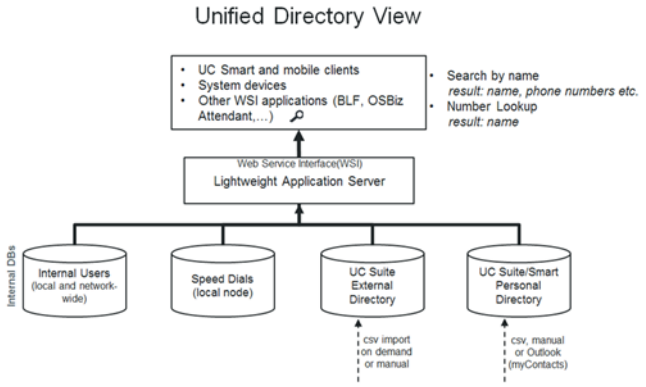
12.5.5 Unified-Verzeichnis

OpenScape Business bietet verschiedene Datenquellen zum Speichern und Abrufen von Teilnehmer- oder Kontaktdaten – von internen Teilnehmerdaten in der internen Benutzerkonfiguration über die interne Kurzwahlliste bis hin zu den verschiedenen Verzeichnissen der UC-Anwendungen.

Jede Datenquelle in OpenScape Business wird von einer bestimmten Client-Anwendung verwendet, die entweder Teil der Systemsoftware auf den Telefongeräten oder Teil einer UC-Client-Anwendung ist. Abhängig von den verwendeten Datenquellen und Clients werden die Daten unterschiedlich abgerufen und dargestellt.

Der Unified-Verzeichnisdienst in OpenScape Business nutzt die bestehenden OpenScape Business-Datenquellen für die Funktionen Rufnummernsuche und Namensauflösung. Er übermittelt an alle Systemgeräte und OpenScape Business-Clients einheitliche Suchergebnisse und Namensauflösungsinformationen.

Der Zugriff auf den Unified-Verzeichnisdienst kann entweder über das Web Service Interface (WSI) mit externen Clients wie myPortal to go oder intern über Anrufbearbeitungsmechanismen (z. B. von OpenStage-Telefonen) erfolgen.



Der Unified-Verzeichnisdienst verwendet die folgenden internen Datenbanken und Verzeichnisse von OpenScape Business:

- Internes Benutzerverzeichnis (netzweit)
- Kurzwahllisten
- UC Smart Persönliches Verzeichnis (optional)
- UC Suite Externes Verzeichnis (optional)
- Persönliche Outlook-Kontakte (falls importiert über myContacts)

Der Unified-Verzeichnisdienst ist auf allen Knoten eines OpenScape Business-Systems ab V2R2 verfügbar. Es erfordert keine spezielle Hardware, Software oder zusätzliche Lizenzen.

Um bei der Verwendung des Unified-Verzeichnisdienstes die besten Ergebnisse zu erzielen, sollten Sie einige Regeln für Rufnummernformate und zur Schreibweise von Namen beachten.

12.5.5.1 Leistungsmerkmale

Unterstützte Geräte/Clients

Der Unified-Verzeichnisdienst stellt folgende Funktionen bereit:

- Telefonbuchsuche in mehreren internen Datenquellen von OpenScape Business
- Einheitliche Bereitstellung des Suchergebnisses für alle unterstützten Kunden
- Rufnummernsuche / Namensauflösung in mehreren internen Datenquellen
- Einheitliche Bereitstellung der Namensauflösungsergebnisse für alle unterstützten Clients
- Externer Datenzugriff über die WebServices-Schnittstelle (WSI)

Die Leistungsmerkmale sind für Einzelknotensysteme wie folgt verfügbar. In OpenScape Business-Netzwerken hängt die Verfügbarkeit der Features hauptsächlich von der Art der Verbindung der Amtsleitungen, Geräte und Clients innerhalb des Netzwerks ab.

Unified Directory unterstützt folgende Clients/Systemgeräte von Unify unter Verwendung der angegebenen Schnittstellen:

Gerät/Client	Verwendete(s) Schnittstelle/Protokoll	Hinweise
OpenStage-Telefone	Anrufverarbeitung/ CorNet-Protokoll	WSI/HTTP(S) ist optional für OpenStage 60/80 für Anrufer-Bilder
OpenScape DeskPhone IP	Anrufverarbeitung/ CorNet-Protokoll	WSI/HTTP(S) ist optional für DeskPhone IP 55 für Anrufer-Bilder
Schnurlose (CMI)-Geräte	Anrufverarbeitung/CMI-Protokoll	
CP 100/110 /200/205/210/ 405	Anrufverarbeitung/ CorNet-Protokoll	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI/HTTP(S)	
myPortal @work	WSI/HTTP(S)	
myPortal to go	WSI/HTTPS	
OpenScape Business Attendant/BLF	Anrufverarbeitung/ CorNet-Protokoll	WSI/HTTP(S) ist optional

Anmerkung: Die UC Suite myPortal-, myAttendant- und myAgent-Clients verwenden eigene Mechanismen für die Verzeichnissuche und Namensauflösung.

Suchfunktion

Die Unified Directory-Suche wird immer unter Verwendung der spezifischen Geräte-/Client-Benutzerschnittstelle durchgeführt. Die Suchkriterien und der verwendete Zeichensatz können abhängig von den verwendeten Clients eingeschränkt sein.

Nach Eingabe des Suchkriteriums wird die Suche in folgenden Verzeichnissen durchgeführt

- Internes Benutzerverzeichnis (netzwerkweit)
- Kurzwahllisten
- UC Smart Persönliches Verzeichnis (optional)
- UC Suite Externes Verzeichnis (optional)
- Persönliche Outlook-Kontakte (falls über myContacts importiert)

Alle Übereinstimmungen innerhalb der obigen Verzeichnisse werden zusammen mit ihrer Herkunft als Suchergebnisse angezeigt. Die Übereinstimmungen enthalten entweder den vollständigen Kontaktdatensatz oder nur Teile davon. Die Informationstiefe der Ergebnisse hängt von der Datenquelle ab.

Anmerkung: Die Suche nach Gruppennamen in myPortal @work wird im UC Suite-Modus nicht unterstützt. Es wird nur die Suche nach lizenzierten Benutzern (Basislizenz) und lizenzierten MULAP-Gruppen (UC-Einträge) unterstützt.

Die Übereinstimmungen werden auf den Geräten oder Clients angezeigt, abhängig von den Anzeigefähigkeiten.

	Internes Benutzerver	Kurzwahllis	UC Smart Persönliche Verzeichnis	UC Suite Externes Verzeichnis	Persönliche Outlook-Kontakte (über myContacts)
Nachname	X	---	X	X	X
Vorname	X	---	X	X	X
Kurz-/ Anzeigename	X	X	---	---	---
Büro-Rufnr.	---	---	X	X	X
Private/ext. Rufnr.	---	---	X	---	X
Mobilrufnr.	---	---	X	X	X
E-Mail-Adr.	---	---	X	X	X
Firmenname	---	---	X	X	X
Ort	---	---	---	---	---
Kontaktbild	---	---	X	---	X
Kontaktbildvorschau		---	X	---	X

Rufnummernsuche

Mit der einheitlichen Rufnummernsuche wird der Anrufer (CLI) durch eine Nummernsuche in allen unterstützten internen Datenquellen aufgelöst. Die Suche wird in den folgenden Rufnummer-Feldern durchgeführt:

- Büro-Rufnummer
- Mobilrufnummer
- Private Rufnummer

Die Rufnummernsuche wird im Allgemeinen bei eingehenden oder ausgehenden Anrufen ausgelöst, wobei bestimmte Routing- und Weiterleitungsfunktionen zusätzlich berücksichtigt werden.

Eine feste Priorisierung der Datenquellen, die für die Rufnummernsuche verwendet werden, wird implementiert, um so schnell wie möglich ein Ergebnis zu erhalten. Das Ergebnis enthält entweder nur den Nachnamen, den Vornamen, den Anzeigenamen oder, sofern verfügbar, die vollständigen Kontaktdaten.

Tabelle 5: Unterstützte Datenquellen und Priorisierung

Priorität	Datenquellen	Bemerkung
1	CO ITSP Name (wie vom Provider gesendet)	Voraussetzung ist, dass das Flag "Name im Amt" aktiviert wird.
2	Kurzwahlliste	
3	Persönliche Kontakte	

Priorität	Datenquellen	Bemerkung
4	UC-Benutzerdetails	

Die abgerufenen Daten werden auf dem Gerät des Benutzers und/oder im UC-Client angezeigt. Die Informationstiefe der Ergebnisse hängt von den Anzeigefähigkeiten ab.

- **Kommende Rufe**

  Unterstütztes Szenario für Einzelknotensysteme:

  – Basic Call
  – Gruppenruf/MULAP-Ruf
  – Rufzuschaltung
  – Einzelschritt-Übergabe (SSCT)
  – Gespräch übergeben/Übergabe nach Melden/Rückfrage
  – Uneingeschränkte Gesprächsumleitung (CFU)
  – Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply)
  – Anrufumleitung bei Besetzt (CFB = Call Forwarding Busy)
  – Übergabe ohne Rückfrage
  – Anrufübernahme

  Anmerkung: Anrufübernahme unterscheidet sich von Anrufübernahmegruppe. Wenn in der Anrufübernahmegruppe eine externe Nummer im Unified Directory gespeichert ist, wird der Name des Anrufers von den Mitgliedern der Gruppe nicht angezeigt.

  Unterstütztes Szenario für mehrere Knoten (Netzwerk). Szenario ist ein Gateway-Anruf.
- **Gehender Anruf**

  Im Falle eines ausgehenden Anrufs wird die Telefonnummer des angerufenen Teilnehmers nur einmal gesucht.

  Das unterstützte Szenario für Systeme mit einem Knoten ist ein Basisanruf an eine externe Nummer.

Die Darstellung der Rufnummer-Suchergebnisse hängt von den Anzeigefähigkeiten der Telefone ab.

12.5.5.2 Regeln und Konventionen

Bei den Rufnummern- und Namensformaten innerhalb der Datenquellen sind einige Konventionen zu beachten, um optimale Ergebnisse mit dem Unified-Verzeichnisdienst zu erhalten.

Unterstütztes Rufnummernformat

Alle externen Rufnummern innerhalb der Datenquellen müssen einschließlich Länder- und Ortsvorwahl im kanonischen Format eingegeben werden, z. B. +4989700712345

Die Kurzwahlliste unterstützt nur das vom System wählbare Format (z.B. 0089700712345 oder 0004989700712345)

Wenn Kurzwahlnummern so konfiguriert sind, dass sie über LDAP zugänglich sind, müssen Sie die Option zur Nummernkonvertierung aktivieren, um den Kontaktnamen anzuzeigen, wenn die Nummer im kanonischen Format vorliegt. Weitere Informationen zum Aktivieren der Nummernkonvertierung finden Sie untere Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen auf Seite 1196.

Unterstützte Namensformate

Bei Namensformaten und Zeichensätzen sind die folgenden Konventionen zu beachten:

- **Namensformat bei Kurzwahl**

  Die Namenssuche innerhalb der Kurzwahlliste wird nur in Kombination mit bestimmten Konfigurationsregeln unterstützt. Vor- und Nachname müssen im vorhandenen Namensfeld nach dem folgenden Muster eingegeben werden:

  <Nachname>, <Vorname> (kommagetrennt)
- **Interne Teilnehmer bei Migrationsszenarien**

  Bei internen Teilnehmern, die diese Konfigurationsregeln nicht beachten, wird hat eine Migration auf V2R1 und höher ggf. unerwartete Folgen und wird nicht ordnungsgemäß unterstützt. Dies bedeutet, dass der Administrator interne Namen vor Durchführung der Migration in das folgende Format konvertieren sollte:

  <Nachname>, <Vorname> (kommagetrennt)

Verfügbarkeit von Verzeichnisänderungen

Nach dem Erstellen, Aktualisieren oder Löschen von Kontakten in den verschiedenen Datenquellen kann es bis zu 10 Minuten dauern, bevor alle Änderungen in den Suchergebnissen sichtbar sind.

12.5.5.3 Funktionale Grenzen

Für Unified-Verzeichnisse gelten die folgenden funktionalen Grenzen:

Namenssuche

- Unterstützung von Gruppennamen

  Gruppennamen (nicht MULAP-Namen) können zurzeit nicht in allen Arten von Konfigurationen durchsucht werden
- Unterstützung von Sonderzeichen

  Auf den meisten Telefongeräten kann der Benutzer nur nach den Standardzeichen "a-z" suchen. Die Eingabe von (diakritischen) Sonderzeichen (wie z.B. der deutschen Umlaute Ää, Öö, Üü oder ß) ist über die Benutzeroberfläche des Telefongeräts nicht möglich.

  Daher beinhaltet ein Suchergebnis mit einfachen Zeichen auch Sonderzeichen. Bei einer Suche mit den Zeichen

„acdegilnorstuyz“ sind auch die entsprechenden Sonderzeichen "àáâãåäąăäçćčďđèéêëęě#ìíîïĺľłñńňòóôõöřŕšśşťùúûůüýÿžźż"

im Suchergebnis enthalten.

Anmerkung: Eine Suche im Telefonbuch mit Platzhalterzeichen am Anfang des Suchbegriffs, z. B. <*jo*>, wird nur für interne Benutzer unterstützt.

- Unterstützung von Kurzwahlnamen

  Die Namenssuche innerhalb der Kurzwahlliste wird nur in Kombination mit bestimmten Konfigurationsregeln unterstützt. Vor- und Nachname müssen im vorhandenen Namensfeld nach einem der folgenden Muster eingegeben werden

  – <Nachname>, <Vorname> (kommagetrennt)
  – <Nachname>, <Vorname> (Leerschritt als Trennzeichen)

Namensanzeige

Persönliche Kontakte aus UC Smart und dem externen Offline-Verzeichnis, bei denen Vorname und Nachname zusammen länger als 24 Zeichen sind, werden zwecks Anzeige auf dem Gerätedisplay auf 24 Zeichen gekürzt.

Rufnummernsuche

Die Funktion Rufnummernsuche (Kontaktname aus Rufnummer des Anrufers ermitteln) wird vom Unified-Verzeichnisdienst für SIP- und S0-Geräte nicht unterstützt.

12.5.5.4 Unified-Verzeichnis in vernetzten Systemen

Der Unified-Verzeichnisdienst ist auf allen Knoten eines OpenScape Business-Netzwerks aktiv und nutzt die Datenquellen des eigenen Systems. Telefongeräte und Clients verwenden innerhalb ihres eigenen Knotens immer den Unified-Verzeichnisdienst.

Es kommt daher auf die Art des Datenquelleninhalts an, ob netzweite Kontakte verfügbar sind oder nicht.

Tabelle 6: Lokale und netzweite Datenquellen

Datenquelle	Lokale Daten	Netzweite Daten
Internes Benutzerverzeichnis	X	X
Kurzwahllisten	X	---
UC Smart Persönliches Verzeichnis	X	---
UC Smart Persönliches Verzeichnis	X	---
Persönliche Outlook-Kontakte (über myContacts)	X	---

Rufnummernsuche

In Vernetzungsszenarien wird die Funktion Telefonnummer suchen nicht verwendet. In solchen Fällen wird der Name über normale Vernetzungsmechanismen zwischen den Netzknoten übertragen.

Für interne Teilnehmer wird der konfigurierte Anzeigename verwendet, so dass eine Suche nicht erforderlich ist.

12.5.6 Journal

Das Journal ist die Liste aller ankommenden und gehenden Anrufe eines Teilnehmers. Aus dem Journal kann der Teilnehmer Kontakte schnell und einfach erneut anrufen oder entgangene Anrufe beantworten.

Dem UC Smart Benutzer werden max. die letzten 100 Anrufe angezeigt.

Ordner für Anrufarten

Die Anrufe können in folgende Gruppen gegliedert sein:

- **Offen**
- **Entgangen**
- **Angenommen**
- **Alle Anrufe**

Anrufdetails

Jeder Anruf wird mit Datum und Uhrzeit angezeigt und sofern vorhanden mit der Rufnummer. Falls ein Verzeichnis zur Rufnummer weitere Informationen enthält wie **Nachname** und **Vorname**, werden auch diese angezeigt. Zusätzlich angezeigt wird die **Richtung** des Anrufs und **Dauer** sowie ggf. erfolgte Weiterleitungen oder Anrufübernahmen.

12.6 Anrufe

Für Anrufe ist das Rufnummernformat von besonderer Bedeutung.

12.6.1 Rufnummernformate

Für die Angabe von Rufnummern existieren unterschiedliche Formate.

Format	Beschreibung	Beispiel
Kanonisch	Beginnt mit + und enthält stets Landeskennzahl, Ortskennzahl und die komplette restliche Rufnummer. Leerzeichen und die Sonderzeichen + ( ) / - : ; sind zulässig.	+49 (89) 7007-98765

Format	Beschreibung	Beispiel
Wählbar	So, wie Sie die Rufnummer am Systemtelefon im Büro wählen würden, stets mit Amtskennzahl.	• 321 (intern) • 0700798765 (eigenes Ortsnetz) • 0089700798765 (fremdes Ortsnetz) • 0004989700798765 (Ausland)

Tipp: Verwenden Sie wo immer möglich das kanonische Rufnummernformat. Damit ist eine Rufnummer in jeder Situation vollständig und eindeutig und für Vernetzung und mobile Teilnehmer konsistent.

Bei der manuellen Wahl (wählbares Format) einer externen Rufnummer muss die Amtskennzahl immer mitgewählt werden.

Bei der Wahl einer externen Rufnummer im wählbaren Format aus einem Verzeichnis (sowie mit bestimmten UC Clients bei Desktop-Wahl und Clipboard-Wahl) ergänzt das Kommunikationssystem die Amtskennzahl automatisch (Richtung 1).

Anmerkung: Bei Anrufen innerhalb der USA über CSTA zu einer Rufnummer im kanonischen Format wird die Rufnummer in das wählbare Format konvertiert.

12.6.2 Voraussetzungen für den Empfang von VoIP-Anrufen auf myPortal to go mit CallKit auf Ihrem iPhone

Die VoIP-Anrufbenachrichtigungen von iOS basieren auf dem APNS-Mechanismus von Apple.

Dieser Dienst erfordert Folgendes:

- Einen konfigurierten DNS-Server, der öffentliche Domänennamen aus dem Internet auflöst.
- Internetzugang für OpenScape Business System (Port TCP/443 ausgehend), um APNS-Anrufbenachrichtigungen zu senden.
- Die Systemsoftware muss auf dem neuesten Stand der Haupt-, Neben- und Korrekturversionen sein. Die neueste Systemversion ist wichtig, da der APNS-Dienst bestimmte Zertifikate benötigt, die bei älterer Systemsoftware ablaufen.

12.7 Konferenzen

In einer Konferenz können mehrere Teilnehmer (darunter auch externe) gleichzeitig miteinander telefonieren. Mit der Konferenz-Management-Funktion können Sie Konferenzen schnell und einfach durchführen und im Voraus planen.

Telefon- und applikationsgesteuerte Konferenzen

Als Teilnehmer können Sie Konferenzen sowohl über das Telefon einleiten als auch über die Applikationen von UC Smart.

Eine telefongesteuerte Konferenz können Sie auf folgende Arten starten und anschließend am Telefon steuern:

- Gewünschte Konferenzteilnehmer anrufen und mit der Konferenz verbinden
- Rückfragegespräch zu einer Konferenz erweitern
- Zweitanruf zu einer Konferenz erweitern

Applikationsgesteuerte Konferenzen können Sie über das Konferenz-Management einleiten, steuern und verwalten. Für die Nutzung des Konferenz-Managements ist eine Konferenz-Lizenz erforderlich.

Unterschiede zwischen den Konferenzarten:

	Telefongesteuerte Konferenz	Applikationsgesteuerte Konferenz
Richtung des Verbindungsaufbaus aus Sicht des Systems	• Gehend	• Ankommend (Einwahl durch den Teilnehmer)
Authentifizierung der Konferenzteilnehmer	-	• Persönliche PIN (Konferenz-ID) • Gast PIN (optional)
Vordefinierte Einladung an die Konferenzteilnehmer	-	• Name der Konferenz • Einwahlnummer (MeetMe) • Persönliche PIN (Konferenz-ID) • Gast PIN (optional)
Max. Anzahl der Teilnehmer pro Konferenz	8	16

Geplante Konferenz

Geplante Konferenzen werden als permanente Konferenzen angelegt. Die Konferenz kann ohne weitere Terminplanung bei Bedarf jederzeit genutzt werden. Geplante Konferenzen belegen keine Konferenz-Channels, solange sich keine Teilnehmer in der Konferenz eingewählt haben. Die Reihenfolge der Einwahl bestimmt über die Belegung der Konferenz-Channels.

Administratoren können bei der Ersteinrichtung über das WBM die festgelegte Einwahlnummer (MeetMe) für Konferenzen ändern. Den Teilnehmern wird die Einwahlnummer angezeigt, mittels derer sie sich in die Konferenz einwählen können. Dabei müssen sie sich mit ihrer persönlichen PIN oder falls zugelassen mit der allgemeinen Gast-PIN authentifizieren.

Moderatoren

Der Initiator einer Konferenz ist automatisch Moderator und hat folgende Möglichkeiten:

- Geplante Konferenzen anlegen, bearbeiten und löschen.
- Konferenzteilnehmer hinzufügen und entfernen.

  Entfernte Teilnehmer bleiben nicht in der Konferenz.
- Konferenzteilnehmer trennen.

  Getrennte Teilnehmer können sich erneut in die Konferenz einwählen.
- Einen anderen internen Teilnehmer desselben Knotens als Moderator festlegen.

- Die Konferenz verlassen, ohne sie sofort zu beenden.

  Verlässt der letzte Moderator die Konferenz, endet sie nach 5 Minuten.
- Aktive Konferenzen beenden.
- In einer aktiven Konferenz eine Web Collaboration-Sitzung starten.
- Vordefinierte Einladungen an alle oder einzelne Konferenzteilnehmer verschicken.

Alle internen Teilnehmer innerhalb eines Knotens können Moderatoren werden. Dafür ist allerdings eine Konferenz-Lizenz erforderlich.

Konferenzteilnehmer, deren Kontaktdaten manuell eingegeben wurden, werden als externe Teilnehmer behandelt und können nicht als Moderatoren festgelegt werden.

Konferenzteilnehmer

Konferenzteilnehmer können die Konferenz verlassen und sich erneut einwählen. Zusätzlich können sie an einer bereits gestarteten Web Collaboration-Sitzung teilnehmen. Solange eine Konferenz nur einen Teilnehmer hat, hört dieser Wartemusik. Die maximale Anzahl der externen Konferenzteilnehmer ist unter anderem durch die Anzahl der verfügbaren Amtsleitungen begrenzt.

Automatisches Beenden ohne Moderator

Verlässt der letzte Moderator die Konferenz, werden die Teilnehmer mit einem Hinweistext informiert, dass die Konferenz ca. in 5 Minuten endet.

Benachrichtigung der Konferenzteilnehmer

Der Moderator kann allen oder einzelnen Konferenzteilnehmern eine Einladung per E-Mail zuschicken. Voraussetzung ist, dass auf dem Client-PC ein E-Mail-Programm installiert ist. Bekannte E-Mail-Adressen werden automatisch in den Verteiler eingefügt. Bei einer Einladung an alle Konferenzteilnehmer wird nur die allgemeine Gast-PIN (falls zugelassen) verschickt, bei individuellen Einladungen wird zusätzlich die persönliche PIN verschickt.

Alternativ kann ein vordefinierter Einladungstext zur Weiterverwendung in anderen Programmen (z. B. Chat) in die Zwischenablage kopiert werden.

12.8 Web Collaboration

myPortal unterstützt innerhalb von Telefongesprächen und Konferenzen die Einbindung des separaten Produktes Web Collaboration für die gleichzeitige multimediale Zusammenarbeit. Diese bietet schnellen Zugriff auf Funktionen wie Desktop- und Anwendungsfreigabe, Dateifreigabe, Co-Browsing, Whiteboarding, URL-Push, IM-Chat und Video-Chat mit mehreren Teilnehmern.

Die Web Collaboration kann von einem Teilnehmer während eines Telefongesprächs über das Anruf-Fenster des UC PC-Clients oder innerhalb einer aktiven Konferenz vom Moderator gestartet werden. Es öffnet sich eine Webseite, über die der Download des Web Collaboration-Clients eingeleitet werden kann. Eine lokale Installation von Web Collaboration auf dem UC PC-Client ist nicht erforderlich. Ist auf dem UC PC-Client ein E-Mail-Programm hinterlegt, kann den Gesprächsteilnehmern eine E-Mail mit dem Link auf den

Web Collaboration-Client zugesendet werden. Detaillierte Informationen zur Web Collaboration finden Sie in der Web Collaboration-Produktdokumentation.

Beim Löschen oder Beenden einer Konferenz wird die zugehörige Web Collaboration-Sitzung automatisch gelöscht.

Einbindung von Web Collaboration

Für die Einbindung von Web Collaboration muss der Administrator im WBM die Lizenznummer und das Passwort für die gehostete Web Collaboration-Verbindung eingeben. Der Hersteller bietet den Web Collaboration-Server im Internet als Dienst an (Öffentlicher Server). Über eine gesicherte https-Verbindung werden Lizenznummer und Passwort übertragen. Standardmäßig wird dafür der TCP-Port 5100 verwendet. Lokale Web Collaboration-Server werden nicht unterstützt.

Anmerkung: Für die Nutzung von Web Collaboration benötigen die UC PC-Clients und das Kommunikationssystem eine Internetverbindung. Verbindungen über Proxy werden vom Kommunikationssystem nicht unterstützt.

Instant Messaging und Web Collaboration

Instant Messaging des Systems und Instant Messaging von Web Collaboration sind voneinander unabhängig: Sofortnachrichten aus einem UC PC Client erscheinen nicht in einer Web Collaboration Sitzung desselben Teilnehmers und umgekehrt.

12.8.1 Wie Sie die Verbindung zum Web Collaboration Server (Public Server) konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Ein Internet-Zugang ist vorhanden.

Für die gesicherte Verbindung zum Web Collaboration Server (Public Server) benötigen Sie eine Lizenznummer und ein Passwort.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Web Services**.
3) Navigieren Sie im Menübaum zu **Web Services** > **Web Collaboration**.
4) Aktivieren Sie das Optionsfeld **Public Server**.
5) Geben Sie im Feld **Lizenznummer** die Lizenznummer für die gesicherte Verbindung zum Web Collaboration Server (Public Server) ein.
6) Geben Sie im Feld **Passwort** das Passwort für die gesicherte Verbindung zum Web Collaboration Server (Public Server) ein.

Anmerkung: Wenn Sie die Web Collaboration 5 min lang testen wollen, können Sie das Optionsfeld **Public**

Server (Demo Mode/Evaluation Mode) aktivieren. Hierfür benötigen Sie keine Lizenznummer und kein Passwort.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.8.2 Wie Sie die Verbindung zum Web Collaboration Server deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Web Services**.
3) Navigieren Sie im Menübaum zu **Web Services** > **Web Collaboration**.
4) Aktivieren Sie das Optionsfeld **Kein Web Collaboration Server**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**. Die Option zum Starten einer Web Collaboration Sitzung ist in den UC Clients deaktiviert.

12.9 Instant Messaging

Instant Messaging ist die Kommunikation mittels Sofortnachrichten (Chat).

12.9.1 Instant Messaging

Mittels Sofortnachrichten können Sie mit anderen Benutzern von UC Smart chatten.

Gesendete und empfangene Sofortnachrichten werden bei den Kommunikationspartnern als Dialog angezeigt. Beim Auswählen eines Empfängers zeigt der Client an, ob der Kommunikationspartner momentan online ist. Falls ein Kommunikationspartner offline ist, kann ihm keine Sofortnachricht übermittelt werden. Die Sofornachrichten-Übersichtsseite zeigt die letzten Streams an. Das System speichert eine begrenze Zahl von Sofortnachrichten. Es werden max. die letzten 100 Sofortnachrichten eines Benutzers angezeigt.

12.10 Sprachbox (SmartVM)

Die Sprachbox (auch SmartVM genannt) spielt Anrufern eine Begrüßung vor und bietet ihnen die Möglichkeit, eine Nachricht aufzusprechen oder sich weitervermitteln zu lassen. Interne Teilnehmer können über ein Telefon und mit dem UC Smart Client auf die Sprachbox zugreifen. Teilnehmer, die eine Sprachbox nutzen wollen, benötigen eine VoiceMail-Lizenz.

Sprachbox-Typen

Es gibt folgende Sprachbox-Typen:

- Standardmailbox:

  Die Standardmailbox ist die persönliche Sprachbox eines Teilnehmers. Sie nimmt den Anruf entgegen, begrüßt den Anrufer mit einer persönlichen Ansage oder einer Standardansage und bietet dem Anrufer die Möglichkeit eine Nachricht aufzusprechen. Die Standard-Sprachbox wird vom Teilnehmer über das Telefon oder über den UC Smart Client konfiguriert (z. B. Aufsprechen einer persönlichen Begrüßung).
- Gruppenmailbox:

  Die Gruppenmailbox hat die gleichen Eigenschaften wie die Standardmailbox, nur dass sie nicht einem einzelnen Teilnehmer zugeordnet ist, sondern einer Gruppe von Teilnehmern. Nachrichten können für eine Gruppenmailbox nur aufgezeichnet werden, wenn mindestens ein Gruppenmitglied eine VoiceMail-Lizenz besitzt. Die Info der Sprachbox wird allen Gruppenmitgliedern mit einer VoiceMail-Lizenz angezeigt. Das Abhören der Nachrichten ist über das Telefonmenü der persönlichen Sprachbox der Gruppenmitglieder möglich.
- Vermittlungsmailbox (AutoAttendant / Company AutoAttendant):

  Die Vermittlungsmailbox bietet Anrufern eine Begrüßung mit oder ohne anschließender Vermittlungsmöglichkeit. Eine spezielle Form der Vermittlungsmailbox ist der Company AutoAttendant. Hier kann der Anrufer automatisch weitergeleitet werden (z.B. zur Vermittlung) oder durch Wahl einer internen Rufnummer oder Kurzwahlnummer (Ziffern 0-9) zu einem Teilnehmer weitergeleitet werden (z.B. zum Service oder zur Hotline). Natürlich muss eine entsprechende Ansage diese Wahlmöglichkeiten erläutern. Außerdem kann ein Abwurfziel eingerichtet werden, zu dem der Anrufer weitergeleitet wird, wenn er keine Ziffer oder eine falsche (nicht belegte) Ziffer drückt. Der Administrator kann bis zu 100 Vermittlungsmailboxen konfigurieren.
- Ansagemailbox:

  Durch Zuweisen eines Ansagenindex zu einem Ansageport und Konfiguration einer Mailbox mit der Rufnummer des Ansageports wird die Ansagefunktion konfiguriert. Als Ansage wird die Begrüßung der Mailbox verwendet. Die Wiedergabe kann je nach eingestelltem Ansagetyp einmalig erfolgen (Ansage) oder zyklisch (Musik). Das Telefonmenü einer Ansagemailbox kann nur von einem anderen Telefon aus benutzt werden, da kein zugehöriges Telefon existiert. Daher muss für die Ansagemailbox eine andere PIN verwendet werden als für die Sprachbox des benutzten Telefons.
- Systemmailbox:

  Als Systemmailbox wird die Sprachmailbox mit der Rufnummer des Sammelanschlusses der SmartVM benutzt. Die Systemmailbox muss eine Standardmailbox (kein AutoAttendant) mit aktivierter Sprachaufzeichnung sein. Die Info der Sprachbox wird dem Besitzer der Sprachbox mit dem Index 1 angezeigt und kann dort auch abgefragt werden. Diese erste Sprachbox sollte keine Gruppenmailbox, Vermittlungsmailbox oder Ansagemailbox ein. Soll die Systemmailbox nicht genutzt werden, sollte keine Sprachmailbox mit der Rufnummer des SmartVM Sammelanschlusses eingerichtet werden.

Funktionen der Sprachbox

- Telefonische Abfrage und Steuerung

  (von extern: eine eigene Rufnummer erforderlich)

- Manuelle oder automatische Auswahl unterschiedlicher Begrüßungen
- Telefonmenü (Telephone User Interface, TUI) mit systemweit umschaltbarer Menüstruktur:
  - Telefonmenü, UC Smart: **SmartVM** (ähnlich dem EVM)
  - Telefonmenü, UC Suite: **OSO** (vergleichbar mit UC Suite)
- Bis zu 320 Sprachboxen pro System einrichtbar
- Bis zu 32 Stunden Sprachaufzeichnungskapazität pro System
- Bis zu 100 abgespeicherte Nachrichten pro Sprachbox
- Bis zu 2 min Aufzeichnungsdauer einer Sprachnachricht pro Sprachbox
- Bis zu 10 gleichzeitig mögliche Vermittlungs- und Anrufbeantwortervorgänge
- Ansage/Musikeinspielung vor dem Melden
- Abspielen individueller Ansagen
- Weiterleitung von Faxanrufen durch automatische Faxtonerkennung an ein vorkonfiguriertes Faxziel

---

Anmerkung: Informationen zum Telefonmenü finden Sie in den beiden Kurzbedienungsanleitungen UC Smart Telephone User Interface (TUI) und UC Suite Telephone User Interface (TUI).

Codenummer-Einstellungen

Vor der ersten Benutzung der Sprachbox muss jeder Teilnehmer die vorbelegte Codenummer ändern (Standard: `123456`).

Die Codenummer besteht aus einer sechsstelligen Ziffernfolge. Sie darf nicht aus sich wiederholenden Ziffern (z. B. `333333`) oder einer auf- bzw. absteigendenden Ziffernfolge (z. B. `987654`) bestehen. Nach sechsmaliger Eingabe einer falschen Codenummer wird der Zugriff auf die entsprechende Sprachbox bis zum Rücksetzen des Kennworts durch den Administrator gesperrt. Nach zweimaliger Eingabe eines falschen Kennworts im Telefonmenü wird die Verbindung getrennt.

Ports

Die Sprachbox nutzt die S_0-Ports 500-509 mit den jeweils zugeordneten Rufnummern 739-748. Die Ports 504 und 505 sind standardmäßig dem Company AutoAttendant (Rufnummer 352) zugeordnet, die restlichen 8 Ports dem Sprachbox-Sammelanschluss (Rufnummer 351). Die Rufnummer 351 ist die allgemeine Rufnummer der Sprachbox, über die das Telefonmenü erreichbar ist.

Amtsberechtigung

Die Sprachbox-Ports sind aus Sicherheitsgründen standardmäßig nur halbamtsberechtigt. Folgende Leistungsmerkmale erfordern die Zuweisung einer amtsberechtigten Berechtigungsgruppe:

- Absender einer Sprachnachricht anrufen
- Abhören von Sprachnachrichten durch Mobility-Teilnehmer via Rückruf
- Übergeben zu externem Ziel durch Company AutoAttendant

Begrüßungen/Ansagen

Individuelle Begrüßungen (=Ansagen) werden entweder über ein Telefon aufgesprochen oder mit dem WBM in das System geladen. Bei der Konfiguration über das Telefon wird die Sprachbox-Rufnummer gewählt und mit

Hilfe der Benutzerführung der Sprachbox kann eine neue Begrüßung über das Telefon aufgesprochen werden.

Begrüßungen können aber auch über den Experten-Modus für jede Sprachbox separat in das System geladen, gespeichert und gelöscht werden.

Anmerkung: Für die Voicemail-Wiedergabe über externe Rufnummern (z. B. die Wiedergabe über ein Mobiltelefon, das von myPortal to go ausgelöst wird) muss die Berechtigungen der Smart VM-Ports angepasst werden. Es wird empfohlen, eine "Erlaubnisliste" für solche bekannten Nummern zu verwenden.

12.10.1 Konfiguration der Sprachbox (SmartVM)

Die Konfiguration der Sprachbox (SmartVM) beinhaltet die Konfiguration der Standardmailboxen/Gruppenmailboxen und der Vermittlungsmailboxen.

Allgemeine Einstellungen zur Sprachbox (SmartVM) werden über den Wizard **SmartVM** durchgeführt, wie z.B. die Anpassung der Sprachbox-Rufnummer an einen 4-stelligen Rufnummernplan.

Spezielle Einstellungen zur Sprachbox (SmartVM) und die Einrichtung von Standardmailboxen/Gruppenmailboxen und Vermittlungsmailboxen werden über den Experten-Modus durchgeführt.

Anmerkung: Das Ändern einer Rufnummer setzt die Sprachbox des betreffenden Teilnehmers zurück. Alle persönlichen Sprachnachrichten, Begrüßungen und Ansagen gehen verloren und das Kennwort wird zurückgesetzt.

Sie können auch einzelne Bergüßungen in die SmartVM laden, speichern und löschen sowie Begrüßungen und Nachrichten einzelner oder aller Sprachboxen sichern und wiederherstellen. Zusätzlich können Sie die geladenen Sprachen der Benutzerführung abfragen und sich die 10 Sprachboxen mit den meisten Nachrichten sowie den von Nachrichten und Begrüßungen belegten Speicherplatz anzeigen lassen.

Die Einrichtung von Vermittlungsmailboxen finden Sie im Kapitel Attendants - AutoAttendants - Company AutoAttendant (UC Smart).

Zuordnung der Mailbox zu den Teilnehmern

Ist die Sprachbox (SmartVM) konfiguriert, können den Teilnehmern ihre Standardmailboxen zugeordnet werden. Das ist möglich über

- eine Rufweiterschaltung für den Teilnehmer mit Hilfe einer Rufzielliste (wird vom Administrator eingerichtet). In diesem Fall wird der Anruf der Reihe nach an die ausgewählten Rufziele weitergeleitet (z.B. zuerst an den Teilnehmer und nach einer einstellbaren Zeit an die Mailbox).
- eine Anrufumleitung am Telefon des Teilnehmers (kann der Teilnehmer selbst ausführen). In diesem Fall geht der Anruf sofort an die Mailbox.

  Ist der Teilnehmer Mitglied eines Sammelanschlusses und wird der Sammelanschluss angerufen, wird der Anruf nicht auf die Sprachbox des Sammelanschlusses umgeleitet.

12.10.1.1 Wie Sie die Sprachbox deaktivieren oder aktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Anschaltungen**.
3) Klicken Sie im Menübaum auf **Anschaltungen** > **SmartVM**.
4) Klicken Sie auf die Registerkarte **SmartVM-Parameter bearbeiten**.
5) Wenn Sie die Sprachbox deaktivieren möchten, aktivieren Sie das Kontrollkästchen **EVM deaktivieren**.
6) Wenn Sie die Sprachbox aktivieren möchten, deaktivieren Sie das Kontrollkästchen **EVM deaktivieren**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.10.1.2 Wie Sie die Sprachbox (SmartVM) konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **SmartVM** zu starten.
4) Aktivieren Sie das Kontrollkästchen **SmartVM aktivieren**.
5) Ändern Sie bei Bedarf die allgemeinen Einstellungen der Systemmailbox unter der Spalte **Voicemail**:
   a) Ändern Sie bei Bedarf im Feld **Rufnummer** die Rufnummer der Sprachbox (Standard: `351`), um sie z.B. an einen 4-stelligen Rufnummernplan anzupassen.
   b) Ändern Sie bei Bedarf im Feld **DuWa** die Durchwahlnummer der Sprachbox (Standard: `351`), um sie z.B. an einen 4-stelligen Rufnummernplan anzupassen.
   c) Ändern Sie bei Bedarf im Feld **Name** den Namen der Sprachbox (Standard: `VOICEMAIL`).
6) Ändern Sie bei Bedarf die allgemeinen Einstellungen für die Vermittlungsmailbox unter der Spalte **AutoAttendant**:
   a) Ändern Sie bei Bedarf im Feld **Rufnummer** die Rufnummer der Sprachbox (Standard: `352`), um sie z.B. an einen 4-stelligen Rufnummernplan anzupassen.
   b) Ändern Sie bei Bedarf im Feld **DuWa** die Durchwahlnummer der Sprachbox (Standard: `352`), um sie z.B. an einen 4-stelligen Rufnummernplan anzupassen.
   c) Ändern Sie bei Bedarf im Feld **Name** den Namen der Sprachbox (Standard: `AutoAttendant`).

7) Klicken Sie auf **OK & Weiter**.
8) Ändern Sie in der Zeile des gewünschten Ports bei Bedarf im Feld **Rufnr.** die Rufnummer des Ports (Standard: `739-748`), um sie z.B. an einen 4-stelligen Rufnummernplan anzupassen.
9) Ändern Sie in der Zeile des gewünschten Ports bei Bedarf im Feld **Name** den Namen des Ports (Standard: `SmartVM 1-10`).
10) Ändern Sie in der Zeile des gewünschten Ports bei Bedarf in der Aufklappliste **Typ** den Typ des Ports:
    - **Phone Mail (Ruf-Nr. 5-stellig)**: der Port ist den Standardmailboxen und den Vermittlungsmailboxen vom Typ AutoAttendant zugeordnet. Ports dieses Typs werden automatisch in den Sammelanschluss 351 aufgenommen.
    - **Standard**: der Port ist den Vermittlungsmailboxen vom Typ Company AutoAttendant und den Ansagemailboxen zugeordnet. Ports dieses Typs werden automatisch in den Sammelanschluss 352 aufgenommen.
11) Ändern Sie in der Zeile des gewünschten Ports bei Bedarf in der Aufklappliste **Modus** den Modus des Ports:
    - **Ansage**: eine Begrüßung/Ansage wird einmalig abgespielt.
    - **Wartemusik**: Begrüßung/Ansage/Musik wird in einer Endlosschleife abgespielt.
    - **Company AutoAttendant**: nach Abspielen einer Begrüßung/Ansage besteht die Möglichkeit der Weitervermittlung.
12) Klicken Sie auf **OK & Weiter**.
13) Wählen Sie aus der Aufklappliste **Mailbox-Auswahl** die gewünschte Sprachbox aus. Anschließend erscheinen Felder für die Konfiguration der Begrüßungen.
14) Wenn Sie eigene Begrüßungen für die ausgewählte Mailbox verwenden wollen, klicken Sie auf **Durchsuchen**, navigieren Sie zum Ablageort der Dateien (Format: wave, PCM, 16 bit, 8kHz, mono) und klicken Sie auf **Laden**. Die ausgewählten Begrüßungen werden in das System geladen.

    Anmerkung: Bereits geladene Begrüßungen können Sie speichern und löschen.

15) Wenn Sie Begrüßungen für weitere Mailboxen einrichten möchten, wiederholen Sie die 13 Schritte bis 14.
16) Klicken Sie auf **OK & Weiter**.
17) Ändern Sie die allgemeinen Parameter nur bei Bedarf. Für eine Beschreibung der allgemeinen Parameter siehe Anschaltungen>SmartVM .
18) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

12.10.1.3 Wie Sie eine Standardmailbox für einen Teilnehmer hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Dem entsprechenden Teilnehmer ist eine Voicemail-Lizenz zugeordnet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Anschaltungen**.
3) Klicken Sie im Menübaum auf **Anschaltungen** > **SmartVM**.
4) Klicken Sie auf die Registerkarte **SmartVM-Mailboxen bearbeiten**.
5) Geben Sie im Feld **Mailbox-Rufnummer** die Rufnummer des Teilnehmers ein, für den die Mailbox hinzugefügt werden soll.
6) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.
7) Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.
8) Vergewissern Sie sich, dass das Kontrollkästchen **AutoAttendant** deaktiviert ist.
9) Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.10.1.4 Wie Sie die Berechtigungsgruppe für einen Sprachbox-Port ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

UC Smart wurde aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie in der Navigationsstruktur auf **Telefonie-Server** > **Dienstklassen** in the navigation tree.
3) Klicken Sie im Menübaum auf **Dienstklassen** > **Station** > **EVM** und dann auf den gewünschten Voicemail-Box-Port.
4) Wählen Sie die gewünschten COS-Gruppen für den Tag- und Nachtdienst auf der Registerkarte **COS-Gruppe bearbeiten** aus den Dropdown-Listen **Dienstklasse Gruppentag** bzw. **Dienstklasse Gruppennacht** aus.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Anmerkung: EVM-Port-Texte werden gemäß dem **Assistenten für die Grundkonfiguration** > **Systemländercode**generiert.

12.10.1.5 Wie Sie die Struktur des Telefonmenüs der Sprachbox ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Hilfsausrüstung** .
3) Klicken Sie im Menübaum auf **Hilfsausrüstung** > **SmartVM** .
4) Klicken Sie auf die Registerkarte **SmartVM-Parameter bearbeiten** .
5) Wenn Sie möchten, dass das Telefonmenü ähnlich wie OpenScape Office aufgebaut ist, wählen Sie den Eintrag **OSO** in der Dropdown-Liste **Telefon-Benutzeroberfläche** .
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.10.1.6 Wie Sie einzelne Begrüßungen laden, sichern und löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Konfiguration**.
3) Klicken Sie im Menübaum auf **Konfiguration** > **SmartVM Konfiguration** > **Dateioperationen**.
4) Klicken Sie auf die Registerkarte **Begrüßungsansagen**.
5) Wählen Sie aus der Aufklappliste **Mailbox-Auswahl** die gewünschte Sprachbox aus.
6) Wenn Sie eine zuvor gespeicherte Begrüßung oder eine Wave-Datei in die SmartVM laden wollen, klicken Sie bei der gewünschten Begrüßung auf **Durchsuchen** und navigieren Sie zum Ablageort der Begrüßung. Klicken Sie anschließend auf **Laden**.

   Anmerkung: Die zu ladende Wave-Datei muss folgendes Format haben: PCM, 16 bit, 8khz, mono. Beim Laden wird die Wave-Datei konvertiert. Je nach Größe der Wave-Datei kann dies einige Zeit in Anspruch nehmen.

7) Wenn Sie eine bestehende Begrüßung sichern wollen, klicken Sie bei der gewünschten Begrüßung auf **Sichern** und speichern Sie die vma-Datei an einem Ort Ihrer Wahl.
8) Wenn Sie eine bestehende Begrüßung löschen wollen, klicken Sie bei der gewünschten Begrüßung auf **Löschen** und bestätigen Sie mit **OK**.

12.10.1.7 Wie Sie Begrüßungen und Nachrichten sichern und wiederherstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Konfiguration**.

3) Klicken Sie im Menübaum auf **Konfiguration** > **SmartVM Konfiguration** > **Dateioperationen**.
4) Wenn Sie Begrüßungen und Nachrichten sichern wollen:
   a) Klicken Sie auf die Registerkarte **Backup**.
   b) Aktivieren Sie das Kontrollkästchen **Nachrichten**, wenn zusätzlich zu den Begrüßungen auch die Nachrichten gesichert werden sollen.
   c) Übernehmen Sie die zu sichernden Sprachboxen aus der Liste **Verfügbare Mailboxen** in die Liste **Zu sichernde Mailboxen**.
   d) Klicken Sie auf **Übernehmen**. Die Begrüßungen (und die Nachrichten, wenn Flag **Messages** aktiviert wurde) der zu sichernden Sprachboxen werden in eine Sicherungsdatei (*.tar) gesichert. Speichern Sie die Datei an einem Ort Ihrer Wahl.
5) Wenn Sie Begrüßungen und Nachrichten wiederherstellen wollen:
   a) Klicken Sie auf die Registerkarte **Restore**.
   b) Klicken Sie auf **Durchsuchen** und navigieren Sie zum Ablageort Ihrer Sicherungsdatei (*.tar) und klicken Sie auf **Öffnen**.
   c) Klicken Sie auf **Laden** und auf **OK**. Die in der Sicherungsdatei enthaltenen Sprachboxen werden angezeigt.
   d) Übernehmen Sie die wiederherzustellenden Sprachboxen aus der Liste **Verfügbare Mailboxen** in die Liste **Wiederherzustellende Mailboxen**.
   e) Aktivieren Sie das Kontrollkästchen **Nachrichten**, wenn nicht nur die Begrüßungen der ausgewählten Sprachboxen, sondern auch die Nachrichten wiederhergestellt werden sollen.
   f) Ist das Kontrollkästchen **Aufschalten** deaktiviert, werden nur die Begrüßungen der ausgewählten Sprachboxen überschrieben. Ist zusätzlich das Kontrollkästchen **Nachrichten** aktiviert, werden auch die in den Sicherungsdaten enthaltenen Nachrichten hinzugefügt. Die bereits existierenden Nachrichten bleiben erhalten
   g) Ist Kontrollkästchen **Aufschalten** aktiviert, werden vor der Wiederherstellung alle Begrüßungen und Nachrichten der ausgewählten Sprachboxen in der SmartVM gelöscht. Sind Sprachboxen ausgewählt, die nicht in den Sicherungsdaten enthaltenen sind, werden diese auch gelöscht! Die in den Sicherungsdaten enthaltenen Begrüßungen werden übertragen. Ist zusätzlich das Kontrollkästchen **Nachrichten** aktiviert, werden auch die in den Sicherungsdaten enthaltenen Nachrichten übertragen.
   h) Klicken Sie auf **Laden** und auf **OK**. Die Begrüßungen und Nachrichten der ausgewählten Sprachboxen wieder hergestellt.

12.10.2 Benachrichtigungsdienst für neue Nachrichten

Das System kann einen UC Smart Benutzer über eine neue Sprachnachricht auf Wunsch per E-Mail informieren.

Voraussetzung für den Benachrichtigungsdienst

- Der E-Mail-Versand (E-Mail-Weiterleitung) muss im System vom Administrator konfiguriert sein.
- Die E-Mail-Adresse des Benutzers muss dem System bekannt sein. Der Administrator kann alle E-Mail-Adressen im WBM während der Erstinstallation über eine XML-Datei importieren oder im UC Smart Assistant für jeden Benutzer eine E-Mail-Adresse eintragen (siehe Wie Sie Benutzer

von UC Smart konfigurieren). Alternativ kann der Benutzer selbst seine E-Mail-Adresse in seinem UC Smart Client angeben.
- Dem Benutzer ist eine VoiceMail-Lizenz zugewiesen.
- Das Leistungsmerkmal **Voicemail an Email** ist aktiviert. Der Administrator kann das Leistungsmerkmal im UC Smart Assistant für jeden Benutzer aktivieren (Wie Sie die E-Mail-Benachrichtigung aktivieren oder deaktivieren). Alternativ kann der Benutzer selbst das Leistungsmerkmal in seinem UC Smart Client aktivieren.

Der UC Smart Benutzer erhält eine E-Mail mit der Sprachnachricht als angehängte WAV-Datei (16 bit, mono), Datum und Uhrzeit des Empfangs, Dauer der Sprachnachricht und sofern verfügbar Rufnummer sowie Name des Absenders.

12.10.2.1 Wie Sie die E-Mail-Benachrichtigung aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Die E-Mail-Adresse des Benutzers ist in seinen Profildetails eingetragen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Smart**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.
4) Klicken Sie im Menübaum auf **Administration** > **Benutzerverwaltung**.
5) Wählen Sie in der Liste **Benutzer** den gewünschten Benutzer aus.
6) Wählen Sie eine der folgenden Möglichkeiten:
   a) Wenn Sie den Benachrichtigungsdienst für neue Nachrichten aktivieren wollen, aktivieren Sie im Bereich **Profildetails** das Kontrollkästchen **Voicemail an Email**.
   b) Wenn Sie den Benachrichtigungsdienst für neue Nachrichten deaktivieren wollen, deaktivieren Sie im Bereich **Profildetails** das Kontrollkästchen **Voicemail an Email**.
7) Klicken Sie auf **Übernehmen**.
8) Wenn Sie einen weiteren Benutzer konfigurieren möchten, wiederholen Sie die Schritte 5 bis 7.

13 UC Suite

UC Suite bietet Unified Communications Leistungsmerkmale wie z.B. Anwesenheitsstatus und CallMe, Konferenzen sowie Sprach- und Faxnachrichten in den Clients myPortal for Desktop und myPortal for Outlook. myAttendant bietet zusätzlich Vermittlungsplatz-Funktionen.

Anmerkung: Für die OpenScape Business Hardwaremodelle X3/X5/X8 benötigt die UC-Lösung UC Suite die UC Booster Hardware (UC Booster Card oder UC Booster Server). Bei OpenScape Business S (Softswitch) ist die UC-Lösung UC Suite bereits integriert.

Anmerkung: Nach Konfigurationsänderungen an Teilnehmern, Gruppen, Mobilitäts- oder anderen Systemparametern wie Amtskennzahlen, müssen die UC-Daten für UC Smart oder UC Suite synchronisiert werden. Die Synchronisierung erfolgt fünf Minuten nach der letzten Konfigurationsänderung. Wird die Konfiguration innerhalb der 5-Minuten-Timerfrist nochmals geändert, wird der Timer neu gestartet. Vor Beginn der Synchronisierung sind die UC-Daten also möglicherweise nicht ganz aktuell. Während der Synchronisierung sind die UC Applikation und die Web Services Interface (WSI)-API nicht verfügbar und alle verbundenen UC-Clients werden getrennt, bis die Synchronisierung der UC-Daten abgeschlossen ist. Nach Abschluss der UC-Datensynchronisation werden die Verbindungen automatisch wiederhergestellt.

13.1 Grundeinstellungen für UC Suite

Die Grundeinstellungen für UC Suite können angepasst werden.

UC Suite kann aktiviert oder deaktiviert werden. Wenn UC Suite verwendet wird, muss UC Smart deaktiviert werden.

Zusätzlich kann bei allen vom System eingeleiteten UC-Anrufen (z.B. über den CallMe-Dienst) vor der Wahl geprüft werden, ob der anfordernde UC-Benutzer die Berechtigung für diesen Anruf hat. Fehlt dem UC-Benutzer die Berechtigung, wird der Anruf nicht ausgeführt.

Anmerkung: Wenn CSTA-Anwendungen verwendet werden, muss der Code-Parameter für alle aktiven Leitungen eingestellt sein.

Zugehörige Tasks

Wie Sie die IP-Adressen von Komponenten des Systems ermitteln auf Seite 494

13.1.1 UC Suite aktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Web Services**.
3) Klicken Sie im Menübaum auf **Applikationsauswahl** > **Applikationsauswahl**.
4) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie UC Suite mit UC Booster Card nutzen möchten, klicken Sie auf **Paket mit UC Suite**.
   - Wenn Sie UC Suite mit UC Booster Server nutzen möchten, klicken Sie auf **Paket mit UC Suite auf OSBiz UC Booster-Server** und geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers an.
5) Klicken Sie auf **Übernehmen**.

13.1.2 Wie Sie die Berechtigung von systemseitig eingeleiteten UC-Anrufe einschränken

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **System Flags**.
4) Wenn vor der Wahl von UC-Anrufen, die vom System eingeleitet werden, geprüft werden soll, ob der anfordernde UC Suite Benutzer die Berechtigung für diesen Anruf hat, aktivieren Sie im Bereich **Einschränkung für UC-Anrufe** das Kontrollkästchen **Einschränkung für UC-Anrufe**.
5) Wenn vor der Wahl von UC-Anrufen, die vom System eingeleitet werden, nicht geprüft werden soll, ob der anfordernde UC Suite Benutzer die Berechtigung für diesen Anruf hat, deaktivieren Sie im Bereich **Einschränkung für UC-Anrufe** das Kontrollkästchen **Einschränkung für UC-Anrufe**.
6) Klicken Sie auf **Übernehmen**.

13.2 UC Suite Clients

UC Suite Clients bieten Teilnehmern komfortable Oberflächen für umfangreiche Unified Communications-Funktionen.

Das System bietet folgende UC Suite Clients für folgende Geräte:

Client-Typ	Client	Gerätetyp
Communications Client	myPortal for Desktop	PC
	myPortal for Outlook	
	myPortal @work	
	Fax Printer	
	myAttendant	
Mobile Client	myPortal to go (UC Suite) (siehe Mobility)	Smartphone, Tablet-PC
Contact Center Client	myAgent (siehe Multimedia Contact Center)	PC
	myReports (siehe Multimedia Contact Center)	

Teilnehmer mit konfigurierter E-Mail-Adresse erhalten eine Begrüßungs-E-Mail mit einer Anleitung für erste Schritte.

Teilnehmer-individuelle Einstellungen

Die teilnehmer-individuellen Einstellungen für myPortal for Desktop werden in ini-Dateien auf dem PC gespeichert. Dabei wir für jeden Benutzer eine eigene ini-Datei angelegt. Die teilnehmer-individuellen Einstellungen für myPortal for Outlook, myAttendant und Fax Printer werden in der Registry des PC gespeichert. Dadurch können unterschiedliche Benutzer die Applikationen myPortal for Desktop, myPortal for Outlook, myAttendant und Fax Printer über einen PC nutzen (Desk Sharing). Dies ermöglicht den Einsatz in Windows Terminalserver- und in Citrix-Server-Umgebungen. Dadurch können unterschiedliche Benutzer mit ihren PCs die Applikationen ohne lokale Installation nutzen.

13.2.1 myPortal for Desktop

myPortal for Desktop ist ein Client für Unified Communications an Ihrem PC. Neben komfortablen Wahlhilfen über Verzeichnisse und Favoriten, Informationen über den Anwesenheitsstatus anderer Teilnehmer, hat der Teilnehmer z.B. auch Zugriff auf Sprach- und Faxnachrichten.

myPortal for Desktop bietet folgende Leistungsmerkmale:

- Verzeichnisse
- Favoritenliste
- Journal
- Desktop-Wahl
- Pop-up-Fenster
- Anwesenheitsstatus
- CallMe-Dienst mit ONS (One Number Service)
- Statusbezogene Anrufumleitung

- Persönlicher AutoAttendant
- Konferenzmanagement
- Aufzeichnen von Konferenzen
- Aufzeichnen von Anrufen
- Sofortnachricht versenden
- Sprach- und Faxnachrichten

13.2.2 myPortal @work

myPortal @work ist eine Unified-Communication-Anwendung, die alle benötigten Funktionen und Dienste wie komfortables Wählen über Telefonverzeichnisse, Favoriten, Gespräche und Informationen zum Anwesenheitsstatus von Kollegen zu einem zentralen Lösungskonzept vereint, um die tägliche Kommunikation zu beschleunigen, die Teamarbeit zu verbessern sowie rasch mit Kollegen, Kunden und Partnern in Verbindung zu treten.

Anmerkung: Wenn der myportal@work VoIP-Client in Kombination mit anderen UC Suite-Clients verwendet wird, empfiehlt es sich, die Rückfrage von myportal@work anstelle der gemeinsamen Rückfrage von UC Suite-Clients zu verwenden.

---

myPortal @work kann mit beiden UC-Lösungen UC Smart und UC Suite verwendet werden. Weitere Informationen siehe myPortal @work.

13.2.3 myPortal for Outlook

myPortal for Outlook ist der Client für Unified Communications in Microsoft Outlook (Plug-In) analog zu myPortal for Desktop.

myPortal for Outlook bietet zusätzlich zu myPortal for Desktop folgende Leistungsmerkmale:

- Outlook-Kontakt anrufen
- Absender einer Sprachnachricht als Outlook-Kontakt anlegen
- Sprachnachricht als E-Mail senden
- Faxnachricht als E-Mail senden

13.2.4 Fax Printer

Fax Printer ist eine Windows-Anwendung für den Versand von Faxnachrichten aus anderen Windows-Anwendungen wie z.B. Microsoft Word mit individuell erstellten Deckblättern.

Fax Printer besteht aus folgenden Komponenten:

- Fax Printer Cover Editor

- Fax Printer Driver - mit folgenden Leistungsmerkmalen:
  - Faxversand an einzelne Empfänger
  - Verzeichnisse
  - Verwendung zentraler Deckblätter
  - Verwendung vordefinierter Kopfzeilen
  - Serienfax
  - Steuerung über die Benutzeroberfläche
  - Steuerung über die Kommandozeile

13.2.5 myAttendant

myAttendant ist eine Unified-Communications-Anwendung für Vermittlungsfunktionen. Neben komfortablen Vermittlungsfunktionen, Wahlhilfen über Verzeichnisse und Informationen über den Anwesenheitsstatus von Teilnehmern besteht z.B. auch Zugriff auf Sprach- und Faxnachrichten. Instant Messaging unterstützt die Kommunikation mit internen Teilnehmern.

myAttendant bietet folgende Leistungsmerkmale:

- Vermittlungsfunktionen
- Verzeichnisse
- Journal
- Pop-Up-Fenster
- Anwesenheitsstatus von Teilnehmern ändern
- Aufzeichnen von Anrufen
- Nachrichten-Center
- Benutzerschaltflächen
- Verwaltung von Sprach- und Faxnachrichten
- Instant Messaging
- Teamfunktionen
- Konferenzmanagement

13.2.6 Voraussetzungen für UC Suite PC-Clients

Um UC Suite PC-Clients nutzen zu können, muss der Client-PC über die entsprechenden Hardware- und Softwarekonfigurationen verfügen. Für die Installation und automatische Updates sind konfigurationsabhängig Administratorrechte erforderlich. Der nutzbare Funktionsumfang ist abhängig von den verwendeten Lizenzen.

Anmerkung: Beachten Sie bitte unbedingt die aktuellen Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Telefone

Die UC Suite PC-Clients können in Verbindung mit folgenden Telefonen genutzt werden:

- OpenStage HFA und SIP
- OpenScape Desk Phone IP 35G/55G HFA und SIP

- OpenScape Desk Phone IP 35G Eco HFA und SIP
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA und SIP
- OpenScape Desk Phone CP 110/210/410/710 HFA und SIP
- SIP-Telefone mit 3PCC-Unterstützung
- Analoge Telefone
- ISDN-Telefone
- OpenScape Personal Edition HFA und SIP
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)
- optiPoint WL3 professional SIP

Ältere Geräte (z. B. optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 und optiPoint WL2 SIP) werden unterstützt. Optiset E-Geräte können nicht betrieben werden. Getestete und freigegebene Geräte entnehmen Sie bitte der Freigabemitteilung.

Anmerkung: Für den OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA integrierten Client sind neben der Standard-Client-Konfiguration und -Lizenz keine besonderen Voraussetzungen erforderlich.

"Favoriten" im Telefonmenü enthält frei programmierbare Tasten und bezieht sich nicht auf UC-Favoriten. Details zu diesen Schlüsseln und eine Anleitung dazu finden Sie in der Gerätedokumentation.

Anmerkung: Bei analogen Telefonen und DECT-Telefonen wird die Message Waiting Indication (MWI) nicht unterstützt, die Anzeige von Informationen im Display wird nur eingeschränkt unterstützt.

Betriebssysteme

Die UC Suite PC-Clients können in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 11 (64 Bit) alle Versionen
- Microsoft Windows 10 (64 Bit) alle Versionen
- Apple macOS 13 / 14 / 15.1 bis 15.4

Tipp: Das verwendete Betriebssystem benötigt stets den aktuellen Stand aller verfügbaren Updates (Service Packs und Patches).

Der Support der UC Suite PC-Clients für Microsoft Office 2003, Microsoft Windows XP und Microsoft Windows Server 2003 endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Die Installation unter Windows erfordert lokale Administratorrechte auf einem Client-PC, automatische Updates jedoch nicht. Die russische und chinesische

Benutzeroberfläche von myPortal for Outlook erfordert eine russische bzw. chinesische Windows-Installation.

myPortal for Desktop für Apple MAC steht mit gleicher Oberfläche wie unter Microsoft Windows zur Verfügung. Aufgrund der Apple-MAC-OS-Systemarchitektur werden derzeit folgende Funktionen nicht unterstützt:

- Fax versenden
- Outlook, Entourage Integration

myPortal for Outlook wird in Microsoft Office 365 Umgebungen unterstützt. Microsoft Office 365 ist eine Cloud-Anwendung. Darin enthalten sind unter anderem ein Exchange-Server für die zentrale Verteilung von E-Mails, sowie auch die klassischen Microsoft Office-Produkte. OpenScape Business unterstützt Microsoft Office 365.

Folgende Funktionen können unter Microsoft Office 365 genutzt werden:

- Exchange-Kalender-Integration
- E-Mail-Weiterleitung

Webbrowser

Für die Tastenprogrammierung der Telefone über die UC-Clients sind folgende Webbrowser freigegeben:

- Microsoft Internet Explorer Version 10 (oder neuer)
- Microsoft Edge
- Mozilla Firefox Version 19 (oder neuer)
- Google Chrome

Zusätzliche Software

Zusätzliche Software	myPortal for Desktop	myAttendant	myPortal for Outlook
Oracle Java JRE 1.8.x oder höher (32 Bit / 64 Bit) OpenJDK V8 oder höher (32 Bit / 64 Bit)	X	X	
Microsoft Outlook / Office • 2021 (32 Bit / 64 Bit) + Office 365 • 2019 (32 Bit / 64 Bit) • 2016 (32 Bit / 64 Bit) – wird unterstützt, ist jedoch nicht mehr Teil des Systemtests – im Fehlerfall wird keine SW-Korrektur bereitgestellt (Ende der Unterstützung durch OpenScape Business)			X
Zugriff auf Microsoft Exchange-Server (für Outlook-Kontakte und -Termine) Exchange 2015 / 2013 / 2010 (64 Bit)	X		X
Microsoft .NET Framework >= 4.0 (ab Outlook 2010)			X

Anmerkung: Um die Exchange-Kalenderintegration mit Microsoft Small Business Server nutzen zu können, muss unter

Umständen die formulargesteuerte Authentifizierung (Form Based Authentication, FBA) dort deaktiviert werden.

Hinweis zu Oracle Java 32 Bit oder 64 Bit

Um die myPortal for Desktop-Funktion „Outlook-Kontakte beim Start importieren" in Verbindung mit der 64-Bit-Version von Microsoft Office 2013 nutzen zu können, ist die Installation der 64-Bit-Variante von Java erforderlich. Wird diese Funktion nicht verwendet, ist Java in der 32 Bit Variante zu empfehlen, da somit der Arbeitsspeicher-Bedarf deutlich geringer ist. Bei allen anderen Installationen wird generell aus diesem Grund die 32-Bit-Variante von Oracle Java oder OpenJDK empfohlen.

Anmerkung: Die kontinuierliche Nutzung der bestehenden Oracle Java-Installation mit OpenScape Business erfordert keine Änderungen. Wenn ein Wechsel der Java-Version erforderlich ist (z. B. Upgrade von Oracle Java 7 auf Oracle Java 8 bzw. Open JDK Version 8), ist eine Neuinstallation des Kommunikationsclients erforderlich.

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbit/s LAN (1 Gbit/s LAN empfohlen)
- XGA (1024x768) Bildschirmauflösung, myPortal for Outlook: SVGA (800x600) Bildschirmauflösung

Anmerkung: 4K-Monitore werden für myPortal und myAttendant nicht unterstützt.

Microsoft Terminalserver, Citrix XenApp Server

Die UC Suite PC-Clients können unter den nachfolgend genannten Voraussetzungen in Microsoft Terminalserver- und Citrix-Server-Umgebungen eingesetzt werden:

Tipp: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

Tipp: Citrix-Server-Umgebungen können einige regionale Buchstaben (z. B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssysteme:

- Microsoft Windows 2022 Server 64 Bit
- Microsoft Windows 2019 Server 64 Bit
- Microsoft Windows 2016 Server 64 Bit
- Microsoft Windows 2025 Server 64 Bit

Office-Anwendungen:

Microsoft Outlook / Office

- 2021 (32 Bit / 64 Bit) + Office 365
- 2019 (32 Bit / 64 Bit)
- 2016 (32 Bit / 64 Bit) – wird unterstützt, ist jedoch nicht mehr Teil des Systemtests – im Fehlerfall wird keine SW-Korrektur bereitgestellt (Ende der Unterstützung durch OpenScape Business)

Hardware-Voraussetzungen:

Die Anzahl der installierbaren Clients hängt von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher ab. Werden auf dem Server weitere Applikationen genutzt, ist deren Arbeitsspeicherbedarf zu berücksichtigen.

Installationsdateien

Für die Bereitstellung der Installationsdateien an die Benutzer bestehen folgende Möglichkeiten:

- Der Administrator kann die Installationsdateien aus dem Service-Center Der Administrator kann die Installationsdateien aus dem **Service-Center** herunterladen und diese den Benutzern bereitstellen, z. B. über ein Netzlaufwerk.
- Der Administrator lädt auch das Offline-Installations-Repository aus dem Beispiel herunter.
- Der Administrator lädt auch das Offline-Installations-Repository aus dem **Service-Center** herunter und die Clients können offline installiert werden.

13.2.7 Silent Installation/Deinstallation für UC Suite PC-Clients

Silent Installation/Deinstallation ist eine kommandozeilenbasierte Methode zur automatischen Installation, Deinstallation und Modifikation von UC Suite PC-Clients auf einem PC ohne weitere erforderliche Eingaben.

Anmerkung: Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first.rtf`.

Silent Installation/Deinstallation erfordert lokale Administrationsrechte auf dem betreffenden PC. Silent Installation/Deinstallation ermöglicht die Protokollierung des Ablaufs in einer Datei.

Für Silent Installation/Deinstallation stehen folgende Parameter zur Verfügung:

Parameter	Komponenten
`/quiet`	Startet den Installationsvorgang ohne Benutzeroberfläche und ohne Eingreifen des Benutzers. Dieser Parameter erfordert, dass das Repository schon gefunden wurde.
`/repository`	Legt die IP-Adresse oder den Hostnamen für die Installation fest. Zum Beispiel: `/repository=192.168.50.50`

Parameter	Komponenten
`/installpath`	Legt den Pfad der installierten Clients fest. Der voreingestellte Wert lautet: `C:\Program Files(x86)\communicationsclients\`
`/autostart`	Startet den Installationsvorgang ohne Eingreifen des Benutzers. Dieser Parameter erfordert, dass das Repository schon gefunden wurde.
`/i`	Wählt das zu installierende Produkt aus. Verfügbare Werte sind `OLI`, `myPortal`, `myAgent`, `FPD`, `myReports` und `all`. Zum Beispiel: `/i="OLI,FPD"`
`/u`	Wählt das zu entfernende Produkt aus. Zum Beispiel: `/u="OLI,FPD"`
`/set`	Wählt die Produkte aus, die im System installiert werden sollen. Dieser Schalter installiert die gewählten Produkte oder ändert bereits installierte Produkte. Es werden auch installierte Produkte entfernt, die nicht angegeben wurden. Zum Beispiel: `/set="OLI,FPD"`
`/repair`	Repariert die angegebenen Produkte. Zum Beispiel: `/repair="OLI,FPD"`

13.2.7.1 Wie Sie eine Silent Installation durchführen

Voraussetzungen

Ihr PC erfüllt die Voraussetzungen für UC Suite PC-Clients.

Sie verfügen über lokale Administrationsrechte auf dem Client-PC.

Die Datei `CommunicationsClients.exe` ist am Client-PC verfügbar.

Anmerkung: Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first`.

Benutzen Sie Kommandozeilen nach den folgenden Mustern in einer Batch-Datei oder in einem Fenster mit der DOS-Eingabeaufforderung.

Schritt für Schritt

1) Wenn Sie den Ablauf nicht protokollieren möchten, führen Sie eine der folgenden Kommandozeilen aus:

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i=all /quiet
   ```

   Wobei `<IP-address>` durch die IP der UC Clients ersetzt werden muss.
2) Wenn Sie den Ablauf in einer Datei, z.B. `C:\ccinstall.log`, protokollieren möchten, führen Sie eine der folgenden Kommandozeilen aus:

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i="myPortal,FPD" /quiet /l="C:\ccinstall.log"
   ```

   Wobei `<IP-address>` durch die IP der UC Clients ersetzt werden muss. Der obere Befehl installiert nur myPortal for Desktop und FaxPrinter. Sie können ihn für die Installation der gewünschten Clients ändern.

13.2.7.2 Wie Sie eine Silent Deinstallation durchführen

Voraussetzungen

Ihr PC erfüllt die Voraussetzungen für UC Suite PC-Clients.

Sie verfügen über lokale Administrationsrechte auf dem Client-PC.

Die Datei `CommunicationsClients.exe` ist am Client-PC verfügbar.

Anmerkung: Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first`.

Benutzen Sie Kommandozeilen nach den folgenden Mustern in einer Batch-Datei oder in einem Fenster mit der DOS-Eingabeaufforderung.

Schritt für Schritt

1) Wenn nach der letzten Silent Installation ein Update des Systems durchgeführt wurde, wiederholen Sie mit der neuen Datei `CommunicationsClients.exe` genau jene Kommandozeilen, die Sie mit der bisherigen Datei `CommunicationsClients.exe` durchgeführt haben (so, als ob Sie die bereits installierten Komponenten mit der neuen Datei `CommunicationsClients.exe` neu installieren wollten). Erst anschließend ist Silent Deinstallation möglich.
2) Wenn Sie den Ablauf nicht protokollieren möchten, wählen Sie eine der folgenden Kommandozeilen:
   - Wenn Sie alle Komponenten deinstallieren möchten:

     ```
     CommunicationsClients.exe /quiet /u=all
     ```
   - Wenn Sie mehrere Komponenten deinstallieren möchten, geben Sie deren entsprechende Parameter als Aufzählung getrennt durch Komma

an nach `/u=`, zum Beispiel, myPortal for Desktop / myAttendant und Fax Printer:

```
CommunicationsClients.exe /quiet /u="myPortal,FPD"
```

- Wenn Sie nur eine Komponente deinstallieren möchten, geben Sie den entsprechenden Parameter an nach `/u=`, z.B., myPortal for Desktop / myAttendant:

```
CommunicationsClients.exe /quiet /u=myPortal
```

3) Wenn Sie den Ablauf z.B. in einer Datei, z.B. `C:\ccuninstall.log`, protokollieren möchten, wählen Sie eine der folgenden Kommandozeilen:

- Wenn Sie alle Komponenten deinstallieren möchten:

```
CommunicationsClients.exe /quiet /l="C:
\ccuninstall.log" /u=all
```

- Wenn Sie mehrere Komponenten deinstallieren möchten, geben Sie deren entsprechende Parameter als Aufzählung getrennt durch Komma an nach `/u=`, zum Beispiel, myPortal for Desktop / myAttendant und Fax Printer:

```
CommunicationsClients.exe /quiet /l="C:
\ccuninstall.log" /u="myPortal,FPD"
```

- Wenn Sie nur eine Komponente deinstallieren möchten, geben Sie den entsprechenden Parameter an nach `/u=`, z.B., myPortal for Desktop / myAttendant:

```
CommunicationsClients.exe /quiet /l="C:
\ccuninstall.log" /u=myPortal
```

13.2.8 Automatische Updates

Automatische Updates halten UC Clients auf dem neuesten Stand.

Ist eine neue Version verfügbar, wird diese entweder automatisch aktualisiert oder es wird über die Möglichkeit der Aktualisierung informiert. Gegebenenfalls erscheint eine Meldung, dass eine oder mehrere Anwendungen geschlossen werden muss/müssen, um das Update durchzuführen.

Anmerkung: Es wird empfohlen, die angebotenen Updates stets durchzuführen. Dies gilt ebenso für Software, die für bestimmte UC-Clients erforderlich ist.

Anmerkung: Automatische Updates von myPortal @work werden in MacOS nicht unterstützt.

13.3 Benutzer und Benutzer-Profile von UC Suite

Benutzer von UC Suite sind Teilnehmer, welche UC Clients von UC Suite nutzen. Benutzer-Profile speichern Einstellungen von Benutzern von UC Suite.

13.3.1 Benutzer von UC Suite

Benutzer von UC Suite nutzen UC Clients von UC Suite. Die Einstellungen der Benutzer von UC Suite sind im Benutzerverzeichnis konfigurierbar.

Das Benutzerverzeichnis enthält alle Teilnehmer des Systems. Für die Benutzung der UC Clients sind zusätzliche Benutzerdaten im Benutzerverzeichnis zu konfigurieren.

Im Benutzerverzeichnis werden zu jedem Benutzer folgende Informationen angezeigt:

- Symbol für Anwesenheitsstatus

  Der Administrator kann den Anwesenheitsstatus für jeden Benutzer ändern.
- **Nebenstelle**
- **Benutzername**

  Anmerkung: UCSuite erlaubt und unterstützt zwar die Änderung von Benutzernamen für seine eigenen Clients, dennoch könnten solche Änderungen die Anmeldung von Nicht-UCSuite-Clients wie myPortalToGo/myPortal@Work (wo zutreffend) beeinträchtigen und werden daher in solchen Situationen nicht empfohlen.
- **Name**

  Vor- und Nachname, wie für den Teilnehmer konfiguriert.
- **Abteilung**

  Falls dem Benutzer eine Abteilung zugeordnet ist.
- **E-Mail**

  E-Mail-Adresse
- **Ist Agent**

  Agentenlevel im Multimedia Contact Center.
- **Voicemail**

  Der Benutzer kann Sprachnachrichten empfangen.
- **Anrufumleitung**

  Für den Benutzer ist eine Anrufumleitung konfiguriert.

Suchfunktionalität sind auch für die Benutzerverzeichnisfelder verfügbar.

Folgende Einstellungen können konfiguriert werden:

Werte und Einstellungen	Stichworte
Persönliche Daten	
Eigene persönliche Daten	Eigener Name, Benutzername, Passwort, E-Mail-Adresse, Abteilung, zusätzliche Telefonnummer
Eigenes Bild	Eigenes Bild Unterstützte Dateiformate: BMP, JPG/JPEG/ JFIFI, PNG. Max. Dateigröße: 10 MB

Werte und Einstellungen	Stichworte
Benutzerebene	Empfang von Sprachnachrichten: siehe Teilnehmer Benutzer als Vermittlungsplatz: siehe Teilnehmer Benutzer als Agent: siehe Teilnehmer
Meine Einstellungen	
Darstellung	Skin-Farben, Sprache der Benutzeroberfläche
Benachrichtigungen	Pop-up-Fenster
Kalender-Anbindung	Automatische Erstellung von Outlook-Terminen bei Abwesenheit, Automatische Aktualisierung des Anwesenheitsstatus durch Outlook-/iCal-Termine
Abkürzungstasten	Abkürzungstaste für Funktionen
Verschiedenes	Automatisches Zurücksetzen des Anwesenheitsstatus, Übergabemethode, Aufbewahrungsdauer für Journaleinträge, Serveradresse, Funktionstasten des Telefons
Anrufregeln	
Anrufweiterleitungsziele	Statusbezogene Anrufumleitung
Regelmodul	Regelbasierte Anrufumleitung
Kommunikation	
Einstellungen für Sprachnachrichten	Aufzeichnungsmodus oder Ansagemodus, Sprache der Sprachbox
Sprachnachricht-Benachrichtigung	Benachrichtigungsdienst für Nachrichten
Fax-Benachrichtigung	Benachrichtigungsdienst für Nachrichten
Profile	
Besetzt, Nicht angenommen, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Privat.	Profil für persönlichen AutoAttendant
Sensibilität	
Sicherheit und Zugriff	Abrufen Ihrer Sprach- und Faxnachrichten durch die Vermittlung, Kennwortabfrage der Sprachbox
Sichtbarkeit des Anwesenheitsstatus	Sichtbarkeit Ihres Anwesenheitsstatus für Andere
VoiceMail-Anwesenheitsstatus	Ansage Ihres Anwesenheitsstatus für externe Anrufer, Ansage Ihres Anwesenheitsstatus für bestimmte Anrufer

Werte und Einstellungen	Stichworte
Andere Benutzer können mein BLF-Layout kopieren	Andere Benutzer können die BLF-Gruppen und -Tasten kopieren Diese Option ist für bereits erstellte Profile nicht verfügbar.
myAttendant	
LAN-Nachrichten	Textbaustein für Sofortnachrichten
DuWas	MSN
Kommunikation	Anrufweiterleitungen

Weitere Informationen zu den Einstellungen der Benutzer finden Sie in den Bedienungsanleitungen der UC Clients unter den in der Tabelle aufgeführten Stichworten.

Das Kennworts für UC Clients ist standardmäßig sechsstellig. Die Länge des Kennworts kann an den eigenen Bedarf angepasst werden (6-10 Stellen). Dasselbe Zeichen darf höchstens zweimal hintereinander stehen und es sind höchstens drei aufeinanderfolgende Zeichen nacheinander zulässig. Der Benutzerkontoname (in umgedrehter sowie tatsächlicher Reihenfolge) kann nicht Teil des Kennworts sein und für die Kennwortänderung muss das alte Kennwort bekannt sein. Der Benutzer muss nach der ersten Verwendung das Standardkennwort ändern. Die maximale Anzahl fehlerhafter Anmeldeversuche beträgt fünf. Ein Administrator mit dem Profil **Advanced** kann das Kennwort eines Benutzers ändern (z.B. falls es der Benutzer vergessen hat).

Anmerkung: Vor- und Nachname eines Benutzers werden im Benutzerverzeichnis überschrieben, wenn sie über einen Wizard oder über den Experten-Modus geändert werden. Werden dagegen Vor- und Nachname eines Benutzers im Benutzerverzeichnis geändert, werden die Daten des Benutzers, wie sie über einen Wizard oder über den Expertenmodus angezeigt werden, nicht überschrieben. In diesem Fall existieren zwei unterschiedliche Benutzernamen für denselben Benutzer. Wenn der Vornamen und der Nachnamen insgesamt länger als 16 Zeichen sind, erfolgt eine Kürzung auf 16 Zeichen, damit der Name am Display angezeigt werden kann.

Teilnehmer, für die eine E-Mail-Adresse konfiguriert ist und die myPortal for Desktop nutzen, erhalten eine Begrüßungs-E-Mail mit einer Erste-Schritte-Anleitung.

Teilnehmerdaten zurücksetzen

DieEinstellungen eines Benutzers können auf Standardwerte zurückgesetzt werden. Durch das Zurücksetzen von Benutzerdaten werden alle Benutzerdaten gelöscht, einschließlich Vorname, Nachname und Anmeldename.

Unabhängig davon, ob der Vor- oder Nachname eines Benutzers über **WBM** > **Expertenmodus** > **Telephony Server** > **Teilnehmer** eingestellt wurde, führt das Zurücksetzen dieses Benutzers über UC Suite letztlich auch zur Zuweisung der Nummer, die als Durchwahl gespeichert ist, im Feld **Name**.

13.3.1.1 Wie Sie einen Benutzer von UC Suite konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.
4) Markieren Sie den gewünschten Benutzer und klicken Sie auf **Bearbeiten**.
5) Ändern Sie die Daten des Benutzers.
6) Klicken Sie auf **Speichern**. Das Fenster wird automatisch geschlossen. Es werden alle Benutzer angezeigt.
7) Wenn Sie einen weiteren Benutzer konfigurieren möchten, wiederholen Sie die Schritte 4 bis 6.

13.3.1.2 Wie Sie einen Benutzer von UC Suite zurücksetzen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.
4) Markieren Sie den gewünschten Benutzer und klicken Sie auf **Benutzer zurücksetzen**.
5) Klicken Sie auf **Speichern**. Das Fenster wird automatisch geschlossen. Es werden alle Benutzer angezeigt.
6) Wenn Sie einen weiteren Benutzer zurücksetzen möchten, wiederholen Sie die Schritte 4 bis 5.

13.3.1.3 Wie Sie einen Benutzer von UC Suite als Agenten konfigurieren (myAgent)

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.

4) Klicken Sie in die Zeile mit dem entsprechenden Benutzer.
5) Klicken Sie auf **Bearbeiten**.
6) Klicken Sie auf **Persönliche Daten** > **Benutzerebene**.
7) Wählen Sie eine der folgenden Möglichkeiten:

   Wenn der Agent dauerverfügbar sein soll, aktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

   Wenn der Agent nicht dauerverfügbar sein soll, deaktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent erhält den Zustand nicht verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.
8) Wählen Sie in der Aufklappliste **Level** die für diesen Agenten gewünschte Rolle: **Agent**, **Supervisor** oder **Adminsitrator**.
9) Klicken Sie auf **Speichern**.
10) Wenn Sie einen weiteren Benutzer als Agent konfigurieren möchten, wiederholen Sie die Schritte 4 bis 9.

13.3.1.4 Anwesenheitsstatus für einen Benutzer von UC Suite ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Erweitert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.
4) Markieren Sie den gewünschten Benutzer.
5) Klicken Sie auf das Symbol für den Anwesenheitsstatus und wählen Sie den entsprechenden Anwesenheitsstatus aus der Aufklappliste aus. Geben Sie gegebenenfalls die Uhrzeit der Rückkehr im Format `jjjj/mm/tt hh:mm`ein, z. B. `2012/12/12 12:00`.
6) Klicken Sie auf **Speichern**.
7) Wenn Sie für einen weiteren Benutzer den Anwesenheitsstatus ändern möchten, wiederholen Sie die Schritte 4 bis 6.
8) Schließen Sie das Fenster.

13.3.1.5 Kennwort für einen Benutzer von UC Suite ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.
4) Markieren Sie den entsprechenden Benutzer und klicken Sie auf **Bearbeiten** > **Persönliche Daten** > **Meine persönlichen Daten**.
5) Klicken Sie bei **Kennwort** auf **Ändern**.
6) Geben Sie unter **Neu** das neue Kennwort ein.
7) Geben Sie unter **Bestätigen** das neue Kennwort ein.
8) Klicken Sie auf **OK**. Das Fenster wird automatisch geschlossen. Es werden alle Benutzer angezeigt.
9) Wenn Sie das Kennwort eines weiteren Benutzers ändern möchten, wiederholen Sie die Schritte 4 bis 8.

Nächste Schritte

Informieren Sie den bzw. die betroffenen Benutzer über das neue Kennwort.

13.3.1.6 Kennwortlänge für Benutzer von UC Suite ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Allgemeine Einstellungen**.
5) Geben Sie die erforderliche Mindestlänge des Kennworts (6-10) für die Zukunft in das Feld **Längen** unter dem Bereich **Kennwortlänge** ein.
6) Klicken Sie auf **Speichern**.

13.3.2 Benutzer-Profile der UC Suite

Benutzer-Profilen von UC Suite speichern Einstellungen von Benutzern von UC Suite. Einem Benutzer-Profil können mehrere Benutzer (Mitglieder) zugeordnet werden. Alle Mitglieder dieses Profils haben die gleichen Einstellungen.

Jeder Benutzer kann Mitglied von höchstens einem Benutzer-Profil sein. Direkte Änderungen an den Einstellungen eines Benutzers - also nicht über das zugeordnetes Profil - löschen den Benutzer automatisch aus dem Profil.

Wenn die Zuordnung eines Benutzers zu einem Profil aufgehoben wird, behält er die durch das Profil dargestellten Einstellungen bei.

Wenn ein Benutzer bereits einem Profil zugeordnet ist, werden nur Änderungen in den gesperrten Profilelementen auf diesen Benutzer angewendet. Wenn das Sperrsymbol entsperrt ist, gelten die Änderungen nicht.

Wenn ein gesamtes Profil gelöscht wird, behalten Benutzer, die diesem Profil zugeordnet sind, ebenfalls die Profileinstellungen bei.

Folgende Werte und Einstellungen können konfiguriert werden:

Menüpunkte	Werte und Einstellungen zu
Persönliche Daten	
Eigene persönliche Daten	Sichtbarkeit von Rufnummern
Meine Einstellungen	
Darstellung	Skin-Farben, Sprache der Benutzeroberfläche
Benachrichtigungen	Popup-Fenster
Outlook-Anbindung	Automatische Erstellung von Outlook-Terminen bei Abwesenheit, Automatische Aktualisierung des Anwesenheitsstatus durch Outlook-/iCal-Termine
Abkürzungstasten	Aktivierung und Einrichtung von Tastaturkombination für den Zugriff auf verschiedene, häufig verwendete Funktionen über die Tastatur. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Verschiedenes	Automatisches Zurücksetzen des Anwesenheitsstatus, Übergabe-Methode, Aufbewahrungsdauer für Journaleinträge, Serveradresse
Anrufregeln	
Anrufweiterleitungsziele	Statusbezogene Anrufumleitung
Kommunikation	
Einstellungen für Sprachnachrichten	Aufzeichnungsmodus oder Ansagemodus, Sprache der Sprachbox
Sprachnachricht-Benachrichtigung	Benachrichtigungsdienst für Nachrichten
Fax-Benachrichtigung	Benachrichtigungsdienst für Nachrichten
Benachrichtigungen über entgangene Anrufe	Benachrichtigungsservice für entgangene Anrufe
Profile	
Profile	Profil für persönlichen AutoAttendant. Verfügbarer Status: Besetzt, Nicht angenommen, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zu Hause
Sensibilität	
Sicherheit und Zugriff	Abrufen Ihrer Sprach- und Faxnachrichten durch die Vermittlung, Kennwortabfrage der Sprachbox

Menüpunkte	Werte und Einstellungen zu
Sichtbarkeit des Anwesenheitsstatus	Sichtbarkeit Ihres Anwesenheitsstatus für Andere
VoiceMail-Anwesenheitsstatus	Ansage Ihres Anwesenheitsstatus für externe Anrufer, Ansage Ihres Anwesenheitsstatus für bestimmte Anrufer
Favoriten	
Favoriten	Favoritengruppen mit einer Liste von Kontakten, die dem Benutzer zugewiesen werden können.

Weitere Informationen zu Einstellungen der Benutzer-Profile finden Sie in den Bedienungsanleitungen der UC Clients unter den in der Tabelle aufgeführten Stichworten.

13.3.2.1 Wie Sie ein Benutzer-Profil von UC Suite hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.
4) Klicken Sie auf **Hinzufügen**.
5) Geben Sie in **Name** den gewünschten Namen für das Profil ein.
6) Klicken Sie auf **Speichern**.
7) Konfigurieren Sie die gewünschten Einstellungen des Benutzer-Profils.
8) Klicken Sie auf **Speichern** und schließen Sie das Fenster.

13.3.2.2 Wie Sie ein Benutzer-Profil von UC Suite ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Profile und deren Benutzer angezeigt.
4) Markieren Sie das gewünschte Profil.
5) Klicken Sie auf **Bearbeiten**.

6) Ändern Sie die gewünschten Werte und Einstellungen.

Anmerkung: Klicken Sie auf **Speichern** bevor Sie zu einem anderen Menüpunkt wechseln, damit Ihre Änderungen übernommen werden.

7) Klicken Sie abschließend auf **Speichern** und schließen Sie das Fenster.

13.3.2.3 Wie Sie die Benutzer-Profile von UC Suite anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.

13.3.2.4 Wie Sie Mitglieder zu einem Benutzer-Profil von UC Suite hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.
4) Markieren Sie das gewünschte Benutzer-Profil und klicken Sie auf **Benutzer zuordnen**.
5) Wählen Sie aus der Liste **Verfügbare Benutzer** die gewünschten Mitglieder aus.
6) Klicken Sie auf **<-** um diese in die in die Liste **Zugewiesene Benutzer** zu übernehmen.

   Es werden alle Teilnehmer-Profile und deren Mitglieder angezeigt.
7) Schließen Sie das Fenster.

13.3.2.5 Wie Sie Mitglieder aus einem Benutzer-Profil von UC Suite löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.
4) Markieren Sie das gewünschte Benutzer-Profil und klicken Sie auf **Benutzer zuordnen**.
5) Wählen Sie aus der Liste **Zugewiesene Benutzer** die betreffenden Mitglieder aus.
6) Klicken Sie diese auf **->** um diese in die Liste **Verfügbare Benutzer** zu übernehmen.

   Es werden alle Teilnehmer-Profile und deren Mitglieder angezeigt.
7) Schließen Sie das Fenster.

13.3.2.6 Wie Sie ein Benutzer-Profil von UC Suite löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.
4) Markieren Sie das gewünschte Benutzer-Profil.
5) Klicken Sie auf **Entfernen**.
6) Bestätigen Sie mit **OK**. Es werden alle Teilnehmer-Profile und deren Mitglieder angezeigt.
7) Schließen Sie das Fenster.

13.4 Anwesenheitsstatus und CallMe-Dienst

Anwesenheitsstatus und CallMe-Dienst zeigen und optimieren die Erreichbarkeit von Teilnehmern. Der Anwesenheitsstatus ermöglicht eine einfache statusbezogene Anrufumleitung sowie eine mit myPortal for Desktop bzw. myPortal for Outlook flexibel konfigurierbare regelbasierte Anrufumleitung.

13.4.1 Anwesenheitsstatus (Präsenz)

Der Anwesenheitsstatus (Präsenz, Presence) informiert in der Favoritenliste, im internen Verzeichnis, im virtuellen Konferenzraum und durch Ansagen der Sprachbox über die Verfügbarkeit interner Teilnehmer (auch mobile Teilnehmer). Darüber hinaus steuert der Anwesenheitsstatus die Erreichbarkeit interner Teilnehmer mit der statusbezogenen Anrufumleitung, der regelbasierten Anrufumleitung und dem persönlichen AutoAttendant.

Sie können als Teilnehmer Ihren Anwesenheitsstatus in myPortal for Desktop, myPortal for Outlook oder über die Menüsteuerung der Sprachbox ändern. Durch Deaktivieren einer Anrufumleitung am Telefon kehren Sie zum

Anwesenheitsstatus **Büro** zurück. Bei jeder Änderung des Anwesenheitsstatus außer für **Büro** und **CallMe** können Sie den Zeitpunkt der geplanten Rückkehr zu **Büro** bzw. **CallMe** festlegen.

Als Teilnehmer können Sie folgende Status auswählen:

- **Büro**
- **Besprechung**
- **Krank**
- **Pause**
- **Außer Haus**
- **Urlaub**
- **Mittagspause**
- **Zu Hause**
- **Anrufschutz**

Anmerkung: Der Systemadministrator kann die Sichtbarkeit des Status „krank“ innerhalb der Systemadministration ein- und ausschalten. Siehe OpenScape Business UC Suite > Server

---

Umleitung zur Sprachbox

Wenn der Anwesenheitsstatus eines Teilnehmers nicht **Büro** oder **CallMe** ist, leitet das Kommunikationssystem Anrufe für ihn standardmäßig zur Sprachbox um und informiert den Anrufer durch statusbezogene Ansagen über die Art der Abwesenheit und den geplanten Zeitpunkt der Rückkehr.

Informationstext

Sie können zu Ihrem aktuellen Anwesenheitsstatus einen beliebigen Informationstext eingeben, z. B. bei einer Besprechung: "Bin in Raum Nr. ...". Der Informationstext wird in der Favoritenliste, im internen Verzeichnis und im virtuellen Konferenzraum angezeigt. Der Informationstext wird bei Änderung Ihres Anwesenheitsstatus gelöscht.

Automatisches Zurücksetzen des Anwesenheitsstatus

Sie können als Teilnehmer zum geplanten Ende-Zeitpunkt Ihrer Abwesenheit den Anwesenheitsstatus automatisch auf **Büro** zurücksetzen lassen. Anderenfalls verlängert das System den aktuellen Anwesenheitsstatus in 15-Minuten-Schritten bis Sie ihn selbst ändern.

Sichtbarkeit Ihres Anwesenheitsstatus

Sie können als Teilnehmer für jeden Teilnehmer des internen Verzeichnisses festlegen, ob dieser Ihren Anwesenheitsstatus abweichend von **Büro** und **CallMe** sowie den geplanten Zeitpunkt Ihrer Rückkehr und von Ihnen eventuell eingegebenen Informationstext sehen kann.

Anmerkung: Sichtbarkeitseinstellungen werden nicht auf myAttendant-Benutzer angewendet, da diese immer den Anwesenheitsstatus anderer Benutzer sehen können.

Automatische Aktualisierung des Anwesenheitsstatus durch Outlook-/ iCal-Termine

Sie können als Teilnehmer Ihren Anwesenheitsstatus durch Termine (nicht jedoch abgesagte oder lediglich vorgeschlagene) mit bestimmten Schlüsselwörtern im Betreff automatisch steuern. Sie können zwischen folgenden Kalendern wählen:

- Exchange-Kalender (auf dem Microsoft Exchange Server)

  Die automatische Aktualisierung des Anwesenheitsstatus durch Outlook-Termine erfolgt unabhängig davon, ob Ihr PC in Betrieb ist. Für diese Funktion muss der Administrator die Exchange-Kalender-Integration konfigurieren.

  Anmerkung: Details zur Nutzung der verschiedenen Microsoft Exchange Server-Versionen finden Sie im Unify Experts Wiki unter: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

- Outlook-Kalender

  Die automatische Aktualisierung des Anwesenheitsstatus durch Outlook-Termine erfordert, dass myPortal for Desktop oder myPortal for Outlook auf Ihrem PC gestartet ist.
- iCal-Kalender (myPortal for Desktop)

Sie können die folgenden Schlüsselwörter verwenden:

- **Besprechung**
- **Krank**
- **Pause**
- **Außer Haus**
- **Urlaub**
- **Mittagspause**
- **Zu Hause**

Die Schlüsselwörter hängen von der eingestellten Sprache der Benutzeroberfläche ab. Die Schlüsselwörter dürfen im Betreff an beliebiger Stelle stehen. Wenn der Betreff mehrere dieser Schlüsselwörter enthält, wird nur das erste wirksam. Wenn diese Funktion aktiviert ist, ändert sich der Anwesenheitsstatus zur Beginn- und Endzeit des betreffenden Termins automatisch. Die Prüfung des Kalenders auf Termine erfolgt in Intervallen von 30 s.

Anmerkung: Wenn Sie diese Funktion aktivieren, beachten Sie bitte, dass beliebige Termine mit entsprechenden Schlüsselwörtern im Betreff zu unerwünschten Änderungen Ihres Anwesenheitsstatus führen können. Ändern Sie gegebenenfalls den Betreff.

Anmerkung: Der Anwesenheitsstatus "krank" ist je nach Systemeinstellung des Administrators möglicherweise nicht verfügbar.

Automatische Erstellung von Outlook-Terminen bei Abwesenheit (Windows)

Sie können als Teilnehmer für Ihre Abwesenheit automatisch entsprechende Outlook-Termine durch Änderung Ihres Anwesenheitsstatus erzeugen lassen. Der Betreff des entsprechenden Outlook-Termins besteht aus dem Anwesenheitsstatus und dem Text „(Auto)“, z. B. „Besprechung (Auto)“. Beginn- und Endezeit des betreffenden Termins entsprechen Ihren Angaben in myPortal for Desktop oder myPortal for Outlook. Die Ende-Zeit des Outlook-Termins bleibt bei einer eventuell verspäteten Rückkehr unverändert. Sie können festlegen, ob die Outlook-Termine in der lokalen PST-Datei oder auf dem Exchange-Server gespeichert werden. Im Fall der lokalen PST-Datei muss Ihr Outlook zum Erstellen der Outlook-Termine geöffnet sein. Im Fall des Exchange-Servers werden die Outlook-Termine erstellt, unabhängig davon, ob Ihr Outlook geöffnet ist. Für diese Funktion muss der Administrator die Exchange-Kalender-Integration konfigurieren.

Anmerkung: Details zur Nutzung der verschiedenen Microsoft Exchange Server-Versionen finden Sie im Unify Experts Wiki unter: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

Pop-up-Fenster bei Änderung des Anwesenheitsstatus

Sie können als Teilnehmer Änderungen Ihres Anwesenheitsstatus durch Popup-Fenster anzeigen lassen.

13.4.2 CallMe-Dienst

Mit dem CallMe-Dienst kann ein Teilnehmer ein beliebiges Telefon an einem alternativen Arbeitsplatz als CallMe-Ziel festlegen, an dem er unter seiner internen Telefonnummer erreichbar ist. Der Teilnehmer kann myPortal for Desktop oder myPortal for Outlook an seinem alternativen Arbeitsplatz wie im Büro nutzen und damit auch gehende Anrufe vom CallMe-Ziel tätigen.

Ankommende Anrufe

Ankommende Anrufe bei der internen Telefonnummer werden zum CallMe-Ziel umgeleitet. Beim Anrufer wird die interne Telefonnummer des gerufenen Teilnehmers angezeigt. Nicht angenommene Anrufe werden nach 60 Sekunden an die Sprachbox weitergeleitet.

Anmerkung: Falls für das gesteuerte Endgerät das Leistungsmerkmal sofortige Rufumleitung aktiviert ist, empfängt der Application Launcher keine anrufbezogenen Ereignisse vom Kommunikationsserver und kann deshalb auch keine Applikationsanreize erzeugen. Gleiches gilt auch für den Fall, das das UC Suite Leistungsmerkmal CallMe aktiviert ist.

Gehende Anrufe

Bei gehenden Anrufen mit myPortal for Desktop oder myPortal for Outlook baut das Kommunikationssystem zwei Verbindungen auf. Zuerst ruft das

Kommunikationssystem den Teilnehmer am CallMe-Ziel an. Wenn er den Anruf annimmt, ruft das Kommunikationssystem das gewünschte Ziel und verbindet ihn mit diesem. Am Ziel wird die interne Telefonnummer des Anrufenden angezeigt (One Number Service).

Anwesenheitsstatus

Bei aktiviertem CallMe-Dienst erscheint im Display des betreffenden Telefons "`CallMe aktiv`" (nicht für analoge Telefone und DECT-Telefone). Andere Teilnehmer sehen den Anwesenheitsstatus **Büro**.

Aktivierung

Als Teilnehmer können Sie den CallMe-Dienst manuell aktivieren. Außerdem wird der CallMe-Dienst durch Automatisches Zurücksetzen des Anwesenheitsstatus nach Abwesenheit erneut aktiviert, wenn er zuvor aktiv war. Folgende Arten von CallMe-Zielen werden nicht unterstützt:

- Gruppe
- Umgeleitetes Telefon

Anzeige des CallMe-Ziels in Favoritenliste

Als Teilnehmer können Sie an Stelle Ihrer Rufnummer die Rufnummer Ihres CallMe-Ziels in der Favoritenliste anderer Teilnehmer anzeigen lassen.

Deaktivierung

Der CallMe-Dienst bleibt bis zur Änderung Ihres Anwesenheitsstatus aktiv.

Anmerkung: Bei Einwahl oder Anrufen in einer offenen Konferenz sollte die CallMe-Funktion nicht verwendet werden.

13.4.3 Statusbezogene Anrufumleitung

Mit der statusbezogenen Anrufumleitung kann der Teilnehmer Anrufer auf Basis seines Anwesenheitsstatus zu einer seiner zusätzlichen Rufnummern oder zur Sprachbox umleiten.

Sie können als Teilnehmer die statusbezogene Anrufumleitung für jeden Anwesenheitsstatus außer **Büro**, **CallMe** und **Anrufschutz** konfigurieren. Wenn Sie Ihren Anwesenheitsstatus ändern, aktiviert das Kommunikationssystem die Anrufumleitung zu dem hierfür von Ihnen festgelegten Ziel, Z.B. wenn Sie außer Haus sind zu Ihrem Mobiltelefon und während Ihres Urlaubs zu Ihrer Vertretung.

13.4.4 Regelbasierte Anrufumleitung

Mit der regelbasierten Anrufumleitung kann der Teilnehmer Anrufer auf Basis vielfältiger Bedingungen oder Ausnahmen noch flexibler umleiten als mit der statusbezogenen Anrufumleitung, z. B. Anrufe von unbekannten Kontakten an seine Sprachbox.

Darüber hinaus unterstützt die regelbasierte Anrufumleitung:

- beliebige Ziele

- Anwesenheitsstatus (**Büro**, **Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zu Hause)**

Anmerkung: CallMe und **DND** gelten nicht für die regelbasierte Anrufumleitung.

Sie können als Teilnehmer mit dem Regelassistenten Regeln festlegen und jederzeit aktivieren oder deaktivieren. Eine Regel ist nur aktiv, wenn Ihr Telefon nicht umgeleitet ist. Eine statusbezogene Anrufumleitung (außer zur Sprachbox) setzt die regelbasierte Anrufumleitung außer Kraft.

Wenn eine Regel für Anrufumleitung aktiv ist, zeigt das Display Ihres Telefons **"Regel aktiv"** an.

Bei einem ankommenden Anruf prüft das Kommunikationssytem die Anwendbarkeit der aktiven Regeln entsprechend ihrer Reihenfolge im Regelassistenten. Nur die erste anwendbare Regel wird ausgeführt. In diesem Fall klingelt Ihr Telefon ein Mal und anschließend leitet das Kommunikationssystem den Anruf zum festgelegten Ziel um.

Sie können in einer Regel mehrere Arten von Bedingungen und Ausnahmen (außer …) definieren. Dabei können Sie keine Bedingung zusammen mit der artverwandten Ausnahme definieren. So ist es z. B. nicht möglich eine Bedingung der Art "an bestimmten Wochentagen" zusammen mit einer Ausnahme der Art "außer an bestimmten Wochentagen" festzulegen.

Arten von Bedingungen und Ausnahmen

- (außer) bei bestimmtem Anwesenheitsstatus
- (außer) von bestimmten Personen (im internen Verzeichnis, im externen Verzeichnis, im persönlichen Verzeichnis oder von beliebiger Rufnummer)
- (außer) an Sie übergeben von bestimmten Personen (im internen Verzeichnis, im externen Verzeichnis, im persönlichen Verzeichnis oder von beliebiger Rufnummer)
- (außer) von einem bestimmten Typ, d. h., **intern**, **extern** oder **Unbekannter Kontakt**
- (außer) an einem bestimmten Datum (auch an mehreren)
- (außer) an bestimmten Wochentagen
- (außer) zwischen einem bestimmten Start- und Endedatum
- (außer) zwischen einer bestimmten Start- und Ende-Uhrzeit

13.5 Verzeichnisse und Journal

Verzeichnisse, die Favoritenliste und das Journal organisieren Kontakte und Anrufe.

13.5.1 Verzeichnisse

Verzeichnisse organisieren die Kontakte der Teilnehmer. Teilnehmer können mit UC Suite Clients sowie mit Systemtelefonen mit Display auf die Kontakte zugreifen.

Das System stellt folgende Verzeichnisse mit den folgenden Funktionen und folgender Prioritätsreihenfolge für die Rufnummernsuche bereit

(Nummernsuche wird nur für externe Anrufe unterstützt, und für den Fall, dass Amt bzw. ITSP den Namen nicht bereitstellen):

Verzeichnis	myPortal for Desktop, my Attendant, myAgent, Fax Printer	myPortal for Outlook	Systemtelefon mit Display
Outlook-Kontakte Mac OS-Kontakte (myPortal for Desktop)	Bei Bedarf kann der Teilnehmer die Outlook-/ Mac OS-Kontakte beim Start von myPortal for Desktop auf Windows importieren.	Enthält die persönlichen Outlook Kontakte eines Teilnehmers. Nur der Teilnehmer selbst hat schreibenden Zugriff auf diese Daten.	Enthält die persönlichen Outlook Kontakte eines Teilnehmers. Nur der Teilnehmer selbst hat schreibenden Zugriff auf diese Daten.
Persönliches Verzeichnis	Der Teilnehmer kann hier entweder beim Start von myPortal for Desktop die Outlook-Kontakte bzw. Mac OS-Kontakte importieren oder persönliche Kontakte manuell pflegen. Die Änderung importierter Kontakte ist nicht möglich.	-	Über den persönlichen Assistenten importierte Outlook-Kontakte.
Internes Verzeichnis	Das interne Verzeichnis von UC Smart bietet mit UC Suite zusätzliche Leistungsmerkmale. Er beinhaltet: • Alle internen Teilnehmer • Gruppen, für die das Anzeigen im System aktiviert ist • Zusätzliche Telefonnummern, wenn der Teilnehmer diese Informationen für andere interne Teilnehmer sichtbar gemacht hat Interne Teilnehmer (mit Systemtelefon) werden mit Anwesenheitsstatus dargestellt und können per Instant Messaging kontaktieren werden. Voraussetzung für die Anzeige des Anwesenheitsstatus eines Teilnehmers ist, dass der betreffende Teilnehmer dies zulässt. Gegebenenfalls wird ein geplanter Zeitpunkt der Rückkehr angezeigt. Zusätzlich wird ein vom Teilnehmer eventuell eingegebener Informationstext angezeigt. Ein Teilnehmer hat nur Lesezugriff auf dieses Verzeichnis. Das interne Verzeichnis enthält das Systemverzeichnis. Suchvorgänge im internen Verzeichnis umfassen aber keine Ergebnisse aus dem Systemverzeichnis, sondern nur Einträge des internen Verzeichnisses.		Enthält alle internen Teilnehmer und Gruppen, für die das Anzeigen im System aktiviert ist.
Externes Verzeichnis	Enthält Kontakte aus einem Unternehmensverzeichnis und ist durch den Administrator zu konfigurieren. Ein Teilnehmer hat nur lesenden Zugriff auf dieses Verzeichnis.		-

Verzeichnis	myPortal for Desktop, my Attendant, myAgent, Fax Printer	myPortal for Outlook	Systemtelefon mit Display
Öffentlicher Exchange-Ordner (nicht nutzbar mit Office 365)	Enthält die Kontakte des öffentlichen Exchange-Ordners, falls vom Administrator konfiguriert. Diese werden im Externen Verzeichnis angezeigt. Details zur Nutzung der verschiedenen Microsoft Exchange Server-Versionen finden Sie im Unify Experts Wiki unter: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.		-
Externes Offline-Verzeichnis (LDAP)	Enthält Kontakte aus dem LDAP-Unternehmensverzeichnis und ist durch den Administrator zu konfigurieren. Das Externe Offline-Verzeichnis kann nur bei der Suche genutzt werden. Der Administrator kann die Anzeige des Externen Offline-Verzeichnisses für Systemtelefone aktivieren und deaktivieren.		
System-Verzeichnis	Enthält alle Systemnummern, UC- und Nicht-UC-Benutzer. Nicht-UC-Benutzer sind Teilnehmer ohne UC-Lizenzen und virtuelle Teilnehmer wie Fax, AutoAttendant. Das Systemverzeichnis gilt nicht für den Faxdrucker		Enthält alle internen Teilnehmer und alle zentralen Kurzwahlnummern. Der Administrator kann die Anzeige eines Teilnehmers im Systemtelefonbuch aktivieren und deaktivieren.

Anmerkung: Telefonnummern, die in den Benutzereinstellungen und allen Verzeichnissen (intern, extern, persönlich, Outlook, Exchange) gespeichert sind, sollten im kanonischen Format eingegeben werden, um sowohl von UC als auch vom Gerät aus erreichbar zu sein.

Der Zugangscode darf nicht in der Nummer enthalten sein.

Anmerkung: Beim Hinzufügen oder Entfernen eines UC-Kontakts kann es aufgrund der verwendeten Caching-Mechanismen mehrere Minuten**(und** bis zu 30 Min.) dauern, bis die Änderungen auf allen Clients und Geräten übernommen werden. Alternativ kann auch ein Neustart des Systems durchgeführt werden, damit die Änderungen **sofort** wirksam werden.

Einfache Suche

Sie können als Teilnehmer in den Verzeichnissen nach **Vorname**, **Nachname** oder einer Rufnummer suchen. Die Verzeichnisse werden in der Reihenfolge wie in der Tabelle oben durchsucht. Die Suche ist sowohl nach ganzen Wörtern als auch mit unvollständigem Suchbegriff möglich, z. B. Teil einer Rufnummer. Die eingestellten Suchoptionen bleiben bis auf Weiteres erhalten. Alle verwendeten Suchbegriffe werden gespeichert. Sie können die Liste der verwendeten Suchbegriffe löschen.

Erweiterte Suche

Sie können wahlweise in den Feldern **Titel**, **Vorname**, **Nachname**, **Firma**, **Durchwahl**, **Firmen-Rufnr.**, **Geschäftlich 1**, **Geschäftlich 2**, **Privat 1**, **Privat 2**, **Mobilrufnummer** und **E-Mail** suchen und die maximale Anzahl von Treffern begrenzen. Die moderne Oberfläche von myPortal for Desktop unterstützt die erweiterte Suche nicht. In einem Gerät werden nur **Geschäftlich 1**, **Privat 1**, **Mobilrufnummer** unterstützt.

Sortierung

Die Kontakte eines Verzeichnisses von myPortal for Desktop und myPortal for Outlook können nach einer Spalte alphanumerisch auf- oder absteigend sortiert werden. Die moderne Oberfläche von myPortal for Desktop unterstützt die Sortierung nicht.

13.5.1.1 Verzeichnisse für Systemtelefone konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Sie können wählen, welche Verzeichnisse an Systemtelefonen mit Display zur Verfügung stehen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **Display**.
4) Wählen Sie in der Aufklappliste **Telefonbuch** eine der folgenden Möglichkeiten:
   - Wenn jedes persönliche/interne/externe/Netzwerk-Verzeichnis als auch das LDAP-Verzeichnis zur Verfügung stehen soll, wählen Sie **Alle**.
   - Wenn nur das persönliche/interne/externe/Netzwerk-Verzeichnis zur Verfügung stehen soll, wählen Sie **Intern**.
   - Wenn nur das LDAP-Verzeichnis zur Verfügung stehen soll, wählen Sie **LDAP**.
   - Wenn kein Verzeichnis zur Verfügung stehen soll, wählen Sie **Nein**.

   Anmerkung: Der Benutzer kann die Suchanfragen aktivieren, die als Anforderungen an das Unified-Verzeichnis behandelt werden sollen, indem **Internes Telefonbuch über Unified Directory** ausgewählt wird. Wenn das Flag deaktiviert ist und kein Zugriff auf das Unified Directory besteht, ist die Listenansicht im Telefonbuchmenü für das OpenScape Desk Phone CP 200/205/210 nicht verfügbar.
5) Klicken Sie auf **Übernehmen**.

Nächste Schritte

Wenn Sie **Alle** oder **LDAP** gewählt haben, sorgen Sie dafür, dass ein entsprechendes LDAP-Verzeichnis (z.B. Open Directory Service) für Systemtelefone zur Verfügung steht.

13.5.2 Internes Verzeichnis

Das interne Verzeichnis enthält die Kontaktdetails der internen Teilnehmer des Kommunikationssystems. UC Suite Clients haben Zugriff auf das Systemtelefonbuch.

Als Administrator haben Sie uneingeschränkten Zugriff auf alle Daten im internen Verzeichnis. Als Teilnehmer können Sie aus dem internen Verzeichnis wählen.

Der Administrator kann die Anzeige für alle analogen Teilnehmer oder für analoge Teilnehmer ohne Namen deaktivieren. Teilnehmer deren Name mit - beginnt werden in letzterem Fall nicht angezeigt.

13.5.2.1 Wie Sie die Anzeige analoger Teilnehmer im internen Verzeichnis aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie im Menübaum auf **Server**.
4) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.
5) Wählen Sie im Bereich **Analoge Nebenstellen** in der Aufklappliste **Modus Analoger Teilnehmer** eine der folgenden Möglichkeiten:
   - Wenn alle analogen Teilnehmer im internen Verzeichnis angezeigt werden sollen, wählen Sie **Alle anzeigen**.
   - Wenn nur analoge Teilnehmer mit einem Namen im internen Verzeichnis angezeigt werden sollen, wählen Sie **Nur Benannte anzeigen**.

     Anmerkung: Analoge Teilnehmer deren Name mit - beginnt werden bei dieser Einstellung nicht angezeigt.

   - Wenn keine analogen Teilnehmer im internen Verzeichnis angezeigt werden sollen, wählen Sie **Nicht angezeigt**.
6) Klicken Sie auf **Speichern**.

13.5.2.2 Wie Sie die Suche im internen Verzeichnis aktivieren oder deaktivieren

Bei Wahl nach Name können Sie die Suche auf das internen Verzeichnis einschränken oder alle Verzeichnisse in der Netzwerkumgebung durchsuchen. Standardmäßig wird nur das im internen Verzeichnis durchsucht.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie im Menübaum auf **Server**.
4) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.
5) Um die Suche nur für das interne Verzeichnis zu aktivieren, aktivieren Sie das Kontrollkästchen **Nach Name wählen – Nur lokale Nebenstelle suchen** unter dem Bereich **Verzeichnisserver**.

   Anmerkung: Das Kontrollkästchen **Nach Name wählen – Nur lokale Nebenstelle suchen** ist standardmäßig aktiviert.

   Bei Wahl nach Name wird jetzt nur das interne Verzeichnis durchsucht. Wenn die lokale Nebenstelle gefunden wurde, wird der Name des Empfängers angezeigt, sofern dieser zuvor erfasst wurde.
6) Um die Suche nur für das interne Verzeichnis zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Nach Name wählen – Nur lokale Nebenstelle suchen** unter dem Bereich **Verzeichnisserver**.

   Bei Wahl nach Name werden jetzt alle Verzeichnisse in der Netzwerkumgebung durchsucht.

13.5.3 Externes Verzeichnis

Das externe Verzeichnis enthält Kontakte von außerhalb des Kommunikationssystems.

Die Daten des externen Verzeichnis stehen allen Teilnehmern in allen UC Suite Clients und über Telefone mit Display zur Verfügung. Teilnehmer können aus dem externen Verzeichnis wählen. Benutzer der UC Suite Clients myAttendant und myAgent können Daten im externen Verzeichnis bearbeiten.

Import einer CSV-Datei

Als Administrator können Sie Kontakte in einer CSV-Datei in UTF-8-Kodierung vom lokalen Dateisystem oder von einer Netzwerkfreigabe in das externe Verzeichnis importieren.

Eine Kopfzeile in der CSV-Datei ermöglicht die Zuordnung der Feldnamen der CSV-Datei zu Feldern im System. Die CSV-Datei kann z.B. wie folgt aufgebaut sein:

- Kopfzeile:

  "Kunden-ID","Nachname","Vorname","Firmentelefonnummer","Firmenname"
- Datenzeile:

  "987654","Dubios","Natalie","+498977712345","Company"

Sie können beim Import Daten der CSV-Datei folgenden Feldern im System zuordnen:

- Kunden-ID
- Anrede
- Vorname
- Nachname
- Firma
- Geschäftlich
- Geschäftlich 2
- Mobilnr.
- Zu Hause
- Faxnr.
- E-Mail
- Ort

Anmerkung: Der Name des Kontakts wird in der Anrufliste nur angezeigt, wenn Sie sowohl das Feld Vorname als auch das Feld Nachname ausfüllen.

Nach Bearbeitung der CSV-Vorlage muss die Datei im UTF-8 Format gespeichert werden, um den korrekten Import von eventuell vorhandenen Sonderzeichen zu gewährleisten.

Wenn Sie beim Import Daten überschreiben möchten, muss die entsprechende **Kunden-ID** identisch sein.

Anmerkung: Eine CSV-Vorlage sowie eine Beschreibung der erforderlichen Syntax für den Import von Daten für das Externe Verzeichnis finden Sie unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**.

13.5.3.1 CSV-Datei vom lokalen Dateisystem in das externe Verzeichnis importieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Eine geeignete CSV-Datei in UTF-8-Kodierung mit Daten für das externe Verzeichnis liegt im lokalen Dateisystem vor.

Für die Länge der Felder in den CSV-Vorlagen gelten bestimmte Beschränkungen. Diese Längenbeschränkungen sind im Folgenden aufgeführt:

- customer_business Zeichen variierend(50)
- customer_business2 Zeichen variierend(50)
- customer_home Zeichen variierend(50)
- customer_mobile Zeichen variierend(50)

- customer_title Zeichen variierend(20)
- customer_firstname Zeichen variierend(50)
- customer_surname Zeichen variierend(50)
- customer_company Zeichen variierend(255)
- customer_id Zeichen variierend (255)
- customer_xmppid Zeichen variierend (256)
- customer_fax Zeichen variierend (50)
- customer_email Zeichen variierend (255)
- customer_city Zeichen variierend (255)
- customer_street_address Zeichen variierend (2048)
- customer_import_source Zeichen variierend (256)

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Externes Verzeichnis** zu starten.

4) Klicken Sie auf die Registerkarte **Externes Verzeichnis importieren**.

5) Wählen Sie eine der folgenden Optionen:

- Wenn Sie die CSV-Datei vom lokalen Dateisystem laden möchten, aktivieren Sie das Optionsfeld **Lokale Datei** und navigieren im Bereich **Datei-Upload** zu der CSV-Datei.
- Wenn Sie die CSV-Datei von einer Netzwerkfreigabe laden möchten, aktivieren Sie das Optionsfeld **Öffentlicher Windows-Ordner** und geben Sie im Bereich **Öffentlicher Windows-Ordner** die Daten für den Zugang zu der Netzwerkfreigabe ein (Name der CSV-Datei, Domänen-Name sowie Benutzername und Kennwort für die Freigabe).

  Die Richtigkeit Ihrer Eingaben können Sie über **Test** verifizieren.

6) Klicken Sie im Bereich **Datei-Upload** auf **Datei auswählen** und wählen Sie die gewünschte Datei aus.

7) Geben Sie im Feld **Kopfzeilen** die Anzahl der Kopfzeilen der CSV-Datei ein.

8) Geben Sie das in der CSV-Datei verwendete **Feldtrennzeichen** ein.

9) Wählen Sie eine der folgenden Optionen:

- Wenn Sie die bestehenden Daten des externen Verzeichnisses löschen möchten, aktivieren Sie das Kontrollkästchen **Daten vor dem Import löschen**.
- Wenn Sie die bestehenden Daten des externen Verzeichnisses nicht löschen möchten, deaktivieren Sie das Kontrollkästchen **Daten vor dem Import löschen**.

Anmerkung: Die Flagge **Daten vor dem Import löschen** entfernt Datensätze nicht, wenn diese bereits in anderen Funktionen wie etwa einem VIP-Anrufer usw. verwendet werden.

Anmerkung: Die Flagge **Daten vor dem Import entfernen** löscht nur Daten, die aus dem CSV-Import stammen. Manuell importierte Daten werden nicht

gelöscht, um unerwarteten Datenverlust zu vermeiden. Die einzige Weise, manuell eingegebene Daten zu löschen, besteht darin, sie manuell zu löschen.

10) Wählen Sie im Bereich **Doppelte Kunden-ID**, wie das System beim Importversuch von Daten mit bereits vorhandener Kunden-ID reagieren soll:

- Wenn Sie vorhandene Kontakte mit den Daten aus der CSV-Datei überschreiben möchten, wählen Sie **Kontakte aktualisieren**.

  Anmerkung: CustomerID ist die Kennung, der bestimmt, ob zwei Datensätze Duplikate sind. Es wird also davon ausgegangen, dass importierte Datensätze mit einer bestehenden CustomerID sich auf einen bestehenden Kunden beziehen und aktualisiert werden. Die Flagge **Bestehenden Kunden aktualisieren** funktioniert nur, wenn die Kunden-ID beim Import zugewiesen wurde. Es wird dringend empfohlen, sich auf die mitgelieferte Vorlage zu verlassen und die Daten auf dieser Grundlage anzupassen, ohne dabei eindeutige Kennungen wegzulassen.

- Wenn Sie vorhandene Kontakte beibehalten möchten, wählen Sie **Import des aktuellen Datensatzes anhalten**.

11) Klicken Sie auf **Weiter**.

12) Wählen Sie in den Dropdown-Menüs der Reihe nach die Zuordnung der Felder der CSV-Datei zu den entsprechenden Feldern im System aus. Wenn die Felder nicht vorhanden sind oder Sie die Daten nicht importieren möchten, klicken Sie auf die leere Option.

13) Klicken Sie auf **Weiter**.

14) Klicken Sie auf **Importieren**. Schließen Sie dieses Fenster nicht, solange die Daten noch importiert werden. Nach Beenden des Imports wird die Anzahl der importierten Datensätze angezeigt.

13.5.3.2 Zugriff auf eine externe Datenbank für das externe Verzeichnis hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Daten für den Zugriff auf die externe Datenbank liegen vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Externes Verzeichnis** zu starten.

4) Klicken Sie auf die Registerkarte **Externes Verzeichnis importieren**.

5) Klicken Sie im Bereich **Datei-Upload** auf **Datei auswählen** und wählen Sie die gewünschte Datei aus.

13.5.3.3 CSV-Datei aus dem externen Verzeichnis exportieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf die Registerkarte **Externes Verzeichnis exportieren**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie eine CSV-Datei in das lokale Dateisystem exportieren möchten, wählen Sie das Optionsfeld **Lokale Datei** aus und klicken Sie auf die Schaltfläche **Start**.
   - Wenn Sie in ein öffentliches Windows-Verzeichnis exportieren möchten, wählen Sie das Optionsfeld **Öffentliches Windows-Verzeichnis**. Geben Sie die gewünschten Werte in die folgenden Felder ein:

     - **Dateiname**

     - **Benutzername**

     - **Domäne**

     - **Kennwort**

     Klicken Sie auf die Schaltfläche **Start**.

13.5.4 Externes Offline-Verzeichnis (LDAP)

Das Externe Offline-Verzeichnis (LDAP) enthält Kontakte von einem LDAP-Server für myPortal for Desktop, myAgent, Fax Printer, myPortal for Outlook und für Systemtelefone mit Display.

Das System unterstützt LDAP Version 2 mit Authentifizierung.

LDAP (Lightweight Directory Access Protocol) ist ein TCP/IP-basiertes Directory-Zugangsprotokoll für den Zugriff auf Netzwerk-Verzeichnisdienste. LDAP hat ein weltweit eindeutiges Format, in dem alle Namen darstellbar sind. Es bietet unterschiedliche Layouts und eine eindeutige Zuordnung zwischen Namen und ihrer internen Repräsentation. Der Administrator definiert zusammen mit dem IT-Administrator des Kunden beim Projektgespräch diese Daten. LDAP kann unter den Betriebssystemen MS Windows und Linux verwendet werden.

In einer Microsoft-Umgebung ist der Active Directory Server (ADS) bzw. der Exchange Server auch gleichzeitig der LDAP-Server. Unter Microsoft Windows können die Benutzerdaten z.B. mit der Applikation Active Directory oder ESTOS Metadir verwaltet werden. Die Verwaltung dieser Daten erledigt im allgemeinen der IT-Administrator des Kunden.

Unter Linux können die Benutzerdaten z.B. mit OpenLDAP verwaltet werden.

Ein LDAP-Browser (z.B. Freeware von Softerra) vereinfacht die Einrichtung eines LDAP-Verzeichnisdienstes.

Rufnummern auf dem LDAP-Server dürfen als Trennzeichen nur "-" und Leerzeichen enthalten. Andere Trennzeichen kann das System nicht ausfiltern.

Bei der Konfiguration eines Externen Offline-Verzeichnisses können Sie als Administrator das Mapping der Felder an die Namen des verwendeten LDAP-Servers anpassen. Gelöschte Felder werden bei der Suche nach Namen mittels Rufnummer ignoriert. Die Suche erfolgt immer mit den letzten 4 Stellen der Rufnummer mit vorangestellter Wildcard. Sie können die Suche nach Namen mittels Rufnummer bei kommenden Gesprächen deaktivieren.

Sollte der standardmäßig verwendet Port 389 belegt sein, ist ein anderer zu konfigurieren.

Anmerkung: Weitere Informationen finden Sie im Internet unter: `http://wiki.unify.com`.

Die Daten des externen Verzeichnis stehen Teilnehmern in myPortal for Desktop, myAttendant, Fax Printer und myPortal for Outlook bei der Suche zur Verfügung.

Systemtelefone mit Display

Als Teilnehmer können Sie im Menü zwischen dem internen Verzeichnis und dem LDAP-Verzeichnis wählen, sofern diese für Systemtelefone konfiguriert sind. Das LDAP-Verzeichnis unterstützt die Suche in den entsprechenden Kontakten und den anschließenden Anruf eines Kontakts.

Die vom LDAP-Server bereitgestellte Namensinformation wird nicht für die Displayanzeige im Ruf- oder Gesprächszustand verwendet. Die Rufnummern kommender Rufe werden ebenfalls nicht durch die vom LDAP-Server bereitgestellten Namensinformationen ersetzt (wie beispielsweise bei der Ersetzung von Rufnummern durch KWZ-Namen).

Ein Teilnehmer des Systems ist nur dann aus dem LDAP-Verzeichnis erreichbar, wenn für ihn eine Durchwahlrufnummer konfiguriert wurde und diese mit dem Eintrag in der LDAP-Datenbank übereinstimmt. Vom LDAP-Server bereitgestellte Rufnummern können nur dann netzintern geroutet werden, wenn interne Rufnummer und Durchwahlrufnummer identisch sind.

13.5.4.1 Wie Sie ein externes Offline-Verzeichnis (LDAP) für PC-Clients hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Ihnen liegen die Zugangsdaten für den LDAP-Server vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf die Registerkarte **Konfiguration externe Anbieter**.

4) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie im Journal für externe ankommende Anrufe die Auflösung von Rufnummern in Namen aktivieren möchten, aktivieren Sie das Kontrollkästchen **Suchen nach Rufnummer**.
   - Wenn Sie im Journal für externe ankommende Anrufe die Auflösung von Rufnummern in Namen deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Suchen nach Rufnummer**.
5) Klicken Sie auf **Hinzufügen**.
6) Geben Sie die Zugangsdaten des LDAP-Servers ein:
   a) Geben Sie in **Name** einen Namen für dieses externe Offline-Verzeichnis ein.
   b) Geben Sie in **Server** den Namen oder die IP-Adresse des LDAP-Servers ein.
   c) Geben Sie in **Port** die Portnummer des LDAP-Servers ein.
   d) Geben Sie in **LDAP Basis-DN** den LDAP Base Distinguished Name ein, z. B. `dc=example-for-a-domain, dc=net`.
   e) Geben Sie **Benutzername** ein.
   f) Geben Sie das **Kennwort** ein.
7) Geben Sie jeweils die entsprechende Feldbezeichnung des LDAP-Servers für die folgenden Felder ein: **Anrede**, **Vorname**, **Nachname**, **Geschäftlich 1**, **Geschäftlich 2**, **Privat**, **Mobil**, **Firma**, **Firmen-Rufnr.**, **Postanschrift**, **Bundesland oder Region**, **Land**, **Postleitzahl**, **E-Mail**, **Pager**, **Faxrufnummer** und **Ort**.
8) Klicken Sie auf **Speichern**.

13.5.4.2 Wie Sie ein externes Offline-Verzeichnis (LDAP) für PC-Clients löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf die Registerkarte **Konfiguration externe Anbieter**.
4) Klicken Sie auf das zu löschende Externe Offline-Verzeichnis.
5) Klicken Sie auf **Entfernen**.

13.5.4.3 Wie Sie ein externes Offline-Verzeichnis (LDAP) für Systemtelefone hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Ihnen liegen die Zugangsdaten für den LDAP-Server vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **LDAP**.
4) Geben Sie die **IP-Adresse des LDAP-Servers** ein.
5) Geben Sie die **Portnummer des LDAP-Zugangs** ein.
6) Geben Sie **Benutzername** ein.
7) Geben Sie das **Kennwort** ein.
8) Geben Sie in **Kennwort bestätigen** das Kennwort ein.
9) Geben Sie in **Basis DN** den LDAP BASE Distinguished Name des LDAP-Servers ein, z.B. `dc=example-for-a-domain, dc=net`.
10) Geben Sie in **Suchanfrage** den Suchstring für den LDAP-Server ein, z.B.: `cn=$*`.
11) Geben Sie **Ergebnisattribut Name** für den LDAP-Server ein, z.B.: `cn`.
12) Geben Sie **Ergebnisattribut Rufnummer** für den LDAP-Server ein, z.B.: `telephoneNumber`.
13) Wählen Sie für die Sortierung der Suchergebnisse eine der folgenden Möglichkeiten:
    - Wenn Sie die Suchergebnisse sortiert haben möchten, aktivieren Sie das Kontrollkästchen **Sortieren der Suchergebnisse**.
    - Wenn Sie die Suchergebnisse nicht sortiert haben möchten, deaktivieren Sie das Kontrollkästchen **Sortieren der Suchergebnisse**.
14) Geben Sie die **LDAP-Belegungskennzahl** ein.
15) Geben Sie das **LDAP-Rufnummernprefix** ein.
16) Klicken Sie auf **Übernehmen**.

13.5.5 Systemverzeichnis

Mit Blick auf UC Suite Clients enthält das Systemverzeichnis alle Systemnummern für UC- und Nicht-UC Benutzer. Nicht-UC-Benutzer sind Teilnehmer ohne UC-Lizenzen und virtuelle Teilnehmer wie Fax, AutoAttendant. In Bezug auf Geräte enthält das Systemverzeichnis alle internen Teilnehmer und alle zentralen Kurzwahlnummern.

Der Administrator kann die Anzeige für jeden Teilnehmer bzw. jede Kurzwahlnummer mit Namen individuell deaktivieren.

13.5.6 Unified-Verzeichnis

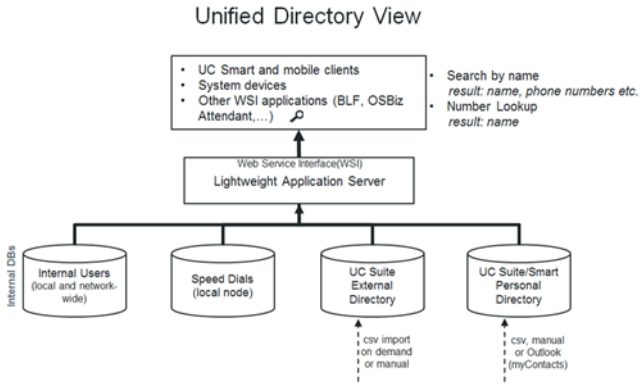
OpenScape Business bietet verschiedene Datenquellen zum Speichern und Abrufen von Teilnehmer- oder Kontaktdaten – von internen Teilnehmerdaten in der internen Benutzerkonfiguration über die interne Kurzwahlliste bis hin zu den verschiedenen Verzeichnissen der UC-Anwendungen.

Jede Datenquelle in OpenScape Business wird von einer bestimmten Client-Anwendung verwendet, die entweder Teil der Systemsoftware auf den Telefongeräten oder Teil einer UC-Client-Anwendung ist. Abhängig von den

verwendeten Datenquellen und Clients werden die Daten unterschiedlich abgerufen und dargestellt.

Der Unified-Verzeichnisdienst in OpenScape Business nutzt die bestehenden OpenScape Business-Datenquellen für die Funktionen Rufnummernsuche und Namensauflösung. Er übermittelt an alle Systemgeräte und OpenScape Business-Clients einheitliche Suchergebnisse und Namensauflösungsinformationen.

Der Zugriff auf den Unified-Verzeichnisdienst kann entweder über das Web Service Interface (WSI) mit externen Clients wie myPortal to go oder intern über Anrufbearbeitungsmechanismen (z. B. von OpenStage-Telefonen) erfolgen.



Der Unified-Verzeichnisdienst verwendet die folgenden internen Datenbanken und Verzeichnisse von OpenScape Business:

- Internes Benutzerverzeichnis (netzweit)
- Kurzwahllisten
- UC Smart Persönliches Verzeichnis (optional)
- UC Suite Externes Verzeichnis (optional)
- Persönliche Outlook-Kontakte (falls importiert über myContacts)

Der Unified-Verzeichnisdienst ist auf allen Knoten eines OpenScape Business-Systems ab V2R2 verfügbar. Es erfordert keine spezielle Hardware, Software oder zusätzliche Lizenzen.

Um bei der Verwendung des Unified-Verzeichnisdienstes die besten Ergebnisse zu erzielen, sollten Sie einige Regeln für Rufnummernformate und zur Schreibweise von Namen beachten.

13.5.6.1 Leistungsmerkmale

Unterstützte Geräte/Clients

Der Unified-Verzeichnisdienst stellt folgende Funktionen bereit:

- Telefonbuchsuche in mehreren internen Datenquellen von OpenScape Business
- Einheitliche Bereitstellung des Suchergebnisses für alle unterstützten Kunden
- Rufnummernsuche / Namensauflösung in mehreren internen Datenquellen
- Einheitliche Bereitstellung der Namensauflösungsergebnisse für alle unterstützten Clients
- Externer Datenzugriff über die WebServices-Schnittstelle (WSI)

Die Leistungsmerkmale sind für Einzelknotensysteme wie folgt verfügbar. In OpenScape Business-Netzwerken hängt die Verfügbarkeit der Features hauptsächlich von der Art der Verbindung der Amtsleitungen, Geräte und Clients innerhalb des Netzwerks ab.

Unified Directory unterstützt folgende Clients/Systemgeräte von Unify unter Verwendung der angegebenen Schnittstellen:

Gerät/Client	Verwendete(s) Schnittstelle/Protokoll	Hinweise
OpenStage-Telefone	Anrufverarbeitung/ CorNet-Protokoll	WSI/HTTP(S) ist optional für OpenStage 60/80 für Anrufer-Bilder
OpenScape DeskPhone IP	Anrufverarbeitung/ CorNet-Protokoll	WSI/HTTP(S) ist optional für DeskPhone IP 55 für Anrufer-Bilder
Schnurlose (CMI)-Geräte	Anrufverarbeitung/CMI-Protokoll	
CP 100/110 /200/205/210/ 405	Anrufverarbeitung/ CorNet-Protokoll	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI/HTTP(S)	
myPortal @work	WSI/HTTP(S)	
myPortal to go	WSI/HTTPS	
OpenScape Business Attendant/BLF	Anrufverarbeitung/ CorNet-Protokoll	WSI/HTTP(S) ist optional

Anmerkung: Die UC Suite myPortal-, myAttendant- und myAgent-Clients verwenden eigene Mechanismen für die Verzeichnissuche und Namensauflösung.

Suchfunktion

Die Unified Directory-Suche wird immer unter Verwendung der spezifischen Geräte-/Client-Benutzerschnittstelle durchgeführt. Die Suchkriterien und der verwendete Zeichensatz können abhängig von den verwendeten Clients eingeschränkt sein.

Nach Eingabe des Suchkriteriums wird die Suche in folgenden Verzeichnissen durchgeführt

- Internes Benutzerverzeichnis (netzwerkweit)
- Kurzwahllisten
- UC Smart Persönliches Verzeichnis (optional)
- UC Suite Externes Verzeichnis (optional)
- Persönliche Outlook-Kontakte (falls über myContacts importiert)

Alle Übereinstimmungen innerhalb der obigen Verzeichnisse werden zusammen mit ihrer Herkunft als Suchergebnisse angezeigt. Die Übereinstimmungen enthalten entweder den vollständigen Kontaktdatensatz oder nur Teile davon. Die Informationstiefe der Ergebnisse hängt von der Datenquelle ab.

Anmerkung: Die Suche nach Gruppennamen in myPortal @work wird im UC Suite-Modus nicht unterstützt. Es wird nur die Suche nach lizenzierten Benutzern (Basislizenz) und lizenzierten MULAP-Gruppen (UC-Einträge) unterstützt.

Die Übereinstimmungen werden auf den Geräten oder Clients angezeigt, abhängig von den Anzeigefähigkeiten.

	Internes Benutzerver	Kurzwahllis	UC Smart Persönliche Verzeichnis	UC Suite Externes Verzeichnis	Persönliche Outlook-Kontakte (über myContacts)
Nachname	X	---	X	X	X
Vorname	X	---	X	X	X
Kurz-/ Anzeigename	X	X	---	---	---
Büro-Rufnr.	---	---	X	X	X
Private/ext. Rufnr.	---	---	X	---	X
Mobilrufnr.	---	---	X	X	X
E-Mail-Adr.	---	---	X	X	X
Firmenname	---	---	X	X	X
Ort	---	---	---	---	---
Kontaktbild	---	---	X	---	X
Kontaktbildvorschau		---	X	---	X

Rufnummernsuche

Mit der einheitlichen Rufnummernsuche wird der Anrufer (CLI) durch eine Nummernsuche in allen unterstützten internen Datenquellen aufgelöst. Die Suche wird in den folgenden Rufnummer-Feldern durchgeführt:

- Büro-Rufnummer
- Mobilrufnummer
- Private Rufnummer

Die Rufnummernsuche wird im Allgemeinen bei eingehenden oder ausgehenden Anrufen ausgelöst, wobei bestimmte Routing- und Weiterleitungsfunktionen zusätzlich berücksichtigt werden.

Eine feste Priorisierung der Datenquellen, die für die Rufnummernsuche verwendet werden, wird implementiert, um so schnell wie möglich ein Ergebnis zu erhalten. Das Ergebnis enthält entweder nur den Nachnamen, den Vornamen, den Anzeigenamen oder, sofern verfügbar, die vollständigen Kontaktdaten.

Tabelle 7: Unterstützte Datenquellen und Priorisierung

Priorität	Datenquellen	Bemerkung
1	CO ITSP Name (wie vom Provider gesendet)	Voraussetzung ist, dass das Flag "Name im Amt" aktiviert wird.
2	Kurzwahlliste	
3	Persönliche Kontakte	
4	UC-Benutzerdetails	

Die abgerufenen Daten werden auf dem Gerät des Benutzers und/oder im UC-Client angezeigt. Die Informationstiefe der Ergebnisse hängt von den Anzeigefähigkeiten ab.

- **Kommende Rufe**

  Unterstütztes Szenario für Einzelknotensysteme:

  – Basic Call
  – Gruppenruf/MULAP-Ruf
  – Rufzuschaltung
  – Einzelschritt-Übergabe (SSCT)
  – Gespräch übergeben/Übergabe nach Melden/Rückfrage
  – Uneingeschränkte Gesprächsumleitung (CFU)
  – Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply)
  – Anrufumleitung bei Besetzt (CFB = Call Forwarding Busy)
  – Übergabe ohne Rückfrage
  – Anrufübernahme

  Anmerkung: Anrufübernahme unterscheidet sich von Anrufübernahmegruppe. Wenn in der Anrufübernahmegruppe eine externe Nummer im Unified Directory gespeichert ist, wird der Name des Anrufers von den Mitgliedern der Gruppe nicht angezeigt.

  Unterstütztes Szenario für mehrere Knoten (Netzwerk). Szenario ist ein Gateway-Anruf.
- **Gehender Anruf**

  Im Falle eines ausgehenden Anrufs wird die Telefonnummer des angerufenen Teilnehmers nur einmal gesucht.

  Das unterstützte Szenario für Systeme mit einem Knoten ist ein Basisanruf an eine externe Nummer.

Die Darstellung der Rufnummer-Suchergebnisse hängt von den Anzeigefähigkeiten der Telefone ab.

13.5.6.2 Regeln und Konventionen

Bei den Rufnummern- und Namensformaten innerhalb der Datenquellen sind einige Konventionen zu beachten, um optimale Ergebnisse mit dem Unified-Verzeichnisdienst zu erhalten.

Unterstütztes Rufnummernformat

Alle externen Rufnummern innerhalb der Datenquellen müssen einschließlich Länder- und Ortsvorwahl im kanonischen Format eingegeben werden, z. B. +4989700712345

Die Kurzwahlliste unterstützt nur das vom System wählbare Format (z.B. 0089700712345 oder 0004989700712345)

Wenn Kurzwahlnummern so konfiguriert sind, dass sie über LDAP zugänglich sind, müssen Sie die Option zur Nummernkonvertierung aktivieren, um den Kontaktnamen anzuzeigen, wenn die Nummer im kanonischen Format vorliegt. Weitere Informationen zum Aktivieren der Nummernkonvertierung finden Sie untere Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen auf Seite 1196.

Unterstützte Namensformate

Bei Namensformaten und Zeichensätzen sind die folgenden Konventionen zu beachten:

- **Namensformat bei Kurzwahl**

  Die Namenssuche innerhalb der Kurzwahlliste wird nur in Kombination mit bestimmten Konfigurationsregeln unterstützt. Vor- und Nachname müssen im vorhandenen Namensfeld nach dem folgenden Muster eingegeben werden:

  <Nachname>, <Vorname> (kommagetrennt)
- **Interne Teilnehmer bei Migrationsszenarien**

  Bei internen Teilnehmern, die diese Konfigurationsregeln nicht beachten, wird hat eine Migration auf V2R1 und höher ggf. unerwartete Folgen und wird nicht ordnungsgemäß unterstützt. Dies bedeutet, dass der Administrator interne Namen vor Durchführung der Migration in das folgende Format konvertieren sollte:

  <Nachname>, <Vorname> (kommagetrennt)

Verfügbarkeit von Verzeichnisänderungen

Nach dem Erstellen, Aktualisieren oder Löschen von Kontakten in den verschiedenen Datenquellen kann es bis zu 10 Minuten dauern, bevor alle Änderungen in den Suchergebnissen sichtbar sind.

13.5.6.3 Funktionale Grenzen

Für Unified-Verzeichnisse gelten die folgenden funktionalen Grenzen:

Namenssuche

- Unterstützung von Gruppennamen

  Gruppennamen (nicht MULAP-Namen) können zurzeit nicht in allen Arten von Konfigurationen durchsucht werden
- Unterstützung von Sonderzeichen

  Auf den meisten Telefongeräten kann der Benutzer nur nach den Standardzeichen "a-z" suchen. Die Eingabe von (diakritischen)

Sonderzeichen (wie z.B. der deutschen Umlaute Ää, Öö, Üü oder ß) ist über die Benutzeroberfläche des Telefongeräts nicht möglich.

Daher beinhaltet ein Suchergebnis mit einfachen Zeichen auch Sonderzeichen. Bei einer Suche mit den Zeichen „acdegilnorstuyz“ sind auch die entsprechenden Sonderzeichen "àáâãåäąăçćčďđèéêëęě#ìíîïĺľłñńňòóôõöőřŕśšşťùúûůüűýÿžźż"

im Suchergebnis enthalten.

Anmerkung: Eine Suche im Telefonbuch mit Platzhalterzeichen am Anfang des Suchbegriffs, z. B. <*jo*>, wird nur für interne Benutzer unterstützt.

- Unterstützung von Kurzwahlnamen

  Die Namenssuche innerhalb der Kurzwahlliste wird nur in Kombination mit bestimmten Konfigurationsregeln unterstützt. Vor- und Nachname müssen im vorhandenen Namensfeld nach einem der folgenden Muster eingegeben werden

  – <Nachname>, <Vorname> (kommagetrennt)
  – <Nachname>, <Vorname> (Leerschritt als Trennzeichen)

Namensanzeige

Persönliche Kontakte aus UC Smart und dem externen Offline-Verzeichnis, bei denen Vorname und Nachname zusammen länger als 24 Zeichen sind, werden zwecks Anzeige auf dem Gerätedisplay auf 24 Zeichen gekürzt.

Rufnummernsuche

Die Funktion Rufnummernsuche (Kontaktname aus Rufnummer des Anrufers ermitteln) wird vom Unified-Verzeichnisdienst für SIP- und S0-Geräte nicht unterstützt.

13.5.6.4 Unified-Verzeichnis in vernetzten Systemen

Der Unified-Verzeichnisdienst ist auf allen Knoten eines OpenScape Business-Netzwerks aktiv und nutzt die Datenquellen des eigenen Systems. Telefongeräte und Clients verwenden innerhalb ihres eigenen Knotens immer den Unified-Verzeichnisdienst.

Es kommt daher auf die Art des Datenquelleninhalts an, ob netzweite Kontakte verfügbar sind oder nicht.

Tabelle 8: Lokale und netzweite Datenquellen

Datenquelle	Lokale Daten	Netzweite Daten
Internes Benutzerverzeichnis	X	X
Kurzwahllisten	X	---
UC Smart Persönliches Verzeichnis	X	---

Datenquelle	Lokale Daten	Netzweite Daten
UC Smart Persönliches Verzeichnis	X	---
Persönliche Outlook-Kontakte (über myContacts)	X	---

Rufnummernsuche

In Vernetzungsszenarien wird die Funktion Telefonnummer suchen nicht verwendet. In solchen Fällen wird der Name über normale Vernetzungsmechanismen zwischen den Netzknoten übertragen.

Für interne Teilnehmer wird der konfigurierte Anzeigename verwendet, so dass eine Suche nicht erforderlich ist.

13.5.6.5 So importieren Sie Kontakte in Unified Directory

Der Assistent zum Importieren von Kontakten bietet die Funktionalität, Verzeichniskontakte aus einer csv-Datei zu importieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie in der Navigationsstruktur auf **Assistenten** > **Unified Directory**.
3) Klicken Sie auf **Bearbeiten** neben **Kontakte importieren**, um mit dem Import der Kontakte in Globales Verzeichnis fortzufahren.
4) Unter Abschnitt **Datei hochladen**, klicken Sie auf **Datei wählen** und wählen Sie die gewünschte csv-Datei zum Hochladen aus.

   Anmerkung: Die maximale Anzahl von Einträgen pro Import beträgt 100.000 (30.000 für eingebettete Systeme).

5) Geben Sie unter Abschnitt **Optionen** das **Dateitrennzeichen**ein. ';' oder ',' sind gültige Einträge.
6) Klicken Sie auf **OK & Weiter**.
7) Das Backend verarbeitet die Datei, liest die Header und präsentiert die Header zusammen mit den vordefinierten Kategorien des Master-Verzeichnisses auf der **CSV-Header-Zuordnungsseite**. Anschließend kann der Benutzer die Einträge der csv-Dateien abgleichen, um die relativen Daten in andere als die vordefinierten Kategorien zu importieren.
8) Klicken Sie auf **OK & Weiter**.

9) In die Seite **Übersicht des Imports**:

a) Wählen Sie eine der folgenden Optionen für die importierte csv-Datei aus:

- Globale Verzeichniskontakte anhängen
- Löschen Sie alle über CSV importierten globalen Verzeichniskontakte
- Löschen Sie alle globalen Verzeichniskontakte

b) Wählen Sie für **Doppelte Kunden-ID** eine der folgenden Optionen aus:

- Aktualisieren Sie bestehenden Kunden
- Stoppen Sie den Import des aktuellen Datensatzes

Die Einträge, die hinzugefügt werden, und die Einträge, die nicht validiert werden konnten, werden in zwei entsprechenden Tabellen präsentiert.

Anmerkung: Doppelte Datensätze werden durch Kombination der Felder Vorname, Nachname, Geschäftstelefon und E-Mail identifiziert. Diese Felder können nicht automatisch aktualisiert werden, indem Sie "**Bestehenden Kunden aktualisieren**" wählen. Um diese Felder zu aktualisieren, löschen Sie zuerst ältere Datensätze in Schritt 9a.

Die flagge **"Bestehenden Kunden aktualisieren"** funktioniert nur, wenn beim Import die Kunden-ID zugeordnet wird.

Nur Datensätze mit derselben **Kunden-ID** werden als "bestehender Kunde" betrachtet und aktualisiert.

Die Flagge "**Daten vor dem Import entfernen**" entfernt keine Datensätze, wenn sie bereits in anderen Funktionen verwendet werden, z.B. als VIP-Anrufer usw.

Die Kunden-ID ist der einzige Schlüssel, um festzustellen, ob der Datensatz dupliziert ist. Wenn die Kunden-ID nicht zugeordnet ist, gibt es keine Weise, Duplikate zu vermeiden.

Wir empfehlen daher dringend, dass Kunden die bereitgestellte Vorlage nutzen und ihre Daten entsprechend anpassen, ohne die eindeutigen IDs auszulassen.

---

10) Klicken Sie auf **OK & Weiter**. Für diesen Prozess können mehrere Minuten erforderlich sein.

11) Die Seite **Import fertig** informiert über die Anzahl der importierten Einträge.

12) Klicken Sie auf **Fertigstellen**.

13.5.6.6 So bearbeiten oder hinzufügen Sie neue Unified Directory-Kontakte

Der Assistent zum Bearbeiten von Kontakten bietet die Funktionalität, bereits importierte Kontakte zu bearbeiten oder neue hinzuzufügen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie in der Navigationsstruktur auf **Assistenten** > **Unified Directory**.
3) Klicken Sie auf **Bearbeiten** neben **Kontakte bearbeiten**, um mit der Bearbeitung der Kontakte des Globales Verzeichnis fortzufahren.
4) Bearbeiten Sie die gewünschten Felder der Kontakte. Erst wenn ein Eintrag bearbeitet wird, wird die Schaltfläche **Anwenden** verfügbar.
5) Klicken Sie auf **Hinzufügen**, um manuell einen neuen Kontakt hinzuzufügen.
6) Füllen Sie die gewünschten Felder des neuen Kontakts aus und klicken Sie auf die Schaltfläche **Anwenden**.

13.5.7 Abteilungen

Abteilungen gruppieren Teilnehmer im internen Verzeichnis nach ihrer organisatorischen Zugehörigkeit. Das interne Verzeichnis ermöglicht die Suche bzw. Sortierung nach Abteilung.

13.5.7.1 Abteilung hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Abteilungen** zu starten.
4) Klicken Sie auf **Hinzufügen**.
5) Geben Sie den **Abteilungsnamen** der Abteilung ein.
6) Geben Sie die Kennung der **Gruppennummer** ein.
7) Klicken Sie auf **Speichern**.

13.5.7.2 Teilnehmer einer Abteilung zuordnen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten.

4) Wählen Sie den betreffenden Teilnehmer aus.
5) > Klicken Sie auf **Bearbeiten** > **Persönliche Daten** > **Meine persönlichen Daten**.
6) Wählen Sie im Feld **Abteilung** aus der Aufklappliste die gewünschte Abteilung aus.
7) Klicken Sie anschließend auf **Speichern**.

13.5.7.3 Abteilung bearbeiten

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Abteilungen** zu starten.
4) Klicken Sie in der Liste der Abteilungen auf die entsprechende Abteilung.
5) Klicken Sie auf **Bearbeiten**.
6) Geben Sie den **Abteilungsnamen** der Abteilung ein.
7) Geben Sie die Kennung der **Gruppennummer** ein.
8) Klicken Sie auf **Speichern**.

13.5.7.4 Wie Sie eine Abteilung entfernen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Abteilungen** zu starten.
4) Klicken Sie in der Liste der Abteilungen auf die entsprechende Abteilung.
5) Klicken Sie auf **Entfernen**.
6) Klicken Sie auf **OK**.

13.5.8 Favoritenliste

In der Favoritenliste haben Sie als Teilnehmer ausgewählte Kontakte stets im Blick. Diese können Sie besonders einfach anrufen. Sie sehen alle internen Teilnehmer mit Systemtelefon sowie externe Kommunikationspartner mit Anwesenheitsstatus und können diese per Sofortnachricht kontaktieren.

Sie können als Teilnehmer Kontakte aus allen Verzeichnissen zur Favoritenliste hinzufügen. Bei Favoriten, die nicht aus dem internen Verzeichnis stammen, erscheint an Stelle des Symbols für den Anwesenheitsstatus das Symbol für die Quelle des Kontakts.

Die Favoritenliste verwaltet Kontakte in Gruppen. Die Kontakte in allen Gruppen sind nach Vorname, Nachname oder in ihrer ursprünglichen Reihenfolge sortierbar.

Bei Abwesenheit eines internen Teilnehmers erfahren Sie den geplanten Zeitpunkt der Rückkehr durch Positionieren des Mauszeigers auf seinem Eintrag, sofern er seinen Anwesenheitsstatus für Sie sichtbar sein lässt.

Bei Favoriten mit mehreren Rufnummern können Sie eine Standard-Rufnummer festlegen, unter welcher der Kontakt angerufen wird. Die Standard-Rufnummer eines Favoriten ist im Kontextmenü am Symbol mit dem aktivierten Kontrollkästchen erkennbar.

13.5.9 Journal

Das Journal ist die Liste aller ankommenden und gehenden Anrufe eines Teilnehmers. Aus dem Journal kann der Teilnehmer Kontakte schnell und einfach erneut anrufen oder entgangene Anrufe beantworten.

Ordner für Anrufarten

Die Anrufe sind in folgende Gruppen gegliedert:

- **Offen**

  Enthält die von Ihnen unbeantworteten entgangenen Anrufe, bei denen eine Rufnummer übermittelt wurde. Sobald einer dieser Anrufe beantwortet wird, werden alle Einträge mit der entsprechenden Rufnummer von der Liste gestrichen.
- **All Anrufe**
- **Entgangen**
- **Angenommen**
- **Intern**
- **Extern**
- **Ankommend**
- **Gehend**
- **Zeitlich geplant**

  Enthält die von Ihnen als Teilnehmer zu bestimmten Terminen geplanten Anrufe. Das Leistungsmerkmal „Geplante Anrufe“ steht für Agenten des Contact Center nicht zur Verfügung. Damit das Kommunikationssystem einen geplanten Anruf ausführt, muss zu dem Termin myPortal for Desktop oder myPortal for Outlook geöffnet sein, der Anwesenheitsstatus muss **Büro** oder **CallMe** sein und Sie müssen die Ausführung des Anrufs in einem Dialog bestätigen. Falls Sie während des Termins für einen geplanten Anruf besetzt sind, stellt das System den geplanten Anruf zurück, bis Sie wieder frei sind. myPortal for Desktop oder myPortal for Outlook weist Sie beim Beenden auf evtl. anstehende geplante Anrufe hin. Beim Starten informiert myPortal for Desktop oder myPortal for Outlook Sie über evtl. inzwischen verstrichene Termine geplanter Anrufe. Sie können diese dann entweder löschen oder zu einem neuen Termin speichern.

In der modernen Benutzeroberfläche von myPortal for Desktop stehen nicht alle Ordner für Anrufarten zur Verfügung.

Beim Start der modernen Benutzeroberfläche myPortal for Desktop werden nur 100 Journaleinträge geladen. Danach und wenn neue Anrufe eingehen, überschreitet die Nummer in der Anrufliste 100 Einträge.

Aufbewahrungsdauer

Das System speichert Anrufe im Journal für eine begrenzte, vom Administrator konfigurierbare maximale Zeit. Als Teilnehmer können Sie diese Zeit reduzieren. Nach Ablauf der Aufbewahrungsdauer löscht das System betreffende Einträge automatisch.

Anmerkung: In der Aufbewahrungsdauer wird auch der maximale Zeitraum für Auswertungen mit myReports festgelegt.

Gruppierung nach Zeitraum

Die Anrufe sind in jeder Gruppe zeitlich gruppiert, z.B.: Heute, Gestern usw., Letzte Woche, Letzten Monat und Älter. Ihr Administrator kann festlegen, wie lange Anrufe im Journal gespeichert bleiben. Nach dieser festgelegten Zeit werden Einträge automatisch gelöscht. In der modernen Benutzeroberfläche von myPortal for Desktop steht die Gruppierung nach Zeitraum nicht zur Verfügung.

Gesprächsdaten

Jeder Anruf wird mit Datum und Zeit angezeigt und sofern vorhanden mit der Rufnummer. Falls ein Verzeichnis zur Rufnummer weitere Informationen wie **Nachname**, **Vorname** und **Firma** enthält, werden auch diese angezeigt. Zusätzlich werden in den meisten Ordnern die Spalten **Richtung**, **Dauer** und **Gespräch abgeschlossen** angezeigt. In der modernen Benutzeroberfläche von myPortal for Desktop stehen nicht alle Gesprächsdaten zur Verfügung.

Sortierung

Sie können die Anrufe im Journal nach Spalten alphanumerisch auf- oder absteigend sortieren.

Sie können im Journal zum ersten Anruf springen, dessen Eintrag in der Spalte, nach der sortiert ist, mit einem bestimmten Zeichen beginnt, z.B. zum ersten Nachnamen, der mit "P" beginnt. Durch die Eingabe nachfolgender Zeichen können Sie die Suche eingrenzen. In der modernen Benutzeroberfläche von myPortal for Desktop steht die Sortierung nicht zur Verfügung.

Export

Als Teilnehmer können Sie das Journal mit myPortal for Desktop oder myPortal for Outlook als CSV-Datei exportieren:

13.5.9.1 Maximale Aufbewahrungsdauer für das Journal ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Wartung**.
5) Geben Sie im Feld **Anrufhistorie aufbewahren für** im Bereich **Wartung der Anrufinformationen** die gewünschte Dauer in Tagen ein.

Anmerkung: In der Aufbewahrungsdauer wird auch der maximale Zeitraum für Auswertungen mit myReports festgelegt.

---

6) Klicken Sie auf **Speichern**.

13.6 Anrufe

Für Anrufe stehen Teilnehmern komfortable Leistungsmerkmale wie Desktop-Wahl, PopUp-Fenster und die Aufzeichnung von Anrufen und Konferenzen zur Verfügung.

13.6.1 Desktop-Wahl und Clipboard-Wahl

Desktop-Wahl und Clipboard-Wahl ermöglicht Teilnehmern mit myPortal for Desktop (Windows) oder myPortal for Outlook aus vielen Windows-Anwendungen ein markiertes Ziel bzw. ein Ziel in der Windows-Zwischenablage mittels Tastenkombination anzurufen, z.B. aus einer Outlook-E-Mail.

Abhängig von der Art der verwendeten Zeichenfolge funktioniert die Wahl folgendermaßen:

- Eine Rufnummer im kanonischen Format wird gewählt.
- Eine Rufnummer im wählbaren Format wird gewählt, sofern das Kommunikationssystem entscheiden kann, ob es sich um ein internes oder externes Ziel handelt. Anderenfalls wird der Benutzer zur entsprechenden Auswahl aufgefordert.
- Eine Zeichenfolge, die Buchstaben enthält, wird in den Verzeichnissen als Vorname oder Nachname gesucht.

Die Desktop-Wahl und Clipboard-Wahl wird nach einer einstellbaren Zeit ausgeführt. Innerhalb dieser Zeitspanne kann die Wahl noch abgebrochen werden. Wird der voreingestellte Wert von 3s auf 0s geändert, wird die Wahl sofort ausgeführt. Der Wert wird in den Einstellungen der UC Suite Clients geändert.

Windows-Anwendungen, die mittels Windows-Standardkomponenten implementiert wurden, unterstützen in der Regel Desktop-Wahl und Clipboard-Wahl, nicht jedoch 16-bit-Anwendungen. Desktop-Wahl wird nur von 32 Bit Applikationen unterstützt.

13.6.2 PopUp-Fenster

PopUp-Fenster in den UC Suite Clients bieten Teilnehmern die komfortable Möglichkeit mit einem Klick zu reagieren, z.B. auf ankommende Anrufe oder neue Sprachnachrichten.

PopUp-Fenster werden in der unteren rechten Ecke des Bildschirms angezeigt. Es gibt unterschiedliche Arten von PopUp-Fenstern. PopUp-Fenster für Anrufe und Nachrichten zeigen Rufnummer, Name und Bild des Anrufers an, wenn möglich. Die Schaltflächen der PopUp-Fenster ändern sich situationsbezogen.

PopUp-Fenster können zu einem Taskleistensymbol minimiert werden. Sobald mehr als drei PopUp-Fenster für Anrufe geöffnet sind, werden diese automatisch minimiert in der Taskleiste dargestellt.

13.6.3 Aufzeichnen von Anrufen

Ein Teilnehmer kann Anrufe aufzeichnen. Aufgezeichnete Anrufe erscheinen in der Sprachbox.

Tipp: Sie müssen der Gesprächspartner darüber informieren, dass Sie das Gespräch aufzeichnen. In bestimmten Ländern (z.B. Frankreich) informiert das System den Gesprächspartner automatisch darüber.

Als Administrator können Sie das Aufzeichnen von Anrufen zusammen mit dem Aufzeichnen von Konferenzen systemweit zulassen oder verhindern. Optional können Sie zu Beginn der Aufzeichnung die Wiedergabe einer Ansage oder eines Hinweistons konfigurieren.

Als Teilnehmer können Sie das Aufzeichnen von Anrufen über myPortal for Desktop oder myPortal for Outlook steuern. Aufgezeichnete Anrufe sind in der Sprachbox durch einen roten Punkt gekennzeichnet und zeigen, sofern verfügbar, die Rufnummer des Gesprächspartners.

Durch Rückfrage, Halten, Übergabe und Einleiten einer Konferenz wird eine laufende Aufzeichnung abgebrochen.

Anmerkung: DTMF wird während der Anrufaufzeichnung nicht unterstützt.

13.6.3.1 Aufzeichnung von Anrufen aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.

4) Klicken Sie auf **Gespräch aufzeichnen**.
5) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie das Aufzeichnen von Anrufen zulassen möchten, aktivieren Sie das Kontrollkästchen **Gespräch aufzeichnen**.
   - Wenn Sie das Aufzeichnen von Anrufen verhindern möchten, deaktivieren Sie das Kontrollkästchen **Gespräch aufzeichnen**.
6) Klicken Sie auf **Speichern**.

Anmerkung: Anrufe, bei denen diese Funktion aktiviert ist, können weder übertragen noch gehalten werden.

13.6.3.2 Ansage für Aufzeichnung aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Gespräch aufzeichnen**.
5) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie zu Beginn einer Aufzeichnung eine Ansage wiedergeben möchten, aktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung eine Ansage wiedergeben**.
   - Wenn Sie zu Beginn einer Aufzeichnung keine Ansage wiedergeben möchten, deaktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung eine Ansage wiedergeben**.
6) Klicken Sie auf **Speichern**.

13.6.3.3 Hinweiston für eine Aufzeichnung aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Gespräch aufzeichnen**.

5) Wählen Sie eine der folgenden Optionen:

- Wenn Sie zu Beginn einer Aufzeichnung einen Hinweiston wiedergeben möchten, aktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung einen Hinweiston wiedergeben**.
- Wenn Sie zu Beginn einer Aufzeichnen keinen Hinweiston wiedergeben möchten, deaktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung einen Hinweiston wiedergeben**.

6) Klicken Sie auf **Speichern**.

Anmerkung: Bitte beachten Sie, dass dieser Prozess nur für **Openscape Business S** gilt. Die Aktivierung des Warntons Aufzeichnung in **Openscape Business X** wird durch das Flag **Warnton während der Sprachaufzeichnung** gesteuert, das Sie im **Expertenmodus** > **Grundeinstellungen** > **System Flags** finden.

13.7 Konferenzen

In einer Konferenz können mehrere Teilnehmer (darunter auch externe) gleichzeitig miteinander telefonieren.

13.7.1 Konferenzmanagement

Mit Konferenzmanagement kann ein Teilnehmer unterschiedliche Arten von Konferenzen nutzen.

Arten von Konferenzen

Die unterschiedlichen Arten von Konferenzen bieten folgende Möglichkeiten:

	Ad-hoc	**Geplant**	**Permanent**	**Offen**
Verwendung	• Telefongesteuert • Applikationsgesteuert	• Applikationsgesteuert	Applikationsgesteuert	Applikationsgesteuert
Beginn	• Manuell	• Geplant	• Manuell	• Manuell
Ende	• Manuell	• Geplant • Manuell	• Manuell	• Manuell
Dauer der Reservierung von Konferenzkanälen	• Standardmäßig 1 Stunde	• Geplant	• Bis zur Deaktivierung oder Löschung der Konferenz	• Bis zur Deaktivierung oder Löschung der Konferenz
Nebenstelle	x	x	-	-
Wiederholung	• Manuell	• Geplant	-	-

	Ad-hoc	Geplant	Permanent	Offen
Richtung des Verbindungsaufbaus aus Sicht des Systems	• Gehend	• Gehend • Ankommend	• Ankommend	• Ankommend
Teilnehmerkreis	• Fest	• Fest	• Fest	• Offen
Authentifizierung der Konferenzteilnehmer	-	• Individuelle Konferenz-ID (optional) • Passwort (optional)	• Individuelle Konferenz-ID (optional) • Passwort (optional)	• Gemeinsame Konferenz-ID (optional)
Aufzeichnung, sofern im System aktiviert	• Manuell (On Demand Conference Recording)	• Automatisch (Auto Conference Recording) • Manuell (On Demand Conference Recording)	• Automatisch (Auto Conference Recording) • Manuell (On Demand Conference Recording)	• Automatisch (Auto Conference Recording) • Manuell (On Demand Conference Recording)
Einladung per E-Mail mit:	• Name der Konferenz • Link für Web Collaboration Sitzung	• Name der Konferenz • Einwahlnummer • Konferenz-ID • Passwort • Datum und Uhrzeit von Beginn und Ende der Konferenz • Link für Web Collaboration Sitzung	• Name der Konferenz • Einwahlnummer • Konferenz-ID • Passwort • Link für Web Collaboration Sitzung	• Name der Konferenz • Einwahlnummer • Konferenz-ID • Passwort
Outlook-Termin als E-Mail-Anlage (.ics)	-	x	-	-

Applikationsgesteuerte Konferenz

Als Teilnehmer können Sie eine Konferenz mit dem Konferenz-Management von myPortal for Desktop oder myPortal for Outlook initiieren, steuern und verwalten.

Telefongesteuerte Konferenz

Als Teilnehmer können Sie eine telefongesteuerte Konferenz auf folgende Arten initiieren und anschließend am Telefon steuern:

- gewünschte Konferenzteilnehmer anrufen und mit der Konferenz verbinden
- Rückfrageverbindung zu einer Konferenz erweitern
- Zweitanruf zu einer Konferenz erweitern

Virtueller Konferenzraum

Im virtuellen Konferenzraum können Sie als Teilnehmer bei applikationsgesteuerten Konferenzen in Echtzeit eine Konferenz mit ihrem Teilnehmerkreis grafisch dargestellt verfolgen und als Konferenzleiter auch steuern. Der virtuelle Konferenzraum zeigt Rufnummer, Name und Anwesenheitsstatus der Konferenzteilnehmer an, sofern verfügbar.

Einwahlnummer

Als Administrator können Sie die bei der Basisinstallation festgelegten Einwahlnummern für Konferenzen ändern. Als Teilnehmer können Sie die Einwahlnummer für eine Konferenz anzeigen.

Konferenzleiter

Der Initiator der Konferenz ist bis auf Weiteres automatisch Konferenzleiter. Dieser kann (abhängig von der Art der Konferenz):

- Konferenzteilnehmer hinzufügen oder entfernen (applikationsgesteuerte Konferenz):

  Entfernte Teilnehmer bleiben nicht in der Konferenz.
- Konferenzteilnehmer trennen oder erneut verbinden:

  Getrennte Teilnehmer können weiterhin in der Konferenz bleiben. Während der Konferenzleiter einen Konferenzteilnehmer verbindet, hört der einzige andere Konferenzteilnehmer Wartemusik bzw. bleiben die anderen Konferenzteilnehmer miteinander verbunden.
- Konferenz aufzeichnen

  Aufgezeichnete Konferenzen erscheinen in der Sprachbox mit einem roten Punkt gekennzeichnet und zeigen, sofern verfügbar, die Rufnummer des ersten Konferenzteilnehmers. Konferenzen, an denen ein gehaltener Teilnehmer beteiligt ist, können nicht aufgezeichnet werden.
- Einen anderen internen Teilnehmer desselben Knotens als Konferenzleiter festlegen
- Die Konferenz verlängern
- Die Konferenz verlassen, ohne sie zu beenden:

  Der am längsten teilnehmende interne Teilnehmer wird automatisch Konferenzleiter.
- Die Konferenz beenden

Konferenzteilnehmer

Konferenzteilnehmer können die Konferenz verlassen oder sich erneut einwählen (geplante Konferenz und permanente Konferenz). Solange eine Konferenz nur einen Teilnehmer hat, hört dieser Wartemusik. Als Administrator können Sie festlegen, ob in Konferenzen mehrere externe Konferenzteilnehmer zulässig sind. Die maximale Anzahl der externen Konferenzteilnehmer ist unter anderem durch die Anzahl der verfügbaren Amtsleitungen begrenzt.

Konferenzton

Beim Verbinden oder Trennen eines Konferenzteilnehmers hören die anderen Konferenzteilnehmer den Konferenzton. Als Administrator können Sie den Konferenzton aktivieren oder deaktivieren.

Automatisches Beenden ohne Konferenzleiter

Verbleiben in einer Konferenz nur externe Teilnehmer, hören die Konferenzteilnehmer nach Ablauf einer bestimmten Zeit einen Aufmerksamkeitston. Nach Ablauf einer weiteren Zeit beendet das System die Konferenz automatisch. Als Administrator können Sie diese Zeiten ändern.

Benachrichtigung per E-Mail und Outlook-Termin

Das System kann Konferenzteilnehmer automatisch per E-Mail und bei geplanten Konferenzen zusätzlich mittels Outlook-Termin als Anlage (.ics) benachrichtigen:

Ereignis	Benachrichtigte Konferenzteilnehmer	Outlook-Termin
Neue Konferenz	Alle	Automatische Erstellung
Löschen der Konferenz		Automatische Löschung
Verschieben der Konferenz		Automatische Aktualisierung
Hinzufügen von Konferenzteilnehmern	Betroffene	Automatische Erstellung (betroffene)
Entfernen von Konferenzteilnehmern		Automatische Löschung (betroffene)

Voraussetzung ist, dass der Administrator den E-Mail-Versand konfiguriert hat. Ferner muss ein interner Konferenzteilnehmer seine E-Mail-Adresse festgelegt haben. Für externe Konferenzteilnehmer muss der Initiator der Konferenz deren E-Mail-Adresse eingeben.

Anmerkung: Zur Benachrichtigung per E-Mail erfolgt keinerlei Rückmeldung über fehlgeschlagene Zustellung oder über eventuelle Abwesenheitsmitteilungen, da E-Mails wegen der Integration von Web Collaboration direkt vom System gesendet werden.

Weitere Anrufe

Während der Teilnahme an einer Konferenz führt das Ausführen oder das Annehmen eines anderen Anrufs zur Trennung von der Konferenz.

Parken, Makeln

In einer Konferenz stehen die Leistungsmerkmale Parken und Makeln nicht zur Verfügung.

Gebühren

Gebühren werden demjenigen Teilnehmer zugeordnet, der das gebührenpflichtige Gespräch aufgebaut hat. Mit Übergabe an einen anderen Konferenzleiter gehen die weiteren Gebühren auf diesen über.

Systemauslastung

Als Administrator können Sie sowohl aktive als auch gespeicherte Konferenzen anzeigen. Inaktive Konferenzen können gelöscht werden.

Tipp: Permanente Konferenzen belegen dauerhaft Systemressourcen. Da jeder Teilnehmer mit myPortal for Desktop oder myPortal for Outlook permanente Konferenzen konfigurieren kann, empfehlen wir Ihnen als Administrator regelmäßig die gespeicherten Konferenzen zu überprüfen, um Ressourcenengpässe zu vermeiden.

Videoübertragung

Eine eventuell laufende Videoübertragung muss vor der Teilnahme an einer Konferenz beendet werden.

13.7.1.1 Wie Sie die Einwahlnummer für einen virtuellen Konferenzraum ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Teilnehmer**.
3) Navigieren Sie im Menübaum zu **Teilnehmer** > **UC Applications** > **Konferenz**.

   Im Arbeitsbereich werden die Rufnummern der virtuellen Konferenzräume angezeigt. Die letzte davon ist jene für geplante Konferenzen und permanente Konferenzen.
4) Klicken Sie im Menübaum auf den betreffenden Eintrag (Index - Rufnummer).
5) Klicken Sie auf die Registerkarte **Teilnehmer-Parameter ändern**.
6) Geben Sie im Feld **Rufnummer** die neue Einwahlnummer ein. Die Einwahlnummer darf nur die Ziffern 0-9 enthalten.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.7.1.2 Mehrere externe Konferenzteilnehmer zulassen oder verhindern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Navigieren Sie im Menübaum zu **System** > **System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie mehrere externe Konferenzteilnehmer zulassen möchten, aktivieren Sie das Kontrollkästchen **Mehr als 1 externer Konferenzteilnehmer**.
   - Wenn Sie mehrere externe Konferenzteilnehmer verhindern möchten, deaktivieren Sie das Kontrollkästchen **Mehr als 1 externer Konferenzteilnehmer**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.7.1.3 Wie Sie den Konferenzton aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Navigieren Sie im Menübaum zu **System** > **System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den Konferenzton aktivieren möchten, aktivieren Sie das Kontrollkästchen **Konferenzton**.
   - Wenn Sie den Konferenzton deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Konferenzton**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.7.1.4 Wie Sie die Zeitspanne für automatisches Beenden von Konferenzen ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Navigieren Sie im Menübaum zu **System** > **Zeitparameter**.
4) Wählen Sie in der Zeile bei **Zeit bis zum Aufmerksamkeitston bei HKZ-Transit-Verbindungen** in **Basis** und **Faktor** die gewünschte Zeit vom Verlassen der Konferenz durch den letzten Konferenzleiter bis zum Aufmerksamkeitston.
5) Wählen Sie in der Zeile bei **Zeit vom Aufmerksamkeitston bis zum Auslösen...** die gewünschte Zeit vom Aufmerksamkeitston bis zum automatischen Beenden der Konferenz.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.7.1.5 Wie Sie Details zu einer gespeicherten Konferenz abfragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Konferenzschaltung** zu starten.
4) Klicken Sie auf die betreffende Konferenz.
5) Klicken Sie auf **Anzeige**.

13.7.1.6 Wie Sie eine gespeicherte Konferenz löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Konferenzschaltung** zu starten.
4) Klicken Sie auf die betreffende Konferenz.
5) Klicken Sie auf **Löschen** und bestätigen Sie die Sicherheitsabfrage.

13.7.1.7 Konfiguration der Aufzeichnung von Konferenzen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Gespräch aufzeichnen**.
5) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie die Aufzeichnung von Konferenzen aktivieren möchten, aktivieren Sie das Kontrollkästchen **Aufzeichnung von Konferenzen verfügbar**.
   - Wenn Sie die Aufzeichnung von Konferenzen verhindern möchten, deaktivieren Sie das Kontrollkästchen **Aufzeichnung von Konferenzen verfügbar**.

6) Klicken Sie auf **Speichern**.

Anmerkung: Konferenzen, bei denen diese Funktion aktiviert ist, können weder übertragen noch gehalten werden.

13.7.2 Ad-hoc-Konferenz

Eine ad-hoc Konferenz findet spontan statt und wird vom Konferenzleiter manuell gestartet. Der Konferenzleiter kann Ad-hoc-Konferenzen speichern, um sie zu einem beliebigen Zeitpunkt erneut einzuberufen.

Starten der Konferenz

Das System öffnet bei allen internen Konferenzteilnehmern automatisch das Fenster mit dem virtuellen Konferenzraum, sofern der Konferenzteilnehmer myPortal for Desktop mit der klassischen Benutzeroberfläche oder myPortal for Outlook gestartet hat. Das System ruft alle Konferenzteilnehmer gleichzeitig an. Bei Eintritt in die Konferenz erhalten die Konferenzteilnehmer eine Begrüßungsansage, welche den Konferenzleiter nennt.

Aufzeichnen der Konferenz

Der Konferenzleiter kann die Konferenz manuell für sich und für alle verbundenen internen Konferenzteilnehmer aufzeichnen, sofern das Aufzeichnen von Gesprächen im System aktiviert ist. Teilnehmer des eigenen Knotens erhalten die Aufzeichnung in der Sprachbox, Teilnehmer an anderen Knoten per E-Mail. Die Dauer der Aufzeichnung ist nur durch die verfügbare Speicherkapazität des Systems begrenzt.

Beenden der Konferenz

Der Konferenzleiter kann die Konferenz im Client beenden oder durch Auflegen. Alternativ wird die Konferenz beendet, wenn alle Konferenzteilnehmer die Konferenz verlassen haben.

Erweitern eines Gesprächs zu einer Konferenz

Ein sich im Gespräch befindlicher interner Teilnehmer kann das Gespräch in eine Ad-hoc-Konferenz überführen und weitere Teilnehmer dazunehmen. Dafür muss der Teilnehmer eine UC Suite Conference Lizenz besitzen. Dieses Leistungsmerkmal ist nicht möglich bei CallMe.

13.7.3 Geplante Konferenz

Eine geplante Konferenz (Meet-Me-Konferenz) findet zu einem vorher festgelegten Termin mit festgelegter Dauer statt, eventuell wiederkehrend zur selben Uhrzeit.

Eine geplante Konferenz bleibt während des gesamten geplanten Zeitraums aktiv, unabhängig davon, ob Teilnehmer verbunden sind. Der Konferenzleiter speichert eine geplante Konferenz unter einem eigenen Namen.

Optionen beim Konfigurieren einer geplanten Konferenz

Der Initiator der Konferenz kann folgende Eigenschaften festlegen:

- Beginn- und Ende-Zeitpunkt
- Regelmäßig stattfindend
- Anwesenheit des Konferenzleiters erforderlich
- Authentifizierung der Konferenzteilnehmer beim Eintreten in die Konferenz erforderlich (durch Eingabe von Konferenz-ID und Kennwort über die Telefontastatur).

  Anmerkung: Mobility-Entry-Teilnehmer müssen vor ihrer Authentifizierung die Kennzahl für MFV-Nachwahl eingeben.

  Das Standardkennwort für Konferenzen ist 123456. Der Konferenzleiter kann dies für Konferenzteilnehmer individuell ändern.
- Sprache der Ansagen zu Konferenzbeginn
- Richtung des Verbindungsaufbaus für jeden einzelnen Konferenzteilnehmer (Standard: **Gehend**)

Starten der Konferenz

Das System öffnet zum geplanten Zeitpunkt bei allen internen Konferenzteilnehmern automatisch das Fenster mit dem virtuellen Konferenzraum, sofern der Konferenzteilnehmer myPortal for Desktop mit der klassischen Benutzeroberfläche oder myPortal for Outlook gestartet hat. Ist die Anwesenheit des Konferenzleiters erforderlich, ruft das System zunächst diesen an und erst nach seiner erfolgreichen Authentifizierung gleichzeitig alle weiteren Konferenzteilnehmer. Konferenzteilnehmer, die zur Sprachbox umgeleitet haben oder deren Anwesenheitsstatus signalisiert, dass sie abwesend sind, werden nicht gerufen. Je nach konfiguriertem Verbindungsaufbau ruft das System die Konferenzteilnehmer an oder diese können sich selbst einwählen. Das System kündigt jeden hinzukommenden Teilnehmer mittels Ansage namentlich an: `"... nimmt an der Konferenz teil."`, vorausgesetzt der Initiator hat seine Namensansage aufgezeichnet.

Anmerkung: Damit die Teilnehmer einer geplanten Konferenz ohne Authentifizierung zu Konferenzbeginn die Ansage mit dem Namen des Konferenzleiters hören, muss dieser zuvor einmal eine Konferenz mit Authentifizierung initiiert haben.

Einwahl

Mittels Einwahlnummer kann sich jeder Konferenzteilnehmer innerhalb des geplanten Zeitraums in die Konferenz einwählen, unabhängig von der für ihn festgelegten Richtung des Verbindungsaufbaus. Bei Einwahl außerhalb des geplanten Zeitraums erfolgt eine entsprechende Ansage. Bei Einwahl über einen ITSP muss dieser RFC 2833 (DTMF-Zeichen) unterstützen.

Erzwingen der Authentifizierung mit *-Taste

Der Konferenzleiter kann die Konferenz so konfigurieren, dass sich jeder Konferenzteilnehmer zumindest durch Drücken der *-Taste authentifizieren muss. Dies gewährleistet, dass nur anwesende Teilnehmer mit der Konferenz verbunden werden, jedoch keine Sprachbox.

Verlängerung der Konferenz

Zehn Minuten vor dem geplanten Konferenzende hören die Konferenzteilnehmer eine Ansage mit dem Hinweis auf das baldige Konferenzende und auf eine mögliche Verlängerung durch Wahl einer bestimmten Ziffer. Ein beliebiger Konferenzteilnehmer kann die Konferenz dann durch Wahl der entsprechenden Ziffer verlängern. Der Konferenzleiter kann die Konferenz in myPortal for Outlook zu einem beliebigen Zeitpunkt verlängern.

Aufzeichnen der Konferenz

Der Konferenzleiter kann die Konferenz automatisch oder manuell für sich und für alle verbundenen internen Konferenzteilnehmer aufzeichnen, sofern das Aufzeichnen von Gesprächen im System aktiviert ist. Teilnehmer des eigenen Knotens erhalten die Aufzeichnung in der Sprachbox, Teilnehmer an anderen Knoten per E-Mail. Die Dauer der Aufzeichnung ist nur durch die verfügbare Speicherkapazität des Systems begrenzt.

Beenden der Konferenz

Die Konferenz endet zum geplanten Konferenzende oder vorzeitig wenn der Konferenzleiter sie beendet.

13.7.4 Permanente Konferenz

Eine permanente Konferenz ist zeitlich unbegrenzt. Die Konferenzteilnehmer können sich jederzeit einwählen.

Der Konferenzleiter speichert eine permanente Konferenz unter einem eigenen Namen. Sie bleibt bestehen bis er sie löscht.

Optionen beim Konfigurieren einer permanenten Konferenz

Der Initiator der Konferenz kann festlegen:

- Ob sich die Konferenzteilnehmer beim Eintreten in die Konferenz durch Eingabe von Konferenz-ID und Kennwort über die Telefontastatur authentifizieren müssen.

  Anmerkung: Mobility-Entry-Teilnehmer müssen vor ihrer Authentifizierung die Kennzahl für DTMF-Nachwahl eingeben.

  Das Standardkennwort für Konferenzen ist 123456. Der Konferenzleiter kann dies für Konferenzteilnehmer individuell ändern.
- In welcher Sprache die Ansagen zu Konferenzbeginn erfolgen sollen.

Starten der Konferenz

Sobald sich der erste Konferenzteilnehmer einwählt, öffnet das System bei allen internen Konferenzteilnehmern automatisch das Fenster mit dem virtuellen Konferenzraum, sofern der Konferenzteilnehmer myPortal xA0;for xA0;Desktop oder myPortal xA0;for xA0;Outlook gestartet hat. Alle Konferenzteilnehmer wählen sich selbst ein. Das System kündigt jeden hinzukommenden Teilnehmer mittels Ansage an: "… nimmt an der Konferenz teil."

Einwahl

Mittels Einwahlnummer kann sich jeder Konferenzteilnehmer jederzeit in die Konferenz einwählen. Bei Einwahl über einen ITSP muss dieser RFC 2833 (DTMF-Zeichen) unterstützen.

Aufzeichnen der Konferenz

Der Konferenzleiter kann die Konferenz für sich und für alle verbundenen internen Konferenzteilnehmer aufzeichnen, sofern das Aufzeichnen von Gesprächen im System aktiviert ist. Teilnehmer des eigenen Knotens erhalten die Aufzeichnung in der Sprachbox, Teilnehmer an anderen Knoten per E-Mail. Die Dauer der Aufzeichnung ist nur durch die verfügbare Speicherkapazität des Systems begrenzt.

Die automatische Aufzeichnung einer permanenten Konferenz beginnt dann, wenn zwei oder mehrere Teilnehmer vorhanden sind und hört wieder auf, wenn weniger als zwei Teilnehmer vorhanden sind. Nach der Aufzeichnung erhalten alle Teilnehmer dieselbe Aufzeichnungsdatei der gesamten Konferenz.

13.7.5 Offene Konferenz

Eine offene Konferenz ist für eine bestimmte Anzahl beliebiger Teilnehmer. Jeder Teilnehmer, der über die Zugangsdaten verfügt, kann sich einwählen.

Der Konferenzleiter speichert eine offene Konferenz unter einem eigenen Namen. Sie bleibt bestehen bis er sie löscht.

Optionen beim Konfigurieren einer offenen Konferenz

Der Initiator der Konferenz kann festlegen:

- Die Anzahl der Konferenzteilnehmer (max. 16).
- Ob sich die Konferenzteilnehmer beim Eintreten in die Konferenz durch Eingabe von Konferenz-ID und Kennwort über die Telefontastatur authentifizieren müssen.

  Anmerkung: Mobility-Entry-Teilnehmer müssen vor ihrer Authentifizierung die Kennzahl für MFV-Nachwahl eingeben.

  Das Standardkennwort für Konferenzen ist 123456. Der Konferenzleiter kann dies für Konferenzteilnehmer individuell ändern.
- Welche gemeinsame Konferenz-ID für alle Konferenzteilnehmer gilt.
- In welcher Sprache die Ansagen zu Konferenzbeginn erfolgen sollen.

Starten der Konferenz

Alle Konferenzteilnehmer wählen sich selbst ein. Das System kündigt jeden hinzukommenden internen Teilnehmer mittels Ansage an: "`... nimmt an der Konferenz teil.`"

Einwahl

Mittels Einwahlnummer kann sich jeder Konferenzteilnehmer jederzeit in die Konferenz einwählen. Bei Einwahl über einen ITSP muss dieser RFC 2833 (DTMF-Zeichen) unterstützen.

Aufzeichnen der Konferenz

Der Konferenzleiter kann die Konferenz automatisch oder manuell für sich und für alle verbundenen internen Konferenzteilnehmer aufzeichnen, sofern das Aufzeichnen von Gesprächen im System aktiviert ist. Teilnehmer des eigenen Knotens erhalten die Aufzeichnung in der Sprachbox, Teilnehmer an anderen Knoten per E-Mail. Die Dauer der Aufzeichnung ist nur durch die verfügbare Speicherkapazität des Systems begrenzt.

13.8 Web Collaboration

Die UC PC Clients myPortal for Desktop (Windows) und myPortal for Outlook unterstützen innerhalb von Telefongesprächen und Konferenzen die komfortable Einbindung des separaten Produktes Web Collaboration für die gleichzeitige multimediale Zusammenarbeit. Diese bietet schnellen Zugriff auf Funktionen wie Desktop- und Anwendungsfreigabe, Dateifreigabe, Co-Browsing, Whiteboarding, URL-Push, IM-Chat und Video-Chat mit mehreren Teilnehmern.

Die Web Collaboration kann von einem Teilnehmer während eines Telefongesprächs über das Popup-Fenster des UC PC Clients oder innerhalb einer aktiven Konferenz vom Konferenzleiter gestartet werden. Dabei öffnet sich die Web Collaboration Sitzung. Eine lokale Installation von Web Collaboration auf dem UC PC Client ist nicht erforderlich. Ist auf dem UC PC Client ein E-Mail-Programm hinterlegt, kann den Gesprächsteilnehmern eine E-Mail mit dem Link auf den Web Collaboration Client zugesendet werden. Informationen zu Web Collaboration finden Sie in der Web Collaboration Produktdokumentation.

Beim Anlegen oder Bearbeiten einer Konferenz kann der Konferenzleiter eine Web Collaboration Sitzung mit einplanen. Beim Löschen oder Beenden einer Konferenz wird die zugehörige Web Collaboration Sitzung automatisch gelöscht.

Anmerkung: Damit UC PC Clients Web Collaboration automatisch starten können, muss beim Internetzugang der UC PC Clients über einen Proxy-Server die Proxy-Authentifizierung deaktiviert sein.

Unterstützte Arten von Verbindungen

Die Web Collaboration-Einbindung unterstützt Telefongespräche, telefongesteuerte Konferenzen sowie folgende Arten von applikationsgesteuerten Konferenzen:

- Ad-hoc-Konferenz
- Geplante Konferenz
- Permanente Konferenz

Einbindung von Web Collaboration

Für die Einbindung von Web Collaboration muss dem Kommunikationssystem die Adresse des Web Collaboration Servers bekannt gegeben werden. Der Hersteller bietet den Web Collaboration Server im Internet als Dienst an (Public Server). Alternativ kann es sich hier auch um einen Server im Kundennetz oder bei einem Partner handeln (Custom Server). Befindet sich der Server

im Kundennetz wird dieser vom Kommunikationssystem im Regelfall via http über den TCP-Port 5004 angesprochen. Bei der gehosteten Lösung im Internet (Public Server) wird hierfür eine gesicherte https-Verbindung verwendet, da über diese Verbindung Lizenznummer und Passwort übertragen werden. Standardmäßig wird dabei der TCP-Port 5100 verwendet.

Anmerkung: Für die Nutzung von Web Collaboration benötigt das Kommunikationssystem eine Internet-Verbindung (Default Router und DNS-Server). Verbindungen über Proxy werden nicht unterstützt.

Interne Konferenzteilnehmer mit UC PC Clients werden beim Starten der Konferenz automatisch mit der entsprechenden Web Collaboration Sitzung verbunden. Hierfür wird FastViewer automatisch im Hintergrund heruntergeladen und geöffnet, was einige Sekunden dauern kann. Externe Konferenzteilnehmer mit bekannter E-Mail-Adresse erhalten per E-Mail einen entsprechenden Link für die Web Collaboration-Sitzung.

Anmerkung: Benutzer unter MAC OS müssen nach Beendigung einer Web Collaboration Sitzung den Hinweisdialog für die beendete Sitzung manuell schließen.

Bei einer geplanten Konferenz ist das Verbinden mit der Web Collaboration Sitzung bereits ab 5 Minuten vor dem geplanten Beginn der Konferenz möglich.

Instant Messaging und Web Collaboration

Instant Messaging des Systems und Instant Messaging von Web Collaboration sind voneinander unabhängig: Sofortnachrichten aus einem UC PC Client erscheinen nicht in einer Web Collaboration Sitzung des selben Teilnehmers und umgekehrt.

13.8.1 Wie Sie die Verbindung zum Web Collaboration Server (Custom Server) konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Ein Internet-Zugang ist vorhanden.

Für eine gesicherte Verbindung zum Web Collaboration Server (Custom Server) benötigen Sie eine Lizenznummer und ein Passwort.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Web Services**.
3) Navigieren Sie im Menübaum zu **Web Services** > **Web Collaboration**.
4) Aktivieren Sie das Optionsfeld **Custom Server**.

5) Wenn Sie eine gesicherte Verbindung zum Web Collaboration Server (Custom Server) aufbauen möchten, gehen Sie folgendermaßen vor:
   a) Geben Sie in Feld **URL / IP-Adresse** die Adresse des Web Collaboration Servers (Custom Server) nach folgendem Muster ein:

      `https://<URL Web Collaboration Server>:5100/xmlrpcsecure`

      oder

      `https://<IP-Adresse Web Collaboration Server>:5100/xmlrpcsecure`
   b) Geben Sie im Feld **Lizenznummer** die Lizenznummer für die gesicherte Verbindung zum Web Collaboration Server (Custom Server) ein.
   c) Geben Sie in dem Feld **Passwort** das Passwort für die gesicherte Verbindung zum Web Collaboration Server (Custom Server) ein.
6) Wenn Sie eine ungesicherte Verbindung zum Web Collaboration Server (Custom Server) aufbauen möchten, gehen Sie folgendermaßen vor:
   a) Geben Sie in Feld **URL / IP-Adresse** die Adresse des Web Collaboration Servers (Custom Server) nach folgendem Muster ein:

      `http://<URL Web Collaboration Server>:5004/OscInterface`

      oder

      `http://<IP-Adresse Web Collaboration Server>:5004/OscInterface`
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.8.2 Wie Sie die Verbindung zum Web Collaboration Server (Public Server) konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Ein Internet-Zugang ist vorhanden.

Für die gesicherte Verbindung zum Web Collaboration Server (Public Server) benötigen Sie eine Lizenznummer und ein Passwort.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Web Services**.
3) Navigieren Sie im Menübaum zu **Web Services** > **Web Collaboration**.
4) Aktivieren Sie das Optionsfeld **Public Server**.
5) Geben Sie im Feld **Lizenznummer** die Lizenznummer für die gesicherte Verbindung zum Web Collaboration Server (Public Server) ein.
6) Geben Sie im Feld **Passwort** das Passwort für die gesicherte Verbindung zum Web Collaboration Server (Public Server) ein.

Anmerkung: Wenn Sie die Web Collaboration 5 min lang testen wollen, können Sie das Optionsfeld **Public**

Server (Demo Mode/Evaluation Mode) aktivieren. Hierfür benötigen Sie keine Lizenznummer und kein Passwort.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.8.3 Wie Sie die Verbindung zum Web Collaboration Server deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Web Services**.
3) Navigieren Sie im Menübaum zu **Web Services** > **Web Collaboration**.
4) Aktivieren Sie das Optionsfeld **Kein Web Collaboration Server**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**. Die Option zum Starten einer Web Collaboration Sitzung ist in den UC Clients deaktiviert.

13.9 Instant Messaging

Instant Messaging ist die Kommunikation mittels Sofortnachrichten (Chat).

13.9.1 Sofortnachricht versenden

Mittels Sofortnachrichten können Sie mit anderen Kommunikationspartnern chatten. Das System unterstützt sowohl Benutzer von UC Smart als auch einen externen Kommunikationspartner und Multi-User-Chat sowie beides in Kombination.

Sofortnachrichten sind mit folgenden Clients möglich:

- myPortal for Desktop
- myPortal for Outlook
- myAgent
- myAttendant

Als Administrator können Sie Sofortnachrichten systemweit aktivieren oder deaktivieren. Gesendete und empfangene Sofortnachrichten werden bei den Kommunikationspartnern als Dialog angezeigt. Beim Auswählen eines Empfängers zeigt der Client an, ob der Kommunikationspartner momentan online ist. Falls ein Kommunikationspartner offline ist, geschieht mit der Sofortnachricht abhängig von der Art des ausgewählten Empfängers Folgendes:

Empfänger	Verhalten
Einzelne Teilnehmer	Die Sofortnachricht wird bei der nächsten Anmeldung angezeigt.

Empfänger	Verhalten
Gruppe in Favoriten	Die Sofortnachricht wird bei jenen Teilnehmern die offline sind nie angezeigt.

Externe Sofortnachrichten

Als Teilnehmer können Sie mit *einem* externen Kommunikationspartner (z. B. Benutzer von Google Talk) chatten.

Multi-User Chat

Multi-User Chat ist der Austausch von Sofortnachrichten mit mehreren Kommunikationspartnern. Dabei unterstützt das System auch hier maximal einen externen Kommunikationspartner.

Instant Messaging und Web Collaboration

Instant Messaging des Systems und Instant Messaging einer Web Collaboration-Sitzung sind voneinander unabhängig: Sofortnachrichten aus einem UC PC-Client erscheinen nicht in einer Web Collaboration-Sitzung desselben Teilnehmers und umgekehrt.

13.9.1.1 Sofortnachrichten aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Allgemeine Einstellungen**.
5) Wählen Sie im Bereich **Sofortnachricht** eine der folgenden Möglichkeiten:
   - Wenn Sie Sofortnachrichten systemweit aktivieren möchten, deaktivieren Sie das Kontrollkästchen **Sofortnachricht versenden deaktivieren**.
   - Wenn Sie Sofortnachrichten systemweit deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Sofortnachricht versenden deaktivieren**.

   Anmerkung: Die Deaktivierung von Sofortnachrichten ist nicht wirksam für aktuell bestehende Sofortnachrichten-Fenster.
6) Klicken Sie auf **Speichern**.

13.10 AutoAttendant

AutoAttendant gibt Anrufern abhängig vom Anwesenheitsstatus des gerufenen Teilnehmers Auswahlmöglichkeiten für die Weiterleitung von Sprachanrufen

zu festgelegten Rufnummern oder zu dessen Sprachbox. Anrufer treffen ihre Auswahl durch Eingabe von Ziffern am Telefon.

13.10.1 Persönlicher AutoAttendant

Der persönliche AutoAttendant ist der vom Teilnehmer konfigurierbare AutoAttendant.

Persönlicher AutoAttendant

Als Teilnehmer können Sie für Ihre Rufnummer mit myPortal for Desktop oder mit myPortal for Outlook:

- Ansagen für den persönlichen AutoAttendant aufzeichnen oder importieren
- Profile für den persönlichen AutoAttendant konfigurieren

Entsprechende Anrufe werden zuerst vom zentralen AutoAttendant behandelt.

13.11 Sprach- und Faxnachrichten

Die im System integrierten Dienste Sprach- und Faxnachrichten ermöglichen Teilnehmern über myPortal for Desktop und myPortal for Outlook das Empfangen und Verwalten von Sprach- und Faxnachrichten. Mit Fax Printer können Teilnehmer Faxnachrichten senden.

13.11.1 Voicemail-Postfach

Die Sprachbox zeichnet zentral Sprachnachrichten und mitgeschnittene Gespräche auf. Teilnehmer können darauf telefonisch sowie mit UC Smart Clients zugreifen.

Anmerkung: Das voreingestellte Sprachbox-Passwort kann nur über eine interne Rufnummer geändert werden.

Es werden nur Sprachnachrichten aufgezeichnet, die länger sind als zwei Sekunden.

Verwaltung von Sprachnachrichten

Als Teilnehmer können Sie Ihre Sprachnachrichten abhören:

- über PC mit myPortal for Desktop oder myPortal for Outlook
- über Ihr Telefon, wenn Ihr Anwesenheitsstatus **Büro** oder **CallMe** lautet
- über ein beliebiges externes Telefon

Mit myAttendant kann der Vermittler auch Sprachnachrichten anderer Teilnehmer abhören, die dies ausdrücklich erlaubt haben.

Der Teilnehmer verwaltet die eingegangenen Sprachnachrichten über Ordner wie Posteingang, Abgespielt, Gespeichert oder Gelöscht.

Sprachnachrichten können auch wiedergegeben, angehalten und an einen anderen Teilnehmer weitergeleitet werden. Zusätzlich kann der Teilnehmer

Sprachnachrichten im .wav-Format abspeichern und an eine beliebige ausgewählte E-Mail-Adresse weiterleiten.

Über die Sprachbox verwaltet der Teilnehmer auch aufgezeichnete (mitgeschnittene) Gespräche. Aufgezeichnete Gespräche werden in der Sprachbox mit einem entsprechenden Symbol gekennzeichnet.

Anmerkung: Informationen zum Telefonmenü finden Sie in der Dokumentation UC Suite Telefon User Interface (TUI), Kurzbedienungsanleitung.

Absender einer Sprachnachricht zurückrufen

Beim Abhören einer Sprachnachricht kann der Teilnehmer direkt die Person zurückrufen, die ihm die Nachricht hinterlassen hat.

Als Administrator können Sie systemweit konfigurieren, ob Rückrufe aus der Sprachbox

- von jeder beliebigen Rufnummer ausgeführt werden können
- nur von eigenen Rufnummern des Teilnehmers ausgeführt werden können, welche in den Clients myPortal for Desktop, myPortal for Outlook, myAttendant bzw. myAgent unter Eigene persönliche Daten konfiguriert sind (**Nebenstelle**, **Mobilrufnummer**, **Externe Rufnummer 1**, **Externe Rufnummer 2**, **Private Rufnummer** und **Assistenten-Rufnummer**).

Aufbewahrungsdauer

Als Administrator können Sie die Aufbewahrungsdauer für Sprachnachrichten konfigurieren.

Priorisierung von Sprachnachrichten

Anrufer können ihre Sprachnachrichten als normal, dringend oder vertraulich markieren.

In myPortal for Desktop und myPortal for Outlook wird die Priorisierung der vorliegenden Sprachnachrichten durch unterschiedliche Farben dargestellt.

Hört der Teilnehmer seine Sprachnachrichten über Telefon ab, dann erhält er als Erstes die Information, wie viele Nachrichten dringend, vertraulich bzw. normal sind. Dringende Nachrichten werden zuerst wiedergegeben.

Werden die Sprachnachrichten als E-Mail weitergeleitet, werden als dringend gekennzeichnete Sprachnachrichten als E-Mail mit hoher Priorität gekennzeichnet.

Funktionsumfang der Sprachbox

Der Administrator kann den Umfang der Sprachbox festlegen. Er kann wählen zwischen:

- **Voll**

  Voller Funktionsumfang der Sprachbox (Standardwert)
- **Kurzmenü**
- Nach der statusbezogenen oder persönlichen Ansage wird das Verbinden zum Empfang angeboten.
- **Kein Menü**

- Nach der Begrüßungsansage wird der Anrufer direkt zur Nachrichten-Aufzeichnung weitergeleitet.

Neue Nachrichten auf dem Telefon anzeigen

Sprachnachrichten werden am Telefon angezeigt. Sobald die Sprachnachricht abgespielt wurde, werden die Anzeigen gelöscht.

Die Art der Signalisierung neuer Sprachnachrichten ist endgerätespezifisch

- Für alle Telefone erfolgt eine akustische Signalisierung mittels Sonderwählton.
- Bei Systemtelefonen ohne Display leuchtet zusätzlich die Briefkasten-Taste (wenn eingerichtet).
- Bei Systemtelefonen mit Display leuchtet die Briefkasten-Taste (wenn eingerichtet) und im Display wird eine Meldung ausgegeben.

Benachrichtigungsdienst

Über myPortal oder myPortal for Desktop kann der Teilnehmer festlegen, ob die Information über das Eintreffen einer neuen Sprachnachricht weitergeleitet werden soll und zu welchem Ziel.

Der Teilnehmer kann bestimmen, ob die Nachricht als E-Mail weitergeleitet wird. Weiterhin kann der Teilnehmer bestimmen, ob er beim Eintreffen einer neuen Sprachnachricht durch einen Telefonanruf oder durch eine SMS benachrichtigt wird.

Sprache der Sprachbox

Als Administrator können Sie systemweit die standardmäßige Sprache der Sprachbox für das Menü und die systemeigenen Ansagen wählen.

Abhängigkeiten

Themenbereich	Abhängigkeit
Nachricht über Telefon wiedergeben	Der Teilnehmer kann Sprachnachrichten über Telefon nur im Anwesenheitsstatus **Büro** oder **CallMe** abspielen. Bei allen anderen Einstellungen kann er die Nachricht nur über PC abspielen.

13.11.1.1 Wie Sie die Rufnummer der Sprachbox konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Voicemail** zu starten.
4) Geben Sie die **VoiceMail Nummer** ein.
5) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

13.11.1.2 Wie Sie die Rufweiterschaltung zur Sprachbox konfigurieren

Mit dem Wizard **Rufweiterschaltung** können Sie für einen Teilnehmer die Rufweiterschaltung zu seiner Sprachbox konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Rufweiterschaltung** zu starten. Es öffnet sich das Fenster **Anrufweiterschaltung konfigurieren**.
4) Wählen Sie im Bereich **Teilnehmer auswählen** den gewünschten Teilnehmer aus.
5) Ziehen Sie die **Sprachbox** mit der Maus und legen Sie sie im Fensterbereich **Rufweiterschaltung für Teilnehmer parametrieren** ab.
6) Ändern Sie ggf. die Zeit bis zur Rufweiterschaltung (Standard: 15 Sekunden).
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

13.11.1.3 Parameter der Sprachbox konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf die Registerkarte **VoiceMail**.
5) Wählen Sie in der Aufklappliste **VoiceMail-Sprache** die Sprache für die Menüsteuerung und die vordefinierten Ansagen Ihrer Sprachbox aus.
6) Legen Sie im Feld **Wiedergabereihenfolge für Sprachnachrichten** fest, in welcher Reihenfolge die Nachrichten abgespielt werden sollen.
7) Geben Sie im Feld **Aufzeichnungszeit Sprachnachricht** die Dauer in Sekunden ein.
8) Legen Sie im Feld **VoiceMail-Modus** den Umfang der Sprachbox fest.
9) Wenn Sie wollen, dass Rückrufe aus der Sprachbox nur an Rufnummern ausgeführt werden sollen, die in den UC Clients unter **Eigene persönliche Daten** eingetragen sind, aktivieren Sie das Kontrollkästchen **Rückruf von VM nur an bekannte Nummer zulassen**.
10) Wenn Sie die letzte vom System wiedergegebene Ansage ausschalten wollen, wählen Sie das Kontrollkästchen **Aufforderung zum Hinterlassen einer Nachricht nach dem Signalton überspringen**. Die Systemansage wird nicht mehr wiedergegeben, auch wenn eine professionell aufgenommene Ansage verwendet wird.

11) Klicken Sie auf **Speichern**.

13.11.1.4 Wie Sie die Aufbewahrungsdauer für Sprachnachrichten konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Wartung**.
5) Geben Sie in den Feldern unter **Nachricht** jeweils die Aufbewahrungszeit in Tagen ein.
6) Klicken Sie auf **Speichern**.

13.11.1.5 Kennwortabfrage der Sprachbox aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Benutzerverzeichnis**.
4) Klicken Sie auf den entsprechenden Eintrag und dann auf **Bearbeiten** > **Sensibilität**.
5) Klicken Sie auf **Sicherheit und Zugriff**.
6) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie die Kennwortabfrage bei Anruf Ihrer Sprachbox aktivieren möchten, deaktivieren Sie das Kontrollkästchen **Bei Anruf der VoiceMail Kennwort umgehen**.
   - Wenn Sie die Kennwortabfrage bei Anruf Ihrer Sprachbox deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Bei Anruf der VoiceMail Kennwort umgehen**.
7) Klicken Sie auf **Speichern**.

13.11.1.6 Wie Sie eine Info für empfangene Sprachnachrichten konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System**.
4) Klicken Sie im Menübaum auf **Display**.
5) Aktivieren Sie im Bereich **Schalter** das Kontrollkästchen **Displaystatusanzeige bei Info-Meldung**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.11.1.7 Wie Sie die Briefkastentaste für die Abfrage von Sprachnachrichten konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Endgeräte / Teilnehmer**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Tastenprogrammierung** zu starten.
4) Wählen Sie den betreffenden Teilnehmer aus.
5) Wählen Sie in der erste Spalte die entsprechende Taste aus.
6) Wählen Sie in der Spalte **Tastenfunktionen** die Funktion **Briefkasten** aus.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.11.2 Ansagen der Sprachbox

Ansagen der Sprachbox informieren Anrufer z.B. über den Anwesenheitsstatus eines Teilnehmers.

Standardansagen sind in allen Sprachen vorhanden. Als Teilnehmer können Sie persönliche Ansagen für die Sprachbox aufzeichnen oder importieren. Die entsprechende Standardansage wird dabei durch die persönliche Ansage überschrieben. Als Administrator können Sie die Standardansagen durch den Import von Ansagen ändern. Persönliche Ansagen von Teilnehmern werden dabei überschrieben. Das System führt beim Importieren von Ansagen automatisch eine Pegelbegrenzung und Normalisierung durch, um die Anforderungen gemäß "USA / TIA 968 Signal Power Limitations" zu erfüllen.

Anmerkung: Stellen Sie vor der Benutzung von Ansagen bzw. Musik aus anderer Quelle sicher, dass Sie keine Copyright-Verletzung begehen.

Systemsprache Ansagen der Sprachbox

Die Systemsprache der Sprachbox wird bei der Länderinitialisierung eingestellt. Zusätzlich kann der Teilnehmer die Sprache seiner Sprachbox selbst

einstellen. Ein Anrufer hört dann die teilnehmerbezogenen Ansagen in vom Teilnehmer eingestellten Sprache und die systembezogenen Ansagen in der Systemsprache.

Ansagen in Abhängigkeit von Anwesenheitsstatus und Profil

Abhängig vom Anwesenheitsstatus ändern sich automatisch die Ansagen der Sprachbox, z.B.: Ist der Anwesenheitsstatus **Besprechung**, dann lautet die Ansage z.B.: Der Teilnehmer ist in einer Besprechung bis heute 15.00 Uhr. Wenn das eingetragene Ende einer Besprechung erreicht ist, aber der Teilnehmer seinen Anwesenheitsstatus noch nicht auf Büro zurückgeändert hat, dann wird die Ansage der Sprachbox automatisch angepasst oder der Anwesenheitsstatus wechselt automatisch zurück auf Büro (durch den Teilnehmer konfigurierbar).

Die folgende Tabelle beschreibt, welche Begrüßung der Anrufer abhängig vom gesetzen Anwesenheitsstatus und dem eingestellten Profil hört. Das Anrufermenü bezieht sich auf den zentralen AutoAttendant. Das Profil bezieht sich auf den persönlichen AutoAttendant des Teilnehmers. Standardbegrüßung, Name und benutzerdefinierte Begrüßung für Profile sind vom Teilnehmer aufzuzeichnen. Abhängig von der Konfiguration kann das Anrufermenü unterschiedlich lang oder auch nicht verfügbar sein.

	Besetzt Nicht angenommen Anrufschutz	Besprechung Sick Pause Außer Haus ...
Sprachbox mit Anwesenheitsstatus	Standardbegrüßung + Anrufermenü	Name + Anwesenheitsstatus + Anrufermenü
Sprachbox bei gesperrtem Anwesenheitsstatus	Standardbegrüßung + Anrufermenü (wenn aktiviert)	
Profile mit dynamischer Ansage	Benutzerdefinierte Begrüßung für Profil	Name + Anwesenheitsstatus + Benutzerdefinierte Begrüßung für Profil
Profile, wenn dynamische Ansage übersprungen werden soll	Benutzerdefinierte Begrüßung für Profil	

Hat ein Teilnehmer eingestellt, dass sein Präsenzstatus nicht an einen externen Anrufer übermitteln werden soll, bekommt der externe Anrufer bei jedem Anwesenheitsstatus außer "Büro" die "Besetzt"-Begrüßung, obwohl der angerufene Teilnehmer u.U. gar nicht besetzt ist. In diesem Fall sollte der Teilnehmer für die Begrüßung "Besetzt" eine Ansage definieren, dass er den Anruf nicht entgegennehmen kann.

13.11.2.1 Ansage für die Sprachbox importieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Einzuspielende Audiodateien liegen als PCM-Dateien mit folgenden Eigenschaften vor: 8 kHz, 16 bit, mono. Die Länge des Audio-Dateinamens beträgt maximal 30 Zeichen.

Anmerkung: Sie können im Vorfeld mit Audio Wizard geeignete Audiodateien erstellen und dabei zwei Quellen abmischen, z.B. Hintergrundmusik und Ansage.

Tipp: Stellen Sie vor der Benutzung sicher, dass Sie keine Copyright-Verletzung begehen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.
4) Wählen Sie in der Registerkarte **Audiodatei-Manager** als **Upload-Ziel** den Eintrag **VoiceMail-Begrüßung** aus.
5) Wenn Sie eine Audio-Datei einspielen wollen, gehen Sie folgendermaßen vor:
   a) Wählen Sie das Optionsfeld **Uploader** und klicken Sie auf **Datei auswählen**, um eine geeignete Audiodatei auszuwählen.
   b) Im Bereich **Details Audiodatei** sehen Sie die Eigenschaften der Audio-Datei, wie Dateiname, Dateigröße, Bitrate usw.
   c) Klicken Sie auf **Upload**.
6) Wenn Sie eine Ansage über ein Telefon aufnehmen wollen, gehen Sie folgendermaßen vor:
   a) Wählen Sie das Optionsfeld **Aufzeichnungsgerät** und unter **Nebenstelle** das Telefon, mit dem die Ansage aufgezeichnet werden soll.
   b) Geben Sie in das Feld **Dateiname** den Namen der Aufnahmedatei ein.
   c) Klicken Sie auf **Anrufen**. Das ausgewählte Telefon klingelt.
   d) Heben Sie den Telefonhörer ab und klicken Sie auf **Aufzeichnen**.
   e) Sprechen Sie Ihre Ansage in den Telefonhörer und klicken Sie abschließend auf **Beenden**.
   f) Mit **Wiedergeben** können Sie sich Ihre Aufzeichnung nochmals anhören.

13.11.2.2 Sprache für Ansagen der Sprachbox ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **VoiceMail**.
5) Wählen Sie die **VoiceMail-Sprache** aus der Aufklappliste aus.
6) Klicken Sie auf **Speichern**.

13.11.3 Faxbox

Die Faxbox ermöglicht Teilnehmern das Empfangen und Verwalten von Faxnachrichten ohne Faxgerät über myPortal for Desktop oder myPortal for Outlook.

Als Administrator können Sie für lizenzierte Teilnehmer eine Faxbox konfigurieren. Außerdem können Sie Faxgeräte oder Faxserver über die a/b- bzw. ISDN-Schnittstelle anschließen.

Über myPortal for Desktop oder myPortal for Outlook können Sie als Teilnehmer auf Ihre Faxnachrichten zugreifen. myAttendant kann auf die Faxnachrichten der Teilnehmer zugreifen, die dies zulassen.

Verwaltung von Faxnachrichten

Der Teilnehmer kann die empfangenen Faxnachrichten verwalten, indem er sie in die Ordner, wie z. B. Gespeichert oder Gelöscht, verschiebt. Die Faxnachrichten können an einen anderen Teilnehmer weitergeleitet werden. Zusätzlich kann der Teilnehmer Faxnachrichten als PDF- oder TIFF-Datei speichern und an eine beliebige E-Mail-Adresse weiterleiten.

Der Administrator kann systemweit einrichten, ob die Faxnachricht als TIFF-Datei (Standard) oder als PDF-Datei gespeichert werden soll.

Anmerkung: Um eine TIFF-Datei in eine PDF-Datei zu konvertieren, muss die Seite im Format A4 vorliegen.

Aufbewahrungsdauer für Faxnachrichten

Das System löscht automatisch Faxnachrichten, deren Alter folgende Aufbewahrungsdauer überschreitet:

Faxnachricht	Aufbewahrungsdauer (Tage)
Neu	120
Gelesen	365
Gesendet	365
Gelöscht	60

13.11.3.1 Wie Sie eine Faxbox für Teilnehmer hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Endgeräte/Teilnehmer**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **IP-Endgeräte** zu starten.
4) Klicken Sie in das Feld **Fax Rufnr** des Teilnehmers und geben Sie die Fax-Rufnummer ein, unter welcher der Teilnehmer Faxnachrichten empfangen kann (der vorbelegte Bindestrich muss gelöscht werden).
5) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, klicken Sie in das Feld **Fax Durchwahl** und geben die Fax-Durchwahlnummer ein (der vorbelegte Bindestrich muss gelöscht werden).
6) Klicken Sie auf **OK & Weiter**. Bei Bedarf können Sie sich über **Drucken** eine Teilnehmerliste mit den konfigurierten Fax-Rufnummern ausdrucken lassen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**, um den Wizard abzuschließen.

13.11.3.2 Wie Sie den Dateityp für gespeicherte Faxnachrichten (UC Suite) konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Allgemeine Einstellungen**.
5) Wenn Sie möchten, das Faxnachrichten als PDF-Dateien abgespeichert werden können, dann aktivieren Sie im Bereich **Faxformat** das Kontrollkästchen **Als Faxformat PDF verwenden**.
6) Wenn Sie möchten, das Faxnachrichten als TIFF-Dateien abgespeichert werden können, dann deaktivieren Sie im Bereich **Faxformat** das Kontrollkästchen **Als Faxformat PDF verwenden**.
7) Klicken Sie auf **Speichern**.

13.11.4 Senden von Faxnachrichten mit Fax Printer

Fax Printer ist eine Anwendung für den Versand von Faxnachrichten aus Windows-Anwendungen wie z. B. Microsoft Word mit zentral bereitgestellten oder individuell erstellten Deckblättern.

Fax Printer besteht aus folgenden Komponenten:

- Fax Printer Cover Editor
- Fax Printer Driver

Fax Printer kann mit allen gängigen Windows-Programmen verwendet werden. Fax-Gruppen erleichtern die Verteilung. Faxnachrichten werden als E-Mail oder

direkt auf den Desktop gesendet. Ein Popup-Fenster informiert den Teilnehmer über den Erfolg des Versands.

Kopfzeilen

Als Administrator können Sie verschiedene Kopfzeilen für die Benutzer von Fax Printer konfigurieren. Sie können eine Kopfzeile als Standard festlegen. Kopfzeilen können folgende Elemente enthalten:

Detail	Platzhalter
Datum / Uhrzeit	{{date_time}}
Firmenname	{{company_name}}
Benutzername	{{user_name}}
Firmen-Rufnr.	{{company_number}}
Seitenzahl	{{page_number}}
Anzahl der Seiten	{{page_count}}

Kopfzeilen von Faxnachrichten, die mit Fax Printer gesendet werden, dürfen nur Zeichen des ANSI-Zeichensatzes enthalten. Anders gesagt, es dürfen keine Sonderzeichen oder Umlaute verwendet werden. Da die Kopfzeile grundsätzlich den Namen des Absenders enthalten kann, dürfen die Namen der Teilnehmer keine Sonderzeichen oder Umlaute enthalten.

13.11.4.1 Zentrales Fax-Deckblatt hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Ein Fax-Deckblatt liegt als .ocp-Datei vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.
4) Klicken Sie auf die Registerkarte **Upload des zentralen Fax-Deckblatts**.
5) Klicken Sie auf **Datei auswählen**.
6) Wählen Sie eine .ocp-Datei aus.
7) Klicken Sie auf **Öffnen**.
8) Geben Sie unter **Name** einen Namen für das Fax-Deckblatt ein.
9) Geben Sie eine **Beschreibung** für das Fax-Deckblatt ein.
10) Klicken Sie auf **Upload**.
11) Klicken Sie nach beendetem Upload auf **OK**.
12) Wenn Sie dieses Fax-Deckblatt als Standardeinstellung übernehmen möchten, klicken Sie in der Liste der Fax-Deckblätter auf dieses Fax-Deckblatt und anschließend auf **Als Standardeinstellung übernehmen**.
13) Klicken Sie auf **Speichern**.

13.11.4.2 Zentrales Fax-Deckblatt bearbeiten

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.
4) Klicken Sie auf die Registerkarte **Upload des zentralen Fax-Deckblatts**.
5) Klicken Sie in der Liste der Fax-Deckblätter auf das entsprechende Fax-Deckblatt.
6) Klicken Sie auf **Bearbeiten**.
7) Geben Sie unter **Name** einen Namen für das Fax-Deckblatt ein.
8) Geben Sie eine **Beschreibung** für das Fax-Deckblatt ein.
9) Klicken Sie auf **Speichern**.

13.11.4.3 Kopfzeile für Fax Printer hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Assistenten **Faxkopfzeilen** zu starten.
4) Klicken Sie auf **Hinzufügen**.
5) Geben Sie den **Template-Namen** für die Faxkopfzeile ein.
6) Um Details zur Kopfzeile hinzuzufügen, klicken Sie in der gewünschten Reihenfolge auf die entsprechende Schaltflächen **Datum/Uhrzeit**, **Firmenname**, **Benutzername**, **Firmen-Rufnr.**, **Seitenzahl** und **Anzahl der Seiten**. Für jedes Detail erscheint ein entsprechender Platzhalter im Feld **Text**.
7) Um ein Detail aus der Kopfzeile zu entfernen, markieren Sie in Feld **Text** den entsprechenden Platzhalter, z. B. `{{page_count}}` (**Anzahl der Seiten**) und drücken Sie die Taste `Entf`.
8) Geben Sie bei Bedarf in Feld **Text** zusätzlichen Text ein, z. B. " von " zwischen den Platzhaltern `{{page_number}}` (**Seitennummer**) und `{{page_count}}` (**Anzahl der Seiten**)
9) Klicken Sie auf **Speichern**.

13.11.4.4 Kopfzeile für Fax Printer ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **UC Suite**.
3) Klicken Sie auf **Faxkopfzeilen**.
4) Klicken Sie in der Liste der Faxkopfzeilen auf die gewünschte Faxkopfzeile.
5) Klicken Sie auf **Bearbeiten**.
6) Geben Sie den **Template-Namen** für die Faxkopfzeile ein.
7) Um Details zur Kopfzeile hinzuzufügen, klicken Sie in der gewünschten Reihenfolge auf die entsprechende Schaltflächen **Datum/Uhrzeit**, **Firmenname**, **Benutzername**, **Firmen-Rufnr.**, **Seitenzahl** und **Anzahl der Seiten**. Für jedes Detail erscheint ein entsprechender Platzhalter im Feld **Text**.
8) Um ein Detail aus der Kopfzeile zu entfernen, markieren Sie in Feld **Text** den entsprechenden Platzhalter, z. B. `{{page_count}}` (**Anzahl der Seiten**) und drücken Sie die Taste `Entf`.
9) Geben Sie bei Bedarf in Feld **Text** zusätzlichen Text ein, z. B. " von " zwischen den Platzhaltern `{{page_number}}` (**Seitennummer**) und `{{page_count}}` (**Anzahl der Seiten**)
10) Klicken Sie auf **Speichern**.

13.11.4.5 Wie Sie eine Kopfzeile für Fax Printer löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Faxkopfzeilen** zu starten.
4) Klicken Sie in der Liste der Faxkopfzeilen auf die gewünschte Faxkopfzeile.
5) Klicken Sie auf **Entfernen**.

13.11.5 Benachrichtigungsdienst für neue Nachrichten (UC Suite)

Das System kann Sie als Teilnehmer über eine neue Nachricht auf Wunsch per E-Mail, telefonisch oder per SMS informieren.

Der Benachrichtigungsdienst arbeitet folgendermaßen:

Benachrichtigung	für Sprachnachricht	für Faxnachricht	Voraussetzungen
E-Mail	Sie erhalten eine E-Mail mit der Nachricht als angehängte WAV-Datei, Datum und Uhrzeit des Empfangs, Dauer der Nachricht und sofern verfügbar Rufnummer sowie Name des Absenders. Falls die Größe der WAV-Datei 10 MB (Durchschnitt: 1 MB/Min.überschreitet, wird sie nicht an die E-Mail angehängt. Sprachnachrichten mit Priorität "Dringend" werden als E-Mail mit Wichtigkeit "Hoch" zugestellt. E-Mails mit einer Sprachnachricht haben in Outlook ein eigenes Symbol. Falls Sie ein IMAP-Postfach verwenden, welches nur die E-Mail-Header anzeigt, erscheint stattdessen das für E-Mails übliche Symbol.	Sie erhalten eine E-Mail mit der Nachricht als angehängte PDF- oder TIFF-Datei, Datum und Uhrzeit des Empfangs, Anzahl der Seiten und sofern verfügbar Rufnummer sowie Name des Absenders. Falls die Größe der PDF- oder TIFF-Datei 10 MB überschreitet, wird sie nicht an die E-Mail angehängt. E-Mails mit einer Faxnachricht haben in Outlook ein eigenes Symbol. Falls Sie ein IMAP-Postfach verwenden, welches nur die E-Mail-Header anzeigt, erscheint stattdessen das für E-Mails übliche Symbol.	E-Mail-Versand ist im System konfiguriert. Die entsprechende Adresse wird als Absender verwendet.
SMS	Sie erhalten eine SMS an die von Ihnen festgelegte Rufnummer über den Eingang der Nachricht		SMS-Template ist konfiguriert
telefonisch	Ihre Sprachbox ruft Sie unter der von Ihnen festgelegten Rufnummer an und spielt die Nachricht ab.	-	

Sie können als Teilnehmer jede Art der Benachrichtigung für jeden Anwesenheitsstatus separat aktivieren oder deaktivieren. Die telefonische Benachrichtigung können Sie auf die vom Administrator konfigurierten Geschäftszeiten einschränken. Sie können Anzahl und Intervalle für wiederholte Versuche der telefonischen Benachrichtigung festlegen.

13.11.6 E-Mail-Versand

E-Mail-Versand ermöglicht die Benachrichtigung von Teilnehmern bei neuen Sprach- und Faxnachrichten sowie des Administrators bei Systemmeldungen.

13.11.6.1 E-Mail-Versand konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Es ist ein E-Mail-Konto mit einem Kennwort bei einem E-Mail-Provider vorhanden und Sie kennen die Zugangsdaten.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Service-Center** > **E-Mail-Weiterleitung**.
3) Geben Sie den **Postausgangs-Server (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll, z. B. `smtp.web.de`. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.

   Anmerkung: In einigen Fällen funktioniert der E-Mail-Versand nicht, weil der Name des Postausgangs-Servers nicht aufgelöst werden kann. Zur Behebung des Problems müssen Sie anstelle des Namens die IP-Adresse des Servers eingeben.

4) Wenn eine sichere Verbindung erforderlich ist, aktivieren Sie das Kontrollkästchen. Erfragen Sie ggf. bei Ihrem E-Mail-Provider, ob diese Option aktiviert werden muss.
5) Geben Sie den **Benutzername** des E-Mail-Kontos ein.
6) Geben Sie unter **Kennwort** und **Kennwort wiederholen** das Kennwort des E-Mail-Kontos ein.
7) Geben Sie die **E-Mail-Adresse** ein, z. B. `max.mustermann@web.de`.
8) Wenn Sie den E-Mail-Versand nun testen möchten, gehen Sie folgendermaßen vor:
   a) Klicken Sie auf **Verbindung testen**.
   b) Geben Sie unter **Senden an E-Mail-Adresse** die E-Mail-Adresse eines E-Mail-Postfachs ein, auf das Sie Zugriff haben.
   c) Geben Sie den **Betreff** in der E-Mail ein.
   d) Klicken Sie auf **Testmail senden**.
   e) Prüfen Sie, ob Sie die E-Mail erhalten haben.
   f) Wenn der E-Mail-Versand nicht erfolgreich war, klicken Sie auf **Zurück** und korrigieren Sie Ihre E-Mail-Einstellungen (ab Schritt 3).
9) Geben Sie die **E-Mail-Adresse 1** ein, um eine Benachrichtigungs-E-Mail zu erhalten, wenn die ALI-Toleranz verwendet wurde. Sie können auch eine zweite E-Mail-Adresse eingeben.
10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Beispiel

Anmerkung: Wenn Sie Konfigurationsänderungen in der E-Mail-Weiterleitung auf einem OpenScape Business X-System mit Booster Server vornehmen, müssen Sie den Booster Server neu starten, damit die Änderungen wirksam werden.

13.11.7 SMS-Template

Ein SMS-Template ermöglicht die SMS-Benachrichtigung von Teilnehmern bei neuen Sprachnachrichten.

Zum Empfang von SMS-Benachrichtigungen muss zunächst eine persönliche mobile E-Mail-Adresse des jeweiligen Providers aktiviert werden. Der Teilnehmer sendet dazu eine Aktivierungs-SMS an eine Kurzwahl-Nummer. Der Teilnehmer erhält dann per SMS seine persönliche E-Mail-Adresse, die sich in der Regel aus der Rufnummer und dem Gateway-Namen zusammensetzt. So wäre z.B. für einen T-Mobile-Kunden mit der Rufnummer 0171/1234 567 die mobile E-Mail-Adresse: 01711234567@t-mobile-sms.de. Analog gilt dies auch für andere Netze.

Ein SMS-Template besteht aus den Bereichen Template-Details und SMS-Details. Der Administrator muss im Bereich Template-Details den Namen des Templates eingeben, der üblicherweise der Name des E-Mail-to-SMS-Providers ist.

Die Angaben im Bereich SMS-Details sind abhängig vom Provider. Bei Empfänger muss der Administrator die E-Mail-Adresse eingeben, an welche die SMS geschickt werden soll. Die Angaben in der Betreffzeile sind entweder frei wählbar oder der Administrator muss hier z.B. die Kundennummer eintragen.

Anmerkung: Jeder Provider benötigt ein spezifisches Template. Die erforderlichen Daten erfahren Sie beim jeweiligen Mobilfunk-Provider.

Platzhalter

SMS-Templates können in Feld **Empfänger**, **Betreff** oder **Text** folgende Platzhalter enthalten:

Detail	Platzhalter
Die Mobilfunknummer, an die gesendet werden soll	`{{MobileNumber}}`
Name oder Rufnr. des Absenders	`{{Sender}}`
Datum und Uhrzeit des Nachrichteneingangs	`{{DateTime}}`
Rufnummer des Anrufers	`{{CallingNumber}}`
Priorität der Nachricht	`{{Priority}}`

Systemspezifische Informationen

Die Länge der Nachricht wird auf die ersten 160 Zeichen reduziert.

13.11.7.1 SMS-Template hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Templates** zu starten.
4) Klicken Sie auf **Hinzufügen**.

5) Geben Sie **Template-Name** ein.

Anmerkung: Der Vorlagenname darf keine Leerzeichen enthalten.

---

6) Geben Sie **Name des Autors** ein.
7) Wenn Sie einen Platzhalter einfügen möchten, führen Sie folgende Schritte durch:
   a) Klicken Sie in das Feld, in dem Sie den Platzhalter einfügen möchten: **Empfänger**, **Betreff** oder **Text**.
   b) Wählen Sie aus der Dropdown-Liste **VSL-Felder** den gewünschten Platzhalter aus.
   c) Klicken Sie auf **Einfügen**.
   d) Wenn Sie weitere Platzhalter einfügen möchten, wiederholen Sie Schritt 7 a-c entsprechend.
8) Geben Sie den **Empfänger** ein.
9) Geben Sie den **Betreff** ein.
10) Geben Sie den **Text** ein.
11) Klicken Sie auf an **Erstellen**.

13.11.7.2 SMS-Template bearbeiten

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Templates** zu starten.
4) Wählen Sie die gewünschte SMS-Vorlage aus der Tabelle **SMS-Dienstanbieter** aus.
5) Klicken Sie auf **Bearbeiten**.
6) Geben Sie **Template-Name** ein.

Anmerkung: Der Vorlagenname darf keine Leerzeichen enthalten.

---

7) Geben Sie **Name des Autors** ein.
8) Wenn Sie einen Platzhalter einfügen möchten, führen Sie folgende Schritte durch:
   a) Klicken Sie in das Feld, in dem Sie den Platzhalter einfügen möchten: **Empfänger**, **Betreff** oder **Text**.
   b) Wählen Sie aus der Dropdown-Liste **VSL-Felder** den gewünschten Platzhalter aus.
   c) Klicken Sie auf **Einfügen**.
   d) Wenn Sie weitere Platzhalter einfügen möchten, wiederholen Sie Schritt 8 a-c entsprechend.
9) Geben Sie den **Empfänger** ein.

10) Geben Sie den **Betreff** ein.
11) Geben Sie den **Text** ein.
12) Klicken Sie auf an **Erstellen**.

13.11.7.3 Wie Sie ein SMS-Template entfernen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Templates** zu starten.
4) Wählen Sie die gewünschte SMS-Vorlage aus der Tabelle **SMS-Dienstanbieter** aus.
5) Klicken Sie auf **Entfernen**.
6) Klicken Sie auf **OK**.

13.11.8 Fax over IP (T.38 / G.711-Fax)

Fax over IP ermöglicht die Übertragung von Faxnachrichten nach Standard G2 und G3 über das Internet mittels Netzwerkprotokoll IFP (Internet Facsimile Protocol).

UC Suite kann generell bis zu 8 gleichzeitige Faxverbindungen verarbeiten. OpenScape Busines X3/X5/X8 als ISDN-Gateway kann abhängig vom DSP-Modul 3 bis 12 gleichzeitige Faxe verarbeiten. Beide Parameter bestimmen die Anzahl gleichzeitiger T.38- oder G.711-Faxverbindungen.

Anmerkung: Sofern möglich wird die Verwendung von T.38-Fax empfohlen.

Das System unterstützt für T.38 oder G.711 folgende Szenarien:

- Ein Teilnehmer erhält Faxnachrichten über einen ITSP (Internet Telefonie Service Provider) an seine Faxbox und versendet mit Fax Printer über den ITSP nach extern.
- Ein Teilnehmer erhält Faxnachrichten über Mediatrix 4102S (SIP) an seine Faxbox und versendet mit Fax Printer über Mediatrix 4102S (SIP).
- Ein Teilnehmer erhält Faxnachrichten über einen ITSP (Internet Telefonie Service Provider) auf ein Faxgerät, das direkt an einer analogen oder ISDN-Schnittstelle angeschlossen ist und versendet von diesem Faxgerät über den ITSP nach extern.
- Ein Teilnehmer erhält Faxnachrichten über einen ITSP auf ein Faxgerät, das an Mediatrix 4102S angeschaltet ist und versendet von diesem Faxgerät über Mediatrix 4102S und ITSP nach extern.
- Ein Teilnehmer erhält Faxnachrichten über ISDN auf ein Faxgerät, das an Mediatrix 4102S angeschaltet ist und versendet von diesem Faxgerät über Mediatrix 4102S und ISDN nach extern.

- Ein Teilnehmer versendet Faxnachrichten von einem Faxgerät, das an Mediatrix 4102S angeschaltet ist auf ein anderes Faxgerät, das auch an Mediatrix 4102S angeschaltet ist.
- Interne Faxnachricht von einem Faxgerät an einer ISDN-Schnittstelle an ein Faxgerät an Mediatrix 4102S und umgekehrt.
- Interne Faxnachricht von einem Faxgerät an einer ISDN-Schnittstelle auf eine Faxbox und umgekehrt.

Anmerkung: Für die Faxbox ist im System T.38 zu aktivieren. Bei Faxversand vom Kommunikationssystem über einen ITSP muss dieser T.38 unterstützen. Wenn der ITSP T.38 nicht unterstützt, wird das Fax als G.711 behandelt.

13.11.8.1 Wie Sie Fax over IP (T.38-Fax) aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Sprachgateway**.
3) Klicken Sie im Menübaum auf **Sprachgateway**.
4) Klicken Sie im Menübaum auf **Codec-Parameter**.
5) Wählen Sie im Bereich **T.38-Fax** eine der folgenden Möglichkeiten:
   - Wenn Sie Fax over IP (T.38-Fax) aktivieren möchten, aktivieren Sie das Kontrollkästchen **T.38-Fax**.
   - Wenn Sie Fax over IP (T.38-Fax) deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **T.38-Fax**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.12 Überblick über Integration von Microsoft Office 365

Sie können problemlos zusammenarbeiten und haben überall Zugriff auf E-Mails, Webkonferenzen, Dokumente und Kalender. Das Paket bietet Sicherheit auf Unternehmensniveau und wird von Microsoft unterstützt. Egal, ob Sie ein kleines Unternehmen oder ein multinationales Unternehmen sind, Office 365 bietet Pläne, die auf die individuellen Bedürfnisse Ihres Unternehmens zugeschnitten sind. Für weitere Informationen oder ein 30-Tage-Konto besuchen Sie bitte

OpenScape Business mit Microsoft Office 365

Wenn ein Benutzer einen Termin in seinem Microsoft Outlook-Kalender einstellt, sucht das OpenScape Business-System automatisch nach Schlüsselwörtern in den Betreffs des Termins, zum Beispiel: "Besprechung", "krank", "Pause", "außer Haus". Wenn ein solches Schlüsselwort gefunden wird, setzt das System den Anwesenheitsstatus des Benutzers automatisch, wenn der Termin erreicht ist, auch wenn die Microsoft Outlook-Sitzung dieses Benutzers nicht mehr aktiv ist.

Der Benutzer konfiguriert die Termine mit diesen Schlüsselwörtern und OpenScape Business setzt automatisch den Telefonpräsenzstatus des Benutzers und leitet die Anrufe je nach Einstellung an die Voicemail oder z. B. an das Mobiltelefon weiter. Der Benutzer kann auch in einem allgemeinen Kundenstatus konfigurieren, ob der Anwesenheitsstatus nach Beendigung des Termins wieder in den Büro-Anwesenheitsstatus wechseln soll.

Dies funktioniert auch dann, wenn der Benutzer nicht den lokalen Outlook-Client verwendet und einen Termin mit den oben genannten Schlüsselwörtern direkt auf der Outlook-Webseite in der Cloud einrichtet.

E-Mail-Weiterleitung:

OpenScape Business ist in der Lage, E-Mails an Microsoft Office 365 inklusive Microsoft Exchange Server zu senden.

Dies ermöglicht es den Benutzern, E-Mails für neue Voicemails, Faxe oder Telefonkonferenzen zu erhalten und automatisch Web-Collaboration-Sitzungen von OpenScape Business aus durchzuführen.

OpenScape Business generiert für solche Aktionen E-Mails und hält die Benutzer auch per E-Mail auf dem Laufenden, wenn eine solche neue Benachrichtigung im OpenScape Business-Nachrichtenfeld eintrifft.

13.12.1 OpenScape Business-System unter Verwendung von einfacher Authentifizierung mit Microsoft Office 365 verbinden

Sie können das OpenScape Business-System unter Verwendung von einfacher Authentifizierung mit Microsoft Office 365 in der Cloud verbinden, um die OpenScape Business Exchange Kalenderintegration und E-Mail-Weiterleitung des integrierten Microsoft Exchange Servers in Microsoft Office 365 zu nutzen.

Voraussetzungen

- Microsoft Office 365- Office 365 Enterprise E3 mit der bekannten lokal installierten "Microsoft Office Professional Plus"-Suite und der Office Web Apps-Nutzung.
- Benutzer sind in Microsoft Office 365 verfügbar und mit dem lokalen Microsoft Outlook mit der zugeordneten E-Mail verbunden; adressiert in Microsoft Exchange von Microsoft Office 365.
- Alle verfügbaren Microsoft-Updates und Service-Packs sind installiert.
- Prüfen Sie, welche Microsoft Enterprise-Lizenzen Sie benötigen.
- Informieren Sie sich in den Versionshinweisen zu OpenScape Business über die freigegebenen Microsoft Office-Versionen.
- Microsoft Office und die Office Web Apps müssen lokal installiert werden.

Wichtige Hinweise:

- Ändern Sie den Wert der Microsoft Office 365-Domäne (Beispiel: test.onmicrosoft.com) so, dass er den Einstellungen Ihrer Umgebung entspricht.
- Der Benutzer "oso" wird in diesem Beispiel als Service Account mit dem Rollenprivileg für "ApplicationImpersonation" verwendet, mit dem OpenScape Business Zugriff auf die Postfachdatenbank des Microsoft Exchange Servers erhält. Dieser Benutzer muss im Benutzerverzeichnis von

Microsoft Office 365 hinzugefügt werden (siehe unten). Dazu ist auch eine konfigurierte E-Mail-Adresse erforderlich.

- Die aus dem Openscape Business Client bekannte "Kontaktsuche im öffentlichen Ordner von Microsoft Exchange" steht zur Verfügung, da Microsoft Office 365 diese Funktionalität anbietet.

Schritt für Schritt

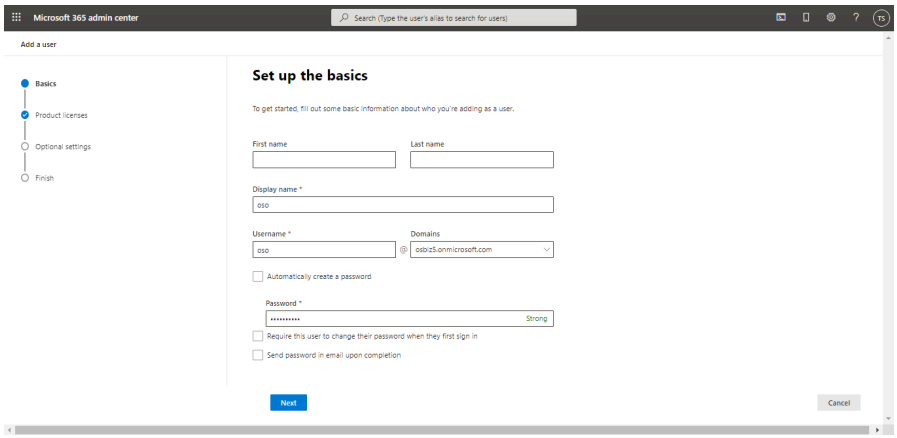
1) Registrieren Sie sich für **Microsoft Office 365 Enterprise E3** auf der offiziellen Webseite von Microsoft.

a) Weisen Sie dem Benutzer "oso" globale Administratorrechte zu.

2) Melden Sie sich im Microsoft 365 Admin Center an und navigieren Sie zu **Benutzer > Aktive Benutzer** , fügen Sie den Benutzer "oso" und die Testbenutzer "user1- user3" hinzu und weisen Sie gültige E-Mail-Adressen zu.

Folgen Sie dem Einrichtungsassistenten, um die Benutzer zu konfigurieren.

Fügen Sie dem Benutzer "oso" globale Administratorrechte hinzu.



3) Melden Sie sich vom Microsoft 365 Admin Center ab und melden Sie sich mit dem neu erstellten Benutzer "oso" an, um das temporäre Passwort zu ändern.

Prüfen Sie, ob der Benutzer "oso" Zugriff auf die Admin-Seite hat: **Integrität > Service-Integrität**. Nachdem die Service-Integritätsprüfung ohne größere Probleme abgeschlossen wurde, melden Sie sich ab und melden sich erneut mit dem Microsoft 365-Administrator an.

Stellen Sie sicher, dass die Benutzer im Microsoft Office 365-Benutzerverzeichnis verfügbar sind und sich bereits einmal in ihrem Profil angemeldet haben, um die temporären Kennwörter zu ändern, und sich mit dem lokal installierten Microsoft Outlook an ihrem Microsoft Office 365-Postfach anmelden können. Diese lokale Microsoft Office 365-Installation muss mit dem Microsoft Office 365-Portal verbunden werden, um alle verfügbaren Microsoft-Updates zu installieren und zu aktualisieren.

4) Laden Sie Microsoft Office vom Microsoft Office 365-Portal herunter, falls noch nicht geschehen. Installieren und aktualisieren Sie es mit den neuesten verfügbaren Microsoft-Updates.

5) Legen Sie den Benutzer "oso" als privilegierten Benutzer fest, um auf die Benutzerkalender für die **Exchange-Kalenderintegration**zugreifen zu können.

a) Öffnen Sie auf einem Microsoft Windows 10-Computer die PowerShell im erweiterten Modus:

- Öffnen Sie das Startmenü und geben Sie "Power" ein. Der Befehl "Windows PowerShell ist markiert.
- Halten Sie die Tasten Umschalt + Strg gedrückt und verwenden Sie die Eingabetaste, um die PowerShell zu starten.
- Beantworten Sie die angezeigte UAC-Meldung mit Ja, um die PowerShell zu starten.

b) Prüfen Sie, ob die lokale Ausführungsrichtlinie die Verwendung von Skripten auf dem Computer zulässt: `Get-ExecutionPolicy`

c) Wenn das Ergebnis nicht "RemoteSigned" lautet, führen Sie den Befehl aus: `Set-ExecutionPolicy RemoteSigned`. Wenn das nicht funktioniert, überprüfen Sie, ob die Berechtigungen auf diesem Computer eine Änderung zulassen und ob Sie die PowerShell im erweiterten Modus gestartet haben.

d) Führen Sie die Befehlszeilen aus, um sich am Online-Microsoft Exchange Server anzumelden, und melden Sie sich mit Ihrem Hauptadministratorkonto für Microsoft Office 365 an:

```
$LiveCred=Get-Credential Import-PSSession $Session -
AllowClobber
```

```
$Session = New-PSSession -ConfigurationName
Microsoft.Exchange -ConnextionUri https://
ps.outlook.com/powershell/-Credential $LiveCred -
Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session -AllowClobber
```

e) Konfigurieren Sie Microsoft Office 365: `Enable-OrganizationCustomization`

f) Ändern Sie den Wert für den privilegierten Benutzer so, dass er Ihren Umgebungseinstellungen entspricht: `New-ManagementRoleAssignment -Name "Impersonatipon-MyApp" -Role "ApplicationImpersonation" -User oso@osbiz5.onmicrosoft.com`

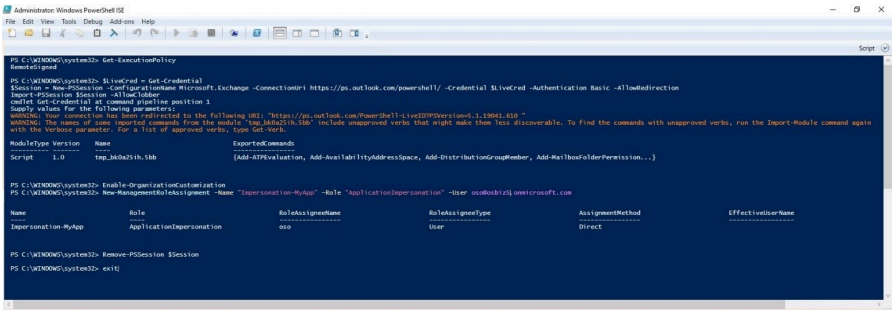
g) Überprüfen Sie den eingestellten Wert: `Get-ManagementRoleAssignment "Impersonatipon-MyApp"`

h) Verlassen Sie die aktuelle Sitzung: `Remove-PSSession $Session exit`

Die PowerShell wird nach dem Befehl Beenden geschlossen. Wenn die PowerShell geschlossen wird, bevor der Befehl `Remove-PSSession`

`$Session` eingegeben wird, kann ein neuer Zugang für 15 Minuten gesperrt werden.

Anmerkung: Vergewissern Sie sich, dass die Befehle funktionieren und keine roten Fehlermeldungen während der Ausführung angezeigt werden.



Anmerkung: Weitere Einzelheiten zur Verwendung der PowerShell finden Sie in der Microsoft Office 365-Hilfe.

6) Melden Sie sich am Microsoft Office 365-Portal an: www.office.com und melden Sie sich mit dem Benutzer "oso" an, um die Informationen zu erhalten und wählen Sie **Outlook** aus dem Baum auf der linken Seite. Navigieren Sie dann zu **Einstellungen > Alle Outlook-Einstellungen anzeigen > Mail > E-Mail synchronisieren**.

   Notieren Sie sich den Servernamen und den Port der SMTP-Einstellung. Zum Beispiel smtp.office365.com und 587. Sie benötigen diese Informationen für die nächsten Schritte.

7) Navigieren Sie zu **WBM > Setup > UC Suite > Konfig. externe Anbieter > Exchange Kalenderintegration** und nehmen Sie die folgenden Einstellungen vor, um eine Verbindung zum Microsoft Office 365-Server herzustellen:

   a) Klicken Sie auf das Kontrollkästchen **Exchange-Kalenderintegration aktivieren** .

   b) Wählen Sie in der Dropdown-Liste **Authentifizierungsmethode** die Option **Einfach**.

   c) Geben Sie die **Server-URL** ein. Zum Beispiel: https://outlook.office365.com/ews/exchange.asmx

   d) Geben Sie den **Benutzernamen** des privilegierten Benutzers aus dem Microsoft Office 365-Verzeichnis ein.

   e) Geben Sie das **Passwort** des privilegierten Benutzers ein, das im Microsoft Office 365-Verzeichnis festgelegt wurde.

   f) Klicken Sie auf **Speichern**.

   Diese Änderungen ermöglichen den Zugriff von OpenScape Business auf den Microsoft Exchange Server innerhalb von Microsoft Office 365 für die Exchange-Kalenderintegration.

Anmerkung: Die Felder für **Kontaktanbieter > Exchange** müssen mit der Online-Exchange-Adresse: https://outlook.office365.com/ews/exchange.asmx und der E-Mail-Adresse des globalen Administrators

(oso@osbiz5.onmicrosoft.com in diesem Beispiel) ausgefüllt werden, um Kontakte aus öffentlichen Ordnern suchen zu können.

8) Navigieren Sie zu **Service Center > E-Mail-Weiterleitung**, um den E-Mail-Zugriff von OpenScape Business auf Microsoft Office 365 zu aktivieren.
   a) Geben Sie im Feld **Postausgangsserver (SMTP)** die Adresse des Microsoft Office 365-Servers ein, den **Port des Postausgangsservers** und aktivieren Sie im Bereich **Serverinformationen** die Option **Dieser Server erfordert eine verschlüsselte Verbindung (TLS/SSL)**.
   b) Wählen Sie in der Dropdown-Liste **Authentifizierungsmethode** die Option **Einfach**.
   c) Geben Sie den **Benutzernamen und das Passwort** ein und **Bestätigen Sie das Passwort** des privilegierten Benutzers in Microsoft Office 365 im Bereich **Anmeldeinformationen**.
   d) Geben Sie die **E-Mail-Adresse** des privilegierten Benutzers in Microsoft Office 365 in den Bereich **Benutzerinformationen (Absender)** ein.
   e) Geben Sie die **E-Mail-Adresse 1** und die **E-Mail-Adresse 2** in den Bereich für die ALI-Änderungsbenachrichtigung ein.
   f) Klicken Sie auf **OK&Weiter**.
   g) Klicken Sie auf **E-Mail-Weiterleitung testen**, um zu überprüfen, ob diese funktioniert.

9) Installieren Sie die OpenScape Business-Client-Einstellungen:

   Ab Februar 2020 ist die OAuth-Authentifizierung für POP3-, IMAP4- und SMTP-AUTH-Verbindungen zu Exchange Online verfügbar. Daher muss die authentifizierte SMTP-Übermittlung (SMTP AUTH) im Online-Austausch aktiviert werden. Folgen Sie den Anweisungen unter: https://docs.microsoft.com/de/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission

   Auch die Identifizierung der Benutzer ist erforderlich. Melden Sie sich mit admin@osbiz5.onmicrosoft.com bei Office 365 an und navigieren Sie in der linken Baumstruktur zur Verwaltungsseite. Eine neue Registerkarte wird geöffnet. Navigieren Sie in dem neuen Fenster unter "Admin Centers" zu "Exchange". Es öffnet sich wieder eine neue Registerkarte und unter "Rollen" in der linken Baumstruktur gehen Sie wieder auf die Registerkarte "Admin-Rollen" und klicken auf "Rollengruppe hinzufügen". Geben Sie einen Namen ein und drücken Sie auf Weiter. Klicken Sie auf den Punkt "ApplicationImpersonation" und dann auf "Weiter". Fügen Sie schließlich die Benutzer zur Gruppe hinzu und schließen Sie den Vorgang ab.

   Stellen Sie sicher, dass die Microsoft Office Suite auf dem Computer des Benutzers installiert und mit Microsoft Office 365 verbunden ist und installieren Sie, falls noch nicht geschehen, die CommunicationsClients mit mindestens der Option myPortal for Outlook.
   a) Öffnen Sie den folgenden Pfad im Windows Explorer: \\198.6.127.12\Anwendungen\installieren-gemeinsam\Kommunikations-Clients.exe

      Syntax: \\<Openscape Business ip-address>\applications\install-common\CommunicationsClients.exe
   b) Melden Sie sich mit den WBM-Zugangsdaten an und folgen Sie dem Einrichtungsassistenten, um mindestens die Option myPortal for Outlook zu installieren.

10) Öffnen Sie Microsoft Outlook und melden Sie sich mit den Anmeldedaten des Benutzers am OpenScape Business-System mit den OpenScape Business-Clients an. Weitere Einzelheiten finden Sie im Benutzerhandbuch zu myPortal for Outlook.

Anmerkung: Sie können auch die Option **Silent Installation** verwenden, um die CommunicationsClients unbeaufsichtigt auf den Computern der Benutzer zu installieren. Lesen Sie bitte weiter auf Silent Installation/ Deinstallation für UC Suite PC-Clients auf Seite 548.

---

11) Navigieren Sie zu **WBM > Setup > UC Suite > Benutzerverzeichnis**, um die E-Mail-Adresse des Benutzers hinzuzufügen.

OpenScapeBusiness sendet bei dieser Konfiguration automatisch eine "Begrüßungs"-Mail an alle neu eingetragenen Mail-Adressen.

Anmerkung: Sie können diesen Schritt auch unter **WBM > Setup > UC Suite > Benutzerverzeichnis** durchführen.

Anmerkung: Eine konfigurierte gültige Mail-Adresse wird für die Nutzung der Exchange-Kalenderintegration und auch für die optionale Mail-Benachrichtigung benötigt, wenn der Benutzer eine Nachricht von OpenScape Business erhält.

Wiederholen Sie diesen Schritt für alle Benutzer.

12) Navigieren Sie zu **WBM > Setup > UC Suite > Profil**, um die Funktion **Exchange-Kalenderintegration** zu konfigurieren.
   a) Wählen Sie den Benutzer aus, für den Sie die Funktion aktivieren möchten, klicken Sie auf **Bearbeiten** und dann auf **Meine Einstellungen > Outlook-Anbindung**.
   b) Wählen Sie die Option **Exchange-Kalenderintegration** in der **Kalenderintegration**
   c) Klicken Sie auf das Kontrollkästchen **Kalendertermine automatisch aus meinen Anwesenheitsänderungen generieren**
   d) Wählen Sie **Exchange PST** aus der Dropdown-Liste.

   Wiederholen Sie diesen Schritt für alle Benutzer.

13) Navigieren Sie zu **WBM > Setup > UC Suite > Profil**. Wählen Sie den Benutzer aus, den Sie konfigurieren möchten, und klicken Sie auf **Sprachnachricht-Benachrichtigung**, um zu konfigurieren, ob Mail-Benachrichtigungen für Sprachnachrichten in bestimmten Anwesenheitsstatus gesendet werden sollen, wenn eine neue Sprachnachricht in der Mailbox des Benutzers gespeichert wird.

   Wiederholen Sie diesen Schritt für alle Benutzer. Dieser Schritt ist optional.

14) Navigieren Sie zu **WBM > Setup > UC Suite > Profil**. Wählen Sie den Benutzer aus, den Sie konfigurieren möchten, und klicken Sie auf **Faxbenachrichtigung**, um festzulegen, ob Faxbenachrichtigungen für Sprachnachrichten in bestimmten Anwesenheitsstatus gesendet werden sollen, wenn ein neues Fax in der Mailbox des Benutzers gespeichert wird.

   Wiederholen Sie diesen Schritt für alle Benutzer. Dieser Schritt ist optional.

13.12.2 OpenScape Business-System unter Verwendung von moderner Authentifizierung mit Microsoft Office 365 verbinden

Sie können Ihr OpenScape Business-System über eine moderne Authentifizierung (Microsoft OAuth 2.0 Token-basierte Autorisierung) mit Microsoft Exchange Online / Office 365 verbinden, um die Funktionen E-Mail-Weiterleitung, Exchange Kalenderintegration, Exchange Verzeichnisintegration und E-Mail-Warteschlangen zu nutzen.

Detaillierte Anweisungen zur Einrichtung der Verbindung finden Sie im Unify Experts Wiki unter `https://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Office_365`.

13.12.3 So überprüfen Sie, ob die Funktionen der Microsoft Office 365-Integration konfiguriert sind

E-Mail:

Sie können die E-Mail-Funktion mit der Schaltfläche **E-Mail-Weiterleitung prüfen** aus dem Bereich **Service Center > E-Mail-Weiterleitung** im WBM überprüfen. Geben Sie eine gültige E-Mail-Adresse als Empfänger ein und überprüfen Sie den Empfang der Testnachricht im Posteingang dieses E-Mail-Kontos.

Exchange-Kalenderintegration:

Wenn Benutzer Termine in ihrem Microsoft Outlook-Kalender einstellen, sucht das OpenScape Business-System automatisch nach Schlüsselwörtern in den Betreffs des Termins, zum Beispiel: "Besprechung", "Krank", "Pause", "Außer Haus", "Urlaub", "Mittagessen" oder "Zu Hause". Der Benutzer konfiguriert einfach die Termine mit diesen Schlüsselwörtern und OpenScape Business setzt automatisch den telefonischen Anwesenheitsstatus und leitet Anrufe an die Voicemail oder z. B. an das Mobiltelefon weiter, je nach eingestelltem Anwesenheitsstatus und dem vom Benutzer gewünschten Weiterleitungsziel. Dies funktioniert auch, wenn der Benutzer nicht den lokalen Outlook-Client verwendet und den Termin mit den oben genannten Betreff-Stichworten direkt in der Outlook-Webseite im Outlook Web Access (OWA) einrichtet.

Der Benutzer, der die Exchange- oder lokale Outlook-Kalenderintegration verwendet, muss eine gültige E-Mail-Adresse in seiner UC Suite-Client-Konfiguration sowie in der im obigen Handbuch genannten Konfiguration der UC Suite-Client-Outlook-Einstellungen haben. Es ist zwingend erforderlich, dass die Kombination UC Suite-Benutzer zu Exchange-Benutzer über die eingegebene Mailadresse erfolgt.

Die Spracheinstellung für die Voicemail des UC Suite-Benutzers wird verwendet, um die Schlüsselwörter zu kombinieren, zum Beispiel: Englische Schlüsselwörter wie "Meeting", "Sick","Break","Out of Office", "Holiday", "Lunch" or "Home" werden an die Spracheinstellung des Benutzers angepasst, d. h. wenn z. B. in der Voicemail die deutsche Sprache ausgewählt ist, dann werden in der Betreffzeile des Termins nur deutsche Schlüsselwörter wie "Besprechung", "Krank", "Pause", "Außeer Haus", "Urlaub", "Mittag" oder "Zu Hause" geprüft.

Wenn die Option "Status automatisch auf 'Im Büro' ändern" nicht verwendet wird, bleibt der Anwesenheitsstatus des Benutzers nach Ablauf des Termins auf dem eingestellten Status und die Rückkehrzeit, die anderen Benutzern oder Anrufern angezeigt wird, wird alle 15 Minuten erhöht. Wenn die Option "Status automatisch auf 'Im Büro' ändern" verwendet wird und die Terminzeit endet, wird die Anwesenheit des Benutzers automatisch wieder auf "Büro" gesetzt.

Termine, die weniger als 3 Minuten in der Zukunft liegen, werden ignoriert, da das System davon ausgeht, dass der Benutzer gerade einen neuen Termin anlegt und sich innerhalb dieser 3 Minuten alles ändern kann. Das Kommunikationssystem prüft alle 30 Sekunden, ob Termine in den Kalendern der Benutzer vorhanden sind. Aus diesem Grund und wegen möglicher Zeitverzögerungen zwischen dem Kommunikationssystem und dem Exchange-Server sollten Sie Testtermine von mehr als 3,5 Minuten verwenden. In Tests funktionierten Termine, die mit mehr als 5 Minuten in die Zukunft gelegt wurden, perfekt, um die kleinen Zeitverzögerungen zwischen dem Kommunikationssystem und dem Exchange-Server und die 30 Sekunden Leseverzögerung der Kalenderleseanforderungen zu vermeiden.

Neue Terminwerte werden innerhalb der Minute, auf die die Startzeit des Termins eingestellt ist, innerhalb der zuvor genannten 30-Sekunden-Abfragen vollständig gelesen. Wenn also die Startzeit gerade erreicht ist, ist zu beachten, dass die 30-Sekunden-Abfrage innerhalb dieser Minute durchgeführt werden muss und dann der Anwesenheitsstatus gesetzt wird. Die Abfrage legt auch die Rückkehrzeit des Benutzers entsprechend der Endzeit des Termins fest.

Wenn Sie die Funktionalität testen möchten, während myPortal for Outlook oder myPortal for Desktop für den Benutzer geschlossen ist, verwenden Sie einfach die Outlook-Webseite im Outlook Web Access (OWA). Melden Sie sich mit den Anmeldedaten des Benutzers an und fügen Sie den Termin mit dem Schlüsselwort zum Kalender hinzu. Überprüfen Sie im Client eines anderen UC Suite-Benutzers, dass sich die Anwesenheit ändert, wenn die Terminzeit erreicht ist.

14 Funktionen am Telefon

Das Kommunikationssystem bietet vielfältige Telefonie-Leistungsmerkmale, angefangen bei z.B. Halten, Makeln und Rückfrage, über unterschiedliche Anrufsignalisierungen bis hin zu Rufweiterschaltung und Anrufumleitung.

14.1 Anrufen

>Das Kommunikationssystem bietet verschiedene Möglichkeiten Anrufe zu tätigen, unter anderem Direktruf oder Kurzwahl.

14.1.1 Ziffernwahl

Bei der Ziffernwahl wird die Wahl jeder Ziffer direkt nach der Eingabe ausgesendet.

Der Verbindungsaufbau beginnt sofort bei Eingabe der ersten Ziffer. Der Teilnehmer hat dadurch keine Möglichkeit zum Editieren der Wahl.

14.1.2 Blockwahl

Bei der Blockwahl wird die Verbindung aufgebaut, wenn die vollständige Rufnummer eingegeben wurde. Die Rufnummer wird in einem einzigen Block übertragen.

Die Aussendung der Wahl kann durch Eingabe des Wahlendekennzeichens # gestartet werden.

Blockwahl ist zwingend vorgeschrieben für:

- ITSP-Amtsanschluss
- ISDN-Primärmultiplexanschluss in USA

Nach Ablauf von 5 Sekunden ohne Zifferneingabe, wird die zuletzt eingegebene Ziffer als letzte Ziffer des Rufnummernblocks interpretiert.

14.1.3 Keypad-Wahl

In verschiedenen Ländern werden Dienste digitaler Amtsanschlüsse über Keypad-Wahl und nicht funktional gesteuert. Um diese Dienste im PSTN zu aktivieren, kann die sogenannte Stimulus-Schnittstelle genutzt werden.

Das Leistungsmerkmal ist in Manager E zu konfigurieren.

Beim Teilnehmer erfolgt die Quittierung des Meldungsverkehrs über Displayanzeigen. Dementsprechend kann Keypad-Wahl ausschließlich über Telefone mit Display (optiPoint, OpenStage), Mobiltelefone (Cordless) mit optiPoint-Menüführung und IP-Telefone mit Stimulus-Schnittstelle erfolgen. ISDN-Telefone werden nicht unterstützt. Der jeweilige Netzprovider bestimmt, welche Dienste über Keypad-Wahl genutzt werden können.

Ein berechtigter Teilnehmer kann Keypad-Wahl über das Servicemenü oder über die Kennzahl *503 aktivieren. Dies ist ausschließlich aus dem Ruhezustand möglich. Anschließend muss eine ISDN-Amtsleitung gewählt werden, über die das Leistungsmerkmal ablaufen soll.

In Abhängigkeit von den vom Amt gesendeten Meldungen (z.B. bei Connect) kann Keypad-Wahl Einträge in die Gesprächsdatenerfassung zur Folge haben. Protokolliert werden die Rufnummer des ausführenden Teilnehmers, die verwendete Leitung und der Zeitraum der Nutzung des Leistungsmerkmals.

Anmerkung: Über Keypad-Wahl ausgeführte Aktionen unterliegen keiner Kontrolle durch das System. Missbräuchliche Nutzung, wie z.B. Gebührenmissbrauch oder Amtsleitungsblockierung, kann durch das System nicht verhindert werden.

Der Kunde ist darüber zu informieren, dass er selbst für Schäden haftet, welche durch Missbrauch dieses Leistungsmerkmals entstehen.

14.1.4 Wahlendeerkennung

Das Wahlende wird entweder automatisch nach 5 Sekunden erkannt oder manuell vom Benutzer durch das Wahlendekennzeichen "#" angezeigt.

14.1.5 Editieren der Wahl

Mit Editieren der Wahl kann der Teilnehmer die eingegebenen Ziffern der Rufnummer verändern. Diese Funktion ist bei Mobiltelefonen üblich. Eine Rufnummer kann nur während der Eingabe korrigiert werden.

Eine eingegebene Ziffernfolge kann von rechts nach links, durch Tastendruck jeweils um eine Ziffer gelöscht werden. Nach vollständiger Eingabe der korrekten Ziffernfolge kann die Wahlaussendung über die Bestätigen-Taste oder durch Abheben des Hörers erfolgen.

Das Editieren einer gespeicherten Rufnummer, z.B. für die Wahlwiederholung, ist nicht möglich.

Tipp: Editieren der Wahl ist für jeden Teilnehmer einzeln aktivierbar.

Abhängigkeiten

Thema	Abhängigkeit
Anklopfen	Anklopfen während des Editierens ist möglich, da sich das Telefon im Wahlaufnahmezustand befindet und damit für kommenden Verkehr belegt ist.
Rückfrage	Nach einer Rückfrage befindet sich das Telefon im Wahlaufnahmezustand. Das Editieren von Rufnummerziffern ist damit möglich.

14.1.5.1 Wie Sie das Editieren der Wahl aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer**.
4) Klicken Sie im Menübaum auf den Teilnehmer (Index - Rufnummer - Name).
5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Editieren der Wahl**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Editieren der Wahl**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.1.6 Wahlwiederholung

Bei jedem externen Gesprächsaufbau erfolgt eine Speicherung der gewählten Rufnummer. Ist das Ziel besetzt oder nicht erreichbar, kann der Teilnehmer die anschließend Wahlwiederholung nutzen um dieselbe Nummer erneut zu wählen.

Kurzwahlnummern werden ebenfalls in den Wahlwiederholungsspeicher geschrieben.

Die Wahl interner Rufnunmmern berührt den Wahlwiederholungsspeicher nicht.

Eventuelle Nachwahlziffern (auch MFV-Zeichen genannt) werden nicht als Wahlinformation angesehen und daher nicht abgespeichert (z.B. Ziffern, die an eine angeschlossene Sprachbox gesendet werden).

Die Funktion Wahlwiederholung kann nur über die Taste erfolgen, nicht über einen Zugangscode.

Durch Betätigen der Wahlwiederholungstaste können diese Rufnummern gezielt aufgerufen und erneut für einen Gesprächsaufbau verwendet werden.
Bei einmaligem Tastendruck erfolgt die Wahl der zuletzt gewählten Rufnummer.
Bei zweifachem Tastendruck erfolgt die Wahl der vorletzten Rufnummer.
Bei dreifachem Tastendruck erfolgt die Wahl der am ältesten gespeicherten Rufnummer.

Nach Drücken der Wahlwiederholungstaste, wird die gespeicherte Rufnummer automatisch nach 2 Sekunden gewählt. Sollten Sie mehr Zeit zum Lesen der angezeigten Rufnummer benötigen, wählen Sie mit der Bestätigen-Taste "Blättern". Mit jedem Druck auf die Taste "Weiter" wird die nächste der gespeicherten Rufnummern angezeigt. Erst durch Auswählen des Befehls "Anrufen" wird diese Rufnummer gewählt. Dadurch haben Sie wesentlich mehr Zeit zu prüfen, ob die richtige Rufnummer ausgewählt wurde.

Bei einem Anruf über LCR wird nur die vom Teilnehmer gewählte Nummer gespeichert.

PKZ werden ebenfalls im Wahlwiederholungsspeicher abgelegt. Voraussetzung dafür ist das Setzen des entsprechenden systemweiten Flags.

14.1.6.1 Wie Sie die automatische Wahlwiederholung aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System**.
4) Klicken Sie auf **System Flags**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Automatische Wahlwiederholung**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Automatische Wahlwiederholung**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.1.7 Kurzwahl zentral KWZ

Häufig benötigte externe Telefonnummern können im Kommunikationssystem gespeichert werden. Jede Nummer wird dann durch eine Kurzwahlnummer vertreten, die anstelle der vollständigen Telefonnummer benutzt wird.

Kurzwahlnummern bestehen aus 4-stelligen Nummern.

Standardmäßig befindet sich jeder Teilnehmer in einer Gruppe, welcher alle KWZ-Nummern zugeordnet sind. Dadurch darf jeder Teilnehmer alle KWZs verwenden.

KWZ setzt die Regeln der Amtsberechtigung außer Kraft. Beachten Sie, dass die Wahl eines Kurzwahlziels, das bei einer Suche im internen Telefonbuch gefunden wurde, die Gebührenbeschränkungsregeln nicht außer Kraft setzt.

Die Nummern der zentralen Kurzwahl werden durch den Administrator in Gruppen konfiguriert. Teilnehmer können jeweils einer dieser Gruppen zugeordnet werden. Ein Teilnehmer kann nur die Kurzwahlnummern der ihm zugeordneten Gruppe verwenden. Einer Gruppe kann aber nur ein KWZ-Bereich zugewiesen werden.

Einträge in Kurzwahllisten können nach Vor- und Nachnamen durchsucht werden, wenn der Name im Format „<Nachname>, <Vorname>“ oder <Vorname>, „<Nachname>“ konfiguriert ist.

Gewählte Kurzwahlnummern werden in den Wahlwiederholungsspeicher geschrieben.

Zum Programmieren einer Wahlpause und einer MFV-Umschaltung für die Nachwahl von MFV-Zeichen (z.B. für die Steuerung von Sprachboxen) wird die Wahlwiederholungstaste "P-Taste" bzw. die "# -Taste" verwendet.

Die Zielwahltaste für den Kunden muss wie folgt festgelegt werden: <Rufnummer><dtmf-Ziffer><Pause-Ziffer><Zugangscode> z.B. 008007728477#P2210344

Rufnummernumwertung in Namen

Jedem Kurzwahlziel kann ein Name zugewiesen werden. Sobald eine gespeicherte Rufnummer anruft, setzt das System automatisch den Namen ein und es wird statt der Rufnummer der Name im Display angezeigt, wenn CLIP eingestellt ist.

Nachwahl

Die Nachwahl wird bei der blockweisen Wahlaussendung (z.B. bei einer ITSP-Konfiguration) nicht unterstützt. Für die "Ziffer für Ziffer"-Ziffern-Übertragung wird sie unterstützt.

Anmerkung: Das Ziffernübertragungsfeld kann im WBM über den **Expertenmodus > Trunks/Routing > Route** geändert werden

---

Es besteht die Möglichkeit einer Nachwahl:

- Manuelle Nachwahl

  Nach Wahl des Zugangscodes und Angabe der Indexnummer (Kurzwahlnummer) kann der Anwender weitere Ziffern wählen. Diese werden der unter diesem Index gespeicherten Rufnummer angefügt und nachgewählt.
- Automatische Nachwahl

  Bei der Einrichtung einer KWZ kann die eingetragene Nummer in zwei Teile aufgeteilt werden. Als Trennzeichen wird "-" verwendet. Der erste Teil wird auf jeden Fall ausgesendet. Dann wird ein Timer gestartet. Wenn der Benutzer vor Ablauf des Timers keine anderen Ziffern wählt, wird automatisch der zweite Teil der eingetragenen Nummer nachgewählt, ansonsten werden die manuell gewählten Ziffern gesendet.

  Zum Beispiel: SSD = 7007–0

  Wählt der Teilnehmer nach dem Aufruf der KWZ und vor Ablauf des Timers keine Durchwahl (manuelle Nachwahl), wird automatisch die 0 nachgewählt (automatische Nachwahl).

Import von Kurzwahlrufnummern

Sie können Kurzwahlnummernlisten aus einer XML-Datei im UTF-8-Format importieren. Bereits bestehende Kurzwahlnummern werden vor dem Import gelöscht.

Eine XML-Vorlage mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center** > **Dokumente** > **CSV-Vorlagen**. In diese Vorlagen können Sie z.B. mit Microsoft Excel Ihre Kurzwahlziele eintragen.

Anmerkung: Der Import von Kurzwahllisten aus CSV-Dateien wird nicht mehr empfohlen und nur noch in Sonderfällen unterstützt.

Export von Kurzwahlrufnummern

Als Administrator mit dem Profil **Expert** können Sie über den **Experten-Modus** Kurzwahlnummern in eine XML-Datei im UTF-8-Format exportieren. Es werden immer alle Datensätze exportiert.

14.1.7.1 Wie Sie ein Kurzwahlziel hinzufügen

Mit dem Wizard **Telefonbuch/Kurzwahl** können Sie Kurzwahlziele für Kurzwahl zentral hinzufügen.

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Telefonbuch/Kurzwahl** zu starten.
4) Tragen Sie in einer freien Tabellenzeile **Kurzwahl**-Nummer, **Rufnummer** und **Name** des Kurzwahlziels ein.
5) Wenn Sie weitere Kurzwahlziele hinzufügen möchten, klicken Sie auf **Daten speichern** und wiederholen der vorherigen Schritt.
6) Klicken Sie auf **OK & Weiter**.
7) Klicken Sie auf **Beenden**.

14.1.7.2 Kurzwahlziele aus einer XML-Datei importieren

Mit dem Wizard **Telefonbuch/Kurzwahl** können Sie Kurzwahlnummern und Rufnummern aus einer XML-Datei importieren. Bereits bestehende Kurzwahlnummern werden vor dem Import gelöscht.

Voraussetzungen

Sie sind am WBM angemeldet.

Eine XML-Datei im UTF-8-Format mit eingetragenen Kurzwahlnummern liegt vor. Ein XML-Template für den Import von Kurzwahlnummern findet sich unter **Service-Center** > **Dokumente** > **CSV Vorlagen**.

Anmerkung: Der Import von Kurzwahllisten aus CSV-Dateien wird nicht mehr empfohlen und nur noch in Sonderfällen unterstützt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Telefonbuch/Kurzwahl** zu starten. Das Fenster **Zentralen Telefonbucheintrag bearbeiten** wird angezeigt.

4) Klicken Sie auf **CSV/XML-Data importieren/exportieren**.
5) Klicken Sie im Bereich **CSV/XML-Datei über HTTP importieren** auf **Durchsuchen** um die gewünschte Datei auszuwählen.
6) Klicken Sie auf **OK**. Vorhandene Kurzwahlnummern werden gelöscht und die in der XML-Datei eingetragenen Kurzwahlnummern in das System importiert.
7) Klicken Sie auf **Fertig**.

14.1.7.3 Wie Sie Kurzwahlziele in eine XML-Datei exportieren

Sie können Kurzwahlnummern in eine XML-Datei exportieren. Es werden immer alle Daten exportiert.

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Telefonbuch/Kurzwahl** zu starten. Das Fenster **Zentralen Telefonbucheintrag bearbeiten** wird angezeigt.
4) Klicken Sie auf **CSV/XML-Data importieren/exportieren**.
5) Klicken Sie im Bereich **XML-Datei über HTTP exportieren** auf **Download**. Die Liste der Kurzwahlnummern wird zum Download vorbereitet.
6) Wählen Sie einen Ablageort für die Datei und klicken Sie auf **Speichern**.

14.1.7.4 Wie Sie Kurzwahlziele bearbeiten

Mit dem Wizard **Telefonbuch/Kurzwahl** können Sie Kurzwahlziele bearbeiten.

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Telefonbuch/Kurzwahl** zu starten.
4) Sie können einen Eintrag suchen, indem Sie in die Suchfelder **Kurzwahl**, **Rufnummer** oder **Name** ein Suchbegriff eingegeben und anschließend die Return-Taste drücken. Alle Treffer werden angezeigt, die den Suchbegriff enthalten. Mit der Eingabe von `521` als Rufnummer werden z.B. die Treffer

+495213535 und +498967521 angezeigt oder mit co als Name die Treffer Collins, Mcoin und Branco.

Anmerkung: Alle Einträge werden angezeigt, wenn in allen Suchfeldern nichts eingetragen ist und anschließend die Return-Taste gedrückt wird.

5) Ändern Sie in dem gewünschten Tabelleneintrag die Werte in den Feldern **Kurzwahl**, **Rufnummer** oder **Name**.
6) Wenn Sie weitere Kurzwahlziele bearbeiten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie den vorherigen Schritt.
7) Klicken Sie auf **OK & Weiter**.
8) Klicken Sie auf **Beenden**.

14.1.8 Kurzwahl individuell (KWI)

Kurzwahl individuell ermöglicht jedem Teilnehmer zusätzlich zu Kurzwahl zentral 10 externe Rufnummern als individuelle Kurzwahlnummern zu speichern.

Bei Telefonen ohne Display muss der Teilnehmer nach Eingabe der Rufnummer auf den Quittungston warten.

Im KWI-Pool können externe Nummern programmiert werden. Der Zugang hängt von den Wahlberechtigungen des Teilnehmers ab. Der Teilnehmer muss vor Eingabe der Rufnummer die Amtskennzahl (z.B. 0) eingeben.

Um eine Wählpause oder eine MFV-Umschaltung zu programmieren, wird die Taste Wahlwiederholung oder die Raute (#)-Taste verwendet.

14.1.9 Direktruf

Die Funktionstasten eines Telefons oder Beistellgerätes können als Direktruftasten eingerichtet werden. Dafür werden diese mit der Rufnummer eines internen Teilnehmers oder einer Gruppe programmiert. Durch Drücken einer solchen Taste wird ein sofortiger Anruf zum programmierten Ziel ausgeführt (Direktruf). Der aktuelle Zustand des Teilnehmers oder der Gruppe ist anhand der zur Direktruftaste gehörenden LED ersichtlich.

Eine Direktruftaste (auch bezeichnet als DSS (Direct Station Selection)-Taste) kann auch verwendet werden, um ein Gespräch schnell an den darunter programmierten Teilnehmer oder die programmierte Gruppe zu übergeben. Durch das Betätigen einer Direktruftaste während eines Gesprächs mit einem externen Gesprächspartner, wird das aktuelle Gespräch in Rückfrage geschaltet. Der übergebende Teilnehmer kann das Gespräch durch Auflegen des Hörers an das Übergabeziel übergeben (Übergabe vor Melden). Ebenso ist es möglich zu warten, bis das Übergabeziel sich meldet und das Gespräch dann zu übergeben (Übergabe nach Melden). Nimmt das Übergabeziel das Gespräch nicht an, wird ein Wiederanruf veranlasst.

Zustände der zu einer Direktruftaste gehörenden LED

Die zu einer Direktruftaste gehörende LED zeigt den aktuellen Zustand des programmierten Teilnehmers an:

- Aus: Der zugehörige Teilnehmer telefoniert nicht.
- Leuchtet: Der zugehörige Teilnehmer telefoniert oder hat Anrufschutz eingeschaltet.
- Blinkt schnell: Der zugehörige Teilnehmer ruft an. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.
- Blinkt langsam: Der zugehörige Teilnehmer wird gerufen und hat den Anruf noch nicht angenommen. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.

Abhängigkeiten

Thema	Abhängigkeit
ISDN-Telefone, SIP-Telefone	Direktruftasten können nicht bei ISDN- oder SIP-Telefonen programmiert werden.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712
Chef/Sekretär / Top-Gruppe auf Seite 716

14.1.10 Direktansprechen / Direktantworten

Direktansprechen ermöglicht einen internen Verbindungsaufbau, ohne dass der gerufene Teilnehmer den Hörer abhebt. Der Lautsprecher des gerufenen Teilnehmers wird dabei automatisch eingeschaltet.

Bei Telefonen mit Freisprecheinrichtung (Mikrofon) ist Direktantworten des gerufenen Teilnehmers durch Einschalten des Mikrofons möglich. Durch Abheben des Hörers erfolgt der Übergang zu einem normalen Zweiergespräch.

Direktansprechen kann mittels einer dafür programmierten Funktionstaste oder über den zugehörigen Menüeintrag oder die Kennzahl und anschließende Wahl der Rufnummer des Zielteilnehmers genutzt werden. Eine Funktionstaste kann auch inklusive einer Teilnehmerrufnummer programmiert werden. Nach Betätigung einer solchen Funktionstaste erfolgt der sofortige Verbindungsaufbau zum programmierten Ziel.

Direktansprechen ermöglicht auch Durchsagen an alle internen Teilnehmer einer Gruppe.

Direktantworten kann über den im Display angebotenen Menüeintrag oder eine dafür programmierte Funktionstaste aktiviert werden.

Das Direktansprechen eines Teilnehmers kann durch Aktivieren des Direktansprechschutzes verhindert werden. In diesem Fall wird das Direktansprechen wie ein normaler Anruf signalisiert.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz, Anrufschutz durchbrechen	Bei Teilnehmern mit aktiviertem Anrufschutz ist kein Direktansprechen möglich. Hat der Teilnehmer, der das Leistungsmerkmal "Direktansprechen" nutzen möchte, die Berechtigung den Anrufschutz zu durchbrechen, erhält dieser für fünf Sekunden den Besetztton. Anschließend wird der Zielteilnehmer gerufen, nicht direkt angesprochen.
Makeln, Rückfrage Übergabe	Die genannten Leistungsmerkmale können nicht in einer Direktansprechen/Direktantworten-Verbindung genutzt werden.
ISDN-Telefone, SIP-Telefone	Die Leistungsmerkmale "Direktansprechen" und "Direktantworten" können nicht mit ISDN- oder SIP-Telefonen genutzt werden.

14.1.10.1 Wie Sie den Direktansprechschutz für Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Navigieren Sie im Menübaum unter **Teilnehmer** > **Teilnehmer** > **...** zum gewünschten Teilnehmer (Index-Rufnummer-Name).
4) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den Direktansprechschutz für Teilnehmer aktivieren möchten, deaktivieren Sie das Kontrollkästchen **Direktansprechschutz aus**.
   - Wenn Sie den Direktansprechschutz für Teilnehmer deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Direktansprechschutz aus**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.1.11 Assoziierte Wahl

Assoziierte Wahl ermöglicht einem berechtigten Teilnehmer für einen beliebigen anderen Teilnehmer stellvertretend eine Rufnummer zu wählen. Die Auswirkung ist die gleiche, wie bei der Wahl der Rufnummer durch den anderen Teilnehmer selbst.

Der Einstieg erfolgt über eine Kennzahl mit Angabe des Teilnehmers, für den die Wahl ausgeführt werden soll. Die nachfolgenden Ziffern werden dabei so interpretiert, als ob der zuvor angegebene Teilnehmer selbst wählen würde.

14.1.12 Leitungsvormerken

Ein Teilnehmer kann sich eine Amtsleitung vormerken, wenn momentan keine freie Amtsleitung zur Verfügung steht. Sobald eine Amtsleitung frei wird, bekommt er diese mittels Wiederanruf angeboten.

Wenn der Teilnehmer zum Zeitpunkt des Wiederanrufs belegt ist, wird beim besetzten Teilnehmer angeklopft. Wird das Anklopfen nicht beantwortet, wird die Reservierung gelöscht und die Leitung dem nächsten Teilnehmer in der Warteliste angeboten. Hat der Teilnehmer vor Eingang eines Wiederanrufs von einer in der Warteliste befindlichen Amtsleitung den Anrufschutz aktiviert, wird die Leitungsreservierung gelöscht und die Amtsleitung dem nächsten Teilnehmer in der Warteliste angeboten.

Merken mehrere Teilnehmer eine Amtsleitung vor, so erfolgt die Zuteilung in der Reihenfolge der Vormerkung.

Pro Telefon ist nur eine Warteliste-/Reservierungsanforderung möglich. Wenn der Teilnehmer eine zweite Reservierung versucht, wird die erste dadurch überschrieben.

Es ist nicht möglich, das Leistungsmerkmal Leitungsvormerken zu aktivieren, wenn die versuchte Verbindung über LCR (Leitweglenkung) eingeleitet wurde.

Das Leistungsmerkmal Leitungsvormerken ignoriert eine vorhandene Rufweiterschaltung. Erfolgt innerhalb von 20 Sekunden keine Antwort, wird die Leitungsreservierung gelöscht.

Eine wieder anrufende Amtsleitung kann nicht übernommen werden – weder durch "Übernahme, gezielt" noch durch "Übernahme, Gruppe".

Die Reservierung der Leitungen kann auf einem der folgenden Wege aktiviert werden:

- Manuelle Reservierungen funktionieren nur bei Telefonen mit Display.
- Automatische Reservierung (bei allen anderen Telefonen)

  Wenn dieses Flag aktiviert ist und einem Teilnehmer nach den üblichen Prozeduren zur Leitungsbelegung keine freie Leitung zugewiesen wird, wird teilnehmerseitig ein Besetztton signalisiert. Nach 5 Sekunden ertönt ein positiver Quittungston und die Leitung wird reserviert, sofern der Teilnehmer über die erforderliche Amtsrufberechtigung verfügt.

Anmerkung: Bei S_0-Telefonen Leistung vormerken nicht möglich.

14.1.12.1 Wie Sie Leitungsvormerken aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System**.

4) Klicken Sie auf **System Flags**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **automatisches Leitungsvormerken**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **automatisches Leitungsvormerken**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.1.13 Privatleitung

Einer Privatleitung ist eine Amtsleitung, die ausschließlich einem bestimmten Teilnehmer zur Verfügung steht.

14.2 Anrufsignalisierung, Rufnummernanzeige

Das Kommunikationssystem bietet verschiedene Möglichkeiten der Anrufsignalisierung und Rufnummernanzeige, wie z.B. CLIP, CLIR, COLP und COLR.

14.2.1 Unterschiedliche Anrufsignalisierung

Unterschiedliche Anrufsignalisierung ermöglicht bei ankommenden Anrufen zwischen internen und externen zu unterscheiden.

Kommende Anrufe werden am Telefon optisch und akustisch signalisiert. Im Display erscheinen folgende Anzeigen:

- Rufnummer des Anrufers
- Bei interner Anrufumleitung: zusätzlich die eigentlich gewählte Rufnummer

Der kommende Anruf kann zusätzlich durch eine LED angezeigt werden. Für interne und externe Anrufe gibt es unterschiedliche akustische Signale.

Rufsignalisierung intern

Es kann jedem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zugewiesen werden. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen unterschieden werden kann. So kann z.B. dem Geschäftsführer ein spezieller interner Rufton bereitgestellt werden und jeder Mitarbeiter erkennt bereits am Rufton, dass er vom Geschäftsführer angerufen wird.

Rufsignalisierung extern

Es gibt drei verschiedene Rufarten, die sich akustisch unterscheiden und für einen externen Ruf eingestellt werden können. Dadurch können z.B. Anrufe für zwei verschiedene Gruppen wie Vertrieb und Lager akustisch unterschieden werden.

- Durch den Administrator werden die drei unterschiedlichen Rufarten in Deutschland für analoge, ISDN- und System-Telefone konfiguriert.
- In anderen Ländern werden die Rufarten von analogen Telefonen gleich signalisiert.

14.2.2 Calling Line Identification Presentation (CLIP)

Rufnummernübermittlung des Anrufers zeigt die Rufnummer des Anrufers beim gerufenen Teilnehmer an.

Die Rufnummernübermittlung des Anrufers CLIP (Calling Line Identification Presentation) bezieht sich auf ankommende Rufe und muss vom Netzanbieter unterstützt werden.

Ist der Name und die Rufnummer des Anrufers unter Kurzwahl zentral (KWZ) des Kommunikationssystems gespeichert, sehen Sie den Namen auf Ihrem Display.

Die Leistungsmerkmale Rufnummernübermittlung des Anrufers (CLIP) und Rufnummernunterdrückung des Anrufers (CLIR) schließen einander gegenseitig aus, d.h. sobald CLIP aktiviert ist, ist CLIR deaktiviert und umgekehrt.

Einstellbare CLIP

Einstellbare CLIP überträgt nach extern anstelle der Rufnummer des Anrufers (z.B. Mitglied eines Sammelanschlusses) eine dafür eingestellte Rufnummer (z.B. Rufnummer des Sammelanschlusses).

Systemspezifische Informationen

Land	standardmäßig aktiviert
USA	LIN (Location Identification Number). Wird CLIP für USA aktiviert, ist LIN automatisch deaktiviert.
Restliche Länder	CLIP

14.2.2.1 Wie Sie einstellbare CLIP aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System**.
4) Klicken Sie auf **System Flags**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie einstellbare CLIP aktivieren möchten, aktivieren Sie das Kontrollkästchen **Einstellbare CLIP**.
   - Wenn Sie einstellbare CLIP deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Einstellbare CLIP**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.3 Calling Line Identification Restriction (CLIR)

Rufnummernunterdrückung des Anrufers unterdrückt die Anzeige der Rufnummer des Anrufers beim angerufenen Teilnehmer.

Rufnummernunterdrückung CLIR (Calling Line Identification Restriction) bezieht sich auf gehende Anrufe. PSTN muss das Leistungsmerkmal unterstützen. Rufnummernunterdrückung hat Vorrang vor Rufnummernübermittlung.

Die Leistungsmerkmale Rufnummernübermittlung des Anrufers (CLIP) und Rufnummernunterdrückung des Anrufers (CLIR) schließen einander gegenseitig aus, d.h. sobald CLIP aktiviert ist, ist CLIR deaktiviert und umgekehrt.

CLIR und COLR können nur gemeinsam aktiviert oder deaktiviert sein.

Rufnummernunterdrückung des Anrufers ist für bestimmte Anrufziele (z.B. Notrufnummern von Polizei und Feuerwehr) nicht wirksam.

Systemweite Rufnummernunterdrückung

Als Administrator können Sie CLIR Rufnummernanzeige systemweit aktivieren oder deaktivieren.

Tipp: Das Flag “Systemweite Unterdrückung der Rufnummernanzeige” gilt nicht für USA.

Temporäre Rufnummernunterdrückung

Als Teilnehmer können Sie die temporäre Rufnummernunterdrückung aktivieren oder deaktivieren. Temporäre Rufnummernunterdrückung ist nur möglich bei deaktivierter systemweiter Rufnummernunterdrückung.

Teilnehmerrufnummer unterdrücken

Als Administrator können Sie bezogen auf jeweils eine Richtung konfigurieren, dass anstelle der Rufnummer des Teilnehmers nur Anlagenrufnummer übertragen werden soll.

14.2.3.1 Wie Sie die Unterdrückung der Teilnehmerrufnummer aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Richtung**.
4) Wählen Sie die betreffende **Rtg.** aus.
5) Aktivieren Sie unter **Anlagenrufnummer gehend** das Kontrollkästchen **TIn-RufNr unterdrücken**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.4 Connected Line Identification Presentation (COLP)

Connected Line Identification Presentation (COLP) übermittelt die Rufnummer des angerufenen Teilnehmers an den Anrufer, sobald die Verbindung hergestellt ist.

COLP ist beispielsweise bei der Anrufweiterleitung sinnvoll, damit der Anrufer die Telefonnummer des tatsächlichen Kommunikationspartners anstelle der ursprünglich gewählten Telefonnummer sehen kann.

Die Funktionen „Connected Line Identification Presentation" (COLP) und „Connected Line Identification Restriction" (COLR) schließen sich gegenseitig aus, d. h., sobald COLP aktiviert ist, wird COLR deaktiviert und umgekehrt.

14.2.4.1 Wie Sie die Rufnummernübermittlung des Angerufenen aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Richtung**.
4) Wählen Sie die entsprechende **Rtg.** aus.
5) Klicken Sie auf die Registerkarte **Spezial Parameter ändern**.
6) Aktivieren Sie das Kontrollkästchen **COLP**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.5 Rufnummernunterdrückung des Angerufenen (COLR)

Rufnummernunterdrückung des Angerufenen unterdrückt die Anzeige der Rufnummer des angerufenen Teilnehmer beim Anrufer.

Rufnummernunterdrückung des Angerufenen (COLR Connected Line Identification Restriction) bezieht sich auf kommende Anrufe.

Rufnummernunterdrückung des Angerufenen (COLR) hat Vorrang vor Rufnummernübertragung des Angerufenen beim Anrufer.

Die Leistungsmerkmale Rufnummernübermittlung des Angerufenen (COLP) und Rufnummernunterdrückung des Angerufenen (COLR) schließen einander gegenseitig aus, d.h. sobald COLP aktiviert ist, ist COLR deaktiviert und umgekehrt.

CLIR und COLR können nur gemeinsam aktiviert oder deaktiviert sein.

14.2.6 CLIP no screening (Übermittlung kundenspezifischer Rufnummerninformationen)

CLIP no screening übermittelt an Stelle der Rufnummer des Anrufers eine vom Anrufer festgelegte Rufnummer.

Die Anlagenrufnummer gehend muss nicht identisch sein mit der Anlagenrufnummer kommend.

Für spezielle Kundenanwendungen kann das Flag "Teilnehmerrufnummer unterdrücken" aktiviert werden. Dadurch wird verhindert, dass die Durchwahlnummer des Teilnehmers mit der Anlagenrufnummer gehend ausgesendet wird.

Beispiel: Ein Service-Mitarbeiter, der zentral über eine allgemeine Service-Rufnummer erreicht wird, soll von seinen Kunden nicht direkt erreicht werden können. Um seine eigene Durchwahlnummer zu verbergen, wird als Anlagenrufnummer gehend die allgemeine Service-Rufnummer eingetragen und das Flag "Teilnehmerrufnummer unterdrücken" aktiviert. Dem angerufenen Teilnehmer wird dann ausschließlich die allgemeine Service-Rufnummer als CLIP angezeigt.

Im Normalfall wird für kommende und gehende Gespräche dieselbe Anlagenrufnummer verwendet. Der Eintrag unter Anlagenrufnummer gehend ist dann leer oder identisch mit dem unter Anlagenrufnummer kommend. Soll dies nicht der Fall sein, kann

- unter Anlagenrufnummer gehend eine andere Nummer eingetragen werden.
- über den Richtungsparameter Nr.-Typ, gehend definiert werden, ob die eingetragene Anlagenrufnummer gehend die Teilnehmernummer ohne Ortsnetzkennzahl, mit Ortsnetzkennzahl (national) oder zusätzlich die internationale Länderkennzahl (international) enthält.

Tipp: CLIP no screening muss vom Netzanbieter unterstützt werden und aktiviert sein.

14.2.6.1 Wie Sie CLIP no screening konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Richtung**.
4) Wählen Sie die betreffende **Rtg.** aus.
5) Geben Sie unter **Anlagenrufnummer gehend** die gewünschte **Anlagenrufnummer** ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.7 CLIP für analoge Endgeräte

CLIP für analoge Endgeräte übermittelt die Rufnummer von einem analogen Endgerät des Anrufers zum Angerufenen und die dortige Anzeige auf dafür geeigneten Endgeräten – CLIP (Calling Line Identification Presentation) analog.

Die zusätzliche Übertragung der Namensinformation CNIP (Calling Name Identification Presentation) ist konfigurierbar.

Tipp: CNIP ist endgeräteabhängig. Beachten Sie die Angaben des Herstellers.

14.2.8 Stiller Ruf / Ruhe

Das Leistungsmerkmal Stiller Ruf / Ruhe signalisiert kommende Rufe akustisch nur mit einem kurzen Aufmerksamkeitston und im Display.

Stiller Ruf / Ruhe ist nur an Telefonen mit Display verfügbar und hat keine Auswirkung auf die Signalisierung von Terminen.

14.2.9 Rufnummernumwertung in Namen bei Kurzwahl zentral

Bei Anrufen mittels Kurzwahl zentral (KWZ) und bei ankommenden Anrufen von Zielen der Kurzwahl zentral, wird nach der Wahl anstelle der Kurzwahlnummer der Name des Kurzwahlzieles angezeigt.

14.3 Funktionen während der Verbindung

Das Kommunikationssystem bietet während der Verbindung verschiedene Funktionen an, z.B. Gespräch halten, weiterleiten oder übergeben.

14.3.1 Halten

Mit Halten bringt ein Teilnehmer ein Gespräch in einen Wartezustand. Der Anrufer hört währenddessen Wartemusik oder eine Ansage.

Halten wird beendet durch die Wiederaufnahme des gehaltenen Gesprächs.

Es gibt folgende Arten von Halten:

- Allgemeines Halten:

  Jeder beliebige Teilnehmer kann das Gespräch durch Drücken einer Leitungs- oder Gesprächstaste wieder aufnehmen.
- Exklusives Halten: (nur bei Team- oder Top-Funktion und beim Vermittlungsplatz)

  Nur der zuvor einleitende Teilnehmer kann das Gespräch wieder aufnehmen.

Halten und Wiederanruf

Ein geparktes Gespräch führt bei Ablauf des Timers **Zeit für Parken + Übergang Halten** (Standard: 160 s) zu einem Wiederanruf.

14.3.2 Parken

Mit Parken bringt ein Teilnehmer ein Gespräch in einen Wartezustand. Der Anrufer hört währenddessen Wartemusik oder eine Ansage. Ein geparktes Gespräch kann von einem beliebigen Telefon aus wieder aufgenommen werden.

Als Teilnehmer weisen Sie einer zu parkenden Verbindung eine Parkposition (0-9) im Kommunikationssystem zu. Ist die Parkposition belegt, ertönt ein negativer Quittungston, die Ziffer wird nicht dargestellt und Sie können eine andere Parkposition wählen. Zur Wiederaufnahme eines geparkten Gesprächs müssen Sie dessen Parkposition angeben.

Die Wiederaufnahme eines geparkten Gesprächs kann über Kennzahl oder eine entsprechend programmierte Taste erfolgen und ist auch während eines anstehenden Rufs möglich.

Parken und Wiederanruf

Ein geparktes Gespräch führt bei Ablauf des Timers **Zeit für Parken + Übergang Halten** (Standard: 160 s) zu einem Wiederanruf.

Parken und Anrufumleitung

Ein geparktes Gespräch folgt bei einem Wiederanruf nicht einer Anrufumleitung.

Parken und DISA

Parken kann nicht über DISA aktiviert werden.

Parken und Konferenz

Eine Konferenz kann nicht geparkt werden.

Parken und Vernetzung

Ein geparkter Anruf kann nur im gleichen Knoten wieder aufgenommen werden. Ein über Vernetzung kommender Anruf kann nur am Zielknoten geparkt werden.

Parken und Anrufschutz

Ein Teilnehmer mit aktiviertem Anrufschutz kann einem Gespräch eine Parkposition zuweisen. Erfolgt ein Wiederanruf durch das geparkte Gespräch und wurde in Call Management kein anderes Ziel festgelegt, wird das Gespräch nach Ablauf des Wiederanruf-Timers automatisch getrennt.

Anmerkung: Detaillierte Anweisungen zum Parken von Anrufen und zur Wiederaufnahme von geparkten Anrufen finden Sie im entsprechenden Kapitel der Bedienungsanleitung des jeweiligen Geräts (OpenStage X / HiPath/OpenScape 3000/4000 Bedienungsanleitung).

14.3.3 Rückfrage

Mit Rückfrage baut ein Teilnehmer während eines Gesprächs ein weiteres Gespräch vom selben Telefon aus auf oder nimmt ein anklopfendes Gespräch an. Das erste Gespräch wird währenddessen gehalten.

Eine Rückfrage wird beendet durch:

- Wiederaufnahme des gehaltenen Gesprächs
- Trennen

  Dadurch erfolgt entweder:

  – Übergabe des gehaltenen Gesprächs oder
  – sofortiger Wiederanruf des gehaltenen Teilnehmers beim Teilnehmer, der die Verbindung getrennt hat

Rückfrage mittels Direktruftaste

Das Drücken einer Direktruftaste während eines Gesprächs leitet eine Rückfrage zum entsprechenden Ziel ein.

Verbinden zweier externer Gesprächspartner

Während eines externen Gesprächs verbindet eine Rückfrage zu einem externen Ziel bei anschließender Übergabe die beiden Gesprächspartner. Dabei können Gebühren anfallen.

14.3.4 Makeln

Mit Makeln kann ein Teilnehmer zwischen zwei Gesprächen wechseln. Während er mit einem der Teilnehmer im Gespräch ist, wird der jeweils andere gehalten.

Teilnehmer können durch Drücken der entsprechenden Leitungstaste zwischen den Gesprächen wechseln.

Makeln und Halten

Ein gehaltener Teilnehmer kann nicht makeln.

14.3.5 Übergeben

Mit Übergabe kann ein Teilnehmer sein Gespräch an ein anderes Ziel übergeben. Sobald ein Teilnehmer die Übergabe einleitet, wird der wartende Teilnehmer bis auf weiteres gehalten.

Es gibt folgende Arten von Übergabe:

- Übergabe vor Melden:

  Sie können den Anruf übergeben, ohne dass sich der Teilnehmer am Ziel der Übergabe meldet. Falls der Teilnehmer am Ziel der Übergabe besetzt ist, wird angeklopft. Versucht noch ein Dritter diesem besetzten Teilnehmer ein Gespräch zu übergeben oder ist Anklopfschutz aktiviert, erfolgt ein sofortiger Wiederanruf. Beantwortet der Teilnehmer am Ziel das übergebene Gespräch nicht innerhalb einer bestimmten Zeit (Timer Rufzeit während Übergeben

vor Melden), erfolgt Wiederanruf. Übergabe vor Melden ist nicht möglich an einen Agenten einer anderen Warteschlange von Multimedia Contact Center.

- Übergabe nur mit Rückfrage:

  Sie können den Anruf erst übergeben, wenn sich der Teilnehmer am Ziel der Übergabe meldet. Sie übergeben den Anruf durch Auflegen des Hörers.

Übergabe bei Anrufumleitung

Einer Anrufumleitung am Ziel der Übergabe wird gefolgt. Das Display zeigt das letztendliche Ziel der Übergabe.

Übergabe bei Anrufschutz

Bei der Übergabe eines Gesprächs an einen Teilnehmer mit aktiviertem Anrufschutz erfolgt sofort ein Wiederanruf beim einleitenden Teilnehmer, unabhängig von dessen Anrufschutz.

Systemspezifische Informationen

Timer "Rufzeit während Übergeben vor Melden": standardmäßig 45 Sekunden

An einen besetzten Teilnehmer können gleichzeitig bis zu 5 Gespräche übergeben werden.

Anmerkung: Bei einer Anrufweiterleitung wird die Aktualisierung der Anzeigeinformationen über die ITSP/NATIVE-SIP-Schnittstelle nicht unterstützt.

14.3.6 Wiederanruf

Mit Wiederanruf erhält der einleitende Teilnehmer automatisch ein zu lange gehaltenes, zu lange geparktes Gespräch oder ein nicht erfolgreich übergebenes Gespräch erneut.

Wiederanruf erfolgt in folgenden Fällen:

- Ein gehaltenes oder geparktes Gespräch wird nicht innerhalb einer bestimmten Zeit wieder aufgenommen (Timer Zeit für Parken + Übergang Halten).
- Bei Übergabe vor Melden unter folgenden Umständen:
  - wird nicht beantwortet vor Ablauf einer bestimmten Zeit (Timer Rufzeit während Übergeben vor Melden)
  - Ziel existiert nicht
  - Ziel ist zweitgradig besetzt
  - digitales Telefon am Ziel ist defekt
  - Übergabe ist nicht zulässig

Ist der einleitende Teilnehmer während des Wiederanrufs besetzt, klopft der Wiederanruf an. Sobald der einleitende Teilnehmer wieder frei ist, wird der Wiederanruf signalisiert. Im Display des einleitenden Teilnehmers kann entweder die Rufnummer des Anrufers oder des Zielteilnehmers angezeigt werden. Beantwortet der Teilnehmer den Wiederanruf nicht bis zum Ablauf des Timers Abwurfzeit für Wiederanruf, erfolgt Abwurf an den Abwurfplatz, wenn das Flag bei nichtbeantwortetem Wiederanruf gesetzt ist. Beantwortet

der Abwurfplatz den Wiederanruf nicht bis zum Ablauf des Timers Zeit für das Auslösen eines Wiederanrufes am VPL, wird der Wiederanruf automatisch getrennt.

Wiederanruf und Anrufübernahme

Jeder Teilnehmer in einer Anrufübernahmegruppe mit dem einleitenden Teilnehmer kann einen Wiederanruf übernehmen, wenn das systemweite Flag AUN nach Wiederanruf gesetzt ist.

Wiederanruf und Anrufschutz

Ein Wiederanruf ignoriert Anrufschutz.

Systemspezifische Informationen

Timer Abwurfzeit für Wiederanruf: standardmäßig 30 s

Timer Zeit für das Auslösen eines Wiederanrufes am VPL: standardmäßig 60 s

14.3.7 Call Supervison

Call Supervision ermöglicht berechtigten Teilnehmern, ein Gespräch eines beliebigen internen Teilnehmers mitzuhören. Das Mikrofon des mithörenden Teilnehmers wird automatisch stummgeschaltet. Die Teilnehmer der überwachten Verbindung erhalten keinerlei Hinweis auf den Vorgang, wie z.B. Ton oder Displayanzeige.

Die Funktion ist in der Standardkonfiguration deaktiviert. Sie kann nur aktiviert werden, wenn die landesspezifische Gesetzgebung dies zulässt. Im Einzelfall muss die landesspezifische Gesetzgebung immer geprüft werden, bevor die Funktion aktiviert wird.

Berechtigte Teilnehmer benötigen ein Systemtelefon und die Berechtigung für Aufschalten.

Der zu überwachende Teilnehmer muss sich in einem aktiven Gesprächszustand befinden. Beim Beginn und beim Beenden der Call Supervision können Gesprächsaussetzer von bis zu zwei Sekunden auftreten. Sobald einer der Gesprächsteilnehmer in der überwachten Verbindung gehalten wird, übergeben wird oder das Gespräch beendet, wird die Mithörverbindung getrennt. Die Mithörverbindung kann erst dann wiederhergestellt werden, wenn sich der zu überwachende Teilnehmer wieder in einem aktiven Gesprächszustand befindet.

Abhängigkeiten

Themenbereich	Abhängigkeit
Schnurlose Telefone	Sie können Call Supervision nicht an einem schnurlosen Telefon verwenden, da dieses die automatische Mikrofon-Stummschaltung nicht unterstützt.
Konferenzschaltung	Call Supervision schränkt die mögliche Anzahl an Konferenzen ein. Maximale Anzahl möglicher Konferenzen im System = maximale Anzahl gleichzeitiger Call-Supervision-Teilnehmer.

Themenbereich	Abhängigkeit
Call Supervison	Der Anruf kann nur mithilfe des Codes *944 + Rufnummer aufgeschaltet werden (nicht über ein Menü).
Call Supervison	Um die Verwendung von Funktionen für einen Teilnehmer zu ermöglichen, müssen das Teilnehmer-Flag **Call Supervision** und das Flag **Aufschalteberechtigung ein** aktiviert werden. (Funktion kann nicht mit CSTA-Monitoring verwendet werden.)

14.3.7.1 Wie Sie Call Supervision für einen Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Für den betreffenden Teilnehmer ist die Aufschalteberechtigung aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer**.
4) Navigieren Sie im Menübaum unter **Teilnehmer** > **Teilnehmer** > **…** zum gewünschten Teilnehmer (Index-Rufnummer-Name).
5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
6) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie einem Teilnehmer die Berechtigung für diese Funktion erteilen möchten, aktivieren Sie das Kontrollkästchen **Call Supervision**.
   - Wenn Sie die einem Teilnehmer die Berechtigung für diese Funktion entziehen möchten, deaktivieren Sie das Kontrollkästchen **Call Supervision**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.3.8 Diskretes Ansprechen

Das Leistungsmerkmal Diskretes Ansprechen ermöglicht es einem Teilnehmer C bei einer einfachen Verbindung zwischen den zwei Teilnehmern A und B mitzuhören und Teilnehmer A Hinweise zu geben, welche für Teilnehmer B nicht hörbar sind, typischerweise in Callcentern oder bei Chef-/Sekretär-Anlagen.

Das Leistungsmerkmal ist in Manager E zu konfigurieren.

Anmerkung: Obwohl es keine Verbindung zwischen Teilnehmer B und Teilnehmer C gibt, kann Teilnehmer B über Rückkopplung beim Telefon von Teilnehmer A eventuell doch gedämpft hören was Teilnehmer C spricht.

Zielendgeräte für das diskrete Ansprechen (Teilnehmer A) können nur Systemtelefone mit Display sein. Die Teilnehmer A und C müssen im selben Knoten sein.

Das Leistungsmerkmal wird von Teilnehmer C im Ruhe/Bereit-Zustand durch Wahl einer Kennzahl aktiviert. Es gibt eine teilbelegte Taste (nur die Kennzahl liegt auf der Taste, die Rufnummer muss nachgewählt werden) am Telefon. Im Servicemenü wird ein Menüpunkt eingebracht, das Idle/Gesprächs-Menü bleibt unverändert.

Die Möglichkeit das Feature zu aktivieren ist an eine benutzerspezifische Berechtigung geknüpft. Mit einer zweiten Berechtigung kann sich Teilnehmer A vor dem diskreten Ansprechen schützen.

Die Deaktivierung erfolgt entweder durch Auslösen des aktivierenden Teilnehmers C oder durch Leistungsmerkmalbeeinflussung.

Anmerkung: Ist nicht mindestens ein Teilnehmer des ursprünglichen Gesprächs ein TDM-Teilnehmer, so ist zum Zeitpunkt des Aktivierens das Koppelfeld noch nicht beteiligt und das Umschalten kann nicht ohne kurzzeitige Unterbrechung der bisherigen Verbindung durchgeführt werden.

Anmerkung: Wenn Diskretes Ansprechen aktiviert ist, sind die Leistungsmerkmale Anruf weiterleiten/übergeben und Konferenz in UC Suite-Produkten nicht verfügbar.

Ist das Leistungsmerkmal Diskretes Ansprechen aktiv und Teilnehmer A oder Teilnehmer B leitet ein anderes verbindungsbezogenes Leistungsmerkmal ein, so wird Diskretes Ansprechen prinzipiell beendet. Details zum Verhalten bei bestimmten Leistungsmerkmalen siehe folgende Tabelle:

Leistungsmerkmal	Teilnehmer A		Teilnehmer B		Teilnehmer C	
	Möglich	Aktion	Möglich	Aktion	Möglich	Aktion
Rückfrage, Halten, Parken, Gemeinsames Halten	Ja	„Diskretes Ansprechen“ beenden	Ja	„Diskretes Ansprechen“ beenden	Nein	Negativ quittieren
Übergabe	--	--	--	--	--	--
Konferenz	--	--	--	--	--	--
Anklopfen	Ja	--	Ja	--	Ja	--
Anklopfen annehmen	Ja	„Diskretes Ansprechen“ beenden	Ja	„Diskretes Ansprechen“ beenden	Ja	Negativ quittieren
Aufschalten	Nein	--	Nein	--	Nein	--
DTMF Übertragung	Ja	--	Ja	--	Nein	--
LM-Zähler	--	--	--	--	--	--
Assoziierte Dienste	--	--	--	--	--	--

Leistungsmerkmal	Teilnehmer A		Teilnehmer B		Teilnehmer C	
DISA / DISI	--	--	--	--	--	--

14.3.9 Live Call Recording (Voice Recording; Sprachaufzeichnung)

Das Leistungsmerkmal ermöglicht die Aufzeichnung der Daten einer aktiven Sprachverbindung zwischen zwei Teilnehmern (ein Teilnehmer muss intern, der andere kann ein externer Teilnehmer sein), also der Aufnahme von Gesprächen. Für die Aufzeichnung ist ein separates Gerät erforderlich.

Der Start/Stop der Aufzeichnung kann per Funktionstaste oder Kennzahl (analoge Endgeräte) erfolgen. In Abhängigkeit von der Konfiguration kann die Aufzeichnung auch durch das Aufzeichnungsgerät angehalten werden.

Die Aufzeichnungsvorrichtung kann von allen unterstützten Endgeräten innerhalb einer CorNet-NQ-Vernetzung genutzt werden. Nicht unterstützt werden Verbindungen mit CorNet N und QSIG (ECMA, ISO). Der Aufzeichnungston während der Aufnahme kann abgeschaltet werden.

Unterstützt werden TDM- und CorNet-IP (HFA)-Telefone (inkl. Geräte ohne Display) sowie auch OpenScape Personal Edition (HFA) und optiClient Attendant. Nicht unterstützt werden Standard H.323-Telefone, SIP-Telefone, EDSS1-Teilnehmer.

Anmerkung: Ein aktivierte Anrufaufnahme wird durch eine LED bzw. durch einen Aufzeichnungston während des Gesprächs angezeigt.

Es kann für jeden Teilnehmer einzeln konfiguriert werden, ob er Voice Recording nutzen darf.

Abhängigkeiten/Einschränkungen

Thema	Abhängigkeit/Einschränkung
Rückfrage, Makeln, Transfer, Konferenz	Wenn Sie während einer Anrufaufzeichnung eines dieser Leistungsmerkmale einleiten, so wird die Aufzeichnung des Gesprächs automatisch abgebrochen.
Halten	Bei Aktivierung von "Halten" wird eine laufende Aufzeichnung abgebrochen. Eine Aktivierung der Aufzeichnung ist nicht möglich, wenn man einen Teilnehmer gehalten hat.
Aufschalten	Anrufaufzeichnung nicht möglich. Man kann sich auf ein Gespräch, welches aufgezeichnet wird, nicht aufschalten. Ebenso ist es nicht möglich nach dem Aufschalten eine Aufzeichnung zu aktivieren.

Thema	Abhängigkeit/Einschränkung
Call Supervision	Anrufaufzeichnung nicht möglich. Man kann ein Gespräch, welches aufgezeichnet wird, nicht mithören. Ebenso ist es nicht möglich nach der Aktivierung von „Call Supervision“ eine Aufzeichnung zu starten.

Anmerkung: Es können nur Zweier-Gespräche aufgezeichnet werden, keine Konferenzen oder Gespräche, bei denen zusätzlich ein gehaltener Teilnehmer beteiligt ist.

Anmerkung: Zusätzliche Hinweise:

-) Das Aufzeichnungsgerät kann in einem beliebigen Knoten eines Cornet-NQ-Netzes adressiert werden.

-) Es kann nur einer beschränkten Anzahl von Teilnehmern in einem Knoten die Berechtigung für Gesprächsaufzeichnung erteilt werden (derzeit: 50).

-) Während der Aufzeichnung werden Konferenz-Ressourcen belegt.

-) Die Standard-Service-Kennzahl zur Aktivierung der Gesprächsaufzeichnung lautet *493.

14.4 Steuern der Erreichbarkeit

Zum Steuern der Erreichbarkeit bietet das System Leistungsmerkmale wie Anrufumleitung, Anrufschutz und Abweisen von Anrufen.

Verschiedene Arten von Anrufumleitungen benutzen Rufziellisten. Rufziellisten legen fest, wie ankommende Rufe für den zugeordneten Teilnehmer bzw. die zugeordnete Gruppe behandelt werden. Ziele in einer Rufzielliste werden nacheinander abgearbeitet. Unterschiedliche Einträge für Intern- und Externrufe (Tag bzw. Nacht) sind möglich.

14.4.1 Anrufumleitung

Die Rufweiterschaltung leitet Anrufe weiter, wenn sie nicht innerhalb einer bestimmten Zeit angenommen werden.

Diese Art der Rufweiterschaltung wird auch als Feste Rufweiterschaltung bezeichnet, weil Sie nur durch den Administrator konfigurierbar ist.

Für jede Rufweiterschaltung gibt es eine oder mehrere Rufziellisten, die den Teilnehmern für folgende Arten von Anrufen zugeordnet werden können:

- Externe Anrufe tagsüber (während inaktiver Nachtschaltung)
- Externe Anrufe nachts (während aktiver Nachtschaltung)
- Interne Anrufe

Pro Rufzielliste können Sie bis zu 4 Rufziele angeben, an die der Anruf nach Ablauf einer einstellbaren Zeit der Reihe nach weitergeschaltet wird.

Beim Rufweiterschaltungsziel werden Rufnummer oder Name des ursprünglich gerufenen Teilnehmers und Rufnummer oder Name des Anrufers angezeigt. Die zusätzliche Anzeige der Rufnummer oder des Namens des Anrufers können Sie als Administrator deaktivieren.

Rufweiterschaltung im Besetztfall

Die Rufweiterschaltung im Besetztfall leitet einen ankommenden Anruf bei einer besetzten Nebenstelle sofort zum nächsten Rufziel weiter.

Ist das Rufziel ebenfalls besetzt, wird dem Anrufer besetzt signalisiert. Bei einem internen Anruf bleibt der Anruf in diesem Fall beim Rufziel, das zyklisch auf Freiwerden geprüft wird. Der Administrator legt den Zyklus fest.

Ist das Rufziel nicht verfügbar und ist hierfür keine weitere Rufweiterschaltung eingerichtet, wird der Anruf nicht weitergeschaltet.

Abhängigkeiten

Themenbereich	Abhängigkeit
Analoge Telefone	Bei diesen Telefonen ist nicht zu erkennen, dass es sich bei dem eingehenden Ruf um einen weitergeleiteten Ruf handelt.
Anklopfen annehmen	Hat ein Teilnehmer Anklopfen freigegeben, wird bei ihm auch dann angeklopft, wenn für ihn Rufweiterschaltung im Besetztfall konfiguriert ist.
Anrufschutz	Ein Rufziel, das den Anklopfschutz aktiviert hat, wird übersprungen.
Anrufumleitung	Eine Rufweiterschaltung wird erst ausgeführt, wenn nach einer vom Administrator eingestellten Zeit das Ziel einer Anrufumleitung nicht antwortet.
Nachtschaltung	Wird für einen Teilnehmer in der Rufweiterschaltung die Möglichkeit "tagsüber / nachts" verwendet und die Nachtschaltung aktiviert, werden externe Anrufe entsprechend der Einstellung bei Nachtschaltung umgeleitet. Interne Anrufe folgen weiterhin der Einstellung "tagsüber".
Rufweiterschaltung ins Amt	Ist eine Rufweiterschaltung ins Amt aktiviert, so hat diese Vorrang vor anderen Rufweiterschaltungen.

Themenbereich	Abhängigkeit
Sammelanschluss / Gruppenruf	Wird eine Gruppe oder ein Sammelanschluss als Ziel einer Rufweiterschaltung eingetragen, so wird diese Gruppe erst vollständig abgearbeitet, d.h. nacheinander gerufen, bevor das nächste Ziel der Rufweiterschaltung ausgewertet wird. Gruppenruf und Sammelanschluss sind wie eine Rufweiterschaltung innerhalb der Rufweiterschaltung anzusehen. Ein Sammelanschluss ist besetzt, wenn alle Mitglieder besetzt sind oder sich aus dem Sammelanschluss herausgeschaltet haben. Eine Gruppe ist immer dann besetzt, wenn alle Gruppenmitglieder besetzt sind.

14.4.1.1 Wie Sie eine Rufweiterschaltung konfigurieren

Mit dem Wizard **Rufweiterschaltung** konfigurieren Sie für interne Teilnehmer eine Rufweiterschaltung bei ankommenden Anrufen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **User Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Rufweiterschaltung** zu starten. Es öffnet sich das Fenster **Rufzielliste - Definition**.

4) Definieren Sie zuerst eine Rufzielliste, indem Sie in der Zeile der zu bearbeitenden Rufzielliste auf das Symbol **Bearbeiten** klicken.

5) Wählen Sie in den Aufklapplisten **1. Ziel** bis **4. Ziel** die gewünschten Ziele aus. Sie haben die folgenden Möglichkeiten:

- **Kein Eintrag**: Ziel wird übersprungen
- **Externes Ziel**: Richtung und externe Rufnummer mit Amtskennzahl
- *** Angewählter Teilnehmer**: der angerufene Teilnehmer
- **** Benutzer definiert**: Ziel der Anrufumleitung nach Zeit (falls eingerichtet).
- **#9 Systemsuchlauf**: nächster verfügbarer Teilnehmer (außer Chef-Nebenstelle)
- **#201 - #260**: Anrufverteilung (UCD-Gruppe)
- **#801 - #817**: Ansagegerät
- **100, 101, ...**: Rufnummer eines internern Teilnehmers oder einer Gruppe (z.B. Sprachbox)

Anmerkung: Um ein Rufziel schneller zu finden, können Sie in den Feldern **1. - 4. Ziel** auch eine oder mehrere Ziffern eingeben. Dann wird direkt zum Listeneintrag

gesprungen, der mit der eingegebenen Ziffernfolge beginnt. Die Eingabe einer Buchstabenfolge ist ebenfalls möglich.

---

6) Wählen Sie in der Aufklappliste **Die Rufweiterschaltung erfolgt immer nach** die Zeit in Sekunden aus, nach der ein Anruf an das nächste Ziel weitergeschaltet wird.

7) Aktivieren Sie das Kontrollkästchen **Rufweiterschaltung**, wenn der Anruf im Besetztfall sofort an das nächste Rufziel weitergeleitet werden soll.

8) Wenn der Anruf bei einem zusätzlichen internen Teilnehmer signalisiert werden soll oder z.B. bei einem Relais (Aktor) für einen zentralen Wecker, wählen Sie in der Aufklappliste **Zweitwecker Ziel** die gewünschte Rufnummer aus. Mit **Zweitwecker Art** wählen Sie, ob der Anruf sofort oder nach der gesamten Rufweiterschaltungszeit beim Teilnehmer signalisiert wird.

9) Klicken Sie auf **OK & Weiter**. Sie befinden sich wieder im Fenster **Basiskonfiguration**.

10) Wenn Sie weitere Rufziellisten definieren wollen, wiederholen Sie die vorherigen Schritte.

11) Klicken Sie auf **OK & Weiter**.

12) Ordnen Sie nun den Teilnehmern die Rufziellisten zu.

13) Sie können einen Teilnehmer suchen, indem Sie in die Suchfelder **Rufnr** oder **Name** ein Suchbegriff eingegeben und anschließend die Return-Taste drücken. Alle Treffer werden angezeigt, die den Suchbegriff enthalten. Mit der Eingabe von `521` als Rufnummer werden z.B. die Treffer `+495213535` und `+498967521` angezeigt oder mit `co` als Name die Treffer `Collins`, `Mcoin` und `Branco`.

Anmerkung: Alle Einträge werden angezeigt, wenn in allen Suchfeldern nichts eingetragen ist und anschließend die Return-Taste gedrückt wird.

---

14) Wählen Sie in der Zeile des gewünschten Teilnehmers für die folgenden Fälle aus den Aufklapplisten die Rufziellisten aus:

- **Tag**: Rufzielliste für kommende Externrufe während der Arbeitszeiten (Tagschaltung)
- **Nacht**: Rufzielliste für kommende Externrufe bei aktivierter Nachtschaltung
- **Intern**: Rufzielliste für kommende Internrufe

15) Speichern Sie Ihre Einträge mit **Sichern**, bevor Sie zu einem Teilnehmer auf einer weiteren Seite wechseln.

16) Wenn Sie einer Rufzielliste komfortabel mehrere Teilnehmer zuordnen wollen, klicken Sie auf **Kopieren**.

a) Wählen Sie unter **Rufzielliste** die Rufzielliste aus, der die Teilnehmer zugewiesen werden sollen.

b) Markieren Sie im Fenster **Auswahl** einen oder mehrere Teilnehmer und übernehmen Sie diese mit **Hinzufügen** in das Fenster **Mitglieder**.

c) Wählen Sie über die Kontrollkästchen **Tag**, **Nacht** und **Intern** aus, ob die Rufzielliste für kommende Externrufe während der Arbeitszeiten (Tagschaltung), bei aktivierter Nachtschaltung oder nur für interne Anrufe gelten soll.

d) Klicken Sie auf **OK & Weiter**.

17) Klicken Sie erneut auf **OK & Weiter**.

18) Sie können sich hier alle Teilnehmer einer Rufzielliste anzeigen lassen. Wählen Sie dazu in **Alle Teilnehmer in Rufzielliste anzeigen** die gewünschte Rufzielliste aus.
19) Klicken Sie auf **OK & Weiter**. Die Rufweiterschaltung für interne Teilnehmer ist eingerichtet.
20) Klicken Sie auf **Beenden**.

14.4.2 Anrufumleitung (CF)

Mit der Anrufumleitung (AUL) können Teilnehmer kommende Anrufe zu einem Ziel ihrer Wahl umleiten.

Falls Leitungstasten (auch MULAP-Leitungstasten) vorhanden sind, kann die Anrufumleitung auch individuell für eine bestimmte Leitung (oder MULAP-Leitung) aktiviert werden.

Folgende Anrufe können umgeleitet werden:

- All Anrufe
- Nur externe Anrufe
- Nur interne Anrufe

Folgende Ziele für eine Anrufumleitung sind möglich:

- Anderes Telefon (intern oder extern)
- Vermittlungsplatz
- Sprachbox
- Gruppennummer
- UCD-Gruppe (UCD Universelle Anrufverteilung)

Abgehende Anrufe sind bei aktivierter Anrufumleitung weiterhin möglich.

Externes Ziel

Bei einem externen Anrufumleitungsziel geben sie die Amtskennzahl gefolgt von der externen Rufnummer des Umleitungsziels ein.

Anrufumleitung zu externen Zielen

Hat ein Teilnehmer in seiner Rufzielliste eine Anrufumleitung zu einem externen Ziel eingetragen, so endet die Rufweiterschaltung bei diesem Ziel. Eventuell eingetragenen weiteren Ziele in der Rufzielliste wird nicht gefolgt.

Soll eine Rufweiterschaltung zu weiteren Zielen erfolgen, muss das Systemflag **Rufweiterschaltung nach AUL zum externen Ziel** durch einen Servicetechniker aktiviert werden.

Soll einer Anrufumleitung zu einem externen Ziel auch bei einem Anruf über eine analoge Amtsleitung gefolgt werden, muss ein Servicetechniker das Systemflag **Anrufumleitung nach HKZ erlaubt** aktiveren.

Anmerkung: Wenn ein Anruf über Smart AA geleitet wird und dieser Anruf an einen Benutzer A weitergeleitet wird, wobei die externe Weiterleitung (*11) an Benutzer B aktiviert ist, wird Benutzer B nicht die CLI des Anrufers, sondern die Durchwahl des Benutzers A angezeigt.

Abhängigkeiten

Themenbereich	Abhängigkeit
Anrufschutz	Zu einem anrufgeschützten Telefon können Sie keine Anrufumleitung programmieren.
Termin, Weckeinrichtung	Wird ein Termin fällig, wird dieser Termin am umgeleiteten Telefon signalisiert und nicht von einer eingestellten Umleitung beeinflusst.
UCD-Gruppe als Anrufumleitungsziel	In folgenden Fällen wird der Anrufumleitung zu einer UCD-Gruppe nicht gefolgt: • Wird ein Sammelanschluss gerufen und ein Teilnehmer mit einer Anrufumleitung zu einer UCD-Gruppe ist an der Reihe, wird nicht der Anrufumleitung gefolgt. In diesem Fall wird direkt der nächste Teilnehmer des Sammelanschlusses gerufen. • Ein Teilnehmer ist Mitglied eines Gruppenrufs mit der Eigenschaft “Gruppe” und hat eine Anrufumleitung zu einer UCD-Gruppe aktiviert. • Ein Teilnehmer ist Mitglied eines Gruppenrufs im Freifall. Wird die Gruppe gerufen, wird nicht der Anrufumleitung zur UCD-Gruppe gefolgt. Ausnahme: Der erste eingetragene Teilnehmer hat eine Anrufumleitung zu einer UCD-Gruppe aktiviert. Dieser AUL wird gefolgt.

14.4.2.1 Wie Sie Anrufumleitung über analoge Amtsleitungen aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.

3) Navigieren Sie im Menübaum zu **System** > **System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Anrufumleitung über analoge Amtsleitungen aktivieren möchten, aktivieren Sie das Kontrollkästchen **Anrufumleitung nach HKZ erlaubt**.
- Wenn Sie Anrufumleitung über analoge Amtsleitungen deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Anrufumleitung nach HKZ erlaubt**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.4.2.2 Wie Sie eine Anrufumleitung nach Anrufumleitung zum externernen Ziel aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Navigieren Sie im Menübaum zu **System** > **System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Anrufumleitung nach Anrufumleitung zum externen Ziel aktivieren möchten, aktivieren Sie das Kontrollkästchen **Rufweiterschaltung nach AUL zum externen Ziel**.
   - Wenn Sie die Anrufumleitung nach Anrufumleitung zum externen Ziel deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Rufweiterschaltung nach AUL zum externen Ziel**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.4.3 Anrufumleitung nach Zeit

Die Anrufumleitung nach Zeit leitet nicht angenommene Anrufe nach einer bestimmten Zeit um. Die Anrufumleitung nach Zeit entspricht einer Rufweiterschaltung nach Zeit, nur dass der Teilnehmer die Umleitung selber einstellen kann.

Der Teilnehmer kann die Anrufumleitung nach Zeit für sein eigenes Telefon einstellen, es können auch externe Ziele und Gruppen eintragen werden.

Das Umleitungsziel wird nicht dauerhaft gespeichert und bei Deaktivierung des Leistungsmerkmals gelöscht.

Im Besetztfall gelten die Regeln der Rufweiterschaltung, d.h. es wird mit dem nächsten Ziel fortgefahren.

Systemspezifische Informationen

Pro Teilnehmer gibt es drei einstellbare Ziele. Außerdem gibt es eine Sonderkennung "Benutzerdefiniert", über die der Administrator das Leistungsmerkmal Anrufumleitung nach Zeit für einen Teilnehmer freigeben oder sperren kann. Standardmäßig ist das Leistungsmerkmal freigegeben.

Wird ein Anruf nach der voreingestellten Zeit nicht beantwortet, wird das vom Teilnehmer gespeicherte Umleitungsziel gesucht und gerufen. Ist vom Teilnehmer kein individuelles Umleitungsziel eingetragen, wird mit dem nächsten Ziel in der Rufzielliste fortgefahren.

Der Administrator muss die Anrufumleitung nach Zeit für den einzelnen Teilnehmer über die Rufziellisten freigeben.

14.4.4 Rufweiterschaltung im Amt (nicht für USA)

Jeder Teilnehmer, dem als Durchwahlrufnummer eine MSN (Multiple Subscriber Number beim ISDN-Mehrgeräteanschluss oder ITSP-Anschluss) zugeordnet ist, kann für diese MSN eine Rufweiterschaltung im Amt aktivieren bzw. deaktivieren. Voraussetzung ist, dass der Teilnehmer die Berechtigung für externe Rufweiterschaltung hat.

Ist einer Teilnehmergruppe eine MSN zugeordnet, kann jeder Teilnehmer dieser Gruppe für diese MSN eine Rufweiterschaltung im Amt aktivieren bzw. deaktivieren.

Das Leistungsmerkmal wird in drei Varianten unterschieden:

- Uneingeschränkte Gesprächsumleitung (CFU): Der Netzanbieter leitet alle für diese MSN bestimmten Rufe direkt weiter, unabhängig von deren Status.
- Anrufumleitung bei Besetzt (CFB = Call Forwarding Busy): Die Rufweiterschaltung wird nur ausgeführt, wenn die gewählte MSN besetzt ist.
- Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply): Die Rufweiterschaltung wird nur ausgeführt, wenn der eingehende Ruf nicht innerhalb einer vorgegebenen Zeit beantwortet wird.

Anmerkung:

Anmerkung: Für alle oben genannten Szenarien der Anrufumleitung kann der Benutzer nur ein Weiterschaltungsziel pro MSN eingeben. Die maximale Anzahl weiterschaltbarer MSN ist 10.

Falls ITSP oder ISDN mit der Durchwahl konfiguriert ist, sind maximal 249 externe Umleitungen möglich.

Abhängigkeiten

Themenbereich	Abhängigkeit
Nachtschaltung	Rufweiterschaltung im Amt hat höhere Priorität als Nachtschaltung.

14.4.5 Rufzuordnung

Die Rufzuordnung ermöglicht eine Rufweiterschaltung von ankommenden Anrufen einer analogen oder S_0-Leitung zu einem Teilnehmer oder einer Gruppe, abhängig von der gewählten Rufnummer und dem Aktivierungszustand der Nachtschaltung.

Für Tag- und Nachtbetrieb sind unterschiedliche Ziele möglich. Ein ankommender Anruf wird nicht beim Teilnehmer signalisiert, sondern gemäß den Rufziellisten für den Teilnehmer.

14.4.5.1 Wie Sie eine Rufzuordnung konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung** > **Leitungen**.
4) Navigieren Sie im Menübaum unter **Leitungen** > **…** (Box-Port-Kennzahl) zur gewünschten analogen oder S_0-Leitung.
5) Wählen Sie in der Aufklappliste **Tag Ruf-Nr.** die gewünschte Rufnummer.
6) Wählen Sie in der Aufklappliste **Nacht Ruf-Nr.** die gewünschte Rufnummer.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.4.6 Rufzuschaltung

Das Leistungsmerkmal Rufzuschaltung ermöglicht jedem internen Teilnehmer eine persönliche Liste interner Rufnummern zu verwalten, welche bei Anrufen an seiner Rufnummer ebenfalls gerufen werden.

Ein Teilnehmer kann auch die eigene Rufnummer eintragen, z.B. wenn die Rufnummer fest auf einen anderen Teilnehmer umgeleitet wird (Chef-Sek.).

Zur Aktivierung/Deaktivierung dieses Leistungsmerkmals kann an IP-Systemtelefonen, OpenStage TDM-Telefonen, optiPoint 500-Telefonen eine Taste programmiert werden. Um Variationen zu ermöglichen können auf einem Telefon mehrere Rufzuschaltungstasten programmiert werden. Es können mehrere Tasten gleichzeitig aktiviert werden, allerdings kann die maximale Anzahl Telefone mit Rufsignalisierung fünf nicht überschreiten.

Dieses Leistungsmerkmal kann durch den Teilnehmer für das eigene Telefon über eine DISA-Verbindung oder für einen anderen Teilnehmer mit Hilfe des Leistungsmerkmals Assoziierte Dienste aktiviert/deaktiviert werden.

Die Bildschirmanzeige Weiterleitung ... ist eine von drei Anzeigen im Menü Systemweit von Manager E, die endgerätespezifische (nicht systemspezifische) Statusinformationen liefert. Mit Hilfe des Fensters Weiterleitung können Sie feststellen, ob bei einem Telefon die Rufzuschaltung aktiviert ist oder ob das Telefon Teil einer Rufgruppe ist.

Wird das Leistungsmerkmal häufig benutzt, kann der Teilnehmer eine freie Taste auf seinem Telefon damit belegen. Der Name der Taste ist Rufzuschaltung ein in der Tastenprogrammierung. Bei aktivem Leistungsmerkmal leuchtet die LED.

Durch das Teilnehmer-Flag “keine Rufzuschaltung bei besetzt" kann gesteuert werden, welche rufzugeschalteten Teilnehmer bei besetztem "Master" (= rufzuschaltender Teilnehmer) gerufen werden sollen und welche nicht. Haben mehrere “Master" den selben Teilnehmer zugeschaltet, gilt das Flag für alle Zuschaltungen dieses Teilnehmers.

Bei nicht gesetztem Flag wird die Rufzuschaltung auf jeden Fall durchgeführt, sofern der zugeschaltete Teilnehmer erreichbar ist (Standardverhalten).

Bei gesetztem Flag hängt die Rufzuschaltung von der Erreichbarkeit des “Masters" ab:

- “Master" ist frei - Rufzuschaltung erfolgt sofort.

  Beim “Master" kann angeklopft werden - Rufzuschaltung erfolgt nach 5 s.

  Beim “Master" kann nicht angerufen oder angeklopft werden - es erfolgt keine Rufzuschaltung.

Thema	Abhängigkeit/Einschränkung
Wiederanruf Systemsuchlauf Rückruf	Bei einem sofortigen Wiederanruf (z.B. Fehlbedienung) Systemsuchlauf oder Rückruf wird die Rufzuschaltung nicht ausgeführt.
Anrufumleitung	Hat der Teilnehmer, der die Rufzuschaltung aktiviert hat, AUL eingeschaltet, so erfolgt keine Rufzuschaltung.
Anrufschutz (DND)	Hat der rufzugeschaltete Teilnehmer Anrufschutz aktiviert, wird er nicht mitgerufen.
Termin	Ein aktiver Terminruf folgt nicht der Rufzuschaltung.
Keine Rufzuschaltung bei besetzt	Ist das Flag gesetzt, wird die Rufzuschaltung nicht ausgeführt, wenn der Teilnehmer besetzt ist.

14.4.7 Anrufe abweisen

Kommende interne und externe Erstanrufe kann der Teilnehmer abweisen. Die Anrufe können durch Betätigen der Trenntaste abgewiesen werden.

Der abgewiesene Anruf folgt anschließend der Rufweiterschaltung. Ist kein Rufweiterschaltungsziel vorhanden, wird ein externer Anruf zum Vermittlungsplatz abgeworfen, sofern die entsprechenden Abwurfkriterien konfiguriert wurden. Wenn kein Ziel gerufen werden kann, dann erhält der Rufende besetzt.

Vermittelte Wiederanrufe, weitergeleitete Anrufe, vorgemerkte Rückrufe, gehaltene oder geparkte Gespräche können nicht abgewiesen werden. Wird ein Gespräch zum Abwurfplatz abgeworfen, kann es nicht abgewiesen werden.

Abhängigkeiten

Themenbereich	Abhängigkeit
Gruppenruf, Sammelruf, MULAP	In diesen Fällen wird der gesamte Gruppenanruf beendet und der Anruf folgt der konfigurierten Rufweiterschaltung. Der Anruf wird beendet, falls kein weiteres Rufziel vorhanden ist.

14.4.8 Zurückstellen eines Anrufs

Ein Teilnehmer hat die Möglichkeit einen kommenden Ruf zurückzustellen. Der angerufene Teilnehmer kann eine Verbindung aufbauen, ohne den kommenden Ruf anzunehmen.

Der wartende Ruf wird anschließend als Anklopfen signalisiert.

Wenn ein kommender Ruf signalisiert wird, betätigt der Teilnehmer eine Gesprächs- oder Leitungstaste und tätigt einen externen Anruf. Dafür müssen zwei Gesprächs- und eine Leitungstaste programmiert sein. Eine der entsprechenden Tasten muss für die Ausführung des Leistungsmerkmals frei sein.

Der rufende Teilnehmer bemerkt keinerlei Änderung bei der Signalisierung, wenn Rufsignalisierung bei Anklopfen eingestellt ist.

14.4.9 Anrufschutz

Anrufschutz verhindert die Durchstellung ankommender Anrufe.

Beim Abheben des Hörers erhält der Teilnehmer, der den Anrufschutz aktiviert hat, einen Sonderwählton. Außerdem wird bei Telefonen mit Display Anrufschutz angezeigt, solange das Leistungsmerkmal aktiv ist. Bei allen anderen Telefonen blinkt die LED der Direktruf-Taste des anrufgeschützen Teilnehmers mit einer kleinen Unterbrechung.

Ein gesetzter Anrufschutz kann durch den Vermittlungsplatz oder einen berechtigten Teilnehmer durchbrochen werden. Das Gespräch kann dann auch bei einem Teilnehmer mit Anrufschutz sofort durchgeschaltet werden.

Bei Anwahl eines anrufgeschützten Telefons erhält der Anrufer Besetztton.

Abhängigkeiten

Thema	Abhängigkeit
Vermittlungsplatz/ Nachtziel	Der Vermittlungsplatz und der aktuelle Abwurfplatz kann keinen Anrufschutz aktivieren.
Anrufumleitung	Anrufschutz kann nicht aktiviert werden, wenn eine Anrufumleitung auf diesem Telefon aktiviert ist. Auf einem anrufgeschütztes Telefon kann keine Anrufumleitung aktiviert werden.
Rückruf	Wird ein Rückruf auf einen anrufgeschützten Teilnehmer gesetzt, so wird dieser erst ausgeführt, wenn der Anrufschutz deaktiviert wird. Wenn der anrufgeschützte Teilnehmer einen Rückruf einleitet, wird sein Anrufschutz durchbrochen.
Termin, Weckeinrichtung	Hat ein Teilnehmer einen Termin gesetzt und aktiviert Anrufschutz, erfolgt bei Fälligkeit des Termins eine akustische Signalisierung am Telefon.
DISA	DISA kann vom Anwender für eigene Telefone oder von einem Anwender für einen anderen aktiviert werden (assoziierte Dienste).

14.5 Optimieren der Kommunikationsabläufe

Das Kommunikationssystem bietet verschiedene Möglichkeiten Anrufe komfortabler und effektiver zu handhaben, z.B. Rückruf oder Anklopfen.

14.5.1 Rückruf

Ein Rückruf kann dann aktiviert werden, wenn sich der angerufene Teilnehmer nicht meldet oder besetzt ist. Ein aktivierter Rückruf löst einen Anruf aus, sobald der angerufene Teilnehmer wieder erreichbar ist.

Automatischer Rückruf bei “Frei” oder “Besetzt”

Wenn ein Gesprächswunsch nicht erfüllt wird, weil der gerufene Teilnehmer besetzt ist oder den Anruf nicht annnimmt, kann der rufende Teilnehmer einen Rückruf aktivieren, um das Gespräch zu einem späteren Zeitpunkt aufzubauen. War der gerufene Teilnehmer besetzt, wird durch Rückruf das Ende des Gesprächs überwacht. Wenn der Teilnehmer wieder frei ist, wird dies dem rufenden Teilnehmer signalisiert, indem er selbst nun durch das Kommunikationssystem angerufen wird. Nimmt er diesen Anruf an, wird der zuvor besetzte Teilnehmer erneut angewählt. Bei Nichtzustandekommen eines Gesprächs durch die Rückruffunktion, bleibt diese aktiv. Sobald der gewünschte Teilnehmer ein neues Gespräch geführt hat, erfolgt erneut ein Rückruf.

Ein Telefon kann bis zu zwei Rückrufanforderungen abschicken und Ziel von bis zu zwei Anforderungen sein. Mehr gehende Anforderungen werden abgewiesen.

Rückrufanforderungen werden gelöscht wenn

- das Gespräch zustande gekommen ist, wenn nicht, bleibt der Rückruf weiter aktiv (bei einem internen Rückruf),
- der Rückruf aufgebaut wurde ohne dass ein Gespräch zustande gekommen ist (bei einem externen Rückruf),
- der einleitende Teilnehmer den Rückruf löscht,
- das System täglich um 23:57 Uhr alle Rückrufe löscht.

Rückrufanforderungen können auf interne Teilnehmer und Gruppen gesetzt werden. Bei einem Gruppenanschluss wird eine Rückrufaufforderung beim ersten Teilnehmer hinterlegt. Bei einem Rückruf auf einen Gruppenanschluss klingeln alle Telefone, die frei sind.

Automatischer Rückruf bei frei auf der Amtsschnittstelle

Ein interner Teilnehmer, der einen externen freien Teilnehmer nicht erreicht, kann einen Rückrufwunsch im Amt aktivieren. Daraufhin wird der Anschluss des angerufenen Teilnehmers überwacht. Sobald der angerufene Teilnehmer selbst einen Verbindungsaufbau einleitet und diese Verbindung wieder beendet, wird vom Amt versucht eine Verbindung zwischen den beiden Teilnehmern herzustellen. Dieses Leistungsmerkmal muss vom Amt unterstützt werden.

Rückruf bei Besetzt

Auf eine externe, besetzte Nebenstelle kann ein manueller Rückruf gesetzt werden. Nach Freiwerden des Teilnehmers wird vom Amt versucht, eine Verbindung zwischen den beiden Teilnehmern herzustellen. Das Leistungsmerkmal muss vom Amt und der Gegenstelle unterstützt und freigeschalten sein.

14.5.2 Anklopfen

Anklopfen signalisiert einem Teilnehmer im Gespräch einen weiteren ankommenden Anruf.

Die Signalisierung wird optisch durch eine Nachricht im Display angezeigt. Die Signalisierung kann auch akustisch durch einen kurzen Anklopfton erfolgen. Der Anklopfton ist alle 5 Sekunden hörbar.

Der gerufene Teilnehmer hat die Möglichkeit, dieses zweite Gespräch anzunehmen oder zu ignorieren. Um den zweiten Anruf anzunehmen, kann der Teilnehmer die erste Verbindung beenden und das zweite Gespräch annehmen oder die im Display angebotene Funktion **Anklopfen annehmen** auswählen. In diesem Fall wird das erste Gespräch gehalten.

Bei einem Teilnehmer kann nicht angeklopft werden, wenn bereits bei diesem Teilnehmer jemand anklopft (max. 4 Teilnehmer können anklopfen) oder dieser Anklopfschutz aktiviert hat. Es erfolgt Besetztsignalisierung zum Anrufer, wenn keine Rufweiterschaltung im Besetztfall konfiguriert ist.

Anklopfen freigeben

Anklopfen durch den Vermittlungsplatz

Das Flag **Anklopfschutz** muss für den Teilnehmer gesetzt sein, damit dieser Teilnehmer zwischen Anklopfen freigeben und Anklopfen unterdrücken über Menü oder Kennzahl wählen kann. Hat ein Teilnehmer Anklopfen freigegeben, wird bei Ihm auch dann angeklopft, wenn er Rufweiterschaltung im Besetztfall konfiguriert hat.

Die Standardeinstellung ist immer Anklopfen nach Zeit. Der Vermittlungsplatz kann aber auch sofort Anklopfen.

Abhängigkeiten

Thema	Abhängigkeit
Stilles Anklopfen	Der Anklopfton kann durch den Teilnehmer mit einer Kennzahl aktiviert/deaktiviert werden. Die optische Signalisierung des Anklopfens im Display des Telefons bleibt erhalten. Standard ist Anklopfton ein.
Aufschalten	Ist Anklopfschutz aktiviert, wird verhindert, dass ein Aufschalten auf eine Verbindung dieses Teilnehmers erfolgen kann.
Gruppenruf	Wenn ein oder mehrere Teilnehmer eines Gruppenrufes frei sind, wird ihnen der Anruf angeboten. Sind alle Teilnehmer besetzt, bekommen alle eine Anklopfsignalisierung, außer alle Teilnehmer haben Anklopfschutz aktiviert.
Direktansprechen	Direktansprechen zu besetzten Teilnehmern ist nicht möglich.

14.5.2.1 Wie Sie Anklopfen aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer**.
4) Klicken Sie z.B. auf **IP Clients**.
5) Klicken Sie z.B. auf **System Clients**.
6) Wählen Sie den betreffenden Teilnehmer aus.
7) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
8) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie Anklopfen aktivieren möchten, deaktivieren Sie das Kontrollkästchen Anklopfschutz ein.
   - Wenn Sie Anklopfen deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Anklopfschutz ein**.
9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.2.2 Wie Sie sofortiges Anklopfen durch Vermittlungsplatz aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System**.
4) Klicken Sie auf **Abwurf/Attendant/Hotline**.
5) Wählen Sie eine der folgenden Möglichkeiten unter **Sonstige Kriterien**:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Sofortiges Anklopfen durch VPL**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Sofortiges Anklopfen durch VPL**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Anmerkung:

Bei CMI DECT - TDM-Tischtelefonen ist bei Anrufen eines besetzten Teilnehmers, bei dem Anklopfen erlaubt ist, der Besetztton für 5 Sekunden aktiv, danach erfolgt das Anklopfen und der Freiton ist zu hören.

Für IP DECT - SIP-Tischtelefone erfolgt bei Anrufen eines besetzten Teilnehmers, bei dem Anklopfen erlaubt ist, das

Anklopfen sofort, sodass der Freiton von Anfang an zu hören ist.

14.5.3 Aufschalten

Mit Aufschalten kann ein berechtigter Teilnehmer sich in ein Gespräch eines internen Teilnehmers einschalten.

Das Aufschalten erfolgt mittels Kennziffer oder Taste und wird den beteiligten Teilnehmern durch einen Aufmerksamkeitston und durch die Anzeige im Display mitgeteilt.

Dieses Leistungsmerkmal kann während des Besetztsignals oder während des Anklopfens aktiviert werden.

Beim Aufschalten auf eine Verbindung gilt Folgendes:

- Wenn der gerufene Teilnehmer auflegt, bekommt er einen Anruf vom vermittelnden Teilnehmer.
- Wenn der aufschaltende Teilnehmer (der das Gespräch vermitteln möchte und sich aufschaltet) auflegt, wird das Gespräch zum Zielteilnehmer vermittelte.
- Wenn der Teilnehmer, der mit dem gerufenen Teilnehmer verbunden wurde, auflegt, bleiben der aufgeschaltete und der gerufene Teilnehmer verbunden.

Aufschalten kann jeder interne Teilnehmer und der Abwurfplatz (Vermittlungsplatz). Um dieses Leistungsmerkmal nutzen zu können, muss der interne Teilnehmer und auch der Abwurfplatz dafür berechtigt werden.

Es ist nicht möglich, das Aufschalten auf ein bestimmtes Telefon zu verhindern.

Abhängigkeiten

Thema	Abhängigkeit
Sprachkanal-Signalisierungsschutz	Ist der angerufene Teilnehmer oder dessen interner Gesprächspartner als Datenstation eingetragen (Sprachkanal-Signalisierungsschutz) oder ist der angerufene Teilnehmer im Wahlzustand, kann nicht aufgeschaltet werden.
Anrufschutz	Wenn der gerufene Teilnehmer den Anrufschutz aktiviert hat, kann nur ein Gespräch aufgeschaltet werden, wenn der Teilnehmer ein Gespräch führt.
Sammelanschluss	Sind beim Rufen einer Gruppe oder eines Sammelanschlusses alle Teilnehmer besetzt, ist kein Aufschalten möglich.
S_0-Teilnehmer	Das Aufschalten auf einen S_0-Teilnehmer ist nicht möglich.

14.5.3.1 Wie Sie einen internen Teilnehmer für das Aufschalten berechtigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer**.
4) Klicken Sie im Menübaum auf den Teilnehmer (Index - Rufnummer - Name).
5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
6) Aktivieren Sie das Kontrollkästchen **Aufschalteberechtigung ein**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.3.2 Wie Sie den Abwurfplatz für das Aufschalten berechtigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **Abwurf/VPL/Hotline**.
4) Aktivieren Sie im Bereich **Sonstige Kriterien** das Kontrollkästchen **Überschreiben durch VPL**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.4 Abwesenheitstexte

Der Abwesenheitstext eines Teilnehmers erscheint im Display des Anrufers.

In Abwesenheitstexten (auch als Antwort-Text bezeichnet) können variable Parameter vergeben werden. Diese Parameter (z.B. Uhrzeit) werden während der Aktivierung eingegeben. Für die Eingabe der ergänzenden Zeichen steht der Ziffernblock des Endgerätes zur Verfügung. Der Abwesenheitstext kann über eine Kennzahl oder über eine zuvor eingerichtete Funktionstaste an einem Telefon aktiviert/deaktiviert werden.

Anrufumleitung

Bei Anrufumleitung wird der Abwesenheitstext des angerufenen Teilnehmers angezeigt und der Anrufumleitung gefolgt.

14.5.4.1 Wie Sie einen Abwesenheitstext ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System**.
4) Klicken Sie auf **Texts**.
5) Klicken Sie in der Spalte **Antwort-Texte** in das entsprechende Feld und geben Sie den Abwesenheitstext ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.5 Mitteilungstexte

Mitteilungstexte sind systeminterne Texte, die ein Teilnehmer auswählen und an interne Teilnehmer senden kann.

Ein Mitteilungstext (Info-Text) kann an einen oder mehrere Empfänger gesendet werden.

Soll der Text an alle Mitglieder einer internen Gruppe oder eines internen Sammelanschlusses verschickt werden, muss man die Rufnummer der Gruppe oder des Sammelanschlusses anstelle eines einzelnen Teilnehmers als Empfänger angeben.

Anmerkung: Der Empfang von Message Waiting Indication (MWI)-Meldungen ist auf 100 Telefone beschränkt; bei weiteren Telefonen schlägt der Empfang fehl.

Das Versenden erfolgt mittels Taste oder Menü Info senden.

Das Senden kann im Ruhe-, Ruf-, Gesprächs- oder Besetztzustand erfolgen. Im Rufzustand entfällt die Angabe der Rufnummer des Empfängers.

14.5.5.1 Wie Sie einen Mitteilungstext ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System**.
4) Klicken Sie auf **Texts**.
5) Klicken Sie in der Spalte **Info-Texte** in das entsprechende Feld und geben Sie den Text ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.6 Assoziierte Dienste

Ein berechtigter Teilnehmer kann für einen beliebigen anderen Teilnehmer Leistungsmerkmale stellvertretend steuern, z.B. Anrufumleitung, Codeschloss oder Sammelanschluss ein / aus. Die Auswirkung ist die gleiche, wie bei der Aktivierung oder Deaktivierung jenes Leistungsmerkmals durch den anderen Teilnehmer für sich selbst.

Folgende Leistungsmerkmale sind stellvertretend steuerbar:

- Anrufumleitung ein / aus
- Codeschloss ein / aus
- Rufzuschaltung ein / aus
- Antworttext ein / aus
- Sammelanschluss und Gruppenruf ein / aus
- Nachtschaltung ein / aus
- Termin ein / aus
- Info senden / gesendete Infos löschen
- Codeschloss Kennwort ändern
- UCD-Agent einloggen / ausloggen
- UCD-Agent verfügbar / nicht verfügbar
- UCD-Agent Nachbearbeitung ein / aus
- UCD-Agent Nachtschaltung ein / aus
- Umleitung MULAP ein / aus
- Aktivierte Leistungsmerkmale zurücksetzen

Die Nutzung erfolgt mittels einer Prozedur. Der Teilnehmer muss Folgendes angeben:

- Die Kennzahl für Assoziierte Dienste
- Die Rufnummer des Teilnehmers, für den eine Aktion ausgeführt werden soll
- Die Kennzahl des zu steuernden Leistungsmerkmales

Bevor ein Teilnehmer Assoziierte Dienste benutzen kann, muss er das Codeschloss des anderen Teilnehmers deaktivieren, falls aktiviert.

14.5.6.1 Wie Sie Assoziierte Dienste aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer**.
4) Klicken Sie im Menübaum auf den Teilnehmer (Index - Rufnummer - Name).
5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Assoziierte Wahl/Dienste**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Assoziierte Wahl/Dienste**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.7 DISA

DISA (Direct Inward System Access) ermöglicht berechtigten Teilnehmern die Nutzung von Leistungsmerkmalen des Kommunikationssystems von außerhalb,

z.B. am Mobiltelefon über myPortal for Mobile (bei Mobile Callback) und Mobility.

Ein Teilnehmer kann über DISA auch gehende Verbindungen aufbauen, sowohl intern als auch extern. Der Teilnehmer muss bei jeder Benutzung von DISA das Passwort für das Codeschloss eingeben. Anschließend stehen bestimmte Leistungsmerkmale zur Verfügung wie bei interner Nutzung.

DISA unterstützt folgende Leistungsmerkmale:

Leistungsmerkmal	durch den Teilnehmer selbst	über Assoziierte Dienste
Anrufumleitung ein / aus	x	x
Anrufschutz ein / aus	x	x
Sammelanschluss ein / aus	x	x
Abwesenheitstext ein / aus	x	x
Rufzuschaltung ein / aus	x	x
Codeschloss ein / aus	x	x
Dienste zuruecksetzen	x	x
Kurzwahl zentral KWZ	x	–
Infotext senden	x	–
Nachtschaltung ein / aus	x	–

Der Administrator legt fest, unter welcher Rufnummer die Teilnehmer DISA nutzen können. Die Rufnummer kann für externe und interne Nutzung unterschiedlich sein. Intern bedeutet an einem anderen mittels IP-vernetzten Knoten.

Das vom Teilnehmer einzugebende Passwort besteht aus der internen Rufnummer und der PIN für das Codeschloss. Nach der Eingabe des Passworts muss der Teilnehmer entweder die Taste # drücken oder warten, bis das Kommunikationssystem seine Eingabe erkannt hat, je nach dem vom Administrator festgelegten Sicherheits-Modus für DISA.

Für eine weitere Aktion über DISA muss sich der Teilnehmer erneut anmelden.

Anmerkung: Wenn in OpenScape Business X eine DISA-Rufnummer angerufen wird, hören Sie einen Dauerton. Wenn in OpenScape Business S eine DISA-Rufnummer angerufen wird, hören Sie Wartemusik.

14.5.7.1 Wie Sie die DISA-Berechtigung für einen Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer**.
4) Klicken Sie im Menübaum auf den Teilnehmer (Index - Rufnummer - Name).
5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **DISA Berechtigung**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **DISA Berechtigung**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.7.2 Wie Sie eine DISA-Nummer konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **DISA**.
4) Geben Sie im Feld **Durchwahl** die Rufnummer ein, über welche die Teilnehmer DISA von extern nutzen können.
5) Geben Sie im Feld **Rufnummer** die Rufnummer ein, über welche die Teilnehmer DISA von intern nutzen können.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.7.3 Wie Sie den DISA-Sicherheitsmodus konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **DISA**.
4) Wählen Sie in der Aufklappliste **Sicherheits-Modus** den Sicherheitsmodus **Nach Zeit** oder **Nach Eingabe #**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.8 Flex Call/Mobile PIN

Mit Flex Call (Mobile PIN) wird ein Systemtelefon für das nächste gehende Gespräch vorübergehend von einem anderen Teilnehmer so genutzt, als wäre es sein eigenes.

Flex Call beinhaltet die Rufnummer, den Namen, die Amtsberechtigung und die Gebührenerfassung dieses Teilnehmers.

Ist Flex Call aktiviert, kann das benutzte Telefon nicht unter seiner eigentlichen Rufnummer erreicht werden. Nach Gesprächsende wird dieser Zustand wieder aufgehoben.

Für die Aktivierung von Flex Call muss ein individuelles Codeschloss für den mobilen Teilnehmer vergeben sein.

Zur Aktivierung ist einer der folgenden Schritte am Systemtelefon durchzuführen:

- OpenStage: Service-Menü > PIN und Berechtigung > Flex Call + mobile Rufnummer + Codeschloss des mobilen Teilnehmers
- Kennzahl für FlexCall + mobile Rufnummer + Codeschloss des mobilen Teilnehmers

14.5.9 Relocate/Rufnummerntausch

Über Relocate/Rufnummerntausch kann ein OpenStage-TDM-Teilnehmer die Zuordnung zwischen physikalischem Anschluss-Port und logischen Teilnehmerdaten (Benutzerprofil) per Prozedur ändern.

Relocate kann angewendet werden, wenn zwei Teilnehmer sich zu einem Tausch ihrer Arbeitsplätze entschließen und beide dieselben Telefontypen benutzen. Relocate ermöglich so die Realisierung von DeskSharing für TDM-Teilnehmer. Die TDM-Teilnehmer können ohne Unterstützung eines Administrators den Rufnummerntausch selbst durchführen.

Es dürfen nur Benutzerprofile des gleichen Telefontyps, d.h. mit identischem Tastenlayout getauscht werden. Beim Tausch von Benutzerprofilen unterschiedlicher Telefontypen werden individuell programmierte Tastenfunktionen des Grundgerätes durch die Default-Werte ersetzt. Bei der Durchführung von Relocate kommt es zu einem Ausfall/Neustart der beteiligten TDM-Telefone. Aktivierte Leistungsmerkmale werden dementsprechend behandelt, d.h. aktuelle Rückrufe und versandte Infos werden gelöscht, alle anderen Leistungsmerkmale bleiben erhalten.

Voraussetzung für die Nutzung von Relocate ist die systemweite Freigabe des Leistungsmerkmals. Für den Rufnummerntausch wählen Sie im Service-Menü des zu tauschenden Telefons Rufnr. tauschen und geben die interne Rufnummer des Zielteilnehmers und die Codeschloss-PIN ein (Codeschloss-PIN ist nicht erforderlich, wenn die PIN dem Default 00000 entspricht). Nach Eingabe der Zielrufnummer ist Relocate bis zum Abschluss der Prozedur für alle anderen Teilnehmer gesperrt. Bei Ausführung des Tausches werden die beiden beteiligten Endgeräte zurückgesetzt. Der erfolgreiche Tausch wird an beiden TDM-Telefonen durch die Anzeige der neuen Rufnummer signalisiert (Display-Anzeige: Neue Rufnr.: XXXXX).

Relocate kann nicht an Systemtelefonen mit Programmierberechtigung (für Assistant T) durchgeführt werden. Also in der Regeln nicht an den ersten zwei aktiven Systemtelefonen.

14.5.9.1 Wie Sie Relocate/Rufnummertausch systemweit freigeben

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Grundeinstellungen** > **System**.
3) Klicken Sie im Menübaum auf **System Flags**.
4) Aktivieren Sie das Kontrollkästchen **Endgerätetausch erlaubt**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.5.10 Rücksetzen aktivierter Leistungsmerkmale

Sie können an Ihrem Endgerät bestimmte Leistungsmerkmale gemeinsam mittels Kennzahl rücksetzen.

Dies ist möglich für folgende Leistungsmerkmale:

- Anrufumleitung
- Empfangene Infos löschen
- Antworttext ein / aus
- Rufzuschaltung ein / aus
- Sammelanschluss ein / aus
- Rufnummernunterdrückung ein / aus
- Stilles Anklopfen ein / aus
- Anrufschutz ein / aus
- Ruhe ein / aus
- Termin
- Alle Rückrufe löschen

14.5.11 Prozeduren

Das Kommunikationssystem ermöglicht dem Teilnehmer das Speichern von Kennzahlen, Rufnummern sowie weiteren Wahlinformationen als Prozeduren auf einer Taste. Drückt der Teilnehmer die Prozedurtaste in Nachwahl oder während eines Gespräches, sendet das Kommunikationssystem die entsprechenden MFV-Zeichen (MFV = Mehrfrequenzwahlverfahren).

Anwendungsbeispiele:

- Kennzahl für Rückruf
- Kennzahl für Anklopfen
- Kennzahl für Aufschalten
- Ziffernfolge für Sprachbox oder Anrufbeantworter
- Amts-Flashkennzahl + Zielrufnummer

- Kennzahl zur Steuerung eines Dienstes + Zielrufnummer, z.B. Kennzahl für Info (Message Waiting) senden / abfragen + Rufnummer + Textnummer
- PKZ (Projektkennzahl) + Bündelkennzahl + Zielrufnummer

Prozeduren, welche die Eingabe einer PIN erfordern, können nicht gespeichert werden.

Nur die ersten Tastenebene unterstützt Prozedurtasten.

Ein Teilnehmer kann in Prozeduren situationsabhängig folgende Leistungsmerkmale nutzen:

Leistungsmerkmal	Wahlbereit	Besetzt	Im Gespräch	Gehender Ruf	Kommender Ruf
Anrufübernahme, gezielt	x	–	x	–	–
Anrufumleitung ein (nicht bei Gemeinschaftsanlagen; nicht für einzelne MSN eines S_0-Amtsanschlusses)	x	–	x	x	–
Anrufumleitung im Amt ein / aus; Umschaltfunktion; (nicht bei Gemeinschaftsanlagen);	x	–	x	x	–
Anrufverteilung, Anmelden / Abmelden; Umschaltfunktion	x	–	x	x	–
Anrufverteilung, Nachtziel ein / aus; Umschaltfunktion	x	–	x	x	–
Anrufumleitung pro Teamschaltung	x	x	x	x	x
Antworttext ein / aus; Umschaltfunktion	x	–	x	x	–
Assoziierte Wahl	x	x	x	x	x
Assoziierte Dienste	x	–	x	x	–
Direktansprechen	x	–	x	–	–
Freischalten von Leitungen (Emergency Trunk Access)	x	–	x	x	–
Info senden (Message Waiting)	x	–	x	x	–
KWI ausspeichen	x	–	x	x	–
KWZ ausspeichen	x	–	x	x	–
MFV-Übertragung	–	–	x	–	–
MFV-Übertragung im Gesprächszustand mittels Prozedurtaste	x	x	x	x	x
Nachtschaltung ein / aus; Umschaltfunktion	x	–	x	x	–
Parken / Wiederaufnehmen; Umschaltfunktion	–	x	x	x	–
Projektkennzahl PKZ	x	–	x	–	–
Projektkennzahl PKZ in Vorwahl	x	–	x	–	–
Rückrufaufträge anzeigen / löschen; Umschaltfunktion	x	–	–	–	–
Rufzuschaltung ein / aus; Umschaltfunktion	x	–	x	x	–
Sprachauswahl	x	x	x	x	x
Telephone Data Service TDS	x	–	x	x	–
Türöffner via Adapterbox	x	x	x	x	x
Termin ein / aus; Umschaltfunktion	x	x	x	x	x

Leistungsmerkmal	Wahlbereit	Besetzt	Im Gespräch	Gehender Ruf	Kommender Ruf
Wiederaufnahme eines externen Gesprächs aus allgemeinem Halten	x	x	x	x	x
Zentrales Codeschloss	x	–	x	–	–

Systemspezifische Informationen

Eine Prozedurtaste kann maximal 32 Zeichen speichern.

14.5.12 Weckeinrichtung und Termine

Jeder Teilnehmer hat die Möglichkeit, einen Termin zu programmieren. Zum Fälligkeitszeitpunkt erfolgt ein Terminruf. Der Termin kann einmalig (innerhalb der nächsten 24 Stunden) oder wiederholt (d. h. täglich) ausgeführt werden.

Die Eingabe der Terminzeit erfolgt durch vier Ziffern, von denen die ersten zwei die Stunde und die letzten zwei die Minute festlegen. Für die USA wird ein 12-Stunden-Modus unterstützt: Der Benutzer gibt die vier Ziffern ein und wählt dann "am" (Taste 2) oder "pm" (Taste 7). Bei fehlender Angabe wird "am" angenommen.

Analoge Telefone, optiPoint 500 entry oder CMI-Telefone können nur einmalige Termine programmieren.

Ein Terminruf dauert standardmäßig 20 Sekunden und wird bis zu fünfmal mit einer jeweils einminütigen Pause wiederholt. Das Löschen des Auftrags erfolgt automatisch durch Abnehmen des Handapparates oder Betätigen der Lautsprechertaste während des Rufes oder nach der fünften Wiederholung (Anzahl konfigurierbar). Ein programmierter Terminruf kann alternativ auch mit einer Prozedur gelöscht werden. Bei Display-Endgeräten besteht zudem eine Abfragemöglichkeit.

Kann ein fälliger Terminruf nicht signalisiert werden (z.B. Teilnehmer besetzt), so wird er bis zum nächsten Zyklus zurückgestellt.

Tipp: Zeitgesteuerte Erinnerungen können für bis zu 50 Benutzer pro System geplant werden.

14.6 Übersicht über Funktionen und Codes

Servicekennzahl	Beschreibung
*0	Zurück zum Wartenden
*1	Anrufumleitung
*2	Makeln
*3	Konferenz
*44	Nachtschaltung ein
*51	Flash zum Amt

Servicekennzahl	Beschreibung
*52	Mute ein
*53	DTMF-Wahl
*55	Anklopfen annehmen
*56	Parken einleiten
*57	Anrufübernahme in AUN-Gruppen
*58	Rückruf einleiten
*59	Anrufübernahme ausserhalb AUN-Gruppen
*60	Projektkennzahl
*61	Türöffner
*62	Aufschalten
*64	Anrufumleitung im Amt (ISDN) ein
*65	Kosten abfragen
*66	Codeschloss ein
*67	Assoziierte Wahl
*68	Info senden
*69	Abwesenheitstext ein
*7	KWZ/KWI ausspeichern
*80	Direktansprechen
*90	Einstieg zur Aktivierung der Aktoren (einschalten)
*91	Tastenprogrammierung
*92	Kurzrufnummer ändern
*93	PIN ändern
*940	Endgerätetest
*95	Systemverwaltung
*97	Anrufschutz DND ein
	Babyphone ein
*81	Rufzuschaltung ein
#1	Anrufumleitung aus
#44	Nachtschaltung aus
#52	Mute aus
#56	Zurück zum Wartenden
#58	Rückrufe abfragen/löschen
#64	Anrufumleitung im Amt (ISDN) aus
#66	Codeschloss aus

Servicekennzahl	Beschreibung
#68	Info (gesendete) lesen/löschen
#69	Abwesenheitstext aus
#97	Anrufschutz DND aus
*96	Direktantworten ein
#96	Direktantworten aus
#90	Einstieg zur Deaktivierung der Aktoren (ausschalten)
#81	Rufzuschaltung aus
#0	Alle Dienste zurücksetzen
#3	Fünferkonferenz aus
#82	Anruferliste abfragen
*83	Assoziierte Dienste
*84	Fangen
*85	Gruppenruf ein
#85	Gruppenruf aus
*82	Anruferliste beschreiben
*86	Rufnummerunterdrückung ein
#86	Rufnummerunterdrückung aus
*87	Stilles Anklopfen ein
#87	Stilles Anklopfen aus
*98	Ruhe ein
#98	Ruhe aus
*991	remote DTMF-Systemverwaltung
*992	remote DTMF-Systemverwaltung freigeben
*993	remote ISDN-Systemverwaltung freigeben (überholt)
*994	remote Anlagendaten-Abfrage freigeben (z.Z. inaktiv)
*89	Türöffner via DTMF Code freigeben
#89	Türöffner via DTMF Code sperren
*63	Wiederaufnahme eines externen Gesprächs nach Haltentaste
*41	Rufnummern zuweisen bei MUSAP
*401	UCD-Agenten einloggen
#401	UCD-Agenten ausloggen
*402	UCD-Agent verfügbar

Servicekennzahl	Beschreibung
#402	UCD-Agent nicht verfügbar
*403	UCD-Nachbearbeitung ein
#403	UCD-Nachbearbeitung aus
*404	UCD-Nachtschaltung ein
#404	UCD-Nachtschaltung aus
*405	UCD-Rufqueue-Status abfragen
*42	Telephone Data Service (TDS)
*43	Ltg freischalten
*45	PSE: Suchen
#45	PSE: Melden
*46	Weckeinrichtung: Termin ein
#46	Weckeinrichtung: Termin aus
*9419	Endgerätetausch aktivieren
#9419	Endgerätetausch deaktivieren
*942	Anmeldebereitschaft (Mobilteil)
*943	Zentrales Codeschloss
*944	Call Supervision
	Drop Last Conference Party within CO (USA only)
*490	Freigeben zum Anklopfen aktivieren
#490	Freigeben zum Anklopfen deaktivieren
*48	Sprachauswahl
*508	Flex Call
*502	Rufumschaltung für MULAP ein
#502	Rufumschaltung für MULAP aus
*501	AUL für MULAP ein
#501	AUL für MULAP aus
*509	Trace einfrieren
*47	DISA intern
*503	Keypad-Wahl
*54	Internes Telefonbuch
*491	analoges Hotelendgerät
#943	Zentrales Codeschloss / Code rücksetzen
*9411	Rufweiterschaltung Gerät ausser Betrieb ein

Servicekennzahl	Beschreibung
#9411	Rufweiterschaltung Gerät ausser Betrieb aus
*493	Sprachaufzeichnung ein
#493	Sprachaufzeichnung aus
*495	Umleitung nach Zeit ein
#495	Umleitung nach Zeit aus
*945	Diskretes Ansprechen
*494	Data I/O
*996	Smart Services via HTTPS für remote Verwaltung freigeben
#996	Smart Services via HTTPS für remote Verwaltung deaktivieren
*997	Kontrolliertes Herunterfahren

15 Arbeiten im Team (Gruppen)

Für das Arbeiten im Team stellt das Kommunikationssystem vielfältige Leistungsmerkmale zur Verfügung. Neben Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen gehören dazu auch Gruppen mit Team- und Chef/Sekretär-Funktionen und Sprachbox- und Faxbox-Gruppen. Durch das Leistungsmerkmal "Anrufverteilung (UCD Uniform Call Distribution)" wird eine gleichmäßige Verteilung von eingehenden Anrufen auf eine Gruppe von Teilnehmern (UCD-Gruppe) ermöglicht.

Tipp: Bei der Konfiguration von Gruppen ist zu beachten, dass die ersten drei reserviert sind:

Die erste Gruppe wird standardmäßig als Sammelanschluss für die externe Voicemail verwendet.

Die zweite Gruppe wird standardmäßig als Sammelanschluss für OpenScape Business Smart VoiceMail verwendet.

Die dritte Gruppe wird standardmäßig als Sammelanschluss für den Company AutoAttendant der OpenScape Business Smart VoiceMail verwendet.

15.1 Anrufübernahmegruppe, Gruppenruf und Sammelanschluss

Das Kommunikationssystem bietet verschiedene Möglichkeiten, um Teilnehmer zu Gruppen zusammenzufassen, damit mehrere Teilnehmer und Telefone zum Beispiel unter einer Rufnummer erreichbar sind oder ein Anruf für einen Teilnehmer auch bei anderen Teilnehmern signalisiert wird.

Bei einer Anrufübernahmegruppe wird der Anruf für ein Mitglied immer auch bei allen anderen Gruppenmitgliedern signalisiert.

Bei einem Gruppenruf sind alle Mitglieder unter einer Rufnummer (Gruppenrufnummer) erreichbar. Der zuerst abhebende Teilnehmer wird mit dem Anrufenden verbunden.

Bei einem Sammelanschluss wird ein ankommender Anruf bei einem der Mitglieder signalisiert. Nimmt dieser den Anruf nicht entgegen, wird das Gespräch dem nächsten Mitglied zugewiesen. Alle Mitglieder des Sammelanschlusses sind unter einer Rufnummer erreichbar.

15.1.1 Anrufübernahmegruppe

Ein Anruf für ein Mitglied einer Anrufübernahmegruppe (AUN-Gruppe) wird auch bei allen anderen Gruppenmitgliedern signalisiert. Der Anruf kann mittels einer dafür programmierten Funktionstaste oder über den zugehörigen Menüeintrag des Telefons oder durch das Wählen der Kennzahl von allen anderen Gruppenmitgliedern angenommen werden.

Beim ursprünglich gerufenen Mitglied der Anrufübernahmegruppe wird der Anruf akustisch und optisch (Display) signalisiert. Falls programmiert, wird der Anruf auch über die LED der Funktionstaste signalisiert.

Die anderen Gruppenmitglieder erhalten zuerst nur eine optische Signalisierung des Anrufs. Im Display werden Rufnummer oder Name des ursprünglich gerufenen Teilnehmers und Rufnummer oder Name des Anrufers angezeigt. Die Anzeige der Rufnummer oder des Namens des Anrufers kann durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** deaktiviert werden. Falls programmiert, wird der Anruf auch über die LED der Funktionstaste signalisiert.

Wird der Anruf nicht innerhalb von vier Rufzyklen (4 x 5 Sekunden) angenommen, erhalten die anderen Gruppenmitglieder einen Aufmerksamkeitston (akustische Signalisierung). Die Zeit vom Start der Anrufsignalisierung bis zum Aufmerksamkeitston ist nicht variabel. Der Aufmerksamkeitston kann durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** für alle Gruppenmitglieder deaktiviert werden.

Bei mehreren Anrufen für eine Anrufübernahmegruppe erfolgt die Signalisierung in der Reihenfolge des Anrufeingangs.

Sollen Wiederanrufe für Mitglieder einer AUN-Gruppe auch durch die anderen Mitglieder übernommen werden können, muss dies durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** aktiviert werden.

Ein Teilnehmer kann nur Mitglied in einer Anrufübernahmegruppe sein.

Eventuell anfallende Gebühren für einen übernommenen Anruf werden dem Teilnehmer zugewiesen, der den Anruf übernommen hat.

Anmerkung: Anführungszeichen (") sind für den Namen einer AUN-Gruppe nicht zulässig.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Anrufübernahmegruppe ist möglich.

Tipp: Zusätzlich kann für SIP-Telefone eine Funktionstaste für die Anrufübernahmegruppe programmiert werden und die spezifische Meldungen einer Anrufübernahmegruppe können im Display der SIP-Telefone angezeigt werden. Um dies zu nutzen, muss das Leistungsmerkmal "Anrufübernahmegruppe" am SIP-Telefon aktiviert werden (siehe Bedienungsanleitung des SIP-Telefons).

Anrufübernahme außerhalb einer AUN-Gruppe

Eine Variante des Leistungsmerkmals ist die "Anrufübernahme außerhalb einer AUN-Gruppe". Ermöglicht wird damit die Übernahme von Anrufen für interne Teilnehmer, die nicht zur gleichen AUN-Gruppe gehören. Die Übernahme des Anrufs ist über eine dafür programmierte Funktionstaste oder über den Menüeintrag oder durch das Wählen der Kennzahl für Anrufübernahme gezielt und die anschließende Eingabe der Rufnummer des gerufenen Teilnehmers möglich.

Abhängigkeiten

Themenbereich	Abhängigkeit
Rückruf	Wiederanrufe und Rückrufe werden bei den anderen Gruppenmitgliedern nur signalisiert, wenn das System-Flag **Anrufübernahme nach Wiederanruf** aktiviert ist.
Anrufschutz	Teilnehmer mit aktiviertem Anrufschutz erhalten keine Anrufübernahme-Signalisierung.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Anrufübernahmegruppen ist nicht möglich.
MULAP	Die Einbindung von MULAP-Rufnummern in Anrufübernahmegruppen ist nicht möglich.

Zugehörige Tasks

Wie Sie eine Anrufübernahmegruppe konfigurieren auf Seite 699
Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen auf Seite 700
Wie Sie die Anzeige der Rufnummer und des Namens des Anrufers aktivieren oder deaktivieren auf Seite 707
Wie Sie den Aufmerksamkeitston aktivieren oder deaktivieren auf Seite 708
Wie Sie die Anrufübernahme von Wiederanrufen aktivieren oder deaktivieren auf Seite 708

15.1.2 Gruppenruf

Sollen mehrere Teilnehmer unter einer Rufnummer (Gruppenrufnummer) erreichbar sein, kann ein Gruppenruf definiert werden. Ankommende externe und interne Anrufe werden gleichzeitig bei allen Gruppenmitglieder-Telefonen signalisiert. Der zuerst abhebende Teilnehmer wird mit dem Anrufenden verbunden.

Jedes Mitglied eines Gruppenrufs ist auch unter seiner Teilnehmerrufnummer erreichbar.

Der Gruppe muss eine der folgenden Eigenschaften zugewiesen werden:

- Gruppe

  Ankommende Anrufe werden gleichzeitig bei allen verfügbaren Gruppenmitgliedern signalisiert. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Sind alle Gruppenmitglieder besetzt, wird ein Anruf durch einen Anklopfton signalisiert. Legt ein Teilnehmer auf, wird der Anruf weiterhin bei allen Gruppenmitgliedern signalisiert (Anklopfton bei besetzten Gruppenmitgliedern).

  Sind alle Gruppenmitglieder besetzt und alle haben das Leistungsmerkmal „Anrufschutz" aktiviert, erhält ein Anrufer den Besetztton. Ist ein Anrufumleitungsziel für diese Gruppe definiert, erhält der Anrufer keinen Besetztton, sondern wird direkt zum nächsten Anrufumleitungsziel weitergeschaltet.

- RNA

  Ankommende Anrufe werden gleichzeitig bei allen Gruppenmitgliedern signalisiert. Ist ein Mitglied der Gruppe besetzt, wird der gesamte Gruppenruf als besetzt gekennzeichnet. Weitere Anrufer erhalten den Besetztton.

  Anmerkung: Der Anwesenheitsstatus eines externen Ziels, das zur Gruppe gehört, kann nicht erkannt werden.

- Anklopfen

  Ankommende Anrufe werden gleichzeitig bei allen verfügbaren Gruppenmitgliedern signalisiert. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Bei besetzten Gruppenmitgliedern wird ein anstehender Anruf sofort durch einen Anklopfton signalisiert.

  Voraussetzung dafür ist, dass bei allen Gruppenmitgliedern der Anrufschutz deaktiviert ist.

Gruppenrufe werden von der Anrufumleitung (Nicht angenommen) wie Teilnehmer behandelt. Das heißt, wenn ein Anruf von keinem Mitglied eines Gruppenrufs angenommen werden kann, wird dieser zu einem Anrufumleitungsziel entsprechend der Rufzielliste weitergeschaltet. Dabei kann festgelegt werden, ob eine Anrufumleitung im Freifall oder im Freifall und Besetztfall erfolgen soll.

Wenn ein Anruf von keinem Mitglied eines Gruppenrufs angenommen wurde, wird dieser als entgangener Anruf im Journal der UC Clients aller Mitglieder angezeigt. Ein angenommener Anruf wird nur im Journal des Mitglieds angezeigt, der den Anruf angenommen hat.

Ein einzelner Teilnehmer kann gleichzeitig mehreren Gruppen angehören. Das Folgende gilt für Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung / Team-Gruppe und Chef/Sekretariat / Top-Gruppe: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht überschreiten.

Im Display eines internen Teilnehmers wird der zugewiesene Gruppenname angezeigt. Nach Annahme eines Anrufs wird der Name des Teilnehmers angezeigt, der den Anruf angenommen hat.

Hat ein Mitglied über den AutoAttendant Regeln definiert, zum Beispiel für die Weiterschaltung von Anrufen, gelten diese nur für Anrufe an seine eigene Teilnehmerrufnummer. Bei Gruppenrufen werden diese Regeln ignoriert.

Bis zu 20 Teilnehmer pro Gruppenruf können eingerichtet werden.

Jedem Gruppenruf kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Sprachbox für Gruppenruf

Bei der Einrichtung eines Gruppenrufs wird automatisch auch eine Sprachbox eingerichtet. Die Rufnummer dieser Gruppenruf-Sprachbox entspricht immer der Rufnummer des Gruppenrufs. Wird ein Gruppenruf von keinem Mitglied angenommen, erfolgt eine Rufweiterschaltung zur Gruppenruf-Sprachbox. Voraussetzung dafür ist, dass die Gruppenruf-Sprachbox als Anrufumleitung - Anrufweiterschaltung (CFNA) dieses Gruppenrufs definiert wurde.

Nimmt ein Mitglied einen kommenden Anruf an seine eigene Teilnehmerrufnummer nicht an, wird dieser Anruf zu einem Anrufumleitungsziel entsprechend der Rufzielliste dieses Teilnehmers weitergeschaltet.

Beispiel für einen Gruppenruf des Typs Freifall mit der Gruppenrufnummer 404 und den Mitgliedern A (Teilnehmerrufnummer 200), B (201) und C (202). Für den Gruppenruf wurde eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Gruppenruf-Sprachbox eingerichtet. Jedes Mitglied hat eine Anrufumleitung (Nicht angenommen, CFNA) nach Zeitüberschreitung zur eigenen Sprachbox definiert.		
Ankommender Anruf für Mitglied A (200)	Alle Mitglieder sind frei.	Mitglied A nimmt den Anruf nicht an. Es erfolgt eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Sprachbox des Mitglieds A.
	Mitglied A hat eine direkte Anrufumleitung (CFU) zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Es erfolgt eine sofortige Rufweiterschaltung zur Sprachbox des Mitglieds A.
Ankommender Anruf für den Gruppenruf (404)	Alle Mitglieder sind frei.	Der Anruf wird bei allen Mitgliedern signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Gruppenruf-Sprachbox.
	Mitglied A hat eine direkte Anrufumleitung (CFU) zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Der Anruf wird bei den Mitgliedern B und C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Gruppenruf-Sprachbox.
	Mitglied A hat eine direkte Anrufumleitung (CFU) zu einem externen Ziel definiert. Mitglieder B und C sind frei.	Der Anruf wird bei den Mitgliedern B und C sowie beim externen Ziel signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Gruppenruf-Sprachbox.
	Mitglied A hat über den AutoAttendant Regeln für Anrufumleitung (Nicht ankommend, CFNA) definiert. Mitglieder B und C sind frei.	Der Anruf wird bei allen Mitgliedern signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Gruppenruf-Sprachbox.

Gruppenruf ein-/ausschalten

Ist ein Teilnehmer Mitglied eines Gruppenrufs, kann er sich mittels Kennzahlen aus dem Gruppenruf hinausschalten und wieder hineinschalten.

Ist ein Teilnehmer sowohl Mitglied mehrerer Gruppenrufe als auch Mitglied mehrerer Sammelanschlüsse, kann er sich über Kennzahlen aus allen Gruppenrufen und Sammelanschlüssen hinausschalten und wieder hineinschalten. Das Hinaus-/Hineinschalten von Teilnehmern aus einem bestimmten Gruppenruf oder Sammelanschluss ist über Kennzahlen und anschließender Auswahl aus den im Display angezeigten Gruppenrufen und Sammelanschlüssen möglich.

Möglich ist auch die Programmierung von Funktionstasten mit Umschaltfunktion für das Hinausschalten und Hineinschalten. Dabei kann eine Funktionstaste so programmiert werden, dass diese für einen bestimmten oder für alle Gruppenrufe und Sammelanschlüsse gilt. Auch eine variable Programmierung ist möglich. Nach Betätigung einer solchen Funktionstaste muss anschließend durch Auswahl aus den im Display angezeigten Gruppenrufen und Sammelanschlüssen definiert werden, für welchen Gruppenruf oder Sammelanschluss das Hinaus-/Hineinschalten gelten soll.

Rufart

Für jeden Gruppenruf kann ein Administrator mit dem Profil **Experte** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Sie haben folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

SIP-Telefone

Die Einbindung von SIP-Telefonen in einen Gruppenruf ist möglich.

Anmerkung: Bei SIP-Telefonen ist keine Programmierung von Funktionstasten möglich. Spezifische Anzeigemeldungen eines Sammelanschlusses werden nicht unterstützt.

Abhängigkeiten

Themenbereich	Abhängigkeit
Anrufumleitung	Aktiviert ein Gruppenmitglied eine Anrufumleitung für alle Anrufe, werden alle Anrufe am Zieltelefon signalisiert.
Anrufschutz	Aktiviert ein Gruppenmitglied den Anrufschutz, werden ankommende Anrufe für sein Telefon nicht durchgestellt. Das betrifft Anrufe über die Gruppenrufnummer und die eigene Teilnehmerrufnummer des Mitglieds.
Aufschalten	Sind alle Mitglieder eines Gruppenrufs besetzt, ist kein Aufschalten möglich.

Themenbereich	Abhängigkeit
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in einen Gruppenruf ist nicht möglich.

Zugehörige Konzepte

Internes Verzeichnis auf Seite 517

Zugehörige Tasks

Wie Sie einen Gruppenruf (Gruppe) hinzufügen auf Seite 700
Wie Sie einen Gruppenruf (Gruppe) ändern auf Seite 702
Wie Sie einen Gruppenruf (Gruppe) löschen auf Seite 703
Wie Sie ein Mitglied zum Gruppenruf (Gruppe) hinzufügen oder löschen auf Seite 703
Wie Sie einen Gruppenruf (Freifall oder Anklopfen) hinzufügen auf Seite 709
Wie Sie einen Gruppenruf (Freifall oder Anklopfen) anzeigen oder ändern auf Seite 710
Wie Sie einen Gruppenruf (Freifall oder Anklopfen) löschen auf Seite 710
Wie Sie ein Mitglied zum Gruppenruf (Freifall oder Anklopfen) hinzufügen oder löschen auf Seite 710
Wie Sie den Anklopfschutz für Gruppenmitglied ein- oder ausschalten auf Seite 711

15.1.3 Gruppennummer

Sammelanschlüsse erlauben die Verteilung eingehender Anrufe an verbundene Abonnenten (Mitglieder). Wenn ein Abonnent besetzt ist oder einen eingehenden Anruf nicht annimmt, wird der Anruf automatisch an das nächste freie Mitglied des Sammelanschlusses weitergeleitet. Alle Mitglieder des Sammelanschlusses sind unter derselben Telefonnummer erreichbar.

Jedes Mitglied eines Sammelanschlusses ist auch unter seiner eigenen Stationsnummer erreichbar.

Dem Sammelanschluss muss eine der folgenden Eigenschaften zugewiesen werden.

- Linear

  Ein eingehender Anruf wird immer zuerst beim ersten Mitglied eines Sammelanschlusses signalisiert. Die weitere Signalisierung erfolgt anhand der Reihenfolge, in der die Mitglieder in die Gruppentabelle eingetragen werden.
- Zyklisch

  Ein eingehender Anruf wird immer zuerst bei dem Mitglied signalisiert, das dem Abonnent, der den letzten Anruf angenommen hat, folgt. Die weitere Signalisierung erfolgt anhand der Reihenfolge, in der die Mitglieder in die Gruppentabelle eingetragen werden.

Der Anruf wird nach Ablauf der Weiterleitungszeit automatisch an das nächste freie Sammelanschlussmitglied weitergeleitet, sofern der Anruf nicht angenommen wird oder ein Mitglied besetzt ist oder DND aktiviert ist.

Sie können ein Rufweiterleitungsziel (Anrufzielliste) programmieren, wenn ein Anruf von keinem Mitglied des Sammelanschlusses angenommen werden kann.

Ein einzelner Teilnehmer kann gleichzeitig mehreren Gruppen angehören. Das Folgende gilt für Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung / Team-Gruppe und Chef/Sekretariat / Top-Gruppe: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht überschreiten.

Im Display eines internen Anrufers wird der zugewiesene Gruppenname angezeigt. Nach Annahme eines Anrufs wird der Name des Teilnehmers angezeigt, der den Anruf angenommen hat.

Hat ein Mitglied über den AutoAttendant Regeln definiert, zum Beispiel für die Weiterschaltung von Anrufen, gelten diese nur für Anrufe an seine eigene Teilnehmerrufnummer. Bei Sammelanschlussanrufen werden diese Regeln ignoriert.

Bis zu 20 Sammelanschluss pro Gruppenruf können eingerichtet werden.

Jedem Sammelanschluss kann ein Name mit bis zu 16-Zeichen zugeordnet werden.

Voicemail-Box für Sammelanschluss

Beim Einrichten eines Sammelanschlusses wird dafür automatisch eine Voicemail-Box erstellt. Die Rufnummer dieser Voicemailbox für den Sammelanschluss stimmt immer mit der des Sammelanschlusses überein. Wird ein Aufruf für einen Sammelanschluss von keinem Mitglied angenommen, wird der Anruf an die Voicemail-Box des Sammelanschlusses weitergeleitet. Dazu muss die Voicemail-Box für den Sammelanschluss als CFNA-Ziel (Call Forwarding on No Response) dieses Sammelanschlusses definiert worden sein.

Nimmt ein Mitglied einen kommenden Anruf an seine eigene Teilnehmerrufnummer nicht an, wird dieser Anruf zu einem Anrufumleitungsziel entsprechend der Rufzielliste dieses Teilnehmers weitergeschaltet.

Beispiel eines linearen Sammelanschlusses mit der Rufnummer 404 und den Mitgliedern A (Rufnummer 200), B (201) und C (202). Anrufweiterleitung - Keine Antwort nach Timeout an die Voicemail-Box des Sammelanschlusses wurde für den Sammelanschluss eingerichtet. Jedes Mitglied hat eine Anrufumleitung (Nicht angenommen, CFNA) nach Zeitüberschreitung zur eigenen Sprachbox definiert.		
Ankommender Anruf für Mitglied A (200)	Alle Mitglieder sind frei.	Mitglied A nimmt den Anruf nicht an. Es erfolgt eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Sprachbox des Mitglieds A.
	Mitglied A hat eine direkte Anrufumleitung (CFU) zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Es erfolgt eine sofortige Rufweiterschaltung zur Sprachbox des Mitglieds A.

Eingehender Aufruf für den Sammelanschluss (404)	Alle Mitglieder sind frei.	Der Anruf wird zuerst bei Mitglied A, dann bei Mitglied B und dann bei Mitglied C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufweiterleitung ohne Antwort nach Zeitüberschreitung zur Voicemail-Box des Sammelanschlusses.
	Mitglied A hat eine direkte Anrufumleitung (CFU) zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Der Anruf wird zuerst an Mitglied B und dann an Mitglied C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufweiterleitung ohne Antwort nach Zeitüberschreitung zur Voicemail-Box des Sammelanschlusses.
	Mitglied A hat eine direkte Anrufumleitung (CFU) zu einem externen Ziel definiert. Mitglieder B und C sind frei.	Der Anruf wird zuerst an Mitglied B und dann an Mitglied C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufweiterleitung ohne Antwort nach Zeitüberschreitung zur Voicemail-Box des Sammelanschlusses.
	Mitglied A hat über den AutoAttendant Regeln für Anrufumleitung (Nicht ankommend, CFNA) definiert. Mitglieder B und C sind frei.	Der Anruf wird zuerst bei Mitglied A, dann bei Mitglied B und dann bei Mitglied C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufweiterleitung ohne Antwort nach Zeitüberschreitung zur Voicemail-Box des Sammelanschlusses.

Aktivieren/Deaktivieren des Sammelanschlusses

Wenn ein Abonnent Mitglied eines Sammelanschlusses ist, kann er oder sie Codes verwenden, um den Sammelanschluss zu verlassen und wieder beizutreten.

Wenn ein Abonnent Mitglied sowohl mehrerer Sammelanschlüsse als auch mehrerer Gruppenanrufe ist, kann er oder sie Codes verwenden, um alle Sammelanschlüsse und Gruppenanrufe zu verlassen und wieder beizutreten. Abonnenten werden zu einem bestimmten Sammelanschluss oder einem Gruppenanruf hinzugefügt oder entfernt, indem sie Codes eingeben und dann eine Auswahl aus den angezeigten Sammelanschlüssen und Gruppenanrufen treffen.

Möglich ist auch die Programmierung von Funktionstasten mit Umschaltfunktion für das Hinausschalten und Hineinschalten. Hier können Sie eine Funktionstaste programmieren, die für eine bestimmte oder alle Sammelanschlüsse und Gruppenanrufe gilt. Auch eine variable Programmierung ist möglich. Nachdem Sie eine Funktionstaste dieser Art gedrückt haben, müssen Sie eine der angezeigten Sammelanschlüssen und

Gruppenanrufe auswählen, um den oder den Gruppenaufruf zu definieren, den Sie verlassen/beitreten möchten.

Rufart

Für jeden Sammelanschluss kann ein Administrator mit dem Profil **Experte** die akustische Signalisierung kommender externer Anrufe über die Klingeltyp-Einstellung definieren. Sie haben folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

SIP-Telefone

SIP-Telefone können in einen Sammelanschluss integriert werden.

Tipp: Bei SIP-Telefonen ist keine Programmierung von Funktionstasten möglich. Spezifische Anzeigemeldungen eines Sammelanschlusses werden nicht unterstützt.

Abhängigkeiten

Themenbereich	Abhängigkeit
Anrufumleitung	Aktiviert ein Sammelanschlussmitglied eine Anrufweiterleitung für alle Anrufe, werden alle Anrufe am Zieltelefon signalisiert.
Anrufschutz	Aktiviert ein Sammelanschlussmitglied den Anrufschutz, werden ankommende Anrufe für sein Telefon nicht durchgestellt. Dies gilt für Anrufe des Sammelanschlusses und der eigenen Stationsnummer des Mitglieds.
Warteschlange	Für zyklische und lineare Sammelanschlüsse ist es nicht möglich, eine Anrufwarteschlange einzurichten.
ISDN-Telefone	Es ist nicht möglich, ISDN-Telefone in Sammelanschlüssen aufzunehmen.

Zugehörige Tasks

Wie Sie einen Sammelanschluss hinzufügen auf Seite 704
Wie Sie einen Sammelanschluss ändern auf Seite 705
Wie Sie einen Sammelanschluss löschen auf Seite 706
Wie Sie ein Mitglied zum Sammelanschluss hinzufügen oder löschen auf Seite 706

15.1.4 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Wizards

Verschiedene Wizards ermöglichen die komfortable Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen.

Mit dem Wizard **Anrufübernahme** können Sie Teilnehmer zu einer Gruppe zusammenfassen, um eine gegenseitige Rufannahme zu ermöglichen. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- Wie Sie eine Anrufübernahmegruppe konfigurieren
- Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe einrichten. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- Wie Sie einen Gruppenruf (Gruppe) hinzufügen
- Wie Sie einen Gruppenruf (Gruppe) ändern
- Wie Sie einen Gruppenruf (Gruppe) löschen
- Wie Sie ein Mitglied zum Gruppenruf (Gruppe) hinzufügen oder löschen
- Wie Sie einen Sammelanschluss hinzufügen
- Wie Sie einen Sammelanschluss ändern
- Wie Sie einen Sammelanschluss löschen
- Wie Sie ein Mitglied zum Sammelanschluss hinzufügen oder löschen

15.1.4.1 Wie Sie eine Anrufübernahmegruppe konfigurieren

Der Wizard **Anrufübernahme** ermöglicht Ihnen das Zusammenfassen von Teilnehmern zu einer Gruppe, mit der Möglichkeit der gegenseitigen Rufannahme.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufübernahme** zu starten. Es wird Ihnen die Liste aller möglichen Anrufübernahmegruppen angezeigt.
4) Um eine Anrufübernahmegruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten Anrufübernahmegruppe auf **Bearbeiten**.
5) Wenn Sie Mitglieder zu der Anrufübernahmegruppe hinzufügen möchten, aktivieren Sie die Kontrollkästchen **Zuordnung Gruppe <Nummer>** der gewünschten Rufnummern/Namen.
6) Wenn Sie Mitglieder aus der Anrufübernahmegruppe entfernen möchten, deaktivieren Sie die Kontrollkästchen **Zuordnung Gruppe <Nummer>** der gewünschten Rufnummern/Namen.
7) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.

8) Geben Sie im Feld **Name** den Namen der soeben konfigurierten Anrufübernahmegruppe ein.
9) Wenn Sie weitere Anrufübernahmegruppen konfigurieren möchten, wiederholen Sie die Schritte 4 bis 8.
10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Anrufübernahmegruppe auf Seite 689

15.1.4.2 Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen

Mit dem Wizard **Anrufübernahme** können Sie Mitglieder zu Anrufübernahmegruppen hinzufügen oder löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufübernahme** zu starten.
4) Klicken Sie in der Zeile der gewünschten Anrufübernahmegruppe auf **Bearbeiten**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie Mitglieder zu der Anrufübernahmegruppe hinzufügen möchten, aktivieren Sie die Kontrollkästchen **Zuordnung Gruppe <Nummer>** der gewünschten Rufnummern/Namen.
   - Wenn Sie Mitglieder aus der Anrufübernahmegruppe entfernen möchten, deaktivieren Sie die Kontrollkästchen **Zuordnung Gruppe <Nummer>** der gewünschten Rufnummern/Namen.
6) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Anrufübernahmegruppe auf Seite 689

15.1.4.3 Wie Sie einen Gruppenruf (Gruppe) hinzufügen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe einrichten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie auf **Hinzufügen**, um einen neuen Gruppenruf einzurichten.
5) Geben Sie im Feld **Rufnummer der Gruppe** die Rufnummer des neuen Gruppenrufs ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer des neuen Gruppenrufs ein.

: Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

---

7) Geben Sie im Feld **Name der Gruppe** den Namen des neuen Gruppenrufs ein.
8) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Gruppe** aus.
9) Wählen Sie eine der folgenden Möglichkeiten für die Übernahme der Rufnummer des Gruppenrufs in das interne Verzeichnis:
   - Wenn die Rufnummer des Gruppenrufs im internen Verzeichnis erscheinen soll, aktivieren Sie das Kontrollkästchen **Tel.-Buch**.
   - Wenn die Rufnummer des Gruppenrufs nicht im internen Verzeichnis erscheinen soll, deaktivieren Sie das Kontrollkästchen **Tel.-Buch**.
10) Wählen Sie in der Aufklappliste **Rufnummer des Teilnehmers, der der Gruppe zugeordnet werden soll** die Rufnummer des gewünschten Teilnehmers aus.
11) Klicken Sie auf **OK & Weiter**.

Tipp: Ist die von Ihnen gewählte Rufnummer und/oder Durchwahlnummer bereits vorhanden, können Sie den aktuellen Rufnummernplan aufrufen, um eine freie Rufnummer und/oder Durchwahlnummer zu ermitteln.

---

12) Klicken Sie in der Zeile des neuen Gruppenrufs auf **Bearbeiten**, um dem Gruppenruf weitere Teilnehmer zuzuordnen.
13) Wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des Teilnehmers aus, der dem Gruppenruf zugeordnet werden soll.
14) Klicken Sie auf **Hinzufügen**.
15) Wenn Sie dem Gruppenruf weitere Teilnehmer zuordnen möchten, wiederholen Sie die Schritte 13 und 14.
16) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.
17) Wenn Sie einen weiteren Gruppenruf einrichten möchten, wiederholen Sie die Schritte 4 bis 16.
18) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.1.4.4 Wie Sie einen Gruppenruf (Gruppe) ändern

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe bearbeiten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie in der Zeile des zu ändernden Gruppenrufs auf **Bearbeiten**.
5) Ändern Sie die gewünschten Gruppenparameter.
6) Nur bei UC Smart: Ordnen Sie bei Bedarf dem Gruppenruf eine Mailbox zu:
   a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Gruppenruf eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.
   b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.
   c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.
   d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

   Anmerkung: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.
7) Wenn Sie ein Mitglied zum Gruppenruf hinzufügen möchten, wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Hinzufügen**.
8) Wenn Sie ein Mitglied aus dem Gruppenruf entfernen möchten, klicken Sie in der Zeile des gewünschten Gruppenmitglieds auf **Löschen** und anschließend auf **OK**.
9) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.
10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.1.4.5 Wie Sie einen Gruppenruf (Gruppe) löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie in der Zeile des zu löschenden Gruppenrufs auf **Bearbeiten**.
5) Klicken Sie auf **Daten löschen**.
6) Klicken Sie auf **OK**, um das Löschen zu bestätigen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.1.4.6 Wie Sie ein Mitglied zum Gruppenruf (Gruppe) hinzufügen oder löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Mitglieder zu Gruppenrufen des Typs Gruppe hinzufügen oder löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie in der Zeile des gewünschten Gruppenrufs auf **Bearbeiten**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zum Gruppenruf hinzufügen möchten, wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Hinzufügen**.
   - Wenn Sie ein Mitglied aus dem Gruppenruf entfernen möchten, klicken Sie in der Zeile des gewünschten Gruppenmitglieds auf **Löschen** und anschließend auf **OK**.
6) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.1.4.7 Wie Sie einen Sammelanschluss hinzufügen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Sammelanschlüsse einrichten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie auf **Hinzufügen**, um einen neuen Sammelanschluss einzurichten.
5) Geben Sie im Feld **Rufnummer der Gruppe** die Rufnummer des neuen Sammelanschlusses ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer des neuen Sammelanschlusses ein.

   : Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

7) Geben Sie im Feld **Name der Gruppe** den Namen des neuen Sammelanschlusses ein.
8) Wählen Sie in der Aufklappliste **Typ** den Typ des neuen Sammelanschlusses aus. Sie haben folgende Möglichkeiten:
   - Wenn ein Anruf immer zuerst beim ersten Mitglied des Sammelanschlusses signalisiert werden soll, wählen Sie den Eintrag **Linearer Sammelanschluss** aus.
   - Wenn ein Anruf zuerst bei dem Mitglied signalisiert werden soll, der dem Teilnehmer nachfolgt, der den letzten Anruf angenommen hat, wählen Sie den Eintrag **Zyklischer Sammelanschluss** aus.
9) Wählen Sie eine der folgenden Möglichkeiten für die Übernahme der Rufnummer des Sammelanschlusses in das interne Verzeichnis:
   - Wenn die Rufnummer des Sammelanschlusses im internen Verzeichnis erscheinen soll, aktivieren Sie das Kontrollkästchen **Tel.-Buch**.
   - Wenn die Rufnummer des Sammelanschlusses nicht im internen Verzeichnis erscheinen soll, deaktivieren Sie das Kontrollkästchen **Tel.-Buch**.
10) Wählen Sie in der Aufklappliste **Rufnummer des Teilnehmers, der der Gruppe zugeordnet werden soll** die Rufnummer des gewünschten Teilnehmers aus.
11) Klicken Sie auf **OK & Weiter**.

Tipp: Ist die von Ihnen gewählte Rufnummer und/ oder Durchwahlnummer bereits vorhanden, können Sie den aktuellen Rufnummernplan aufrufen, um eine freie Rufnummer und/oder Durchwahlnummer zu ermitteln.

12) Klicken Sie in der Zeile des neuen Sammelanschlusses auf **Bearbeiten**, um dem Sammelanschluss weitere Teilnehmer zuzuordnen.
13) Wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des Teilnehmers aus, der dem Sammelanschluss zugeordnet werden soll.
14) Klicken Sie auf **Hinzufügen**.
15) Wenn Sie dem Sammelanschluss weitere Teilnehmer zuordnen möchten, wiederholen Sie die Schritte 13 und 14.
16) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.
17) Wenn Sie einen weiteren Sammelanschluss einrichten möchten, wiederholen Sie die Schritte 4 bis 16.
18) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Gruppennummer auf Seite 695

15.1.4.8 Wie Sie einen Sammelanschluss ändern

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Sammelanschlüsse bearbeiten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie in der Zeile des zu ändernden Sammelanschlusses auf **Bearbeiten**.
5) Ändern Sie die gewünschten Parameter des Sammelanschlusses.
6) Nur bei UC Smart: Ordnen Sie bei Bedarf dem Sammelanschluss eine Mailbox zu:
   a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Sammelanschluss eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.
   b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.
   c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.
   d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

Anmerkung: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der

Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

7) Wenn Sie ein Mitglied zum Sammelanschluss hinzufügen möchten, wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Hinzufügen**.
8) Wenn Sie ein Mitglied aus dem Sammelanschluss entfernen möchten, klicken Sie in der Zeile des gewünschten Gruppenmitglieds auf **Löschen** und anschließend auf **OK**.
9) Wenn Sie die Position der Mitglieder innerhalb des Sammelanschlusses ändern möchten, klicken Sie auf **Reihenfolge ändern**. Geben Sie im Feld **Position** für jedes Mitglied die gewünschte Positionsnummer ein. Klicken Sie auf **OK & Weiter**.
10) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.
11) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Gruppennummer auf Seite 695

15.1.4.9 Wie Sie einen Sammelanschluss löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Sammelanschlüsse löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie in der Zeile des zu löschenden Sammelanschlusses auf **Bearbeiten**.
5) Klicken Sie auf **Daten löschen**.
6) Klicken Sie auf **OK**, um das Löschen zu bestätigen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Gruppennummer auf Seite 695

15.1.4.10 Wie Sie ein Mitglied zum Sammelanschluss hinzufügen oder löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Mitglieder zu Sammelanschlüssen hinzufügen oder löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie in der Zeile des gewünschten Sammelanschlusses auf **Bearbeiten**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zum Sammelanschluss hinzufügen möchten, wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Hinzufügen**.
   - Wenn Sie ein Mitglied aus dem Sammelanschluss entfernen möchten, klicken Sie in der Zeile des gewünschten Gruppenmitglieds auf **Löschen** und anschließend auf **OK**.
6) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Gruppennummer auf Seite 695

15.1.5 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Experten-Modus

Neben den Konfigurationsmöglichkeiten über Wizards stehen einem Administrator mit dem Profil **Expert** zusätzliche Möglichkeiten zur Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über den **Experten-Modus** zur Verfügung.

Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den **Experten-Modus** eingerichtet werden können:

- Wie Sie die Anzeige der Rufnummer und des Namens des Anrufers aktivieren oder deaktivieren
- Wie Sie den Aufmerksamkeitston aktivieren oder deaktivieren
- Wie Sie die Anrufübernahme von Wiederanrufen aktivieren oder deaktivieren
- Wie Sie einen Gruppenruf (Freifall oder Anklopfen) hinzufügen
- Wie Sie einen Gruppenruf (Freifall oder Anklopfen) anzeigen oder ändern
- Wie Sie einen Gruppenruf (Freifall oder Anklopfen) löschen
- Wie Sie ein Mitglied zum Gruppenruf (Freifall oder Anklopfen) hinzufügen oder löschen
- Wie Sie den Anklopfschutz für Gruppenmitglied ein- oder ausschalten

15.1.5.1 Wie Sie die Anzeige der Rufnummer und des Namens des Anrufers aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Rufnummer und Name des Anrufers angezeigt werden sollen, aktivieren Sie das Kontrollkästchen **A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungsziel / RWS-Ziel**.
   - Wenn Rufnummer und Name des Anrufers nicht angezeigt werden sollen, deaktivieren Sie das Kontrollkästchen **A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungsziel / RWS-Ziel**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Anrufübernahmegruppe auf Seite 689

15.1.5.2 Wie Sie den Aufmerksamkeitston aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den Aufmerksamkeitston einschalten möchten, aktivieren Sie das Kontrollkästchen **Aufmerksamkeitssignalisierung bei AUN-Gruppen**.
   - Wenn Sie den Aufmerksamkeitston ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Aufmerksamkeitssignalisierung bei AUN-Gruppen**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Anrufübernahmegruppe auf Seite 689

15.1.5.3 Wie Sie die Anrufübernahme von Wiederanrufen aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Anrufübernahme von Wiederanrufen möglich sein soll, aktivieren Sie das Kontrollkästchen **Anrufübernahme nach Wiederanruf**.
   - Wenn die Anrufübernahme von Wiederanrufen nicht möglich sein soll, deaktivieren Sie das Kontrollkästchen **Anrufübernahme nach Wiederanruf**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Anrufübernahmegruppe auf Seite 689

15.1.5.4 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Klicken Sie im Menübaum auf **Kommende Rufe** > **Gruppen-/ Sammelanschluss**.
4) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer des neuen Gruppenrufs ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer des neuen Gruppenrufs ein.

   : Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

7) Geben Sie im Feld **Name** den Namen des neuen Gruppenrufs ein.
8) Wählen Sie in der Aufklappliste **Typ** eine der folgenden Möglichkeiten aus:
   - Wenn Sie einen Gruppenruf des Typs Freifall einrichten möchten, wählen Sie den Eintrag **Freifall** aus.
   - Wenn Sie einen Gruppenruf des Typs Anklopfen einrichten möchten, wählen Sie den Eintrag **Anklopfen** aus.
9) Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des Teilnehmers aus, der dem Gruppenruf zugeordnet werden soll.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.1.5.5 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) anzeigen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Gruppenruf.
4) Klicken Sie auf die Registerkarte **Gruppen-Parameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppen-Parameter angezeigt.
5) Ändern Sie bei Bedarf die gewünschten Parameter des Gruppenrufs.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.1.5.6 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Gruppenruf.
4) Klicken Sie auf die Registerkarte **Gruppe löschen**.
5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.1.5.7 Wie Sie ein Mitglied zum Gruppenruf (Freifall oder Anklopfen) hinzufügen oder löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.

3) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Mitglied zum Gruppenruf hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Gruppenruf. Klicken Sie auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
- Wenn Sie ein Mitglied aus dem Gruppenruf entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Mitglied des Gruppenrufs ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.1.5.8 Wie Sie den Anklopfschutz für Gruppenmitglied ein- oder ausschalten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Navigieren Sie im Menübaum unter **Teilnehmer** > **Teilnehmer** > **...** zum gewünschten Teilnehmer (Index-Rufnummer-Name).
4) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.
5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den Anklopfschutz einschalten möchten, aktivieren Sie das Kontrollkästchen **Anklopfschutz ein**.
- Wenn Sie den Anklopfschutz ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Anklopfschutz ein**.

Anmerkung: Wenn eine Gruppe als VPL-Gruppe konfiguriert ist, wird das Anrufschutz-Flag aller vorhandenen Gruppenmitglieder automatisch auf False gesetzt. Dies gilt ebenfalls für alle neuen Mitglieder der VPL-Gruppe. Der Benutzer kann das Flag "Anrufschutz ein" für beliebige VPL-Gruppenmitglieder manuell auf True setzen, um für diese den Besetztton zu aktivieren. Dies ist aber nicht das Standardverhalten.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Gruppenruf auf Seite 691

15.2 Teamschaltung / Team-Gruppe und Chef/Sekretär / Top-Gruppe

Eine Teamschaltung / Team-Gruppe bietet komfortable Teamfunktionen. Die Rufnummern aller Teammitglieder werden auf MULAP-Tasten (Leitungstasten) programmiert. Damit hat jedes Teammitglied Zugriff auf alle Leitungen (zum Beispiel zur Anrufübernahme) und kann auch gleichzeitig über mehrere Leitungen telefonieren. Eine Chef/Sekretär / Top-Gruppe bietet komfortable Chef- und Sekretär-Funktionen (Topfunktion) für bis zu drei Chefs und bis zu drei Sekretäre.

Anmerkung: Beim Erstellen einer MULAP über die Team/ Top-Optionen im WBM/Manager E dürfen keine Rufnummern angegebenen werden, die mit ** oder *** beginnen.

15.2.1 Teamschaltung / Team-Gruppe

Bei einem Telefon mit Funktionen für Teams werden die eigene und die Rufnummern der weiteren Teammitglieder auf MULAP (Multiple Line Appearance)-Tasten (Leitungstasten) programmiert. Jedes Teammitglied hat Zugriff auf alle Leitungen (z.B. zur Anrufübernahme) und kann auch gleichzeitig über mehrere Leitungen telefonieren. Darüber hinaus werden automatisch Direktruftasten programmiert, über die die Teammitglieder sich direkt anrufen können.

Über die MULAP-Tasten haben die Teammitglieder Zugriff auf die Rufnummern aller Mitglieder.Ein kommender Anruf für ein Teammitglied kann dementsprechend auch von allen anderen Mitgliedern durch Drücken der blinkenden MULAP-Taste angenommen werden.Ebenso möglich ist das Makeln zwischen mehreren Leitungen.Durch Drücken einer MULAP-Taste kann ein Teammitglied einen gehenden Anruf über die zugehörige Leitung tätigen. Dem Angerufenen wird die zu dieser Leitung gehörende Rufnummer im Display angezeigt.

Ankommende Anrufe werden gleichzeitig bei allen Teammitgliedern optisch, über die LED der MULAP-Taste signalisiert. Für jedes Teammitglied kann zusätzlich angegeben werden, ob ankommende Anrufe auch akustisch signalisiert werden sollen.

Über eine Gruppenruftaste kann jedes Teammitglied die Signalisierung der ankommenden Anrufe für jede einzelne Leitung ein- oder ausschalten.

Bis zu drei Teilnehmer pro Teamschaltung/Team-Gruppe kann ein Administrator mit dem Profil **Advanced** über den Wizard **Teamschaltung** einrichten. Bis zu zehn Teilnehmer pro Teamschaltung/Team-Gruppe kann ein Administrator mit dem Profil **Expert** über den **Experten-Modus** einrichten.

Ein einzelner Teilnehmer kann gleichzeitig mehreren Gruppen angehören. Das Folgende gilt für Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung / Team-Gruppe und Chef/Sekretariat / Top-Gruppe: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht überschreiten.

Jeder Teamschaltung/Team-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Bei der Einrichtung einer Teamschaltung/Team-Gruppe werden den Mitgliedern folgende Eigenschaften zugewiesen (Änderungen der Einstellungen können durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** durchgeführt werden.):

- **Master**

  Durch diesen Parameter wird ein Mitglied zu einem Master der Teamschaltung/Team-Gruppe. Aktiviert ein Master eine Anrufumleitung, gilt diese für alle Mitglieder (Telefone) der Teamschaltung/Team-Gruppe.

  Standardeinstellung: Master ist das erste Mitglied der Teamschaltung/Team-Gruppe.
- **Akustischer Ruf**

  Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert.

  Standardeinstellung: Der Parameter ist aktiviert.
- **Automatische Belegung gehend**

  Ist dieser Parameter aktiviert, wird beim Abheben des Hörers automatisch über die MULAP-Leitung dieses Mitglieds gerufen. Bei nicht aktiviertem Parameter muss der Teilnehmer die MULAP-Taste betätigen, bevor er wählen kann.

  Standardeinstellung: Der Parameter ist aktiviert.
- **Keine automatische Rufannahme kommend**

  Ist dieser Parameter aktiviert, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.

  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **Automatische Konferenzfreigabe**

  Bei aktiviertem Parameter wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen.

  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **MULAP-Taste eingerichtet**

  Bei aktiviertem Parameter wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf über die MULAP-Leitung des Masters. Dem Angerufenen wird die MULAP-Teilnehmernummer des Masters im Display angezeigt.

  Standardeinstellung: Der Parameter ist nicht aktiviert.

MULAP-Tasten nutzen

Jedem Teammitglied ist eine eigene Leitung (MULAP-Leitung) zugeordnet. Die eigene und die Leitungen aller anderen Mitglieder sind bei jedem Teammitglied als MULAP-Tasten (Leitungstasten) eingerichtet. Somit kann jedes Teammitglied alle vorhandenen MULAP-Leitungen nutzen.

Die LED einer MULAP-Taste (Leitungstaste) hat folgende Bedeutung:

- Aus: Die zugehörige Leitung ist frei und kann verwendet werden.
- Leuchtet: Die zugehörige Leitung ist belegt.

- Blinkt schnell: Anruf auf der zugehörigen Leitung.
- Blinkt langsam: Ein gehaltenes Gespräch wartet auf der zugehörigen Leitung.

Direktruftasten nutzen

Jedes Teammitglied hat für jedes andere Teammitglied eine Direktruftaste. Somit sind die Teammitglieder untereinander direkt per Tastendruck erreichbar.

Eine Direktruftaste kann auch verwendet werden, um ein bestehendes Gespräch schnell an das darunter programmierte Teammitglied zu übergeben.

Die LED einer Direktruftaste hat folgende Bedeutung:

- Aus: Das zugehörige Teammitglied telefoniert nicht.
- Leuchtet: Das zugehörige Teammitglied telefoniert oder hat Anrufschutz eingeschaltet.
- Blinkt schnell: Das zugehörige Teammitglied ruft an. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.
- Blinkt langsam: Das zugehörige Teammitglied wird gerufen und hat den Anruf noch nicht angenommen. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.

Rufart

Für jede Teamschaltung/Team-Gruppe kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren.Sie haben folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

Faxbox für Teamschaltung/Team-Gruppe

Für jede Teamschaltung/Team-Gruppe kann eine Faxbox eingerichtet werden, über die die Mitglieder Faxnachrichten direkt über myPortal for Desktop oder myPortal for Outlook empfangen können.

Wurde für den Master (das erste Mitglied) der Teamschaltung/Team-Gruppe bereits eine Faxbox konfiguriert, wird diese Faxbox bei der Einrichtung der Teamschaltung/Team-Gruppe übernommen. Bereits konfigurierte Faxboxen der anderen Mitglieder werden gelöscht.

Nach dem Auflösen einer Teamschaltung/Team-Gruppe kann nur noch der ehemalige Master (das erste Mitglied) die Faxbox nutzen.

Bestellung der Mulap-Mitgliedsgeräte

SIP-Telefone können in ein Basis-MULAP integriert werden, solange ein TDM/HFA-Gerät als erstes Mitglied des Basis-MULAP definiert wurde. IP-Telefone können in ein Basis-MULAP integriert werden, solange ein TDM/HFA als erstes Mitglied des Basis-MULAP definiert wurde.

Eingebunden werden können beispielsweise Dual-Mode-Mobiltelefone, die als Mobility Entry-Teilnehmer eingerichtet sind. Dual-Modus-Mobiltelefone unterstützen sowohl GSM-/UMTS-Netzwerke als auch WLAN-Netzwerke. Über

WLAN ist die Registrierung eines Dual-Mode-Mobiltelefons als IP-Teilnehmer (SIP Client) am Kommunikationssystem möglich.

Mobilitätsbenutzer, einschließlich GSM Mobilitätsbenutzer, Unify Phone und Microsoft Teams Clients, können in ein Basis-MULAP integriert werden, sofern ein TDM/HFA Gerät als erstes Mitglied des Basis-MULAP definiert wurde.

Anmerkung: Die obige erweiterte Beschreibung gilt sowohl für OpenScape Business X als auch für OpenScape Business S-Systeme, beschränkt sich jedoch auf Team und Basis-Mulap und nicht auf Unterkapitel mit ähnlichen Anweisungen wie Exekutiv-/Sekretär-/Top-Gruppe.

Tipp: Für SIP-Telefone ist keine Programmierung von MULAP-Tasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Anzeigemeldungen der Basis-MULAP werden nicht unterstützt.

Anmerkung: High-End-Telefone wie CP 400/600/600E/700/700X/710 führen ihre eigenen Journaleinträge und sie haben die Fähigkeit, mehr Informationen zu präsentieren Bei Gruppenkonfigurationen sind sie jedoch auf Systemdaten angewiesen, da die Gruppen auf dem System und nicht auf den Telefonen konfiguriert werden. Daher kann es vorkommen, dass Informationen über Gruppen in Journaleinträgen nicht angezeigt werden, da sie den Einschränkungen und der Konfiguration des Systems folgen.

Abhängigkeiten

Themenbereich	Abhängigkeit
Anrufumleitung	Ein Teammitglied hat eine Anrufumleitung für alle Anrufe aktiviert. In diesem Fall werden alle Anrufe für seine eigene Teilnehmerrufnummer umgeleitet.
Anrufschutz	Aktiviert ein Teammitglied den Anrufschutz, werden ankommende Anrufe nicht durchgestellt. **Anmerkung:** Ein ganzes Team ist nur dann besetzt, wenn alle Teammitglieder das Merkmal Nicht stören aktiviert haben.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Teamschaltungen/Team-Gruppen ist nicht möglich.
Gruppen-/ Sammelanschlüsse	Die Einbindung eines Basic-/Chef-MULAPs in Teamschaltungen/Team-Gruppen ist nicht möglich.

Zugehörige Konzepte

Direktruf auf Seite 644

Zugehörige Tasks

Wie Sie eine Teamschaltung / Team-Gruppe hinzufügen auf Seite 721
Wie Sie eine Teamschaltung / Team-Gruppe ändern auf Seite 722
Wie Sie eine Teamschaltung / Team-Gruppe löschen auf Seite 723
Wie Sie ein Mitglied zur Teamschaltung / Team-Gruppe hinzufügen oder löschen auf Seite 727
Wie Sie ein Mitglied einer Teamschaltung / Team-Gruppe ändern auf Seite 727
Wie Sie die Eigenschaften der Mitglieder einer Teamschaltung / Team-Gruppe ändern auf Seite 728
Wie Sie die Telefon-Tastenbelegung für Teamschaltung / Team-Gruppe ändern auf Seite 728
Wie Sie eine Faxbox zur Teamschaltung / Team-Gruppe hinzufügen auf Seite 729

15.2.2 Chef/Sekretär / Top-Gruppe

Top-Gruppen können eingerichtet werden, wenn komfortable Chef- und Sekretär-Funktionen (Topfunktion) benötigt werden.

Chef-Sekretär-Funktionen können für Gruppen mit bis zu drei Chefs und bis zu drei Sekretären eingerichtet werden.

Tipp: Die Formulierungen “der Chef” und “der Sekretär” gelten auch für Gruppen mit mehr als einem Chef und mehr als einem Sekretär. In diesem Text steht "der Chef” stellvertretend sowohl für Chef als auch Chefin und “der Sekretär” stellvertretend sowohl für Sekretär als auch Sekretärin.

Jedem Topmitglied (jedem Chef und jedem Sekretär) ist eine eigene Leitung, die sogenannte MULAP (Multiple Line Appearance)-Leitung zugeordnet. Die eigene und die MULAP-Leitungen aller anderen Mitglieder sind bei jedem Topmitglied als MULAP-Tasten (Leitungstasten) eingerichtet. Bei gehenden Anrufen über die MULAP-Leitung wird den Angerufenen die MULAP-Rufnummer im Display angezeigt. Der Sekretär kann gehende Anrufe über seine eigene oder über die MULAP-Leitung aller Chefs und anderer Sekretäre tätigen. Soll beispielsweise eine Verbindung für einen Chef aufgebaut werden, könnte dafür die MULAP-Leitung dieses Chefs genutzt werden.

Darüber hinaus werden Direktruftasten programmiert, über die der Chef den Sekretär und umgekehrt direkt anrufen kann.

Ankommende Anrufe werden gleichzeitig bei allen Topmitgliedern optisch, über die LED der Leitungstaste signalisiert. Für jedes Topmitglied kann zusätzlich angegeben werden, ob ankommende Anrufe auch akustisch signalisiert werden sollen. Dabei erfolgt die akustische Signalisierung in Abhängigkeit von der Rufumschaltetaste.

Über eine Rufumschaltetaste kann die Signalisierung der ankommenden Anrufe umgeschaltet werden. Ankommende Anrufe werden entweder beim Chef oder beim Sekretär signalisiert. Betätigt der Chef die Rufumschaltetaste, werden ihm ankommende Anrufe weiterhin über Popup-Fenster angezeigt. Die Annahme

eines Anrufes ist aber nur über eine entsprechende Taste am Telefon und nicht über das Popup-Fenster möglich.

Sekretär-Telefone können sich über eine Gruppenruftaste aus der Chef/Sekretär-Konfiguration/Top-Gruppe hinaus- und wieder hineinschalten. Dabei hat die Rufumschaltung Priorität.

Tipp: Schaltet sich der Sekretär mit der Gruppenruftaste aus der Chef/Sekretär-Konfiguration/Top-Gruppe hinaus, ohne die Rufumschaltung für den Chef zu aktivieren, werden ankommende Anrufe weder beim Chef noch beim Sekretär signalisiert.

Bis zu zwei Chefs und bis zu zwei Sekretäre pro Chef/Sekretär-Konfiguration/Top-Gruppe kann ein Administrator mit dem Profil **Advanced** über den Wizard **Chef/Sekretär** einrichten. Bis zu drei Chefs und bis zu drei Sekretäre pro Chef/Sekretär-Konfiguration/Top-Gruppe kann ein Administrator mit dem Profil **Expert** über den **Experten-Modus** einrichten.

Für jeden Chef können maximal drei Telefone und für jeden Sekretär können maximal zwei Telefone eingerichtet werden.

Ein einzelner Teilnehmer kann gleichzeitig mehreren Gruppen angehören. Das Folgende gilt für Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung / Team-Gruppe und Chef/Sekretariat / Top-Gruppe: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht überschreiten.

Jeder Chef/Sekretär-Konfiguration/Top-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Bei der Einrichtung einer Chef/Sekretär-Konfiguration oder Top-Gruppe werden den Mitgliedern folgende Eigenschaften zugewiesen (Änderungen der Einstellungen können durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** durchgeführt werden.):

- **Master**

  Durch diesen Parameter erhält ein Mitglied Chef-Funktionen. Beim Abheben des Hörers wird automatisch die Chef-MULAP-Leitung für einen Ruf ausgewählt. Kommende Rufe über die zugehörige Chef-MULAP-Rufnummer werden standardmäßig ausschließlich optisch signalisiert.

  Standardeinstellung: Chef-Funktionen erhalten alle Chefs der Chef/Sekretär-Konfiguration oder Top-Gruppe.
- **Akustischer Ruf**

  Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert.

  Standardeinstellung: Der Parameter ist für alle Mitglieder mit Sekretär-Funktion aktiviert.
- **Automatische Belegung gehend**

  Ist dieser Parameter aktiviert, wird beim Abheben des Hörers automatisch über die MULAP-Leitung dieses Mitglieds gerufen. Bei nicht aktiviertem Parameter muss der Teilnehmer die MULAP-Taste betätigen, bevor er wählen kann.

  Standardeinstellung: Der Parameter ist für alle Mitglieder aktiviert.

- **Keine automatische Rufannahme kommend**

  Ist dieser Parameter aktiviert, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.

  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **Automatische Konferenzfreigabe**

  Bei aktiviertem Parameter wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen.

  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **MULAP-Taste eingerichtet**

  Bei aktiviertem Parameter wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt.

  Standardeinstellung: Der Parameter ist aktiviert.

MULAP-Tasten nutzen

Jedem Topmitglied ist eine eigene Leitung (MULAP-Leitung) zugeordnet. Die eigene und die Leitungen aller anderen Mitglieder sind bei jedem Topmitglied als MULAP-Tasten (Leitungstasten) eingerichtet. Somit kann jedes Topmitglied alle vorhandenen MULAP-Leitungen nutzen.

Die LED einer MULAP-Taste (Leitungstaste) hat folgende Bedeutung:

- Aus: Die zugehörige Leitung ist frei und kann verwendet werden.
- Leuchtet: Die zugehörige Leitung ist belegt.
- Blinkt schnell: Anruf auf der zugehörigen Leitung.
- Blinkt langsam: Ein gehaltenes Gespräch wartet auf der zugehörigen Leitung oder die zugehörige Leitung wurde für eine Konferenz freigegeben.

Direktruftasten nutzen

Jedes Topmitglied hat für jedes andere Topmitglied eine Direktruftaste. Somit sind die Topmitglieder untereinander direkt per Tastendruck erreichbar.

Eine Direktruftaste kann auch verwendet werden, um ein bestehendes Gespräch schnell an das darunter programmierte Topmitglied zu übergeben.

Die LED einer Direktruftaste hat folgende Bedeutung:

- Aus: Das zugehörige Topmitglied telefoniert nicht.
- Leuchtet: Das zugehörige Topmitglied telefoniert oder hat Anrufschutz eingeschaltet.
- Blinkt schnell: Das zugehörige Topmitglied ruft an. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.
- Blinkt langsam: Das zugehörige Topmitglied wird gerufen und hat den Anruf noch nicht angenommen. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.

Rufart

Für jede Chef/Sekretär-Konfiguration/Top-Gruppe kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Sie haben folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

Faxboxen für Chef/Sekretär-Konfiguration/Top-Gruppe

Für jedes Mitglied einer Chef/Sekretär-Konfiguration/Top-Gruppe kann eine Faxbox eingerichtet werden, über die das Mitglied Faxnachrichten direkt über myPortal for Desktop oder myPortal for Outlook empfangen kann.

Wurde für den ersten Chef der Chef/Sekretär-Konfiguration/Top-Gruppe bereits eine Faxbox konfiguriert, wird diese Faxbox bei der Einrichtung der Chef/Sekretär-Konfiguration/Top-Gruppe übernommen. Bereits konfigurierte Faxboxen der anderen Mitglieder werden gelöscht.

Nach dem Auflösen einer Chef/Sekretär-Konfiguration/Top-Gruppe kann nur noch der ehemalige erste Chef seine Faxbox nutzen.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Chef/Sekretär-Konfiguration/Top-Gruppe ist möglich. Voraussetzung dafür ist, dass ein Systemtelefon (zum Beispiel IP-Telefon, HFA oder SIP) als erstes Mitglied der Chef/Sekretär-Konfiguration/Top-Gruppe (Chef 1) definiert wird.

Eingebunden werden können beispielsweise Dual-Mode-Mobiltelefone, die als Mobility Entry-Teilnehmer eingerichtet sind. Dual-Mode-Mobiltelefone unterstützen sowohl GSM/UMTS-Netze als auch WLAN-Netze. Über WLAN ist die Registrierung eines Dual-Mode-Mobiltelefons als IP-Teilnehmer (SIP Client) am Kommunikationssystem möglich.

Tipp: Bei SIP-Telefonen ist keine Programmierung von MULAP-Tasten und Direktruftasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen der Chef/Sekretär-Konfiguration/Top-Gruppe werden nicht unterstützt.

Anmerkung: Hochwertige Telefone, wie das CP600, führen eigene Journaleinträge und können mehr Informationen anzeigen. Bei Gruppenkonfigurationen sind sie jedoch auf Systemdaten angewiesen, da die Gruppen auf dem System und nicht auf den Telefonen konfiguriert werden. Daher kann es vorkommen, dass Informationen über Gruppen in Journaleinträgen nicht angezeigt werden, da sie den Einschränkungen und der Konfiguration des Systems folgen.

Abhängigkeiten

Themenbereich	Abhängigkeit
Anrufumleitung	Ein Topmitglied hat eine Anrufumleitung für alle Anrufe aktiviert. In diesem Fall werden alle Anrufe für seine eigene Teilnehmerrufnummer umgeleitet.
Anrufschutz	Aktiviert ein Topmitglied den Anrufschutz, werden ankommende Anrufe nicht durchgestellt.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Chef/Sekretär-Konfigurationen/Top-Gruppen ist nicht möglich.
Gruppen-/Sammelanschlüsse	Die Einbindung eines Basic-/Chef-MULAPs in Chef/Sekretär-Konfigurationen/Top-Gruppen ist nicht möglich.

Zugehörige Konzepte

Direktruf auf Seite 644

Zugehörige Tasks

Wie Sie eine Chef/Sekretär- / Top-Gruppe hinzufügen auf Seite 724
Wie Sie eine Chef/Sekretär- / Top-Gruppe ändern auf Seite 725
Wie Sie eine Chef/Sekretär- / Top-Gruppe löschen auf Seite 726
Wie Sie ein Mitglied zur Chef/Sekretär / Top-Gruppe hinzufügen oder löschen auf Seite 729
Wie Sie ein Mitglied einer Chef/Sekretär / Top-Gruppe ändern auf Seite 730
Wie Sie die Eigenschaften der Mitglieder einer Chef/Sekretär / Top-Gruppe ändern auf Seite 730
Wie Sie eine Faxbox zur Chef/Sekretär / Top-Gruppe hinzufügen auf Seite 731

15.2.3 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Wizards

Verschiedene Wizards ermöglichen die komfortable Konfiguration von Teamschaltungen (Team-Gruppen) und von Chef- und Sekretär-Funktionen (Topfunktion).

Mit dem Wizard **Teamschaltung** können Sie Teamschaltungen (Team-Gruppen) konfigurieren. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- Wie Sie eine Teamschaltung / Team-Gruppe hinzufügen
- Wie Sie eine Teamschaltung / Team-Gruppe ändern
- Wie Sie eine Teamschaltung / Team-Gruppe löschen

Mit dem Wizard **Chef / Sekretär** können Sie komfortable Chef- und Sekretär-Funktionen (Topfunktion) konfigurieren. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- Wie Sie eine Chef/Sekretär- / Top-Gruppe hinzufügen
- Wie Sie eine Chef/Sekretär- / Top-Gruppe ändern
- Wie Sie eine Chef/Sekretär- / Top-Gruppe löschen

Zugehörige Konzepte

Konfiguration von myPortal to go und Mobility Entry auf Seite 965

15.2.3.1 Wie Sie eine Teamschaltung / Team-Gruppe hinzufügen

Mit dem Wizard **Teamschaltung** können Sie Teamschaltungen (Team-Gruppen) einrichten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teamschaltung** zu starten.
4) Klicken Sie auf **Hinzufügen**, um eine neue Teamschaltung einzurichten.
5) Wählen Sie in der Aufklappliste **Erstes Telefon** die Rufnummer des ersten Telefons der neuen Teamschaltung aus.
6) Klicken Sie auf **OK & Weiter**.
7) Geben Sie im Feld **Name** den Namen der neuen Teamschaltung ein, falls kein Name angezeigt wird oder eine Änderung des angezeigten Namens erforderlich ist.

   Hinweis: Das Feld **Name** ist bereits mit dem Namen des ersten Telefons der Teamschaltung vorbelegt, falls für dieses Telefon ein Name vergeben wurde.
8) Geben Sie im Feld **Interne Rufnummer** die interne Rufnummer der neuen Teamschaltung ein, falls eine Änderung der angezeigten Rufnummer erforderlich ist.

   Das Feld **Interne Rufnummer** ist bereits mit der internen Rufnummer des ersten Telefons der Teamschaltung vorbelegt.

   : Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.
9) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der neuen Teamschaltung ein, falls eine Änderung der angezeigten Durchwahlnummer erforderlich ist.

   Hinweis: Das Feld **Durchwahlnummer** ist bereits mit der Durchwahlnummer des ersten Telefons der Teamschaltung vorbelegt.
10) Geben Sie unter **Fax** im Feld **Interne Rufnummer** die interne Rufnummer der Faxbox für die neue Teamschaltung ein, falls keine Rufnummer angezeigt wird oder eine Änderung der angezeigten Rufnummer erforderlich ist.

    Das Feld **Interne Rufnummer** ist bereits mit der internen Rufnummer der Faxbox des ersten Telefons der Teamschaltung vorbelegt, falls für dieses Telefon eine Faxbox konfiguriert wurde.
11) Geben Sie unter **Fax** im Feld **Durchwahlnummer** die Durchwahlnummer der Faxbox für die neue Teamschaltung ein, falls keine Durchwahlnummer

angezeigt wird oder eine Änderung der angezeigten Durchwahlnummer erforderlich ist.

Das Feld **Durchwahlnummer** ist bereits mit der Durchwahlnummer der Faxbox des ersten Telefons der Teamschaltung vorbelegt, falls für dieses Telefon eine Faxbox konfiguriert wurde.

12) Aktivieren Sie das Flag **Team als Gruppenmitglied**.

Das Flag **Team als Gruppenmitglied** ist nur konfigurierbar, wenn die Team-Gruppe Mitglieder mit demselben Teilnehmertyp hat, was zu einer einzelnen MULAP-Gruppe führt. Wenn dieses Flag aktiviert ist, kann die MULAP-Gruppe als Mitglied unter Gruppen hinzugefügt werden.

13) Wählen Sie in der Aufklappliste **Zweites Telefon** die Rufnummer des zweiten Telefons der neuen Teamschaltung aus.

14) Wählen Sie in der Aufklappliste **Drittes Telefon** die Rufnummer des dritten Telefons der neuen Teamschaltung aus.

15) Klicken Sie auf **OK & Weiter**.

16) Wenn Sie eine weitere Teamschaltung einrichten möchten, wiederholen Sie die Schritte 4 bis 15.

17) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712

15.2.3.2 Wie Sie eine Teamschaltung / Team-Gruppe ändern

Mit dem Wizard **Teamschaltung** können Sie Teamschaltungen (Team-Gruppen) bearbeiten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teamschaltung** zu starten.

4) Klicken Sie in der Zeile der zu ändernden Teamschaltung auf **Bearbeiten**.

5) Ändern Sie die gewünschten Parameter.

6) Nur bei UC Smart: Ordnen Sie bei Bedarf der Teamschaltung eine Mailbox zu:
   a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob die Teamschaltung eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.
   b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.
   c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.
   d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

   Anmerkung: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

7) Klicken Sie auf **OK & Weiter**.
8) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712

15.2.3.3 Wie Sie eine Teamschaltung / Team-Gruppe löschen

Mit dem Wizard **Teamschaltung** können Sie Teamschaltungen (Team-Gruppen) löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teamschaltung** zu starten.
4) Klicken Sie in der Zeile der zu löschenden Teamschaltung auf **Bearbeiten**.
5) Klicken Sie auf **Daten löschen**.
6) Klicken Sie auf **OK**, um das Löschen zu bestätigen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

   Anmerkung: Für Applikationen bei denen die CSTA-Schnittstelle (UC, OSCC, usw.) verwendet wird: Wenn eine Team-Gruppe oder ein Team-Gruppenmitglied gelöscht wird, ist ein Neustart des Systems erforderlich.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712

15.2.3.4 Wie Sie eine Chef/Sekretär- / Top-Gruppe hinzufügen

Mit dem Wizard **Chef / Sekretär** können Sie komfortable Chef- und Sekretär-Funktionen (Topfunktion) einrichten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Chef / Sekretär** zu starten.
4) Klicken Sie auf **Hinzufügen**, um eine neue Chef/Sekretär-Konfiguration (Top-Gruppe) einzurichten.
5) Geben Sie im Feld **Name** den Namen der neuen Chef/Sekretär-Konfiguration ein.
6) Wählen Sie in den zugehörigen Aufklapplisten die gewünschten Rufnummern der neuen Chef/Sekretär-Konfiguration aus.
7) Klicken Sie auf **OK & Weiter**.
8) Geben Sie unter **Fax** im Feld **Rufnummer** die interne Rufnummer der Faxbox für die neue Chef/Sekretär-Konfiguration ein, falls keine Rufnummer angezeigt wird oder eine Änderung der angezeigten Rufnummer erforderlich ist.

   Das Feld **Rufnummer** ist bereits mit der internen Rufnummer der Faxbox des ersten Chefs der Chef/Sekretär-Konfiguration vorbelegt, falls für dieses Telefon eine Faxbox konfiguriert wurde.
9) Geben Sie unter **Fax** im Feld **Durchwahl** die Durchwahlnummer der Faxbox für die neue Chef/Sekretär-Konfiguration ein, falls keine Durchwahlnummer angezeigt wird oder eine Änderung der angezeigten Durchwahlnummer erforderlich ist.

   Das Feld **Durchwahl** ist bereits mit der Durchwahlnummer der Faxbox des ersten Chefs der Chef/Sekretär-Konfiguration vorbelegt, falls für dieses Telefon eine Faxbox konfiguriert wurde.

   : Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

   ---
10) Wählen Sie eine Vorgabe für die Tastenbelegung aus:
    - Wenn die Tasten für die Chef/Sekretär-Funktionen auf dem ersten oder zweiten Beistellgerät eingerichtet werden sollen, aktivieren Sie das Kontrollkästchen auf **erste/zweite Konsole**.
    - Wenn die Tasten für die Chef/Sekretär-Funktionen auf den ersten freien Funktionstasten des Telefons eingerichtet werden sollen, aktivieren Sie das Kontrollkästchen **auf erste freie Tasten**.
11) Klicken Sie auf **OK & Weiter**.
12) Wenn Sie eine weitere Chef/Sekretär-Konfiguration einrichten möchten, wiederholen Sie die Schritte 4 bis 11.
13) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Chef/Sekretär / Top-Gruppe auf Seite 716

15.2.3.5 Wie Sie eine Chef/Sekretär- / Top-Gruppe ändern

Mit dem Wizard **Chef / Sekretär** können Sie komfortable Chef- und Sekretär-Funktionen (Topfunktion) bearbeiten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Chef / Sekretär** zu starten.
4) Klicken Sie in der Zeile der zu ändernden Chef/Sekretär-Konfiguration (Top-Gruppe) auf **Bearbeiten**.
5) Ändern Sie die gewünschten Parameter.
6) Nur bei UC Smart: Ordnen Sie bei Bedarf der Top-Gruppe eine Mailbox zu:
   a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob die Top-Gruppe eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.
   b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.
   c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.
   d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

   Anmerkung: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.
7) Klicken Sie auf **OK & Weiter**.
8) Ändern Sie die gewünschten Angaben für die Faxbox (**Fax**) und die **Tastenvergabe**.
9) Klicken Sie auf **OK & Weiter**.
10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Zugehörige Konzepte

Chef/Sekretär / Top-Gruppe auf Seite 716

15.2.3.6 Wie Sie eine Chef/Sekretär- / Top-Gruppe löschen

Mit dem Wizard **Chef / Sekretär** können Sie komfortable Chef- und Sekretär-Funktionen (Topfunktion) löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Chef / Sekretär** zu starten.
4) Klicken Sie in der Zeile der zu löschenden Chef/Sekretär-Konfiguration (Top-Gruppe) auf **Bearbeiten**.
5) Klicken Sie auf **Daten löschen**.
6) Klicken Sie auf **OK**, um das Löschen zu bestätigen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Anmerkung: Für Applikationen bei denen die CSTA-Schnittstelle (UC, OSCC, usw.) verwendet wird: Wenn ein Chef/Sekretär, eine Top-Gruppe oder ein Mitglied einer Chef/Sekretär- oder Top-Gruppe gelöscht wird, ist ein Neustart des Systems erforderlich.

Zugehörige Konzepte

Chef/Sekretär / Top-Gruppe auf Seite 716

15.2.4 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Experten-Modus

Neben den Konfigurationsmöglichkeiten über Wizards stehen einem Administrator mit dem Profil **Expert** zusätzliche Möglichkeiten zur Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über den **Experten-Modus** zur Verfügung.

Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den **Experten-Modus** eingerichtet werden können:

- Wie Sie ein Mitglied zur Teamschaltung / Team-Gruppe hinzufügen oder löschen
- Wie Sie ein Mitglied einer Teamschaltung / Team-Gruppe ändern
- Wie Sie die Eigenschaften der Mitglieder einer Teamschaltung / Team-Gruppe ändern
- Wie Sie die Telefon-Tastenbelegung für Teamschaltung / Team-Gruppe ändern
- Wie Sie eine Faxbox zur Teamschaltung / Team-Gruppe hinzufügen
- Wie Sie ein Mitglied zur Chef/Sekretär / Top-Gruppe hinzufügen oder löschen
- Wie Sie ein Mitglied einer Chef/Sekretär / Top-Gruppe ändern

- Wie Sie die Eigenschaften der Mitglieder einer Chef/Sekretär / Top-Gruppe ändern
- Wie Sie eine Faxbox zur Chef/Sekretär / Top-Gruppe hinzufügen

15.2.4.1 Wie Sie ein Mitglied zur Teamschaltung / Team-Gruppe hinzufügen oder löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Tipp: Mit dem Wizard **Teamschaltung** kann ein Administrator mit dem Profil **Advanced** bis zu drei Mitglieder (Telefone) für eine Teamschaltung (Team-Gruppe) definieren. Zusätzliche Mitglieder muss ein Administrator mit dem Profil **Expert** über den **Experten-Modus** hinzufügen (siehe folgende Beschreibung).

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zur Team-Gruppe (Teamschaltung) hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zur gewünschten Team-Gruppe (Teamschaltung). Klicken Sie auf die Registerkarte **Team/Top Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Typ** den Teilnehmer-Typ aus. Wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
   - Wenn Sie ein Mitglied aus der Team-Gruppe (Teamschaltung) entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zum gewünschten Mitglied der Team-Gruppe (Teamschaltung) ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Team/Top Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712

15.2.4.2 Wie Sie ein Mitglied einer Teamschaltung / Team-Gruppe ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zum gewünschten Mitglied der Team-Gruppe (Teamschaltung) ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Team/Top Mitglied ändern**.
5) Ändern Sie die gewünschten Parameter.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712

15.2.4.3 Wie Sie die Eigenschaften der Mitglieder einer Teamschaltung / Team-Gruppe ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zum gewünschten Mitglied der Team-Gruppe (Teamschaltung) ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Team/Top Gruppen-Parameter ändern**.
5) Ändern Sie die gewünschten Eigenschaften.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712

15.2.4.4 Wie Sie die Telefon-Tastenbelegung für Teamschaltung / Team-Gruppe ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zur gewünschten Team-Gruppe (Teamschaltung).
4) Klicken Sie auf die Registerkarte **Team/Top Gruppe ändern**.

5) Wählen Sie eine Vorgabe für die Tastenbelegung aus:
   - Wenn die Tasten auf dem ersten oder zweiten Beistellgerät eingerichtet werden sollen, aktivieren Sie das Kontrollkästchen **auf erste /zweite Konsole**.
   - Wenn die Tasten auf den ersten freien Funktionstasten des Telefons eingerichtet werden sollen, aktivieren Sie das Kontrollkästchen **auf erste freie Tasten**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712

15.2.4.5 Wie Sie eine Faxbox zur Teamschaltung / Team-Gruppe hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zur gewünschten Team-Gruppe (Teamschaltung).
4) Klicken Sie auf die Registerkarte **Fax Box hinzufügen**.
5) Geben Sie im Feld **Fax Rufnr.** des gewünschten Mitglieds der Team-Gruppe (Teamschaltung) die interne Rufnummer der Faxbox ein.
6) Geben Sie im Feld **Fax DuWa** des gewünschten Mitglieds der Team-Gruppe (Teamschaltung) die Durchwahlnummer der Faxbox ein.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Teamschaltung / Team-Gruppe auf Seite 712

15.2.4.6 Wie Sie ein Mitglied zur Chef/Sekretär / Top-Gruppe hinzufügen oder löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Tipp: Mit dem Wizard **Chef / Sekretär** kann ein Administrator mit dem Profil **Advanced** bis zu zwei Chefs und bis zu zwei Sekretäre pro Chef/Sekretär-Konfiguration (Top-Gruppe) definieren. Zusätzliche Mitglieder muss ein Administrator mit dem Profil **Expert** über den **Experten-Modus** hinzufügen (siehe folgende Beschreibung).

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zur Top-Gruppe (Chef/Sekretär-Konfiguration) hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zur gewünschten Top-Gruppe (Chef/Sekretär-Konfiguration). Klicken Sie auf die Registerkarte **Team/Top Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Typ** den Teilnehmer-Typ aus. Wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
   - Wenn Sie ein Mitglied aus der Top-Gruppe (Chef/Sekretär-Konfiguration) entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zum gewünschten Mitglied der Top-Gruppe (Chef/Sekretär-Konfiguration) ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Team/Top Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Zugehörige Konzepte

Chef/Sekretär / Top-Gruppe auf Seite 716

15.2.4.7 Wie Sie ein Mitglied einer Chef/Sekretär / Top-Gruppe ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zum gewünschten Mitglied der Top-Gruppe (Chef/Sekretär-Konfiguration) ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Team/Top Mitglied ändern**.
5) Ändern Sie die gewünschten Parameter.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Chef/Sekretär / Top-Gruppe auf Seite 716

15.2.4.8 Wie Sie die Eigenschaften der Mitglieder einer Chef/Sekretär / Top-Gruppe ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zum gewünschten Mitglied der Top-Gruppe (Chef/Sekretär-Konfiguration) ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Team/Top Gruppen-Parameter ändern**.
5) Ändern Sie die gewünschten Eigenschaften.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Chef/Sekretär / Top-Gruppe auf Seite 716

15.2.4.9 Wie Sie eine Faxbox zur Chef/Sekretär / Top-Gruppe hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Team/Top** > **…** zur gewünschten Top-Gruppe (Chef/Sekretär-Konfiguration).
4) Klicken Sie auf die Registerkarte **Fax Box hinzufügen**.
5) Geben Sie im Feld **Fax Rufnr.** des gewünschten Mitglieds der Top-Gruppe (Chef/Sekretär-Konfiguration) die interne Rufnummer der Faxbox ein.
6) Geben Sie im Feld **Fax DuWa** des gewünschten Mitglieds der Top-Gruppe (Chef/Sekretär-Konfiguration) die Durchwahlnummer der Faxbox ein.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Chef/Sekretär / Top-Gruppe auf Seite 716

15.3 Basic-MULAP und Chef-MULAP

Eine Basic-MULAP ermöglicht einem Teilnehmer, der mehrere Telefone (zum Beispiel Festnetztelefon und Mobiltelefon) nutzt, unter einer Rufnummer erreichbar zu sein. Chef-MULAPs können eingerichtet werden, wenn eingeschränkte Chef- und Sekretär-Funktionen genutzt werden sollen.

15.3.1 Basis-MULAP

Basis-MULAPs können konfiguriert werden, wenn ein Teilnehmer mehrere verschiedene Telefone (z. B. Festnetztelefon und Mobiltelefon) verwendet, aber unter einer einzigen Telefonnummer (MULAP-Basistelefonnummer) erreicht werden möchte.

Klingelt ein Anrufer bei der MULAP-Basistelefonnummer, wird der Anruf an allen Telefonen, die zum Basis-MULAP gehören, optisch signalisiert. Der Abonnent kann auch einstellen, ob eingehende Anrufe auch für jedes einzelne Mitglied akustisch signalisiert werden sollen. Der Status der Basis-MULAP

ändert sich in besetzt und andere Anrufer hören das besetzt Signal, wenn ein Anruf angenommen wird.

Bei ausgehenden Anrufen über den MULAP-Basistrunk wird die MULAP-Basistelefonnummer auf dem Display des Angerufenen angezeigt.

Pro Basis-MULAP können bis zu 20 Mitglieder konfiguriert werden.

Jedem Basis-MULAP kann ein Name mit bis zu 16 Zeichen zugewiesen werden.

Jedes Telefon des Abonnenten ist Mitglied des Basis-MULAP und jedem Mitglied können die folgenden Eigenschaften zugewiesen werden:

- **Master**

  Dieser Parameter wandelt ein Mitglied in einen Master des Basis-MULAP um. Wenn ein Master die Anrufweiterleitung aktiviert, gilt diese Funktion für alle Mitglieder (Telefone) im Basis-MULAP. Aktiviert der Master einen automatischen Rückruf auf einem Basis-MULAP, wird der Rückruf initiiert, sobald alle Master frei sind.

  Ein Abonnent darf nicht mehr als 25-mal als MULAP Master in Sammelanschlüssen aufgenommen werden.

  Standardeinstellung: Master ist das erste Mitglied des Basis-MULAP.
- **Akustischer Ruf**

  Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert.

  Standardeinstellung: Der Parameter ist für alle Master aktiv.
- **Automatische Belegung gehend**

  Ist dieser Parameter aktiv, wird der MULAP-Basistrunk automatisch angerufen, wenn der Abonnent den Hörer abhebt. Bei nicht aktiviertem Parameter muss der Teilnehmer die MULAP-Taste betätigen, bevor er wählen kann.

  Standardeinstellung: Die automatische ausgehende Beschlagnahme wird allen Mastern zugewiesen.
- **Keine automatische Rufannahme kommend**

  Ist dieser Parameter aktiviert, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.

  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **Automatische Konferenzfreigabe**

  Bei aktiviertem Parameter wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen.

  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **MULAP-Taste eingerichtet**

  Bei aktiviertem Parameter wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Sie können die Taste drücken, um ein ausgehendes

Gespräch über den Basis-MULAP-Trunk aufzubauen. Auf dem Display des Angerufenen erscheint die MULAP-Basisnummer.

Standardeinstellung: Der Parameter ist aktiviert.

Anzeige von Nummer/Name

Beim Einrichten eines ausgehenden Anrufs wird eine Stationsnummer vergeben (lokale Stationsnummer oder MULAP-Gruppennummer).

Wenn ein eingehender MULAP-Anruf angenommen wird, wird die MULAP-Gruppennummer zugewiesen.

Bei Anrufen an eine MULAP:

- Bevor der Anruf angenommen wird, zeigt das Display des Anrufers den MULAP-Namen und/oder die MULAP-Nummer, die angerufen wird, an.
- Nach der Anrufannahme zeigt das Display des Anrufers den Sendernamen und/oder die MULAP-Nummer des Anrufers an.
- Bei Anrufen von einer MULAP-Station (MULAP-Taste oder Präferenz) zeigt die Anzeige der angerufenen und entgegennehmenden Parteien immer den Sendernamen und/oder die MULAP-Nummer an.
- Für ausgehende Anfälle gilt generell Folgendes: Wenn eine Station ein Gespräch mit der Ortsstationsnummer führt und die ausgehende Präferenz von der Ortsstationsnummer abweicht, zeigt das Display des angerufenen immer die Stationsnummer der ausgehenden Präferenz an.

MULAP-Tasten nutzen

Die LED auf einem MULAP-Schlüssel kann verschiedene Zustände haben, mit der folgenden Bedeutu:

- Aus: Die zugehörige Leitung ist frei und kann verwendet werden.
- Leuchtet: Die zugehörige Leitung ist belegt.
- Blinkt schnell: Anruf auf der zugehörigen Leitung.
- Langsam blinkt: Ein Warteruf wartet auf den entsprechenden Trunk oder der entsprechende Trunk wurde für eine Konferenz freigegeben.

Rufart

Für jedes Basis-MULAP kann ein Administrator mit dem **Expertenprofi** die akustische Signalisierung eingehender externer Anrufe über die Einstellung Klingeltyp festlegen. Sie haben folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

Bestellung der Mulap-Mitgliedsgeräte

SIP-Telefone können in ein Basis-MULAP integriert werden, solange ein TDM/HFA-Gerät als erstes Mitglied des Basis-MULAP definiert wurde. IP-Telefone können in ein Basis-MULAP integriert werden, solange ein TDM/HFA als erstes Mitglied des Basis-MULAP definiert wurde.

Eingebunden werden können beispielsweise Dual-Mode-Mobiltelefone, die als Mobility Entry-Teilnehmer eingerichtet sind. Dual-Modus-Mobiltelefone unterstützen sowohl GSM-/UMTS-Netzwerke als auch WLAN-Netzwerke. Über

WLAN ist die Registrierung eines Dual-Mode-Mobiltelefons als IP-Teilnehmer (SIP Client) am Kommunikationssystem möglich.

Mobilitätsbenutzer, einschließlich GSM Mobilitätsbenutzer, Unify Phone und Microsoft Teams Clients, können in ein Basis-MULAP integriert werden, sofern ein TDM/HFA Gerät als erstes Mitglied des Basis-MULAP definiert wurde.

Anmerkung: Die obige erweiterte Beschreibung gilt sowohl für OpenScape Business X als auch für OpenScape Business S-Systeme, beschränkt sich jedoch auf Team und Basis-Mulap und nicht auf Unterkapitel mit ähnlichen Anweisungen wie Exekutiv-/Sekretär-/Top-Gruppe.

Tipp: Für SIP-Telefone ist keine Programmierung von MULAP-Tasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Anzeigemeldungen der Basis-MULAP werden nicht unterstützt.

Abhängigkeiten

Themenbereich	Abhängigkeit
Anrufschutz	Wenn "Nicht stören" aktiviert ist, werden eingehende Anrufe nicht mehr durchgesetzt.
ISDN-Telefone	Es ist nicht möglich, ISDN-Telefone in Basis-MULAPs aufzunehmen.

Zugehörige Tasks

Basic-MULAP hinzufügen auf Seite 737
Wie Sie Basic-MULAP anzeigen oder ändern auf Seite 738
Wie Sie eine Basic-MULAP löschen auf Seite 738
Wie Sie ein Mitglied zur Basic-MULAP hinzufügen oder löschen auf Seite 739
Wie Sie ein Mitglied einer Basic-MULAP ändern auf Seite 739

15.3.2 Chef-MULAP

Chef-MULAPs können eingerichtet werden, wenn eingeschränkte Chef- und Sekretär-Funktionen genutzt werden sollen.

Alle Mitglieder einer Chef-MULAP sind unter der Chef-MULAP-Rufnummer sowie unter ihren eigenen Teilnehmerrufnummern erreichbar.

Tipp: In diesem Text steht "der Chef” stellvertretend sowohl für Chef als auch Chefin und “der Sekretär” stellvertretend sowohl für Sekretär als auch Sekretärin.

Bis zu 20 Mitglieder pro Chef-MULAP können eingerichtet werden.

Jeder Chef-MULAP kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Über die nachfolgend beschriebenen Parameter wird definiert, welche Mitglieder einer Chef-MULAP Chef-Funktionen (Chef) und welche Sekretär-Funktionen (Sekretär) nutzen können.

Wählt ein Anrufer die Chef-MULAP-Rufnummer, wird der Anruf bei allen zur Chef-MULAP gehörenden Telefonen optisch signalisiert. Bei Mitgliedern mit Sekretär-Funktionen werden ankommende Anrufe auch akustisch signalisiert.

Bei gehenden Anrufen über die Chef-MULAP-Leitung wird den Angerufenen die Chef-MULAP-Rufnummer im Display angezeigt.

Den Mitgliedern einer Chef-MULAP können folgende Eigenschaften zugewiesen werden:

- **Master**

  Durch diesen Parameter werden einem Mitglied Chef-Funktionen zugewiesen. Beim Abheben des Hörers wird automatisch über die Chef-MULAP-Leitung gerufen. Ankommende Anrufe über Chef-MULAP-Rufnummer werden ausschließlich optisch signalisiert.

  Ein Teilnehmer darf als MULAP-Master in Sammelanschlüssen nicht mehr als 25 mal aufgenommen werden.

  Standardeinstellung: Chef-Funktionen erhält das erste Mitglied der Chef-MULAP.
- **Akustischer Ruf**

  Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert.

  Standardeinstellung: Der Parameter ist für alle Mitglieder mit Sekretär-Funktion aktiviert.
- **Automatische Belegung gehend**

  Ist dieser Parameter aktiviert, wird beim Abheben des Hörers automatisch über die Chef-MULAP-Leitung gerufen. Bei nicht aktiviertem Parameter muss der Teilnehmer die MULAP-Taste betätigen, bevor er wählen kann.

  Dieser Parameter kann nicht von Mitgliedern mit Sekretär-Funktion genutzt werden.

  Standardeinstellung: Der Parameter ist für alle Mitglieder mit Chef-Funktion aktiviert.
- **Keine automatische Rufannahme kommend**

  Ist dieser Parameter aktiviert, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.

  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **Automatische Konferenzfreigabe**

  Bei aktiviertem Parameter wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen.

  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **MULAP-Taste eingerichtet**

  Bei aktiviertem Parameter wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf

über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt.

Standardeinstellung: Der Parameter ist aktiviert.

MULAP-Tasten nutzen

Die LED einer MULAP-Taste hat folgende Bedeutung:

- Aus: Die zugehörige Leitung ist frei und kann verwendet werden.
- Leuchtet: Die zugehörige Leitung ist belegt.
- Blinkt schnell: Anruf auf der zugehörigen Leitung.
- Blinkt langsam: Ein gehaltenes Gespräch wartet auf der zugehörigen Leitung oder die zugehörige Leitung wurde für eine Konferenz freigegeben.

Rufart

Für jede Chef-MULAP kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Sie haben folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Chef-MULAP ist möglich. Voraussetzung dafür ist, dass ein Systemtelefon (z. B. HFA oder UP0-Telefon) als erstes Mitglied der Chef-MULAP (Chef 1) definiert wird.

Eingebunden werden können beispielsweise Dual-Mode-Mobiltelefone, die als Mobility Entry-Teilnehmer eingerichtet sind. Dual-Mode-Mobiltelefone unterstützen sowohl GSM/UMTS-Netze als auch WLAN-Netze. Über WLAN ist die Registrierung eines Dual-Mode-Mobiltelefons als IP-Teilnehmer (SIP Client) am Kommunikationssystem möglich.

Tipp: Bei SIP-Telefonen ist keine Programmierung von MULAP-Tasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen der Chef-MULAP werden nicht unterstützt.

Abhängigkeiten

Themenbereich	Abhängigkeit
Anrufschutz	Nach Aktivierung des Anrufschutzes, werden ankommende Anrufe nicht durchgestellt.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Chef-MULAPs ist nicht möglich.

Zugehörige Tasks

Chef-MULAP hinzufügen auf Seite 740

Wie Sie eine Chef-MULAP anzeigen oder ändern auf Seite 740
Wie Sie eine Chef-MULAP löschen auf Seite 741
Wie Sie ein Mitglied zur Chef-MULAP hinzufügen oder löschen auf Seite 741
Wie Sie ein Mitglied einer Chef-MULAP ändern auf Seite 742

15.3.3 Konfiguration von Basic-MULAPs und Chef-MULAPs

Die Konfiguration von Basic-MULAPs und von Chef-MULAPs ist ausschließlich durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** möglich.

Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den **Experten-Modus** eingerichtet werden können:

- Wie Sie eine Basic-MULAP hinzufügen
- Wie Sie Basic-MULAP anzeigen oder ändern
- Wie Sie eine Basic-MULAP löschen
- Wie Sie ein Mitglied zur Basic-MULAP hinzufügen oder löschen
- Wie Sie ein Mitglied einer Basic-MULAP ändern
- Wie Sie eine Chef-MULAP hinzufügen
- Wie Sie eine Chef-MULAP anzeigen oder ändern
- Wie Sie eine Chef-MULAP löschen
- Wie Sie ein Mitglied zur Chef-MULAP hinzufügen oder löschen
- Wie Sie ein Mitglied einer Chef-MULAP ändern

15.3.3.1 Basic-MULAP hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Klicken Sie im Menübaum auf **Kommende Rufe** > **Gruppen-/ Sammelanschluss**.
4) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer der neuen Basic-MULAP ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der neuen Basic-MULAP ein.

: Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

---

7) Geben Sie in den Feldern **Vorname** und **Nachname** den Namen der neuen Basic-MULAP ein.
8) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Basic-MULAP** aus.

9) Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des Teilnehmers aus, der der Gruppe „Basic-MULAP“ zugeordnet werden soll.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Anmerkung: Wenn in Anwendungen mit CSTA-Schnittstelle (UC, OSCC usw.) eine Gruppe „Basic-MULAP“ oder ein Mitglied einer Gruppe „Basic-MULAP“ erstellt wird, ist ein Systemneustart erforderlich.

Zugehörige Konzepte

Basis-MULAP auf Seite 731

15.3.3.2 Wie Sie Basic-MULAP anzeigen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Basic-MULAP.
4) Klicken Sie auf die Registerkarte **Gruppen-Parameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppen-Parameter angezeigt.
5) Ändern Sie bei Bedarf die gewünschten Parameter der Basic-MULAP.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Basis-MULAP auf Seite 731

15.3.3.3 Wie Sie eine Basic-MULAP löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Basic-MULAP.
4) Klicken Sie auf die Registerkarte **Gruppe löschen**.
5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

Anmerkung: Für Applikationen bei denen die CSTA-Schnittstelle (UC, OSCC, usw.) verwendet wird: Wenn eine Basic-MULAP-Gruppe oder ein Basic-MULAP-

Gruppenmitglied gelöscht wird, ist ein Neustart des Systems erforderlich.

Zugehörige Konzepte

Basis-MULAP auf Seite 731

15.3.3.4 Wie Sie ein Mitglied zur Basic-MULAP hinzufügen oder löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zur Basic-MULAP hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Basic-MULAP. Klicken Sie auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
   - Wenn Sie ein Mitglied aus der Basic-MULAP entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Mitglied der Basic-MULAP ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Zugehörige Konzepte

Basis-MULAP auf Seite 731

15.3.3.5 Wie Sie ein Mitglied einer Basic-MULAP ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Mitglied der Basic-MULAP ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Mitglied ändern**.
5) Ändern Sie die gewünschten Parameter.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Basis-MULAP auf Seite 731

15.3.3.6 Chef-MULAP hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Klicken Sie im Menübaum auf **Kommende Rufe** > **Gruppen-/ Sammelanschluss**.
4) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer der neuen Chef-MULAP ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der neuen Chef-MULAP ein.

   : Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

7) Geben Sie in den Feldern **Vorname** und **Nachname** den Namen der neuen Chef-MULAP ein.
8) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Chef-MULAP** aus.
9) Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des Teilnehmers aus, der der Gruppe „Chef-MULAP“ zugeordnet werden soll.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Chef-MULAP auf Seite 734

15.3.3.7 Wie Sie eine Chef-MULAP anzeigen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Chef-MULAP.
4) Klicken Sie auf die Registerkarte **Gruppen-Parameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppen-Parameter angezeigt.
5) Ändern Sie bei Bedarf die gewünschten Parameter der Chef-MULAP.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Chef-MULAP auf Seite 734

15.3.3.8 Wie Sie eine Chef-MULAP löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Chef-MULAP.
4) Klicken Sie auf die Registerkarte **Gruppe löschen**.
5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

Anmerkung: Für Applikationen bei denen die CSTA-Schnittstelle (UC, OSCC, usw.) verwendet wird: Wenn eine Chef-MULAP-Gruppe oder ein Chef-MULAP-Gruppenmitglied gelöscht wird, ist ein Neustart des Systems erforderlich.

Zugehörige Konzepte

Chef-MULAP auf Seite 734

15.3.3.9 Wie Sie ein Mitglied zur Chef-MULAP hinzufügen oder löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zur Chef-MULAP hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Chef-MULAP. Klicken Sie auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
   - Wenn Sie ein Mitglied aus der Chef-MULAP entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Mitglied der Chef-MULAP ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Zugehörige Konzepte

Chef-MULAP auf Seite 734

15.3.3.10 Wie Sie ein Mitglied einer Chef-MULAP ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Mitglied der Basic-MULAP ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Mitglied ändern**.
5) Ändern Sie die gewünschten Parameter.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Chef-MULAP auf Seite 734

15.3.3.11 Basic-MULAP in Gruppe hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Klicken Sie im Menübaum unter **Kommende Rufe > Gruppen-/ Sammelanschluss** auf die gewünschte Basic-MULAP.
4) Klicken Sie auf die Registerkarte **Gruppenparameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppenparameter angezeigt.
5) Aktivieren Sie das Flag **Mulap als Gruppenmitglied**.
6) Klicken Sie im Menübaum unter **Kommende Rufe > Gruppen-/ Sammelanschluss** auf die gewünschte Gruppe, um eine Basic-MULAP als Mitglied in der Gruppe hinzuzufügen.
7) Klicken Sie auf die Registerkarte **Mitglied hinzufügen** und wählen Sie aus dem Aufklappmenü im Feld **Rufnummer** die Basic-MULAP aus.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Einschränkungen:

- Alle Mitglieder der Basic-MULAP müssen mit den Parametern M, R, A konfiguriert werden.
- Die maximale Anzahl der Gruppenmitglieder muss bis zu 20 betragen, einschließlich der Mitglieder der Basic-MULAP.

- Die Mitglieder der Basic-MULAP können nicht bereits Mitglieder der Gruppe sein.
- Es ist möglich, eine MULAP hinzuzufügen:

  1) Lineare Gruppennummer
  2) Zyklische Gruppennummer
  3) Gruppe
- Es ist nicht möglich, eine MULAP hinzuzufügen:

  1) Anklopfen
  2) RNA
- Eine Gruppe kann nicht in "Anklopfen" oder "Freifall" umgewandelt werden, wenn sie ein MULAP enthält.

15.4 Sprachbox-Gruppe und Faxbox-Gruppe

Durch eine Sprachbox-Gruppe (Anrufbeantworter-Gruppe) kann einer Teilnehmergruppe der Zugriff auf Sprachnachrichten ermöglicht werden. Über die Rufnummer der Sprachbox-Gruppe werden nicht die Mitglieder dieser Gruppe gerufen, sondern wird direkt die Sprachbox (der Anrufbeantworter) der Gruppe erreicht. Durch eine Faxbox-Gruppe (Faxgruppe) kann einer Teilnehmergruppe der Zugriff auf Faxnachrichten ermöglicht werden. Über die Rufnummer der Faxbox-Gruppe wird direkt die Faxbox der Gruppe erreicht.

15.4.1 Sprachbox-Gruppe

Durch eine Sprachbox-Gruppe (Anrufbeantworter-Gruppe) kann einer bestimmten Gruppe von Teilnehmern der Zugriff auf Sprachnachrichten ermöglicht werden. Über die Rufnummer der Sprachbox-Gruppe werden nicht die Mitglieder dieser Gruppe gerufen, sondern wird direkt die Sprachbox (der Anrufbeantworter) der Gruppe erreicht. Nachdem eine Sprachnachricht auf der Sprachbox der Gruppe hinterlassen wurde, erfolgt eine Weiterleitung an die Sprachboxen aller Mitglieder.

Alle Mitglieder erhalten die Sprachnachricht gleichzeitig. Löscht ein Mitglied der Gruppe eine Sprachnachricht, wird diese auch aus den Sprachboxen aller anderen Mitglieder und aus der Sprachbox der Gruppe gelöscht. Die persönlichen Sprachnachrichten aller Mitglieder bleiben davon unbeeinflusst.

Jedes Mitglied einer Sprachbox-Gruppe ist unter seiner eigenen Teilnehmerrufnummer erreichbar.

Bis zu 20 Mitglieder pro Sprachbox-Gruppe können eingerichtet werden.

Jeder Sprachbox-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Mindestens ein Teilnehmer einer Sprachbox-Gruppe benötigt eine VoiceMail-Lizenz.

Abhängigkeiten

Thema	Abhängigkeit
Rufzuschaltung	Die Nutzung des Leistungsmerkmals *Rufzuschaltung* ist nicht möglich.

Zugehörige Tasks

Wie Sie eine Sprachbox-Gruppe hinzufügen auf Seite 745
Wie Sie eine Sprachbox-Gruppe anzeigen oder ändern auf Seite 745
Wie Sie eine Sprachbox-Gruppe löschen auf Seite 746
Wie Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen oder löschen auf Seite 746
Wie Sie ein Mitglied einer Sprachbox-Gruppe ändern auf Seite 746

15.4.2 Faxbox-Gruppe

Durch eine Faxbox-Gruppe (Faxgruppe) kann einer bestimmten Gruppe von Teilnehmern der Zugriff auf Faxnachrichten ermöglicht werden. Über die Rufnummer der Faxbox-Gruppe wird direkt die Faxbox der Gruppe erreicht. Nachdem eine Faxnachricht auf der Faxbox der Gruppe hinterlassen wurde, erfolgt eine Weiterleitung an die Faxboxen aller Mitglieder.

Alle Mitglieder erhalten die Faxnachricht gleichzeitig. Löscht ein Mitglied der Gruppe eine Faxnachricht, wird diese auch aus den Faxboxen aller anderen Mitglieder und aus der Faxbox der Gruppe gelöscht.

Jedes Mitglied einer Faxbox-Gruppe ist unter seiner eigenen Teilnehmerrufnummer erreichbar.

Bis zu 20 Faxbox-Gruppen können eingerichtet werden.

Jeder Faxbox-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Mindestens ein Teilnehmer einer Faxbox-Gruppe benötigt eine Fax-Lizenz.

Zugehörige Tasks

Faxbox-Gruppe konfigurieren auf Seite 747
Wie Sie eine Faxbox-Gruppe anzeigen oder ändern auf Seite 748
Mitglied zur Faxbox-Gruppe hinzufügen oder löschen auf Seite 748

15.4.3 Konfiguration von Sprachbox-Gruppen und Faxbox-Gruppen

Die Konfiguration von Sprachbox-Gruppen und von Faxbox-Gruppen ist ausschließlich durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** möglich.

Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den **Experten-Modus** eingerichtet werden können:

- Wie Sie eine Sprachbox-Gruppe hinzufügen
- Wie Sie eine Sprachbox-Gruppe anzeigen oder ändern
- Wie Sie eine Sprachbox-Gruppe löschen
- Wie Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen oder löschen
- Wie Sie ein Mitglied einer Sprachbox-Gruppe ändern
- Wie Sie eine Faxbox-Gruppe konfigurieren
- Wie Sie eine Faxbox-Gruppe anzeigen oder ändern
- Wie Sie eine Faxbox-Gruppe löschen
- Wie Sie ein Mitglied zur Faxbox-Gruppe hinzufügen oder löschen

15.4.3.1 Wie Sie eine Sprachbox-Gruppe hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Klicken Sie im Menübaum auf **Kommende Rufe** > **Gruppen-/ Sammelanschluss**.
4) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer der neuen Sprachbox-Gruppe ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der neuen Sprachbox-Gruppe ein.

   : Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

7) Geben Sie im Feld **Name** den Namen der neuen Sprachbox-Gruppe ein.
8) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Anrufbeantworter** aus.
9) Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des Teilnehmers aus, der der neuen Sprachbox-Gruppe zugeordnet werden soll.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Sprachbox-Gruppe auf Seite 743

15.4.3.2 Wie Sie eine Sprachbox-Gruppe anzeigen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Sprachbox-Gruppe.
4) Klicken Sie auf die Registerkarte **Gruppen-Parameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppen-Parameter angezeigt.
5) Ändern Sie bei Bedarf die gewünschten Parameter der Sprachbox-Gruppe.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Sprachbox-Gruppe auf Seite 743

15.4.3.3 Wie Sie eine Sprachbox-Gruppe löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Sprachbox-Gruppe.
4) Klicken Sie auf die Registerkarte **Gruppe löschen**.
5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

Zugehörige Konzepte

Sprachbox-Gruppe auf Seite 743

15.4.3.4 Wie Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen oder löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zur gewünschten Sprachbox-Gruppe. Klicken Sie auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
   - Wenn Sie ein Mitglied aus der Sprachbox-Gruppe entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Mitglied der Sprachbox-Gruppe ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Zugehörige Konzepte

Sprachbox-Gruppe auf Seite 743

15.4.3.5 Wie Sie ein Mitglied einer Sprachbox-Gruppe ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **Gruppen-/ Sammelanschluss** > **…** zum gewünschten Mitglied der Sprachbox-Gruppe ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Mitglied ändern**.
5) Ändern Sie die gewünschten Parameter.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Sprachbox-Gruppe auf Seite 743

15.4.3.6 Faxbox-Gruppe konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer** > **UC Applications** > **Fax-Gruppe**. Angezeigt werden die bereits konfigurierten Faxbox-Gruppen.
4) Wählen Sie die nächste freie Reihe aus und geben Sie im Feld **Rufnummer** die Rufnummer der neuen Faxbox-Gruppe ein.
5) Geben Sie im Feld **Durchwahl** die Durchwahlnummer der neuen Faxbox-Gruppe ein.

   : Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

   ---

6) Geben Sie im Feld **Name** den Namen der neuen Faxbox-Gruppe ein.
7) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Fax-Gruppe** aus.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
9) Schließen Sie das Fenster **Fax-Gruppe**.
10) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
11) Klicken Sie auf **Gruppen**.
12) Klicken Sie auf die Registerkarte **Fax-Gruppe**.
13) Markieren Sie die neue Faxbox-Gruppe und klicken Sie auf **Bearbeiten**.
14) Wählen Sie eine der folgenden Optionen:
    - Wenn Sie ein Mitglied zur Faxbox-Gruppe hinzufügen möchten, markieren Sie das gewünschte Mitglied in der Liste **Benutzer**.
    - Wenn Sie mehrere Mitglieder zur Faxbox-Gruppe hinzufügen möchten, drücken Sie <Strg> und markieren Sie die gewünschten Mitglieder in der Liste **Benutzer**.

15) Klicken Sie auf **Speichern**.

Zugehörige Konzepte

Faxbox-Gruppe auf Seite 744

15.4.3.7 Wie Sie eine Faxbox-Gruppe anzeigen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer** > **UC Applications** > **Fax Gruppe**.
4) Klicken Sie im Menübaum auf die gewünschte Faxbox-Gruppe.
5) Klicken Sie auf die Registerkarte **Teilnehmer-Parameter ändern**.
6) Ändern Sie bei Bedarf die gewünschten Parameter der Faxbox-Gruppe.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Zugehörige Konzepte

Faxbox-Gruppe auf Seite 744

15.4.3.8 Faxbox-Gruppe löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Gruppen**.
4) Klicken Sie auf die Registerkarte **Fax-Gruppe**.
5) Markieren Sie die gewünschte Faxbox-Gruppe und klicken Sie auf **Entfernen**.

15.4.3.9 Mitglied zur Faxbox-Gruppe hinzufügen oder löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Gruppen**.
4) Klicken Sie auf die Registerkarte **Fax-Gruppe**.
5) Markieren Sie die gewünschte Faxbox-Gruppe und klicken Sie auf **Bearbeiten**. Angezeigt wird die Liste **Benutzer**, in der die bereits vorhandenen Mitglieder markiert sind.
6) Wählen Sie eine der folgenden Optionen:
   - Wenn Sie ein Mitglied zur Faxbox-Gruppe hinzufügen möchten, drücken Sie <Strg> und markieren Sie das neue Mitglied, zusätzlich zu den bereits vorhandenen Mitgliedern, in der Liste **Benutzer**.
   - Wenn Sie ein Mitglied aus der Faxbox-Gruppe entfernen möchten, drücken Sie <Strg> und entfernen Sie die Markierung des gewünschten Mitglieds in der Liste **Benutzer**.
7) Klicken Sie auf **Speichern**.

Zugehörige Konzepte

Faxbox-Gruppe auf Seite 744

15.5 Direktansprechen für Gruppen

Direktansprechen für Gruppen ermöglicht Durchsagen an die internen Teilnehmer einer Gruppe.

15.5.1 Durchsage an Gruppe

Durchsage an Gruppe ermöglicht das Direktansprechen von internen Teilnehmern einer Gruppe. Dieses Leistungsmerkmal wird auch als "Paging Intern" bezeichnet. Gruppenmitglieder, die besetzt sind oder den Anrufschutz aktiviert haben, empfangen Paging Intern nicht. Für die gerufenen Gruppenmitglieder besteht keine Möglichkeit einer Direktantwort. Das Antworten ist nur durch Abheben des Hörers möglich, wodurch der Übergang zu einem normalen Zweiergespräch erfolgt.

Durchsage an Gruppe kann mittels einer dafür programmierten Funktionstaste oder über den Menüeintrag **Direktansprechen** oder die zugehörige Kennzahl und anschließender Wahl der Rufnummer der Zielgruppe genutzt werden. Eine Funktionstaste kann auch inklusive einer Gruppenrufnummer programmiert werden. Nach Betätigung einer solchen Funktionstaste erfolgt der sofortige Verbindungsaufbau zur programmierten Gruppe.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz	Gruppenmitglieder mit aktiviertem Anrufschutz erhalten keine Durchsage.

Thema	Abhängigkeit
ISDN-Telefone, SIP-Telefone	Das Leistungsmerkmal "Durchsage an Gruppe (Paging Intern)" kann nicht mit ISDN- oder SIP-Telefonen genutzt werden.

15.5.2 Übergabe an Gruppe aus Durchsage

Ein in Rückfrage befindliches Gespräch kann durch Übergabe aus Durchsage an eine Gruppe übergeben werden. Dazu wird eine Durchsage an die Gruppe gestartet (Paging Intern). Sobald ein Teilnehmer der Gruppe den Hörer abhebt oder den Lautsprecher aktiviert und der übergebende Teilnehmer auflegt, besteht eine Zweierverbindung. Für die anderen Gruppenmitglieder wird die Verbindung getrennt.

Durchsage an Gruppe kann mittels einer dafür programmierten Funktionstaste oder über den Menüeintrag **Direktansprechen** oder die zugehörige Kennzahl und anschließender Wahl der Rufnummer der Zielgruppe genutzt werden. Eine Funktionstaste kann auch inklusive einer Gruppenrufnummer programmiert werden. Nach Betätigung einer solchen Funktionstaste erfolgt der sofortige Verbindungsaufbau zur programmierten Gruppe.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz	Gruppenmitglieder mit aktiviertem Anrufschutz erhalten keine Durchsage.
ISDN-Telefone, SIP-Telefone	Das Leistungsmerkmal "Übergabe an Gruppe aus Durchsage" kann nicht mit ISDN- oder SIP-Telefonen genutzt werden.

15.6 Anrufverteilung (UCD Uniform Call Distribution)

Durch das Leistungsmerkmal "Uniform Call Distribution UCD" ermöglicht das Kommunikationssystem eine gleichmäßige Verteilung von eingehenden Anrufen auf eine Gruppe von Teilnehmern (UCD-Gruppe).

UCD-Gruppen werden vor allem im Umfeld von technischen Hotlines (zum Beispiel Kundendienst-Hotline), beim Beschwerde-Management, in der Marktforschung, Auftrags- und Bestellannahme (z.B. Versandhäuser, Ticket Service) oder auch für Notfall-Services eingesetzt.

Im Regelfall erfolgt die Anrufverteilung so, dass ein kommender Anruf an eine UCD-Gruppe an denjenigen Teilnehmer in der Gruppe (Agent) weitergeleitet wird, dessen letztes Gespräch am längsten zurückliegt. Es ist ebenfalls möglich andere Verteilungsregeln festzulegen.

Ist kein Agent frei, um einen kommenden Anruf entgegenzunehmen, wird der Anruf automatisch an eine Warteschlange (Queue) weitergeleitet. In Abhängigkeit von Priorität und Wartezeit werden die wartenden Anrufe an die frei werdenden Agenten verteilt.

Anrufern, die sich im Wartezustand befinden, können Ansagen oder Musik eingespielt werden.

Konfiguration

Mit dem Wizard **Anrufverteilung** können Sie die Gruppen und Teilnehmer für eine intelligente Anrufverteilung (UCD) konfigurieren. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- Wie Sie eine Anrufverteilung / UCD-Gruppen konfigurieren
- Wie Sie UCD-Agenten hinzufügen oder löschen
- Wie Sie Ansagen / Wartemusik bei UCD ändern

Neben den Konfigurationsmöglichkeiten über Wizards stehen einem Administrator mit dem Profil **Expert** zusätzliche Möglichkeiten zur Konfiguration über den **Experten-Modus** zur Verfügung.

15.6.1 Anrufverteilung / UCD-Gruppe

Eine UCD-Gruppe enthält Agenten (Teilnehmer), die zu einer Arbeitsgruppe gehören und unter einer Rufnummer zu erreichen sind. Ein ankommender interner oder externer Anruf wird automatisch dem Agenten zugeteilt, der sich am längsten in Ruhe befindet.

Jede UCD-Gruppe kann über das WBM (**Experten-Modus**) so konfiguriert werden, dass Anrufe bei einem Agenten automatisch vom Kommunikationssystem angenommen werden (Automatic Incoming Call Connection AICC).

Sind alle Agenten einer UCD-Gruppe belegt, können kommende Anrufe in eine Warteschlange eingetragen werden. Für jede UCD-Gruppe kann die maximale Anzahl der Anrufe in der Warteschlange individuell festlegt werden. Wird die maximale Anzahl der wartenden Anrufe überschritten, können die weiteren Anrufe an ein Überlaufziel (ein externes Ziel, eine andere UCD-Gruppe, ein interner Teilnehmer oder eine Gruppe) geleitet werden.

Ist das Überlaufziel eine andere UCD-Gruppe und sind auch alle Agenten dieser UCD-Gruppe belegt, bleibt der Anruf in der Warteschlange der ursprünglichen Gruppe und wird darüber hinaus in die Warteschlange der anderen UCD-Gruppe (Überlaufziel) eingereiht.

Wartenden Anrufern können Ansagen oder Musik eingespielt werden.

Jeder UCD-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Abhängigkeiten

Thema	Abhängigkeit
Anrufumleitung	In folgenden Fällen wird der Anrufumleitung zu einer UCD-Gruppe nicht gefolgt: • Wird ein Sammelanschluss gerufen und ein Teilnehmer mit einer Anrufumleitung zu einer UCD-Gruppe ist an der Reihe, wird nicht der Anrufumleitung gefolgt. In diesem Fall wird direkt der nächste Teilnehmer des Sammelanschlusses gerufen. • Ein Teilnehmer ist Mitglied eines Gruppenrufs mit der Eigenschaft “Gruppe” und hat eine Anrufumleitung zu einer UCD-Gruppe aktiviert. • Ein Teilnehmer ist Mitglied eines Gruppenrufs im Freifall. Wird die Gruppe gerufen, wird nicht der Anrufumleitung zur UCD-Gruppe gefolgt. Ausnahme: Der erste eingetragene Teilnehmer hat eine Anrufumleitung zu einer UCD-Gruppe aktiviert. Dieser Anrufumleitung wird gefolgt.

15.6.1.1 Wie Sie eine Anrufverteilung / UCD-Gruppen konfigurieren

Mit dem Wizard **Anrufverteilung** können Sie eine intelligente Anrufverteilung auf eine Gruppe mit ausgewählten Teilnehmern konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UCD** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.
4) Um eine UCD-Gruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer der UCD-Gruppe ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der UCD-Gruppe ein.

: Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

---

7) Geben Sie im Feld **Name** den Namen der UCD-Gruppe ein.
8) Klicken Sie auf **OK & Weiter**. Das Fenster **Zuweisung der UCD-Agenten** wird angezeigt.
9) Markieren Sie die gewünschten UCD-Agenten-IDs in der **Auswahl** und weisen Sie diese der UCD-Gruppe durch Klicken auf **Hinzufügen** zu.

10) Klicken Sie auf **OK & Weiter**. Das Fenster **Ansagen / Überlauf bearbeiten** wird angezeigt.
11) Wählen Sie in der Aufklappliste **Ansageeinrichtungen** die Ansageeinrichtung der UCD-Gruppe aus. Sie haben die Möglichkeit, eine Ansage (falls eingerichtet) oder die interne Wartemusik (Music On Hold MOH) auszuwählen. Nach Auswahl der Ansageeinrichtung erscheint das Feld **Ansageverzögerung**.
12) Geben Sie im Feld **Ansageverzögerung** die Zeit in Sekunden ein, nach der ein Anrufer in der Warteschlange eine Ansage erhalten soll.
13) Wählen Sie in der Aufklappliste **Zeit bis zum Ruf des nächsten Agenten** die Zeit aus, nach der ein Anruf an den nächsten UCD-Agenten der UCD-Gruppe weitergegeben werden soll.
14) Wählen Sie in der Aufklappliste **Überlauf-Ziel** das Überlauf-Ziel der UCD-Gruppe aus. Sie haben die Möglichkeit ein externes Ziel, eine andere UCD-Gruppe, einen internen Teilnehmer oder eine Gruppe auszuwählen.

    Wenn Sie **Externes Ziel** als Überlauf-Ziel auswählen, erscheint das Feld **Externes Ziel** und die Aufklappliste **Richtung**.

    a) Geben Sie in das Feld **Externes Ziel** die Rufnummer des externen Überlauf-Ziels ein.
    b) Wenn das externe Überlaufziel über eine bestimmte Richtung erreicht werden soll, wählen Sie die gewünschte Richtung in der Aufklappliste **Richtung** aus.
15) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.
16) Wenn Sie weitere UCD-Gruppen konfigurieren möchten, wiederholen Sie die Schritte 4 bis 15.
17) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

15.6.2 UCD-Agenten

Die Teilnehmer einer UCD-Gruppe (Agenten) bilden eine Arbeitsgruppe, die zum Beispiel bei technischen Hotlines oder in der Auftrags- und Bestellannahme zum Einsatz kommen kann. Alle kommenden Anrufe werden gleichmäßig auf die verfügbaren Teilnehmer einer UCD-Gruppe verteilt.

Die Zuordnung der Agenten zu den UCD-Gruppen erfolgt über Kennungen (IDs). Eine ID kann maximal einer UCD-Gruppe zugeordnet werden. Einem Agenten können mehrere IDs zugewiesen werden. Dadurch wird einem Agenten ermöglicht, in mehr als einer UCD-Gruppe zu arbeiten. Ein Agent kann jedoch nur in jeweils einer UCD-Gruppe angemeldet und damit aktiv sein.

Um die UCD-Funktionen effektiv nutzen zu können, sollten Agenten über Telefone mit Display, Funktionstasten und Headset verfügen.

Anmelden / Abmelden

Ein Agent kann sich mittels seiner ID (Kennung) an jedem Telefon (außer ISDN- und SIP-Telefonen) des Kommunikationssystems anmelden. Nach erfolgreicher Anmeldung ist der Agent verfügbar und bis zu seiner Abmeldung permanent dem betreffenden Telefon zugeordnet. Eine weitere Anmeldung an einem anderen Telefon ist nicht möglich. Nach seiner Abmeldung wird der Agent von der Anrufverteilung nicht mehr berücksichtigt.

Die UCD-Funktionen Anmelden, Abmelden und Änderung des Teilnehmerzustands können die Agenten am Telefon über dafür programmierte

Funktionstasten oder über die zugehörigen Menüeinträge oder über Kennzahlen aufrufen.

Teilnehmerzustände

Nach erfolgreicher Anmeldung befindet sich ein Agent im Teilnehmerzustand **verfügbar**. Bei Bedarf kann ein Agent selbst einen anderen Teilnehmerzustand einstellen oder der Teilnehmerzustand ändert sich automatisch, in Abhängigkeit von der Agententätigkeit. Der jeweils aktuelle Teilnehmerzustand wird im Display des Telefons angezeigt.

Folgende Anzeigen sind möglich:

Anzeige	Bedeutung
Verfügbar	Der Agent ist verfügbar und kann UCD-Anrufe annehmen.
Nicht verfügbar	Der Agent hat sich kurzfristig von seinem Arbeitsplatz abgemeldet (zum Beispiel für eine Pause).
Nachbearbeitung	Der Agent befindet sich in der Nachbearbeitungszeit. Innerhalb der Nachbearbeitungszeit erhält er keine UCD-Anrufe. Je nach Konfiguration kann es sich dabei um eine individuelle Nachbearbeitungszeit (Der Agent selbst bestimmt die Länge der Nachbearbeitungszeit durch Änderung seines Teilnehmerzustands.) oder um eine automatische Nachbearbeitungszeit (Allen Agenten steht nach einem UCD-Anruf automatisch eine Nachbearbeitungszeit zur Verfügung.) handeln.
für <UCD-Gruppenname>	Der Agent erhält einen UCD-Anruf.

Nach Ende der Arbeitszeit meldet sich ein Agent ab und steht damit für UCD-Anrufe nicht mehr zur Verfügung. Er kann weiterhin über seine persönliche Teilnehmerrufnummer erreicht werden.

Befinden sich alle Agenten einer UCD-Gruppe im Teilnehmerzustand **nicht verfügbar**, erfolgt eine Rufweiterschaltung der kommenden Anrufe an ein Überlaufziel (ein externes Ziel, eine andere UCD-Gruppe, ein interner Teilnehmer oder eine Gruppe).

Nimmt ein Agent einen Anruf nicht an, obwohl er angemeldet und verfügbar ist, wird er vom Kommunikationssystem automatisch in den Teilnehmerzustand **nicht verfügbar** versetzt.

Abhängigkeiten

Thema	Abhängigkeit
Anrufumleitung	Aktiviert ein Agent das Leistungsmerkmal "Anrufumleitung", wird er automatisch abgemeldet und steht damit für UCD-Anrufe nicht mehr zur Verfügung.
ISDN-Telefone, SIP-Telefone	Die Nutzung von ISDN- und SIP-Telefonen ist nicht möglich.

15.6.2.1 Wie Sie UCD-Agenten hinzufügen oder löschen

Mit dem Wizard **Anrufverteilung** können Sie UCD-Agenten zu einer UCD-Gruppe hinzufügen oder aus einer UCD-Gruppe löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UCD** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.
4) Für das Hinzufügen oder Löschen von UCD-Agenten einer UCD-Gruppe, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.
5) Klicken Sie auf **OK & Weiter**, um zum Fenster **Zuweisung der UCD-Agenten** zu gelangen.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie UCD-Agenten hinzufügen möchten, markieren Sie die gewünschten UCD-Agenten-IDs in der **Auswahl** und weisen Sie diese der UCD-Gruppe durch Klicken auf **Hinzufügen** zu.
   - Wenn Sie UCD-Agenten löschen möchten, markieren Sie die gewünschten **Mitglieder** und löschen Sie diese aus der UCD-Gruppe durch Klicken auf **Löschen**.
7) Klicken Sie auf **OK & Weiter**, um die Eingaben zu bestätigen.
8) Klicken Sie auf **OK**.
9) Wenn Sie die UCD-Agenten einer weiteren UCD-Gruppe ändern möchten, wiederholen Sie die Schritte 4 bis 8.
10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

15.6.3 Nachbearbeitung

Durch dieses Leistungsmerkmal wird ein Agent kurzzeitig von der Anrufverteilung ausgenommen, um Nacharbeiten für den soeben beendeten Anruf durchführen zu können. Innerhalb der Nachbearbeitungszeit erhält der Agent keine UCD-Anrufe.

Es wird unterschieden zwischen

- der individuellen Nachbearbeitungszeit

  Der Agent selbst bestimmt die Länge der Nachbearbeitungszeit durch Änderung seines Teilnehmerzustands.
- der automatischen Nachbearbeitungszeit

  Dafür wird das Leistungsmerkmal "Anrufverteilung (Uniform Call Distribution UCD)" so konfiguriert, dass allen Agenten aller UCD-Gruppen nach einem UCD-Anruf automatisch eine Nachbearbeitungszeit zur Verfügung steht. Die

Definition der automatischen Nachbearbeitungszeit erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten.

Ein Agent kann die automatische Nachbearbeitungszeit manuell verlängern, indem er seinen Teilnehmerzustand ändert.

Innerhalb der Nachbearbeitungszeit kann ein Agent weiterhin über seine persönliche Teilnehmerrufnummer erreicht werden.

15.6.3.1 Wie Sie die automatische Nachbearbeitungszeit ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Klicken Sie im Menübaum auf **Kommende Rufe** > **UCD**.
4) Klicken Sie auf die Registerkarte **UCD-Parameter ändern**.
5) Wählen Sie in der Aufklappliste **Nachbearbeitungszeit (Zyklen)** die Zeit aus, die allen UCD-Agenten zur Nachbearbeitung zur Verfügung stehen soll. Die Angabe erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.6.4 Priorisierte Anrufordnung

Kommende interne und externe Anrufe für eine UCD-Gruppe können mit einer Priorität versehen werden. Die in der Warteschlange wartenden Anrufe werden in Abhängigkeit von der Priorität und der Wartezeit den Agenten einer UCD-Gruppe zugeteilt.

Ein wartender Anruf mit hoher Priorität wird früher beantwortet, als ein länger wartender Anruf mit niedrigerer Priorität. Ein wartender Anruf mit niedriger Priorität wird früher an ein Überlaufziel geleitet, als ein wartender Anruf mit höherer Priorität.

Für externe Anrufe erfolgt die Prioritätsvergabe leitungsbezogen (pro B-Kanal), unabhängig davon, ob es sich um IP- oder TDM-Leitungen handelt.

Beispiele:

- Kommunikationssystem mit ISDN-Primärmultiplexanschluss (S_{2M}-Schnittstelle) und ISDN-Mehrgeräteanschluss (S_0-Schnittstelle)

  Bei den über den ISDN-Primärmultiplexanschluss eingehenden Anrufen handelt es sich um normale Kundenanrufe. Alle B-Kanäle der S_{2M}-Schnittstelle erhalten dementsprechend eine mittlere Priorität. Bei Anrufen über den ISDN-Mehrgeräteanschluss handelt es sich um dringende Anrufe, wie zum Beispiel eilige Ersatzteilbestellungen. Alle B-Kanäle der S_0-Schnittstelle erhalten dementsprechend eine hohe Priorität.

- Kommunikationssystem mit Anlagenanschluss zu einem Internet-Telefonie Service Provider ITSP und einem ISDN-Mehrgeräteanschluss (S_0-Schnittstelle)

  Bei den eingehenden Anrufen über die Anlagenrufnummer für die IP-Telefonie handelt es sich um normale Kundenanrufe. Alle B-Kanäle der LAN-Schnittstelle erhalten dementsprechend eine mittlere Priorität. Bei Anrufen über den ISDN-Mehrgeräteanschluss handelt es sich um dringende Anrufe, wie zum Beispiel eilige Ersatzteilbestellungen. Alle B-Kanäle der S_0-Schnittstelle erhalten dementsprechend eine hohe Priorität.

Für interne Anrufe wird die Priorität systemweit eingestellt und gilt damit gleichermaßen für alle internen Anrufe.

10 Prioritätsebenen (1 = hoch, 10 = niedrig) sind verfügbar.

Im Standard ist für interne Anrufe die Priorität = 10 und für externe Anrufe die Priorität = 1 eingestellt.

15.6.4.1 Wie Sie die Priorisierung der Anrufordnung ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.

3) Klicken Sie im Menübaum auf **Kommende Rufe** > **UCD**.

4) Klicken Sie auf die Registerkarte **UCD-Parameter ändern**.

5) Wählen Sie in der Aufklappliste **Priorität intern** die Priorität aus, die für alle internen Anrufe an alle UCD-Gruppen gelten soll (1 = höchste Priorität, 10 = niedrigste Priorität).

6) Wählen Sie für jede Leitung (B-Kanal) in der zugehörigen Aufklappliste **Priorität** die Priorität aus, die für die externen Anrufe über diese Leitung an alle UCD-Gruppen gelten soll (1 = höchste Priorität, 10 = niedrigste Priorität). Für jeden B-Kanal kann eine individuelle Priorität eingestellt werden.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.6.5 UCD-Anrufe automatisch annehmen

Durch dieses Leistungsmerkmal können Agenten kommende Anrufe ohne zusätzliche Bedienschritte annehmen (Automatic Incoming Call Connection AICC).

Um das Leistungsmerkmal nutzen zu können, muss das Telefon eines Agenten mit Headset und Trenntaste ausgestattet sein. Der Agent wird durch einen Hörton im Headset auf das Eintreffen eines Anrufes aufmerksam gemacht, der anschließend automatisch durchgeschaltet wird.

Ein bestehendes Gespräch kann ein Agent durch Drücken der Trenntaste beenden.

Standardmäßig ist das Leistungsmerkmal "AICC" nicht aktiviert. Eine Aktivierung erfolgt gruppenindividuell und gilt für alle Agenten einer UCD-

Gruppe, unabhängig davon, ob das Telefon eines Agenten mit Headset ausgestattet ist oder nicht.

15.6.5.1 Wie Sie das automatische Annehmen von UCD-Anrufen ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **UCD** > **...** zur gewünschten UCD-Gruppe.
4) Klicken Sie auf die Registerkarte **UCD-Gruppe ändern**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die UCD-Agenten dieser UCD-Gruppe kommende Anrufe ohne zusätzliche Bedienschritte annehmen sollen, wählen Sie in der Aufklappliste **AICC** den Eintrag **ja** aus.
   - Wenn die UCD-Agenten dieser UCD-Gruppe kommende Anrufe nicht ohne die herkömmlichen Bedienschritte (zum Beispiel durch das Abnehmen des Hörers) annehmen sollen, wählen Sie in der Aufklappliste **AICC** den Eintrag **nein** aus.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.6.6 UCD-Warteschlange

Sind alle Agenten einer UCD-Gruppe belegt, können kommende Anrufe in eine Warteschlange eingetragen werden. Wartenden Anrufern können Ansagen oder Musik eingespielt werden.

Wird ein Anruf in der Warteschlange für eine bestimmte Zeit (primärer Rufzyklus) nicht von dem am längsten im Zustand **verfügbar** befindlichen Agenten angenommen, wird dieser Agent in den Zustand **nicht verfügbar** versetzt. Anschließend wird der Anruf an den nächsten Agenten weitergegeben. Wird der Anruf auch von diesem Agenten nicht innerhalb einer bestimmten Zeit (sekundärer Rufzyklus) angenommen, wird auch dieser Agent in den Zustand **nicht verfügbar** versetzt. Wenn alle Agenten im Zustand **nicht verfügbar** sind, kann der Anruf an ein Überlaufziel geleitet werden.

Für jede UCD-Gruppe kann individuell festlegt werden, wie hoch die maximale Anzahl der Anrufe in der Warteschlange ist. Wird die maximale Anzahl der wartenden Anrufe überschritten, können die weiteren Anrufe an ein Überlaufziel geleitet werden.

Als Überlaufziel kann ein externes Ziel, eine andere UCD-Gruppe, ein interner Teilnehmer oder eine Gruppe definiert werden. Ist das Überlaufziel eine andere UCD-Gruppe und sind auch alle Agenten dieser UCD-Gruppe belegt, bleibt der Anruf in der Warteschlange der ursprünglichen Gruppe und wird darüber hinaus in die Warteschlange der anderen UCD-Gruppe (Überlaufziel) eingereiht.

Ein Agent kann über eine dafür programmierte Funktionstaste oder über den zugehörigen Menüeintrag oder die Kennzahl die Anzahl der Anrufe abfragen, die sich in der Warteschlange seiner UCD-Gruppe befinden.

Anrufe in einer Warteschlange

Die maximale Anzahl von Anrufen in der Warteschlange beträgt 30 für die UCD-Gruppen 1 bis 59 und 72 für die UCD-Gruppe 60.

Die minimale Anzahl von Anrufen in der Warteschlange ist Null. Ist Null als Minimalanzahl konfiguriert, gibt es keine Warteschlange. Anrufe werden direkt an ein Überlaufziel weitergeleitet oder abgewiesen, wenn kein Agent verfügbar ist.

15.6.6.1 Wie Sie eine UCD-Warteschlange ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **UCD** > **...** zur gewünschten UCD-Gruppe.
4) Klicken Sie auf die Registerkarte **UCD-Gruppe ändern**.
5) Wählen Sie in der Aufklappliste **Prim. Rufzykl.** die Anzahl der primären Rufzyklen aus. Die Angabe erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Eingestellt wird die Zeit, die ein Anruf in der Warteschlange verbleibt, falls er nicht von dem am längsten im Zustand verfügbar befindlichen Agenten angenommen wird. Anschließend wird der Anruf zum nächsten verfügbaren Agenten weitergegeben.
6) Wählen Sie in der Aufklappliste **Sek. Rufzykl.** die Anzahl der sekundären Rufzyklen aus. Die Angabe erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Eingestellt wird die Zeit, die ein Anruf in der Warteschlange verbleibt, falls er nicht von dem nächsten verfügbaren Agenten angenommen wird.
7) Wählen Sie aus, ob ein Ansagewechsel stattfinden soll:
   - Wenn die in der Warteschlange befindlichen Anrufer eine einmalige Ansage erhalten sollen, wählen Sie in der Aufklappliste **Ansagewechsel** den Eintrag **Einmalig** aus.
   - Wenn die in der Warteschlange befindlichen Anrufer zyklisch wechselnde Ansagen erhalten sollen, wählen Sie in der Aufklappliste **Ansagewechsel** den Eintrag **Zyklisch** aus.
8) Geben Sie im Feld **Ansageverzögerung** die Zeit ein, nach der ein Anrufer in der Warteschlange eine Ansage erhält. Die Angabe erfolgt in Sekunden.
9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.6.7 UCD-Überlauf

UCD-Anrufe können an ein Überlaufziel geleitet werden, falls diese nicht von den Agenten einer UCD-Gruppe angenommen werden und keine Warteschlange eingerichtet wurde oder die Maximalanzahl der Anrufe in der Warteschlange erreicht wurde.

Anmerkung: Beim UCD-Überlauf-Konzept wird nur ein Überlauf-Ziel definiert (zweiter CDL-Eintrag). Daher werden Ansagen erst dann wiedergegeben, wenn der Anruf beim UCD-Überlauf-Ziel eintrifft und nicht während des gesamten Rufzyklus. Wenn ein Anruf das UCD-Überlauf-Ziel verlässt, erklingt die Standard-Wartemusik.

Für jede UCD-Gruppe kann die maximale Anzahl der Anrufe in der Warteschlange individuell festlegt werden. Wird diese Anzahl überschritten, können die weiteren Anrufe an ein Überlaufziel geleitet werden.

Ist keine Warteschlange erwünscht, kann Null als maximale Anzahl der Anrufe in der Warteschlange definiert werden. Nicht angenommene Anrufe werden dann sofort an ein Überlaufziel geleitet.

Abhängigkeiten

Thema	Abhängigkeit
AutoAttendant	Die Verwendung eines AutoAttendants als Überlaufziel ist nicht möglich.

15.6.7.1 Wie Sie den UCD-Überlauf ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe** > **UCD** > **...** zur gewünschten UCD-Gruppe.
4) Klicken Sie auf die Registerkarte **UCD-Gruppe ändern**.
5) Geben Sie im Feld **Wart. Anrufe** die maximale Anzahl der wartenden Anrufe ein. Die über diese Anzahl hinausgehenden Anrufe werden an ein Überlaufziel geleitet.
6) Geben Sie im Feld **Overflow-Zeit** die gewünschte Zeit ein. Die Angabe erfolgt in Sekunden.

   Hinweis: Diese Einstellung ist ausschließlich relevant, wenn eine externe UCD-Applikation angeschlossen ist. Wird ein wartender Anruf nicht innerhalb der Overflow-Zeit durch die UCD-Applikation angenommen, wird der Anruf anhand der Angaben im Call Management durch das Kommunikationssystem weiterverarbeitet.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.6.8 UCD-Nachtschaltung

Für jede UCD-Gruppe kann eine individuelle Nachtschaltung konfiguriert werden. Jeder Agent einer UCD-Gruppe kann die Nachtschaltung aktivieren und deaktivieren. Nach der Aktivierung werden alle Anrufe für diese UCD-Gruppe zum Nachtziel geleitet.

Als Nachtschaltungsziel kann zum Beispiel ein interner Teilnehmer, eine andere Gruppe, eine Ansage/Wartemusik, die Sprachbox des Kommunikationssystems oder ein externes Ziel definiert werden.

Aktivierung / Deaktivierung

Die Aktivierung oder Deaktivierung der UCD-Nachtschaltung kann mittels einer dafür programmierten Funktionstaste oder über die zugehörigen Menüeinträge oder die Kennzahlen erfolgen. Mit der Aktivierung ist die Rufnummer des gewünschten Nachtschaltungsziels einzugeben.

Informationen zur Nachtschaltung des Kommunikationssystems siehe Nachtschaltung.

Abhängigkeiten

Thema	Abhängigkeit
Teilnehmerzustand	Eine Aktivierung der UCD-Nachtschaltung verändert nicht den jeweils aktuellen Teilnehmerzustand der einzelnen Agenten. Die Zwangsabmeldung der noch angemeldeten Agenten erfolgt nicht.
Nachtschaltung des Kommunikationssystems	Die UCD-Nachtschaltung und die Nachtschaltung des Kommunikationssystems können unabhängig voneinander aktiviert und deaktiviert werden. Beispiel: Eine UCD-Gruppe wurde als Nachtschaltungsziel des Kommunikationssystems eingetragen. Anrufe, die diese UCD-Gruppe über die Nachtschaltung des Kommunikationssystems erreichen, verbleiben in dieser UCD-Gruppe, unabhängig von einer UCD-Nachtschaltung.
Bestehende Gespräche	Bestehende Gespräche werden durch die Aktivierung der UCD-Nachtschaltung nicht beeinflusst.

15.6.9 Ansagen / Wartemusik bei UCD

Anrufern können Wartemusik (Music On Hold MOH) oder Ansagen eingespielt werden, falls diese nicht sofort an die Agenten einer UCD-Gruppe vermittelt werden. Wartemusik und Ansagen können jeder UCD-Gruppe individuell zugeordnet werden.

Sie haben die folgenden Möglichkeiten:

- Wartemusik (Music On Hold MOH)

  Wartenden Anrufern kann Musik aus der integrierten Quelle des Kommunikationssystems eingespielt werden. Zusätzliche Wartemusik-

Dateien können von einem PC in das Kommunikationssystem geladen werden.

Weitere Informationen siehe Wartemusik

- Ansagen

  Wartenden Anrufern können integrierte Ansagen eingespielt werden. Zusätzliche Ansagen können von einem PC in das Kommunikationssystem geladen werden.

  Weitere Informationen siehe Ansagen

Die Zeit bis zum Start der Ansage ist einstellbar (**Ansageverzögerung**). Um die Ansage zu unterdrücken, kann der Höchstwert (600 Sekunden) eingestellt werden. Dabei wird angenommen, dass der Anruf innerhalb dieser Zeit angenommen wird.

15.6.9.1 Wie Sie Ansagen / Wartemusik bei UCD ändern

Mit dem Wizard **Anrufverteilung** können Sie Ansagen und/oder Wartemusik für UCD-Gruppen konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UCD** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.
4) Um die Ansagen / Wartemusik (Music On Hold MOH) einer UCD-Gruppe zu ändern, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.
5) Klicken Sie so oft auf **OK & Weiter**, bis das Fenster **Ansagen / Überlauf bearbeiten** angezeigt wird.
6) Wählen Sie in der Aufklappliste **Ansageeinrichtungen** die Ansageeinrichtung der UCD-Gruppe aus. Sie haben die Möglichkeit, eine Ansage (falls eingerichtet) oder die interne Wartemusik (Music On Hold MOH) auszuwählen. Nach Auswahl der Ansageeinrichtung erscheint das Feld **Ansageverzögerung**.
7) Geben Sie im Feld **Ansageverzögerung** die Zeit in Sekunden ein, nach der ein Anrufer in der Warteschlange eine Ansage erhalten soll.
8) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.
9) Wenn Sie die Ansagen / Wartemusik (Music On Hold MOH) einer weiteren UCD-Gruppe ändern möchten, wiederholen Sie die Schritte 4 bis 8.
10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

15.6.10 Übergabe an UCD-Gruppen

Interne und externe Gespräche können UCD-Gruppen übergeben werden. Wird ein Anruf innerhalb einer bestimmten Zeit nicht angenommen, erfolgt ein Wiederanruf.

Die Wiederanrufzeit wird über den Zeitparameter **Überwachung eines Übergeben vor Melden an eine UCD-Gruppe** definiert. Die Standardeinstellung beträgt 300 Sekunden. Eine Änderung dieser Einstellung ist durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** möglich.

Abhängigkeiten

Thema	Abhängigkeit
Ansagen	Den übergebenen externen Gesprächen können Ansagen eingespielt werden. Bei internen Gesprächen ist das nicht möglich.
Wiederanrufzeit	Für eine Übergabe an UCD-Gruppen gilt eine andere Wiederanrufzeit als für eine Übergabe an Teilnehmer.

15.6.10.1 Wie Sie die Wiederanrufzeit für übergebene Gespräche an UCD-Gruppen ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Zeitparameter**.
4) Geben Sie für den Zeitparameter **Überwachung eines Übergeben vor Melden an eine UCD-Gruppe** die gewünschte Wiederanrufzeit an (Standardeinstellung = 300 Sekunden). Wird ein Gespräch nach Ablauf dieser Zeit nicht angenommen, erfolgt ein Wiederanruf.
   a) Wählen Sie in der Aufklappliste **Basis** die gewünschte Zeitbasis aus.
   b) Geben Sie im Feld **Faktor** den Wert ein, mit dem die Zeitbasis multipliziert werden soll.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.6.11 Auslösen von UCD-Anrufen über analoge Leitungen

Werden UCD-Anrufe über analoge Leitungen nicht innerhalb einer bestimmten Zeit angenommen, werden diese Anrufe ausgelöst. Damit wird ein Hängenbleiben von analogen Leitungen verhindert.

Die Auslösezeit wird über den Zeitparameter **Überwachung eines UCD-Rufes auf einer analogen Leitung** definiert. Die Standardeinstellung beträgt 300 Sekunden. Eine Änderung dieser Einstellung ist durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** möglich (von 0 bis 255 Minuten).

15.6.11.1 Wie Sie die Auslösezeit für UCD-Anrufe über analoge Leitungen ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Zeitparameter**.
4) Geben Sie für den Zeitparameter **Überwachung eines UCD-Rufes auf einer analogen Leitung** die gewünschte Auslösezeit an (einstellbar von 0 bis 255 Minuten, Standardeinstellung = 300 Sekunden). Wird ein Anruf nach Ablauf dieser Zeit nicht angenommen, wird dieser Anruf ausgelöst.
   a) Wählen Sie in der Aufklappliste **Basis** die gewünschte Zeitbasis aus.
   b) Geben Sie im Feld **Faktor** den Wert ein, mit dem die Zeitbasis multipliziert werden soll.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16 Anruf-Routing

Das Kommunikationssystem bietet verschiedene Möglichkeiten Anrufe einem gewünschten Ziel zuzuordnen, wie Berechtigungen (Wahlkontrolle), Tag- und Nachtschaltung, Least Cost Routing und Anrufsteuerungsdienst. Das Absetzen von Notrufen ist aus jeder Konfiguration möglich.

16.1 Berechtigungen (Wahlkontrolle)

Berechtigungen (Wahlkontrolle) regeln den Zugang der Teilnehmer zu möglicherweise kostenpflichtigen externen Verbindungen.

Zugehörige Konzepte

Konfiguration der Teilnehmer auf Seite 454

16.1.1 Berechtigungsgruppen und Berechtigungsklassen

Jedem Teilnehmer ist eine Berechtigungsgruppe zugeordnet, in der definiert ist, welche Berechtigung der Teilnehmer für kommende und gehende Anrufe hat.

In der Berechtigungsgruppe ist für jede Richtung eine der folgenden Berechtigungsklassen definiert:

- **Intern**

  Der Teilnehmer darf nur intern telefonieren.
- **Halbamt**

  Der Teilnehmer darf externe Gespräche nur annehmen.
- **Erlaubnisliste** 1-6

  Der Teilnehmer darf nur die in der Erlaubnisliste definierten externen Rufnummern wählen. Ist keine Rufnummer eingetragen gilt Halbamtsberechtigung.
- **Verbotsliste** 1-6

  Der Teilnehmer darf die in der Verbotsliste definierten externen Rufnummern nicht wählen. Ist keine Rufnummer eingetragen gilt Vollamtsberechtigung.
- **Vollamt**

  Der Teilnehmer darf ohne Einschränkung kommende und gehende externe Gespräche annehmen und aufbauen.

Einige der 15 möglichen Berechtigungsgruppen sind für alle Richtungen mit der gleichen Berechtigungsklasse vorbelegt und aussagekräftig benannt (z.B. Berechtigungsgruppe **International** mit der Berechtigungsklasse **Vollamt** oder Berechtigungsgruppe **Kommend** mit der Berechtigungsklasse **Halbamt**. Die Namen aller Berechtigungsgruppen können vom Administrator geändert werden.

Anmerkung: Standardmäßig gehört jeder Teilnehmer zur Berechtigungsgruppe 7; dies kann jedoch geändert werden. Darüber hinaus gehört auch jede Amtsleitung zur Berechtigungsgruppe 7, diese Einstellung ist aber nicht

konfigurierbar. Daher sollten Sie die Berechtigungsgruppe 7 nicht verwenden und uneingeschränkten Zugriff (Vollamtszugriff) auf alle Bündel erlauben.

Abhängigkeiten

Thema	Abhängigkeit
Kurzwahlziele	Zentrale Kurzwahlziele können unabhängig von zugeordneten Berechtigungsgruppe angewählt werden.
LCR	Berechtigungsgruppen (Wahlkontrolle) und LCR-Berechtigung sind unterschiedlich.
Anrufumleitung	Bei einer Anrufumleitung gilt die Berechtigung des Anrufenden.

16.1.1.1 Wie Sie den Namen einer Berechtigungsgruppe ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Tag:Berechtigsgruppe**.

Anmerkung: Sie können im Menübaum auch auf **Nacht:Berechtigungsgruppe** klicken, das führt zum selben Ergebnis.

4) Klicken Sie im Menübaum auf die gewünschte Berechtigungsgruppe.
5) Klicken Sie auf die Registerkarte **Berechtigungsgruppe ändern**.
6) Ändern Sie im Feld **Berechtigungsgruppe** den Namen der Berechtigungsgruppe.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.1.1.2 Wie Sie die Berechtigungsklassen einer Berechtigungsgruppe ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Tag:Berechtigsgruppe**.
4) Klicken Sie im Menübaum auf die gewünschte Berechtigungsgruppe.
5) Klicken Sie auf die Registerkarte **Berechtigungsgruppe ändern**.

6) Wählen Sie für den Tag-Betrieb bei jeder genutzten Richtung aus der Aufklappliste die gewünschte Berechtigungsklasse aus.
7) Wählen Sie bei Bedarf die Berechtigungsklasse für **Networking** für den Tag-Betrieb.
8) Klicken Sie im Menübaum auf **Nacht:Berechtigungsgruppe**.
9) Klicken Sie im Menübaum auf die zuvor bearbeitete Berechtigungsgruppe.
10) Klicken Sie auf die Registerkarte **Berechtigungsgruppe ändern**.
11) Wählen Sie jetzt für den Nacht-Betrieb bei jeder genutzten Richtung aus der Aufklappliste die gewünschte Berechtigungsklasse aus.
12) Wählen Sie auch hier bei Bedarf die Berechtigung für **Networking** für den Nacht-Betrieb.
13) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.1.1.3 Wie Sie alle Teilnehmer einer Berechtigungsgruppe anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Tag:Berechtigsgruppe**.

Anmerkung: Sie können im Menübaum auch auf **Nacht:Berechtigungsgruppe** klicken, das führt zum selben Ergebnis.

---

4) Klicken Sie im Menübaum auf die gewünschte Berechtigungsgruppe.
5) Klicken Sie auf die Registerkarte **Gruppenmitglieder anzeigen**. Alle Teilnehmer, denen die ausgewählte Berechtigungsgruppe zugewiesen ist, werden Ihnen mit Rufnummer und Name angezeigt.

16.1.2 Erlaubnis- und Verbotslisten

Mit Erlaubnis- und Verbotslisten kann festgelegt werden, welche externen Rufnummern die Teilnehmer wählen dürfen und welche nicht.

Erlaubnislisten enthalten die am Anfang einer Rufnummer zulässigen Ziffernfolgen. Der Teilnehmer darf nur die in der Erlaubnisliste definierten externen Rufnummern wählen. Stellen Sie sicher, dass in der Liste auch alle benötigten Notrufnummern enthalten sind!

Verbotslisten enthalten die am Anfang einer Rufnummer unzulässigen Ziffernfolgen. Der Teilnehmer darf die in der Verbotsliste definierten externen Rufnummern nicht wählen. Stellen Sie sicher, dass in der Liste keine Notrufnummern enthalten sind!

Die **Liste der Notrufnummern** ist ein Spezialfall der Erlaubnisliste. Der Teilnehmer darf nur die in der Liste erfassten Notrufnummern wählen. Stellen Sie sicher, dass in der Liste alle benötigten Notrufnummern enthalten sind!

In die Listen müssen nicht die vollständigen Rufnummern eingetragen werden. Um Teilnehmer beispielsweise zur Anwahl aller (kostenlosen) 0800xxxer-Nummern zu berechtigen, muss hier lediglich die 0800 eingeben werden. Da sich die Listen nur auf gehende Externgespräche beziehen, muss die Amtskennzahl bei den eingetragenen Rufnummern nicht mit angegeben werden. Der Eintrag des Zeichens # an erster Stelle einer verbotenen Rufnummer verhindert eine Umgehung der Wahlkontrolle für Systemtelefone, die eine analoge Amtsleitung mit MFV-Wahlverfahren belegen und während der Wahl auf MFV umschalten wollen.

Über **Auswertungsfilter** kann der Administrator zu einer beliebigen Verbotsliste festlegen, welche Ziffern nicht mit der entsprechenden Verbotsliste verglichen werden sollen. Das Kommunikationssystem blendet den eingestellten Ziffernbereich vor der Wahlbewertung aus. Durch ein Verbot der Zeichen * und # wird erreicht, dass ein Teilnehmer bei der Eingabe dieser Zeichen die Wahlkontrolle umgehen kann.

Konfigurationsgrenzen

Leistungsmerkmal	Anzahl
Erlaubnisliste 1: lang, 100 Einträge	1
Erlaubnislisten 2-6: kurz, 10 Einträge	5
Verbotsliste 1: lang, 50 Einträge	1
Verbotslisten 2-6: kurz, 10 Einträge	5
Zeichenlänge der Listeneinträge (Ziffern 0 - 9 sowie die Zeichen * und #)	26

16.1.2.1 Wie Sie eine Notrufnummernliste erstellen

Mit dem Wizard **Berechtigung** können Sie eine Liste mit Notrufnummern für die Berechtigungsgruppe "Notrufnummern" erstellen.

Voraussetzungen

Sie sind am WBM angemeldet.

Das Kommunikationssystem ist an eine Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Berechtigung** zu starten.
4) Geben Sie im Eingabefeld eine Notrufnummer ein und klicken Sie auf **Hinzufügen**. Die Rufnummer wird in die Liste der Notrufnummern übernommen.
5) Wenn Sie weitere Rufnummern in die Notrufnummernliste eintragen wollen, wiederholen Sie den vorherigen Schritt.
6) Klicken Sie so oft auf **OK & Weiter** bis Sie mit **Beenden** die Konfiguration abschließen.

16.1.2.2 Wie Sie eine Erlaubnis- und eine Verbotsliste erstellen

Mit dem Wizard **Berechtigung** können Sie eine Erlaubnisliste und eine Verbotsliste erstellen.

Voraussetzungen

Sie sind am WBM angemeldet.

Das Kommunikationssystem ist an eine Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Berechtigung** zu starten.
4) Klicken Sie auf **OK & Weiter**.
5) Geben Sie im Eingabefeld eine erlaubte Rufnummer ohne Amtskennzahl ein und klicken Sie auf **Hinzufügen**. Die Rufnummer wird in die Erlaubnisliste übernommen.
6) Wenn Sie weitere Rufnummern in die Erlaubnisliste eintragen wollen, wiederholden Sie den vorherigen Schritt.
7) Klicken Sie auf **OK & Weiter**.
8) Geben Sie im Eingabefeld eine verbotene Rufnummer ohne Amtskennzahl ein und klicken Sie auf **Hinzufügen**. Die Rufnummer wird in die Verbotsliste übernommen.
9) Wenn Sie weitere Rufnummern in die Verbotsliste eintragen wollen, wiederholden Sie den vorherigen Schritt.
10) Klicken Sie so oft auf **OK & Weiter** bis Sie mit **Beenden** die Konfiguration abschließen.

16.1.2.3 Wie Sie weitere Erlaubnislisten erstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **Erlaubnislisten**.
4) Klicken Sie im Menübaum auf die gewünschte Erlaubnisliste.
5) Klicken Sie auf die Registerkarte **Rufnummer hinzufügen**.
6) Geben Sie die externe **Rufnummer** ohne Richtungskennzahl ein.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
8) Wenn Sie weitere Rufnummern hinzufügen wollen, wiederholen Sie die Schritte 6 und 7.
9) Wenn Sie weitere Erlaubnislisten erstellen wollen, wiederholen Sie die Schritte 4 bis 7.
10) In der Registerkarte **Liste anzeigen** können Sie sich alle Rufnummern der ausgewählten Erlaubnisliste anzeigen lassen.

16.1.2.4 Wie Sie weitere Verbotslisten erstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **Verbotslisten**.
4) Klicken Sie im Menübaum auf die gewünschte Verbotsliste.
5) Klicken Sie auf die Registerkarte **Rufnummer hinzufügen**.
6) Geben Sie die externe **Rufnummer** ohne Richtungskennzahl ein.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
8) Wenn Sie weitere Rufnummern hinzufügen wollen, wiederholen Sie die Schritte 6 und 7.
9) Wenn Sie weitere Verbotslisten erstellen wollen, wiederholen Sie die Schritte 4 bis 7.
10) In der Registerkarte **Liste anzeigen** können Sie sich alle Rufnummern der ausgewählten Verbotsliste anzeigen lassen.

16.1.2.5 Wie Sie alle Rufnummern einer Verbotsliste anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **Verbotslisten**.
4) Klicken Sie im Menübaum auf die Verbotsliste mit der gewünschten Nummer.

16.1.2.6 Wie Sie alle Rufnummern einer Erlaubnisliste anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **Erlaubnislisten**.
4) Klicken Sie im Menübaum auf die Erlaubnisliste mit der gewünschten Nummer.

16.1.2.7 Wie Sie den Auswertungsfilter für eine Verbotsliste ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **Verbotslisten**.
4) Klicken Sie im Menübaum auf die Verbotsliste mit der gewünschten Nummer.
5) Klicken Sie auf die Registerkarte **Auswertungsfilter ändern**.
6) Wählen Sie in den Aufklapplisten **ab Ziffer** und **bis Ziffer** einen Bereich aus.

   Ein Bereich innerhalb einer Rufnummer ist hiermit konfigurierbar. Die Start-Position des Bereichs wird über die Klappliste **ab Ziffer**, die Ende-Position über **bis Ziffer** ausgewählt. .

   Die Vorbelegung dieses Feldes mit ***** und **#** ist zur Sperrung dieser Zeichen gedacht, denn * und # könnten als "Dummy"-Zeichen verwendet werden, die im Amt nicht ausgewertet werden und damit eine Wahlkontrolle umgehen. Durch Eingabe von * und # in die Verbotsliste haben diese Zeichen keinen Einfluß und nur die gewählten Ziffern werden ausgewertet.
7) Geben Sie im Feld **Zeichen** das oder die auszublendende(n) Zeichen ein.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.1.3 Blacklist

Im OpenScape Business-System steht eine Blacklist zur Verfügung, die es ermöglicht, eingehende Anrufe von bestimmten Rufnummern (CLI) und von Anrufen ohne Rufnummer oder eingeschränkte Darstellung der Rufnummer zu blockieren.

Die Blacklist unterstützt bis zu 100 Nummern mit maximal 25 Ziffern, entweder im kanonischen Format (z.B. +4989) oder im internationalen Format (z.B. 004989). Unterstützte Zeichen sind die Ziffern 0-9und das Zeichen "+".
Das Zeichen "+" bezieht sich auf das internationale Präfix, das im System konfiguriert ist. Es muss immer an der ersten Stelle eingegeben werden. Nummernfragmente ab Beginn der Rufnummer (CLI) sind erlaubt. Bei der Eingabe einer Nummer in die Blacklist wird eine logische Prüfung durchgeführt. Die Nummer wird abgelehnt, wenn sie bereits eingegeben wurde oder wenn sie durch ein Zahlenfragment abgedeckt ist.

Die Überprüfung der übertragenen Anrufer-Nummern erfolgt immer im internationalen Format. Wenn Anrufer-Nummern in anderen Formaten übertragen werden, werden sie entsprechend den Routendaten in das internationale Format umgewandelt.

Die Blacklist wird auf alle im System konfigurierten Leitungen der Zentrale angewendet. Sie unterstützt mehrere Zentralstellen/Telefonie-Anbieter mit unterschiedlichen Landes- und Ortsvorwahlen.

Für jeden gesperrten Anruf wird von der Blacklist ein Ereignisprotokolleintrag erstellt.

Innerhalb eines OpenScape Business-Netz muss die Blacklist in jedem Knoten, der mit der Zentralstelle/den Telefonie-Anbietern verbunden ist, bzw. in den Gateways konfiguriert werden. Interne Anrufe im Netz werden durch die Blacklist nicht eingeschränkt.

Die Blacklist kann vom Systemadministrator aktiviert/deaktiviert werden. Zusätzlich kann ein separates Flag für die Sperrung von anonymen Anrufen gesetzt werden.

Serviceprotokolle enthalten Informationen über blockierte angerufene Nummern. Protokolleinträge, die blockierten angerufenen Nummern entsprechen, enthalten den EventText **!BlackListed Call:**. Um die angerufene Nummer zu finden, die gesperrt wurde, überprüfen Sie die letzten beiden Ziffern des Protokolleintrags. Diese Ziffern (in hexadezimaler Form) entsprechen der Position in der Blacklist, in der die gesperrte Nummer enthalten ist. Wenn diese Ziffern ff sind, dann ist der blockierte Anruf anonym.

Abhängigkeiten

Anrufe mit CLI-Unterdrückung werden vom System nicht als anonyme Anrufe blockiert, wenn das Flag **Rufnummern-Unterdrückung ignorieren** innerhalb des Systems gesetzt ist. Die Rufnummer des Anrufers muss in diesem Fall explizit in die Blacklist eingetragen werden. Das Flag **Rufnummern-Unterdrückung ignorieren** ist in der werkseitigen Voreinstellung deaktiviert. Es kann nur über den Manager E aktiviert werden.

Die Mobilitätsfunktion des Systems kann von der Blacklist gestört werden, wenn Handynummern von Mobility Teilnehmern in die Blacklist eingetragen werden. In diesem Fall wird der Anruf zum DISA Zugang im Call Through-Modus durch die Blacklist blockiert.

16.1.3.1 Wie Sie im Experten-Modus in eine Blacklist für kommende Gespräche erstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **TelefonieBerechtigungsklassen**.
3) Klicken Sie im Menübaum auf **Berechtigungen > Blacklist**.
4) Klicken Sie auf die Registerkarte **Rufnummer hinzufügen**.
5) Geben Sie die **Rufnummer** ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
7) Wenn Sie weitere Rufnummern hinzufügen wollen, wiederholen Sie die Schritte 5 und 6.

8) Die hinzugefügten Rufnummern in der Blacklist werden auf der Registerkarte **Liste Anzeigen** unter **Blacklist** oder unter **Blacklist** im Menübaum angezeigt.

   Der Systemadministrator sollte in der Lage sein, unerwünschte Anrufer dauerhaft zu blockieren.

   - Aktivieren Sie das Kontrollkästchen **Anonyme Anrufe blockieren** im Bereich „Anonyme Anrufe“, um einen anonymen eingehenden Anruf zu blockieren.

     Anmerkung: Anonyme Anrufe sind definiert als Anrufe, bei denen die Nummer des einleitenden Teilnehmers dem Benutzer nicht angezeigt wird.

   - Aktivieren Sie das Kontrollkästchen für die **Blacklist-Funktion** im Blacklist-Bereich, um bestimmte Rufnummern zu sperren.

     Anmerkung: Die Blacklist-Funktion basiert nur auf der vom Anbieter angegebenen Rufnummer des Anrufers (Call Originator).

16.1.3.2 Bearbeiten/Löschen von Rufnummern in der Blacklist

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **TelefonieBerechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen > Blacklist**.
4) Klicken Sie im Menübaum in der Blacklist auf die gewünschte Nummer.
5) Der Administrator kann den ausgewählten Eintrag bearbeiten oder löschen.

   Ausgewählten Eintrag bearbeiten:

   - Klicken Sie auf die Registerkarte **Rufnummer ändern**.
   - Geben Sie die gewünschte Rufnummer in das Feld **Rufnummer** ein.
   - Klicken Sie auf **Übernehmen** und anschließend auf OK.

   Ausgewählten Eintrag löschen:

   - Klicken Sie auf die Registerkarte **Rufnummer löschen**.
   - Geben Sie die gewünschte Rufnummer in das Feld **Rufnummer** ein.
   - Klicken Sie auf **Übernehmen** und anschließend auf OK.

6) Der Systemadministrator sollte in der Lage sein, unerwünschte Anrufer dauerhaft zu blockieren.

   - Aktivieren Sie das Kontrollkästchen **Anonyme Anrufe blockieren** im Bereich **Anonyme Anrufe**, um einen anonymen eingehenden Anruf zu blockieren

     Anmerkung: Anonyme Anrufe sind definiert als Anrufe, bei denen die Nummer des einleitenden Teilnehmers dem Benutzer nicht angezeigt wird.

   - Aktivieren Sie das Kontrollkästchen für die **Blacklist-Funktion** im **Blacklist**-Bereich, um bestimmte Rufnummern zu sperren.

     Anmerkung: Die Blacklist-Funktion basiert nur auf der vom Anbieter angegebenen Rufnummer des Anrufers (Call Originator).

16.1.3.3 Anzeige von Rufnummern in der Blacklist

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **TelefonieBerechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen > Blacklist**.
4) Die Rufnummern werden im Menübaum unter **Blacklist** oder auf der Registerkarte **Liste Anzeigen** unter **Blacklist** angezeigt.

16.1.3.4 Wie Sie in der Einrichtung eine Blacklist für kommende Gespräche erstellen

Sie können eine Blacklist mithilfe des Wizards **Blacklist für kommende Anrufe** erstellen.

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Blacklist für kommende Anrufe** zu starten.
4) Geben Sie im Eingabefeld eine zugelassene Rufnummer ein und klicken Sie auf **Hinzufügen**. Die Rufnummer wird in die Blacklist übernommen.
5) Klicken Sie auf OK & Weiter.

6) Wenn Sie weitere Rufnummern in die Blacklist eintragen wollen, wiederholden Sie die Schritte 4 und 5.
7) Wenn Sie eine Rufnummer löschen möchten, klicken Sie auf **Löschen**.
8) Klicken Sie so oft auf **OK & Weiter** bis Sie mit **Beenden** die Konfiguration abschließen.

16.1.4 Nachtschaltung

Während der Nacht können kommende und gehende Anrufe anders behandelt werden als während des Tages. Kommende Anrufe können zu einem Nachtschaltungsziel umgeleitet werden und interne Teilnehmer können andere Berechtigungen für ihr Telefon haben als tagsüber. Die systemweite Umschaltung zwischen Tag- und Nacht-Betrieb wird automatisch zu einem vom Administrator vorgegebenen Zeitpunkt durchgeführt.

Zeitgesteuerte Nachtschaltung

Variable Nachtschaltung

Jedes Telefon kann als Nachtschaltungsziel dienen, sofern die zugehörige Berechtigungsgruppe ankommende Rufe gestattet. Ein Telefon mit nur interner Berechtigung kann nicht als Nachtschaltungsziel eingetragen werden. Hat das Nachtschaltungsziel eine Anrufumleitung aktiviert, so wird dieser gefolgt.

Einer Berechtigungsgruppe können im Nacht-Betrieb andere Berechtigungsklassen zugewiesen sein als im Tag-Betrieb, um z.B. Gebührenmissbrauch vorzubeugen.

Für den Nachtbetrieb können Sie zusätzlich einen anderen Abwurfplatz festlegen als für den Tag-Betrieb. Der Abwurfplatz kann ein einzelner Teilnehmer oder eine Gruppe sein.

Das Kommunikationssystem aktiviert und deaktiviert die Nachtschaltung nach einem vom Administrator festgelegten Zeitplan.

Tipp: Bei der zeitgesteuerten Nachtschaltung gilt die eingestellte Regelung für ALLE Teilnehmer des Kommunikationssystems. Es gibt auch eine automatische Berechtigungsumschaltung nach Zeit, dabei werden Teilnehmer zu Gruppen (Profilen) zusammengefasst.

Die variable Nachtschaltung wird manuell von einem berechtigten Teilnehmer aktiviert und deaktiviert. Die Anrufe folgen den vom Administrator konfigurierten Rufziellisten.

Standardmäßig kann der erste Teilnehmer (die Rufnummer "100") im Kommunikationssystem die Nachtschaltung aktivieren und deaktivieren. Der Administrator kann bis zu fünf Teilnehmer dazu berechtigen, die Nachtschaltung zu aktivieren und deaktivieren.

UCD-Nachtschaltung

Für jede UCD-Gruppe kann eine individuelle Nachtschaltung konfiguriert werden. Diese ist unabhängig von der systemweiten Nachtschaltung aktivierbar und deaktivierbar. Jeder Agent einer UCD-Gruppe kann diese aktivieren und deaktivieren. Der jeweils aktuelle Status der einzelnen Agenten sowie

bestehende Gespräche sind davon nicht berührt. Nach der Aktivierung werden alle Anrufe für diese UCD-Gruppe zum Nachtschaltungsziel geleitet.

Als Nachtschaltungsziel ist eine andere UCD-Gruppe, ein interner Teilnehmer oder ein externes Ziel möglich.

16.1.4.1 Wie Sie Berechtigungen für die manuelle Nachtschaltung vergeben

Mit dem Wizard **Berechtigungen** vergeben Sie die Berechtigung für einzelne Teilnehmer, die das Kommunikationssystem über Ihr Telefon von Tag- auf Nachtschaltung (und umgekehrt) umschalten können. Die Umschaltung zwischen Tag- und Nachtschaltung erfolgt über das Telefon durch eine Kennzahl.

Voraussetzungen

Sie sind am WBM angemeldet. Das Kommunikationssystem ist an eine Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Berechtigung** zu starten.
4) Klicken Sie so oft auf **OK & Weiter** bis Sie das Fenster **Berechtigte Teilnehmer für Nachtschaltung** sehen.
5) Markieren Sie den gewünschten Teilnehmer in der Liste unter **Teilnehmer** und klicken Sie auf **Hinzufügen**. Der Teilnehmer erscheint anschließend in der Liste unter **Berechtigte Teilnehmer**.
6) Klicken Sie auf **OK & Weiter**.
7) Im Fenster **Systemüberblick** sehen Sie eine Aufstellung über alle vergebenen Berechtigungen.
8) Klicken Sie auf **Beenden**.

16.1.4.2 Wie Sie Berechtigungen für die manuelle Nachtschaltung löschen

Mit dem Wizard **Berechtigungen** können Sie die Berechtigung von Teilnehmern für die Umschaltung von Tag- auf Nachtschaltung löschen.

Voraussetzungen

Sie sind am WBM angemeldet. Das Kommunikationssystem ist an eine Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Berechtigung** zu starten.
4) Klicken Sie so oft auf **OK & Weiter** bis Sie das Fenster **Berechtigte Teilnehmer für Nachtschaltung** sehen.

5) Markieren Sie den gewünschten Teilnehmer (dessen Berechtigung Sie löschen wollen) in der Liste unter **Berechtigte Teilnehmer** und klicken Sie auf **Löschen**.
6) Klicken Sie auf **OK & Weiter**.
7) Im Fenster **Systemüberblick** sehen Sie eine Aufstellung über alle vergebenen Berechtigungen.
8) Klicken Sie auf **Beenden**.

16.1.4.3 Zeitgesteuerte Nachtschaltung konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Automatische Nachtschaltung** > **Montag** (Montag als Beispiel; alle Tage der Woche stehen zur Auswahl).
4) Wählen Sie unter **Bearbeiten Zone** eine von vier möglichen Zonen aus, für die eine bestimmte Berechtigung gelten sollte.
5) Legen Sie mit **Beginn** und **Ende** die Zeit (in Stunden und Minuten) für diese Berechtigung fest.
6) Wählen Sie unter **Nachtrufnr.** den berechtigten Teilnehmer aus.

   Im Feld **Autom. Nachtschaltung** wird Ihre Einstellung für die jeweilige Zone angezeigt.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
   Wenn die Nachtschaltung aktiv ist, wird auf der Landing Page des Admin-Portals die Meldung **Das System läuft derzeit im Nachtbetrieb** angezeigt.

16.1.4.4 Wie Sie einen Sondertag für die zeitgesteuerte Nachtschaltung konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **Sondertage**.
4) Wählen Sie mit **>>** oder **<<** das Jahr, für das Sie einen Feiertag festlegen möchten.
5) Wählen Sie mit **>>** oder **<<** den Monat, für den Sie einen Feiertag festlegen möchten.
6) Klicken Sie im Kalender auf den Tag, den Sie als Feiertag festlegen möchten.
7) Geben Sie unter **Name** die Bezeichnung des Feiertags ein.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.1.4.5 Wie Sie einen Sondertag für die zeitgesteuerte Nachtschaltung löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **Automatische Nachtschaltung** > **Sondertage**.
4) Klicken Sie unter **Tag** links von dem zu löschenden Feiertag auf den Papierkorb.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.1.5 Automatische Berechtigungsumschaltung nach Zeit

Bei der automatischen Berechtigungsumschaltung nach Zeit werden die Teilnehmer in sogenannte Teilnehmer-Profile zusammengefasst, in denen definiert ist, welche Berechtigungsgruppe in welchem Zeitintervall der Woche gültig ist. Für jedes Teilnehmer-Profil kann ein Zeitplan konfiguriert werden.

Abhängigkeiten

Unterschiede zwischen der automatischen Berechtigungsumschaltung nach Zeit und der zeitgesteuerten Nachtschaltung:

- Die automatische Berechtigungsumschaltung nach Zeit gilt nur für den Tagbetrieb und nicht für die Nachtschaltung.
- Erreichen des Anrufziels über Call Management:

  Die Abwicklung erfolgt über das Call Management und ist unabhängig von der automatischen Berechtigungsumschaltung nach Zeit. Es gibt verschiedene Anruflisten für Tag und Nacht.
- Bei der zeitgesteuerten Nachtschaltung kann nur zwischen Tag- und Nachtschaltung unterschieden werden und sie gilt für ALLE Teilnehmer.
- Abwurfziele

  Das Abwurfziel wird nur durch die zeitgesteuerte Nachtschaltung bestimmt.
- Berechtigungsgruppe:

  Während der Nacht ist die Berechtigungsgruppe in einer konstanten (konfigurierbaren) Relation zum Teilnehmer, die automatische Berechtigungsumschaltung nach Zeit hat darauf keinen Einfluss.

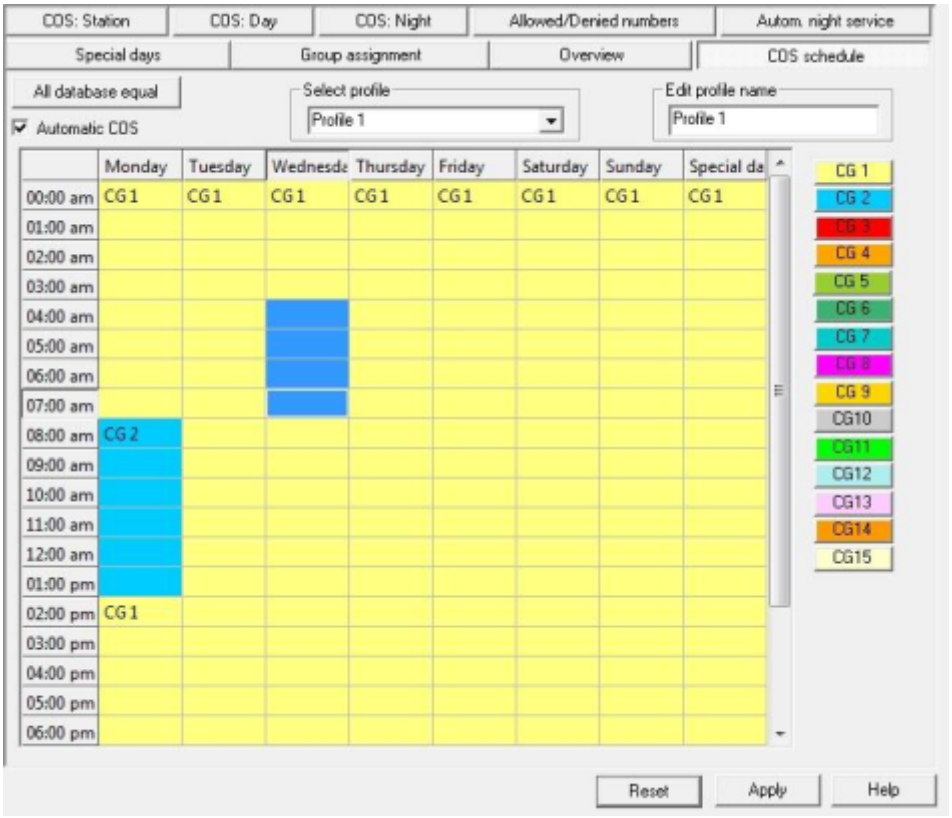
  Während des Tages kann die Berechtigungsgruppe zwischen bestimmten Tageszeiten wechseln oder ist ebenfalls in einer festen (konfigurierbaren) Relation zum Teilnehmer.

Thema	Abhängigkeiten
Nachtschaltung	Das Leistungsmerkmal "Nachtschaltung" hat Priorität vor dem Leistungsmerkmal "Automatische Berechtigungsumschaltung nach Zeit". Wenn die Nachtschaltung aktiviert ist, wird die Berechtigungsgruppe wie gewohnt gehandhabt und die Berechtigungsgruppe für die Nacht übernommen. Der Zeitplan ist nur tagsüber relevant.
Vernetzung	Die automatische Berechtigungsumschaltung und die Nachtumschaltung funktionieren nicht knotenübergreifend.

16.1.5.1 Zeitplan

Der Zeitplan dient der Steuerung der Berechtigungsklassen bei der automatischen Berechtigungsumschaltung nach Zeit. Es ist möglich bis zu acht Berechtigungsumschaltungen pro Tag für jeden Tag der Woche zu konfigurieren.

Jeder Tag beginnt um 00:00 Uhr. Die Eingabe der Ende-Zeit in den einzelnen Spalten markiert die Zeitzonen. Im folgenden Beispiel für einen Zeitplan sind die einzelnen Berechtigungsumschaltungen mit CG2, CG4 und CG5 bezeichnet.



Ein Teilnehmer kann unterschiedliche Berechtigungsgruppen für Tag und Nacht haben.

Wenn systemweit die automatische Berechtigungsumschaltung für den Tag gesetzt ist, hat ein Teilnehmer die ihm zugewiesene Berechtigungsgruppe je nach eingestelltem Profil und Zeitplan. In der Nacht hat der Teilnehmer die gleiche Berechtigungsgruppe die ihm bisher (über die Nachtschaltung) zugewiesen wurde.

Die automatische Berechtigungsumschaltung nach Zeit ist standardmäßig deaktiviert

Das Kommunikationssystem unterstützt nur eine Zeitzone (Weltzeit). Abgesetzte Teilnehmergruppen, die in unterschiedlichen Zeitzonen arbeiten, werden auf die Zeitzone des Kommunikationssystems gesetzt.

Der Zeitplan kann nur über den Manager E konfiguriert werden.

16.1.6 VBZ (Verkehrsbeziehungen)

Über das Leistungsmermal VBZ (Verkehrsbeziehungen) wird festgelegt, welche Teilnehmer des Kommunikationssystems Verbindungen zu welchen anderen Teilnehmern des Kommunikationssystems herstellen können. Dieses Leistungsmerkmal wird z.B. für Teilanlagen verwendet.

Durch VBZ lässt sich ebenfalls einrichten, auf welche Leitungen die einzelnen Teilnehmer für kommende und gehende Rufe Zugriff haben..

Die VBZ-Funktionalität greift nicht auf die Applikationen zu, sie hat ausschließlich für die Telefonie Bedeutung. Die Darstellung des Anwesenheitsstatus z.B. wird nicht über eine Zugriffsbeschränkung durch VBZ verhindert.

Das Leistungsmerkmal VBZ wird in zwei Schritten realisiert:

- VBZ-Gruppen bilden
- VBZ-Matrix konfigurieren

Tipp: Das Leistungsmerkmal VBZ sollte nicht in Verbindung mit UC-Funktionalität genutzt werden, da es Einschränkungen zur Folge hätte.

16.1.6.1 VBZ-Gruppen (Verkehrsbeziehungsgruppen)

VBZ-Gruppen (Verkehrsbeziehungsgruppen) regeln erlaubte und verbotene Verbindungen zwischen Teilnehmern und Leitungen des Kommunikationssystems.

Mit Hilfe von VBZ-Gruppen können bestimmte Teilnehmer und Leitungen zu Gruppen zusammen geschlossen werden.

Über VBZ-Gruppenzuordnung weisen Sie den einzelnen Teilnehmern und Leitungen im Kommunikationssystem eine VBZ-Gruppe zu. Beim Kodieren der Verbindungsmatrix können Sie dann auf diese Gruppen zurückgreifen und festlegen, welche Teilnehmer welche anderen Teilnehmer erreichen können und welche Teilnehmer auf welche Leitungen zugreifen können.

Standardmäßig sind alle Teilnehmer und Amtsleitungen der VBZ-Gruppe 1 zugeordnet. Damit haben alle Teilnehmer uneingeschränkten Zugang zu anderen Teilnehmer sowie zu Leitungen, sowohl kommend als auch gehend.

Welche VBZ-Gruppen Verbindungen zu welchen anderen VBZ-Gruppen herstellen können, ist in der VBZ-Matrix festzulegen.

Es sind maximal 64 VBZ-Gruppen konfigurierbar.

16.1.6.2 Zuordnung der KWZ-Nummern zu VBZ-Gruppen

Jeder VBZ-Gruppe wird ein Bereich von zentralen Kurzwahlzielen (KWZ-Zielen) zugeordnet. Wählt ein Teilnehmer eine KWZ, wird anhand der zugehörigen VBZ-Gruppe geprüft, ob er hierzu berechtigt ist. Liegt diese KWZ im zugeordneten Bereich KWZ für die entsprechende VBZ-Gruppe, wird die Wahl ausgeführt, ansonsten erfolgt eine Fehlermeldung.

Wählt ein Teilnehmer ein Kurzwahlziel, wird die dazugehörige VBZ-Gruppe ermittelt. Daraus leitet sich ab, ob der Teilnehmer dazu berechtigt ist, dieses Kurzwahlziel zu wählen. Bei fehlender Berechtigung wird die Wahl mit einer Fehlermeldung abgewiesen

Die Kurzwahlziel-Bereiche können sich in den VBZ-Gruppen überschneiden.

Standardmäßig sind alle Kurzwahlziel-Nummern der VBZ-Gruppe 1 zugeordnet.

Die KWZ-Bereiche können sich in der VBZ-Gruppe überschneiden. Zulässig sind z.B.:

VBZ-Gruppe	KWZ-Bereich
1	0000-7999
2	0050-0150
3	0200-0500

Es ist jedoch nicht zulässig, in einer VBZ-Gruppe anstelle eines Bereichs einzelne KWZ oder mehrere KWZ-Bereiche einzutragen. Unzulässig sind z.B.:

VBZ-Gruppe	KWZ-Bereich
1	0000, 0005, 0010
2	0050-0100, 0300-0500

16.1.6.3 Wie Sie Teilnehmer einer VBZ-Gruppe zuweisen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **VBZ-Gruppenzuordnung** > **VBZ-Gruppenzuordnung**.
4) Wählen Sie für einen in der Spalte **Teilnehmer** angezeigten Teilnehmer in der Aufklappliste **Gruppe** den Eintrag mit der gewünschten Verkehrsbeziehungsgruppe.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.1.6.4 Wie Sie die Leitung einer VBZ-Gruppe zuweisen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **VBZ-Gruppenzuordnung** > **Zuordnung Leitung zu VBZ-Gruppe**.
4) Wählen Sie für eine in der Spalte **Leitungen** angezeigte Leitung in der Aufklappliste **Gruppe** den Eintrag mit der gewünschten Verkehrsbeziehungsgruppe.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.1.6.5 Wie Sie die VBZ-Matrix ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen** > **VBZ-Matrix**.
4) Ändern Sie die Verbindungsmöglichkeiten wie folgt:
   - Wenn Sie alle Verbindungsmöglichkeiten sperren möchten, klicken Sie auf **Alles Sperren**.
   - Wenn Sie alle Verbindungsmöglichkeiten freigeben möchten, klicken Sie auf **Alles Freigeben**.
   - Wenn Sie nur gruppeninterne Verbindungsmöglichkeiten freigeben möchten, klicken Sie auf **Nur Gruppenintern**.
   - Wenn Sie eine Verbindungsmöglichkeit zwischen zwei VBZ-Gruppen gezielt bearbeiten möchten, klicken Sie in das Feld am Kreuzungspunkt dieser VBZ-Gruppen in der VBZ-Matrix. Klicken Sie wiederholt in das Feld, um Verbindungsmöglichkeiten in die eine Richtung, in die andere Richtung oder in beide Richtungen freizugeben oder zu sperren.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.1.7 Zentrales Codeschloss, Berechtigungsumschaltung

Das zentrale Codeschloss ermöglicht eine weitgehende Sperre der Telefonfunktionen durch einen berechtigten Teilnehmer (evtl. Administrator) für einen anderen Teilnehmer. Nur folgende Leistungsmerkmale stehen dann noch zur Verfügung: interne Anrufe, Kurzwahl zentral und Konferenz mit internen Teilnehmern. Dieses Codeschloss kann der gesperrte Teilnehmer durch Eingabe seines Telefonschloss-Codes oder wiederum der berechtigte Teilnehmer deaktivieren.

Der Telefonschloss-Code des Telefons, für den das Codeschloss vom berechtigten Teilnehmer aktiviert oder deaktiviert werden soll, ist für eine Sperrung nicht erforderlich.

Der berechtigte Teilnehmer ist standardmäßig der Teilnehmer mit der Rufnummer "100" (umkonfiguriert).

16.1.8 Individuelles Codeschloss (Telefon abschließen)

Mit dem Individuellen Codeschloss wird erreicht, dass von diesem Telefon aus keine externen Gespräche geführt oder Benutzereinstellungen geändert werden können.

Notrufnummern können trotz abgeschlossenem Telefon gewählt werden.

Interne Gespräche sind weiterhin möglich.

Ein Weiterverbinden von kommenden Rufen zu internen Teilnehmern ist möglich.

Bei abgeschlossenem Telefon sind nur noch Leistungsmerkmale möglich, die kein externes Wählen erfordern. Die Ausnahme ist das Leistungsmerkmal Kurzwahl zentral.

Als Erinnerung, dass dieses Telefon abgeschlossen ist, erhält der Teilnehmer einen Dauerton (Sonderwählton). Bei Telefonen mit Display wird dem Teilnehmer außerdem im Display "Telefon aufschliessen" angezeigt.

Ein Teilnehmer kann sein Telefon über eine Taste oder Kennzahl durch Eingabe seines persönlichen Telefonschloss-Codes abschließen und auch wieder entsperren.

Vor der ersten Nutzung des Telefonschlosses ist der Telefonschloss-Code zu konfigurieren. Der Telefonschloss-Code wird für alle Telefone standardmäßig auf 00000 gesetzt und kann individuell geändert werden. Dafür muss das Telefon aber entsperrt sein. Der Telefonschloss-Code muss immer 5stellig sein. Es sind nur die Ziffern 0 bis 9 zulässig. Wenn der Teilnehmer den Telefonschloss-Code vergessen hat, kann er durch einen berechtigten Teilnehmer (1. Teilnehmer im System mit der Rufnummer "100" oder der Administrator) auf den Standardwert 00000 zurückgesetzt werden.

16.1.8.1 Wie Sie das individuelle Codeschloss zurücksetzen

Über den Wizard **Teilnehmername und Freischaltung** kann das individuelle Codeschloss eines Telefons zurückgesetzt werden.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Teilnehmername und Freischaltung** zu starten. Das Fenster **Teilnehmer Name und Freischaltung** wird angezeigt.

4) Aktivieren Sie das Kontrollkästchen **Codeschloss zurücksetzen**.
5) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

16.1.9 R-Gesprächsschutz je Amtsleitung (nur für Brasilien)

R-Gesprächsschutz je Amtsleitung ermöglicht das automatische Auslösen ankommender R-Gespräche. Dieses Leistungsmerkmal ist ausschließlich in der Ländereinstellung Brasilien verfügbar. In allen anderen Ländern wird die Einstellung ignoriert.

Die individuelle Konfiguration für jede analoge Amtsleitung ist möglich. R-Gesprächsschutz kann individuell für jede analoge Amtsleitung konfiguriert werden. Ist das Leistungsmerkmal für eine Amtsleitung freigegeben, wird 1 s (Defaultwert) nach Annahme eines kommenden Rufs die Schleife für 2 s (Defaultwert) geöffnet. Dadurch werden R-Gespräche im Netz ausgelöst, andere Gespräche bleiben unverändert bestehen.

16.1.10 R-Gesprächsschutz je Teilnehmer (nur für Brasilien)

Mit dem R-Gesprächsschutz je Teilnehmer kann für jeden Teilnehmer individuell ein R-Gesprächsschutz eingerichtet und damit ankommende R-Gespräche automatisch ausgelöst werden. Dies gilt auch im Fall einer Anrufumleitung, einer Anrufübernahme, eines Abwurfs usw.

Zusätzlich besteht die Möglichkeit einen systemweiten R-Gesprächsschutz einzustellen. Dieser kommt zum Tragen, wenn kein einzelner Teilnehmer angewählt wird, sondern beispielsweise ein Sammelanschluss (oder bei Falschwahl).

16.2 LCR (Least Cost Routing, Leitweglenkung)

Durch die Funktion Leitweglenkung (LCR Least Cost Routing) wird automatisch gesteuert, über welchen Weg eine gehende Verbindung geschaltet wird. Der Weg kann über das öffentliche Netz, unterschiedliche Netzanbieter (ITSP) oder über ein privates Netz erfolgen. Anhand von Wahlplan, Wegetabellen und Wahlregeln wird der am besten geeignete Verbindungsweg für das Gespräch gesucht.

Verbindungen sind Gesprächsverbindungen, analoge Datenverbindungen über Fax und Modem und ISDN-Datenverbindungen.

16.2.1 LCR-Funktionalität

Mit Hilfe der Funktion LCR legen Sie fest, über welchen Anbieter z.B. ein Ortsgespräch, ein Handygespräch oder Auslandsgespräche geführt werden. Sie legen über das Kommunikationssystem den kostengünstigsten Anbieter fest und führen alle entsprechenden Gespräche über diesen definierten Weg.

Wird im Wahlplan ein Muster gefunden, das mit der gewählten Rufnummer übereinstimmt, wird in den Wegetabellen nach einer passenden Richtung gesucht (Jeder Leitung ist eine Richtung zugeordnet. Siehe Amtszugang über digitale und analoge Leitungen). Dabei wird überprüft, ob die LCR-

Berechtigung für diesen Wegetabelleneintrag zutrifft. Die LCR-Berechtigung und der Unterschied zur Berechtigung (Wahlkontrolle) wird im Kapitel LCR-Berechtigung beschriebenen.

Über die LCR-Funktionalität kann gesteuert werden, welche Teilnehmer des Kommunikationssystems welche Richtungen bzw. Leitungen nutzen dürfen (z.B. um sicherzustellen, dass Faxe ausschließlich über TDM-Amtsleitungen und nicht über ITSP geführt werden). Geprüft wird auch, ob der Anrufer die erforderlich Berechtigung gemäß Wahlkontrolle zur Belegung der gerade von LCR betrachteten Richtung hat. Diese Prüfung ist für Querverkehr (PABX Leitungen) per Konfiguration abschaltbar.

Die gewählten Zeichen werden zwischengespeichert bis die Wegetabellen mit den LCR-Berechtigungen durchlaufen sind. Erst danach erfolgt der Aufbau der Verbindung unter Berücksichtigung der Wahlregeln. Um die Wahlbereitschaft zu signalisieren kann dem Teilnehmer ein Wählton eingeblendet werden.

Sie können bei der Konfiguration der Wahlregeln eine Information für den wählenden Teilnehmer eingeben, z.B. dass diese Verbindung über einen bestimmten Telefondienstanbieter (Angabe des Providers) geroutet wird oder es sich bei einer Verbindung um eine teure Verbindung handelt. Diese Information kann entweder im Display angezeigt werden, als Ton ausgegeben oder im Display und gleichzeitig als Ton ausgegeben werden.

Generell gilt:

- Wenn LCR aktiviert ist, wird die Prüfung für jede externe Wahl durchgeführt. Ausnahme: bei gezielter Wahl einer Leitungskennzahl bzw. Leitungstaste.
- Wenn LCR feststellt, dass die bevorzugte Leitung nicht genutzt werden kann, so sucht das Kommunikationssystem eine alternative (möglicherweise teuerere) Richtung aus der Wegetabelle aus.
- Ziffern können je nach Zugangsverfahren und je Wegetabelle einzeln oder blockweise übertragen werden.
- Wenn die Durchwahlnummerntabelle leer ist, wird ersatzweise die Tabelle der internen Rufnummern verwendet. Es gelten die entsprechenden Regeln für diese Tabelle.

Tipp: Auch bei Kommunikationssystemen mit analogen Amtsleitungen (HKZ) muss eine Standortnummer konfiguriert werden (Ländervorwahl / ggf. Ortsnetzkennzahl / ggf. Anlagenrufnummer).

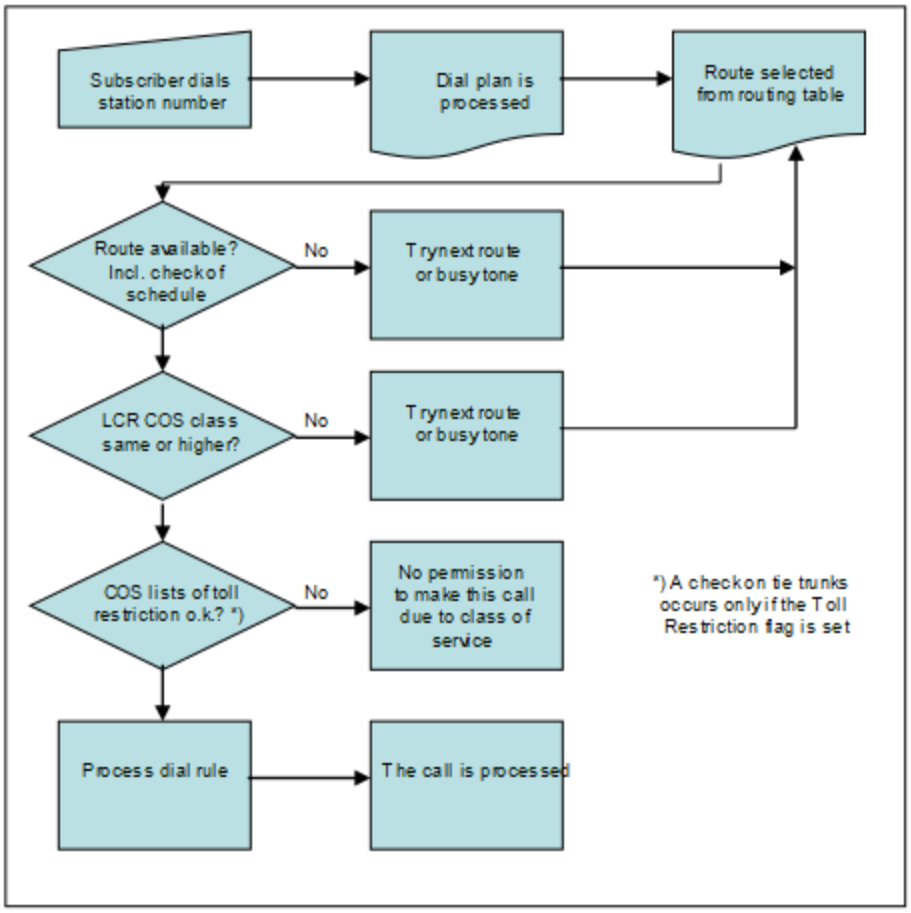
Darüber hinaus muss eine Durchwahlnummer oder, im Falle eine leeren Durchwahlnummerntabelle, eine Durchwahlnummer des eigenen analogen Amtsanschlusses (HKZ) konfiguriert werden. Nur so ist sichergestellt, dass alle externen Ziele erreicht werden können.

Systemspezifische Informationen

Das Kommunikationssystem wertet insgesamt 24 Zeichen aus.

Das Kommunikationssystem kann bis zu 1000 Wahlpläne und 254 Wegetabellen, mit je 16 Einträgen, verwalten.

LCR-Flußdiagramm



Wahlaussendung

Bei der Wahlaussendung wird zwischen Schritthaltend und Blockweise unterschieden. Bei Schritthaltend wird jede Ziffer direkt nach der Wahl ausgesendet und verarbeitet (Voraussetzung: LCR-Bewertung ist komplett, d.h. Wahlplaneintrag ist eindeutig identifiziert und Berechtigungen sind geprüft). Bei Blockwahl werden Ziffernblöcke gebildet und gesendet (d.h. Leitungsbelegung und Wahl erfolgen erst nach Zeit bzw. bei vorhandener expliziter Wahlendekennung).

Die Wahlaussendung für ITSP-Richtungen muss immer blockweise erfolgen. Die Einstellung der Richtung ist für die gesamte Wegetabelle wirksam.

Nur für USA: Carrier Select Override

Carrier Select Override kann mittels gezielter Leitungsbelegung realisiert werden (Kennzahl, Taste). Der LCR-Mechanismus wird dabei komplett umgangen.

Abhängigkeiten

Thema	Abhängigkeit
Zeitplan	Wenn in einem von HiPath 3000 migrierten System eine LCR-Konfiguration mit Zeitplan vorliegt, sind diese Einträge weiterhin wirksam und können mit dem Manager E administriert werden.
Kurzwahl zentral (KWZ)	Damit zentrale Kurzwahlziele ordnungsgemäß funktionieren, muss im Kurzwahlziel die LCR-Zugangskennziffer, gefolgt von der Zielrufnummer eingetragen sein.
Namentasten	Namentasten für externe Ziele müssen mit der LCR-Zugangskennziffer programmiert sein, damit sie ordnungsgemäß funktionieren.
Berechtigung (Wahlkontrolle)	Die Berechtigungsklassen der Wahlkontrolle werden auch bei LCR angewendet. Für PBX-Leitungen kann die Wahlkontrolle abgeschaltet werden, die Konfiguration erfolgt durch ein Flag.
Prime Line	Wenn die "Automatische Leitungsbelegung" (Prime Line) zum Amt aktiviert ist, dann ist LCR nicht möglich. Diese beiden Leistungsmerkmale schließen sich gegenseitig aus.

16.2.1.1 Wie Sie die LCR freigeben

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Tipp:

Bestimmte Einträge wie z.B. Ortsnetzkennzahl oder Teilnehmernummer werden bereits im Wizard **Basisinstallation** vorgenommen. Manuelle Änderungen dieser Einträge sind nur durch geschultes Techniker auszuführen. Bei Fehlkonfiguration im LCR besteht die Gefahr, dass gehende Verbindungen nicht oder nur eingeschränkt möglich sind.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie auf die Registerkarte **LCR Flags**.
4) Aktivieren Sie das Kontrollkästchen **Activate LCR**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.2.2 LCR-Wahlplan

Im Wahlplan wird nach Mustern gesucht, die auf die gewählten Ziffern (Wählfolge) zutreffen. Das Ergebnis dient als Kriterium für die Auswahl der Wegetabelle. Dabei wird überprüft, ob die LCR-Berechtigung des Teilnehmers für diesen Wahlplaneintrag zutrifft.

Das Muster einer Wählfolge ist im Wahlplan einer Wegetabelle zugeordnet, die weitern Parameter für diesen Verbindungaufbau definiert.

Der Wahlplan wird für Identifizierungs- und Konfigurationszwecke in einzelne Felder gegliedert. Die Tabelle stellt die Nummern 4922000 und 1603656260 bei Eingabe in den Wahlplan dar.

Feld 1		Feld 2		Feld 3		Feld 4		Feld 5
0	C	492	–	2000				
0	C	160	–	365	–	62	–	60

Für die Rufnummern sind folgende Einträge gültig:

0 . . . 9	Erlaubte Ziffern
–	Feldtrennzeichen
C	Simulierter Wählton (kann max. dreimal eingetragen werden). Dieser Eintrag wird auch als Feldtrennzeichen interpretiert
Globalzeichen	
X	Beliebige Ziffer zwischen 0 . . 9
N	Beliebige Ziffer zwischen 2 und . . 9
Z	Eine oder mehrere Ziffern folgen bis Wahlende

Eine Ziffernfolge kann in maximal 10 Felder unterteilt werden.

Feldtrennzeichen dienen der Unterteilung der Ziffernfolge in einzelne, getrennt auswertbare Felder. Beispiel: Nach der ersten Wählziffer wird ein Feldtrennzeichen eingefügt, damit eine gewählte “0” als separates Feld erkannt wird und somit eine Amtsberechtigung simuliert.

Durch die Trennung der Felder, können diese Felder im Wahlplan wiederholt bzw. anders angeordnet werden. Die durch die Feldtrennzeichen “–” und “C” gebildeten Felder im Wahlplan können einzeln angesteuert werden, um Ziffern zu wiederholen, zu unterdrücken, auszutauschen oder einzufügen.

Ein "#"- oder "*"-Zeichen in der vom Teilnehmer gewählten Ziffernfolge bezeichnen das Wahlende bzw. die Umschaltung des Wahlverfahrens. Aus diesem Grund sind diese Zeichen keine gültigen Einträge im Wahlplan.

Einträge mit Globalzeichen müssen immer durch eine eindeutige Wahlziffer eingeleitet werden, um Konflikte zwischen verschiedenen Globalzeicheneinträgen zu vermeiden.

Die PKZ-Eingabe kann pro Wahlplan erzwungen werden. Dabei gilt das PKZ-Prüfverfahren.

Wenn zu einem Wahlstring mehrere Wahlplaneinträge passen, wird der am meisten übereinstimmende verwendet. Beispiel: 00894711 wird gewählt, Wahlplaneinträge 0CZ und 0C089Z sind vorhanden -> 0C089Z wird ausgeführt.

Die Position der Einträge innerhalb des Wahlplans ist irrelevant, es ist kein "sortierter" Eintrag erforderlich.

OpenScape Business kann eine Wählfolge bis zu einer Länge von 24 Zeichen auswerten.

LCR-Einträge bei Ersteinrichtung des Kommunikationssystems

Bei der erstmaligen Inbetriebnahme des Kommunikationssystem erfolgen länderabhängig bestimmte Default-Einträge im LCR-Wahlplan. Bis Wahlplan 34 werden systemseitige Einträge für Notrufe, Auskunft, Sonderrufnummern, Standard-Amtsbelegung für PSTN und ITSP, für UC Suite, Ansageanschalten und Networking und die Berücksichtigung der Wahl im internationalen Format auf ISDN-Amtsleitungen vorbelegt. Dieser Bereich kann durch Konfigurationsänderungen an anderer Stelle (z.B. Änderung des Flags **Standortnummer**) beeinflusst werden. Daher ist sicherzustellen, dass die Standard-Amtsbelegung mit der Änderung der Standortnummer weiterhin funktioniert (wichtig bei Wahl mit öffentlichen Rufnummern).

Tipp: Ab LCR-Wahlplan 36 stehen Einträge zur freien Verfügung.

16.2.2.1 Wie Sie den Wahlplan bearbeiten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie auf **Wahlplan**.
4) Unter **Wahlplan ändern** werden die einzelnen Wahlpläne aufgelistet und Sie können folgende Felder bearbeiten:
   - **Name**
   - **Gewählte Ziffern**
   - **Wegetabelle**
   - **PKZ**
   - **Amtsberechtigung**

     Das Flag Wahlkontrolle bezieht sich ausschließlich auf die Richtungsart PABX. Für die Richtung Amt hat es keine Bedeutung, d.h. es ist nicht möglich die Wahlkontrolle für Amtsleitungen an dieser Stelle auszuschalten.
   - **Notbetrieb**

     Anmerkung: Durch Klicken auf den blauen Pfeil neben dem Feld **Wegetabelle** öffnet sich direkt die zugehörige Wegetabelle.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**

16.2.3 LCR-Wegetabelle

In den Wegetabellen der Leitweglenkung LCR wird nach einer passenden Richtung gesucht (jeder Leitung muss eineRichtung zugeordnet sein). Dabei wird überprüft, ob die Berechtigung (Wahlkontrolle) für diese Richtung zutrifft. Vom zugewiesenen Weg ist auch die Wahlregel abhängig.

Die Wegetabelle beschreibt

- die dem betreffenden Weg zugewiesene Richtung,
- die Wahlregel,
- die für eine Belegung erforderliche LCR-Berechtigung (Class Of Service COS),
- die Möglichkeit zur Warnung vor einer teuereren Verbindung (Warnsignal).
- das dedizierte Gateway und
- die GW Knoten-ID.

Die Tabelle wird von oben nach unten in hierarchischer Reihenfolge durchsucht. Es wird jeweils überprüft, ob die Richtung frei ist bzw. der Teilnehmer die erforderliche LCR-Berechtigung (Class Of Service COS) hat. Ist dies der Fall, erfolgt die Wahl gemäß der in der Wegetabelle eingetragenen Wahlregel, wenn die Berechtigung (Wahlkontrolle) und die VBZ-Zuordnung zwischen Teilnehmer und Leitung das zulassen.#

Wenn der primäre Verbindungsweg in der Wegetabelle belegt ist, kann LCR den nächsten (möglicherweise kostspieligeren) in der Tabelle konfigurierten Weg wählen. Dies kann dem Anwender durch ein akustisches und/oder optisches Signal angezeigt werden.

Es können bis zu 254 Wegetabellen mit jeweils 16 Wegen angelegt werden.

Dediziertes Gateway

Ein dediziertes Gateway ist in einem IP-Netzverbund ein fest eingestellter Partnerknoten (Dediziertes Gateway -> erzwungen). Wenn ein Dediziertes Gateway mit der entsprechenden GW Knoten-ID für die IP-Netorking-Richtung eingetragen ist, so wird zwingend zu diesem Gateway geroutet.

Bei einer Multigateway-Konfiguration wird ein Dediziertes Gateway anhand der Teilnehmerkonfiguration ermittelt.

16.2.3.1 Wie Sie Wegetabellen bearbeiten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.

3) Klicken Sie auf **Wegetabelle**.

4) Alle Wegetabellen werden Ihnen angezeigt:

- **1-Table**
- **2-Table**
- **nn-Table**

> **Tipp:** Die Wegetabellen 1 bis 15 sind für Default-Einträge bzw. für eine Konfiguration über Wizards vorgesehen. Bei einer Migration werden automatisch die vorhandenen Einträge in diese Wegetabellen eingetragen.
>
> Dieser Mechanismus verhindert allerdings keine Duplikate bei den Einträgen. Eine manuelle Nachbearbeitung der Wegetabellen wird empfohlen.

5) Klicken Sie auf die gewünschte Wegetabelle. Die ausgewählte Tabelle mit der Registerkarte **Wegetabelle ändern** wird angezeigt.

6) Unter **Wegetabelle ändern** werden die einzelnen Wegetabellen aufgelistet und Sie können folgende Felder bearbeiten:

- **Richtung**
- **Wahlregel**

> **Anmerkung:** Klicken Sie auf den blauen Pfeil neben der gewünschten Regel, um die Wahlregeleigenschaften anzuzeigen und zu bearbeiten.

- **Min. Ber. (LCR-Berechtigung)**
- **Warnung**
- **Dediziertes Gateway**
- **GW Knoten-ID**

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.2.4 LCR-Berechtigung

Jedem Teilnehmer wird eine eigene LCR-Berechtigung (Class Of Service COS) zugewiesen. Ein Teilnehmer kann einen Weg nur dann belegen, wenn seine Berechtigung größer oder gleich der LCR-Berechtigung in der Wegetabelle ist, das heißt ein Teilnehmer mit Berechtigung 7 kann einen Weg mit Berechtigung 8 nicht belegen. Standardmäßig sind alle Teilnehmer mit maximaler LCR-Berechtigung (15) eingetragen.

Abhängigkeiten

Thema	Abhängigkeit
Amtsberechtigung	Die Berechtigungen (Wahlkontrolle) ist vorrangig vor der LCR-Berechtigung. Die Berechtigung (Wahlkontrolle) kann für Querleitungen ein- und ausgeschaltet werden.
VBZ Gruppenzuordnung	Eine Wahl erfolgt nur, wenn auch die VBZ-Matrix dies zulässt.

16.2.4.1 Wie Sie die LCR-Berechtigung vergeben und ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie auf **Classes of Service**.
4) Vergeben Sie unter **Berechtigungen ändern** im Feld **Berechtigung** eine LCR-Berechtigung bzw. ändern eine vorhandene Berechtigung.

   Hierbei handelt es sich ausschließlich um die Berechtigung eines Teilnehmers für LCR. Das Feld hat keinen Einfluss auf die Amtsberechtigung.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.2.5 LCR-Wahlregeln

Durch die LCR-Wahlregeln können eingegebene Rufnummern zur Weiterverarbeitung in beliebige neue Ziffernfolgen umgewandelt werden. Durch Ziffernumwandlung wird der Zugang zu verschiedenen Netzanbietern ermöglicht. Die verwendete Wahlregel wird bestimmt durch den Weg bzw. die Richtung in der Wegetabelle.

Systemspezifische Informationen

Das Kommunikationssystem ist in der Lage bis zu 254 Wahlregeln in der LCR-Wahlregeltabelle zu verwalten. Der Name einer Wahlregel kann bis zu 16 Zeichen umfassen.

Die Regeln sprechen die einzelnen Felder im Wahlplan für nachstehende Vorgänge selektiv an:

- Wiederholen von Ziffern
- Unterdrücken von Ziffern
- Austauschen von Ziffern
- Einfügen von Ziffern
- Umschalten des Wahlverfahrens
- Erkennen eines Wähltons
- Einfügen von Wahlpausen

Wahlregel

Sie können hier bis zu 254 Wahlregeln mit einer Länge von jeweils maximal 40 Zeichen definieren.

Die LCR-Wahlregeltabelle wird auch als Routingtabelle bezeichnet.

Definition der Wahlregeln (Wahlregelformat)

- A:

  Restliche Felder wiederholen (aussenden). "A" bewirkt, dass alle nachfolgenden Ziffernfelder gesendet werden. Bezugspunkt ist das letzte Feldtrennzeichen im Feld gewählte Ziffern im Wahlplan.

  Wird "A" ohne expliziten Bezug eingetragen, bezeichnet dies alle Ziffern nach dem Acces Code, d. h, "A" entspricht dann "E2A"#
- B:

  Wird für die Multi-Gateway-Vernetzung genutzt, wenn eine von extern angerufene Rufnummer vom TON (Type Of Number) "unknown" ist, um sie zum Multi-Gateway-Knoten zu routen. Damit diese Rufnummer eindeutig ist, wird sie entsprechend der TON im LCR auf national oder international erweitert. Dies ist erforderlich, wenn die Durchwahlnummern nicht eindeutig sind und ins nationale oder internationale Format konfiguriert werden müssen.
- D (n):

  Ziffernfolge wählen (1 bis 25 Ziffern). "D" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen.
- E (n):

  Aussenden des Feldinhaltes (1 bis 10). "E" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen. Die Reihenfolge von "E" in Abhängigkeit von (n) ist beliebig. Ein bestimmtes Feld darf mehrmals, auch aufeinanderfolgend, angesprochen werden. "E" darf mit Ausnahme von "E1" (Access Code) von beliebigen anderen Parametern eingeschlossen sein

  Bei schritthaltender Wahl (Gegensatz zur Blockwahl) darf das letzte Element in der Wahlregel nicht E(n) heißen, sondern E(n)A.
- M (n):

  Autorisierungscode (1 bis 16). Dieser Buchstabe darf nicht an der letzten Stelle stehen.
- P (n):

  P(n) darfin der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen. P(n) darf von beliebigen anderen Parametern eingeschlossen sein. (1- bis 60-fache der systemweiten Pauseneinheit).
- S:

  Switch, Umschalten des Wahlverfahrens von IWV auf MFV (bei CONNECT, PROGRESS oder CALL PROC mit PI). "S" darf in der Zeichenkette nur einmal vorkommen und darf nicht an der letzten Stelle stehen. Nach "S" darf nicht mehr der Parameter "C" verwendet werden.
- C:

  Carrier "C" darf in der Zeichenkette nur einmal vorkommen. Die nachfolgenden Zeichen werden ohne Wahlpause gesendet und für den Carrierzugang bei "Single Stage", "Two Stage", "DICS" und "PRI" verwendet.
- U:

  Anwenden des Wahlverfahrens SUB-Adresse. "U" darf in der Zeichenkette nur einmal vorkommen und darf nicht an der letzten Stelle stehen. Nach "U" dürfen die Parameter "S", "P" "M" und "C" nicht mehr verwendet werden.

- N (n) (Nur für USA!):

  Netz-SFG-Gruppe (1 bis 5) oder Bandnummer (1).
- L (Nur für USA!):

  "L" darf nur am Ende der Zeichenkette vorkommen. "L" bewirkt, dass der Anruf als Notruf behandelt wird.

Beispiel:

Das System soll automatisch eine Providervorwahl voranstellen.

Wahlregel D010xxA bedeutet: das System wählt zunächst die Provider-Vorwahl (010xx), dann alle Ziffern nach dem Access Code, die der Teilnehmer gewählt hat (A).

16.2.5.1 Wie Sie Wahlregeln bearbeiten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie auf **Wahlregel**. Alle Wahlregeln werden Ihnen angezeigt.
4) Klicken Sie auf die gewünschte Wahlregel im Menübaum.
5) Sie können folgende Felder bearbeiten:
   - **Regelname**
   - **Wahlregelformat**
   - **Verfahren des Netzanbieters** (**Unbekannt**, **Hauptnetzanbieter**, **MCL Single Stage**, **MCL Two Stage**, **Corporate Network**, **Dial In Control Server**, **Primary Rate Interface**)
   - **Type** (**Unbekannt**, **Ländervorwahl**, **Ortnetzvorwahl**, **Anlagenrufnummer**)
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.2.6 Netzanbieter

Netzanbieter können mit jeder Richtung verbunden werden. Die Auswahl des jeweiligen Netzanbieters wird durch die Wahlregeln für LCR definiert.

Unbekannt

Keine explizite Angabe über einen Netzanbieter.

Hauptnetzanbieter

Bei einer Belegung über den Hauptnetzanbieter erfolgt die einfache Wahl durch Blockwahl oder Wahl einzelner Ziffern in das öffentliche Netz.

MCL Single Stage

Bei MCL Single Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt und anschließend die Rufnummer gewählt. Die Wahl erfolgt dabei bei ISDN im D-Kanal bzw. als normale Wahl bei HKZ.

MCL Two Stage

Bei MCL Two Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt. Nach einer Synchronisationsphase wird zunächst ein ebenfalls konfigurierbarer Authorisierungscode und darauffolgend die Ziel-Rufnummer als DTMF-Zeichen gesendet

Bei Synchronisation durch Zeit muss eine Pause von 2 bis 12 s programmiert werden.

Corporate Network

Ein Corporate Network ist direkt am Kommunikationssystem angeschlossen. Die LCR-Funktion bestimmt aus der vom Teilnehmer gewählten Nummer die entsprechende Richtung und routet das Gespräch entweder über das Leitungsbündel des öffentliches Amtes oder über das Leitungsbündel mit dem firmeneigenen Netz.

Dial In Control Server

Bei dieser Art LCR wird mit einem Präfix der gewünschte Netzanbieter über einen Dial-In Control Server (DICS) angewählt und dabei die Rufnummer und ein konfigurierbarer Authorisierungscode in der Subadresse übermittelt. Die Wahl erfolgt dabei im D-Kanal.

Primary Rate Interface (Primärmultiplexschnittstelle) (nur für USA)

Beim Primary Rate Interface erfolgt die Auswahl des Netzanbieters bzw. des Calling Service in der SETUP-Meldung über die Informationselemente Network Specific Facility, Operator System Access und Transit Network Selection.

Abhängigkeiten

Thema	Abhängigkeit
Anrufinformationen erhalten/weitergeben	Temporäre oder permanente Rufnummernunterdrückung darf nicht aktiviert sein.
ISDN/SUB-Addressing	Das ISDN-Leistungsmerkmal "SUB" muss im öffentlichen Netz beantragt bzw. freigegeben sein.

16.2.7 Gezielte Belegung von Amtsleitungen

Amtsleitungen können von Teilnehmern gezielt belegt werden.

Normalerweise ist eine Priorisierung für die Amtsholung über Least Cost Routing vorgegeben. Meistens ist dabei der günstigste Anbieter an erster Stelle, der zweitgünstigste an zweiter Stelle usw.

Möchte ein Teilnehmer ein Gespräch über einen Anbieter, der nicht an erster Stelle geroutet wird, führen (weil dieser z.B. für Ferngespräche noch günstiger

ist), so kann er diesen Anbieter gezielt über eine Leitungs-Kennzahl oder über eine Leitungstaste anwählen.

Ebenso hat der Teilnehmer über die gezielte Wahl per Kennzahl die Möglichkeit eine Rufnummer zu wählen, deren Wahl nur über ISDN möglich ist (sollte als Anbieter ansonsten z.B. Vodafone vorgegeben sein).

Standardmäßig wird eine Kennzahl (88) für eine gezielte Amtsbelegung über ISDN eingerichtet. Alle Kennzahlen können vom Administrator nachträglich eingericht bzw. geändert werden.

16.2.7.1 Wie Sie die Kennzahl für gezielte Belegung von ISDN-Amtsleitungen konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie auf **Wahlplan**. Die einzelnen Wahlpläne werden aufgelistet.
4) Geben Sie unter **Name** den gewünschten Namen für den Wahlplan ein.
5) Geben Sie unter **Gewählte Ziffern** die Kennzahl und die Kürzel exakt ein (z.B. **88CZ**).

   Anmerkung: 88 ist die standardmäßig vom System vergebene Kennzahl für die gezielte Belegung einer ISDN-Amtsleitung.

   Informationen zu den Kürzeln C und Z siehe LCR-Wahlplan.
6) Geben Sie unter **Wegetabelle** eine **1** ein.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.2.7.2 Wie Sie Kennzahlen für die gezielte Amtsbelegung anzeigen

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** können Sie die Kennzahlen für die gezielte ISDN-Amtsbelegung anzeigen lassen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Das Kommunikationssystem ist an eine analoge Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Amtsleitung ISDN / Analog / ITSP** zu starten.

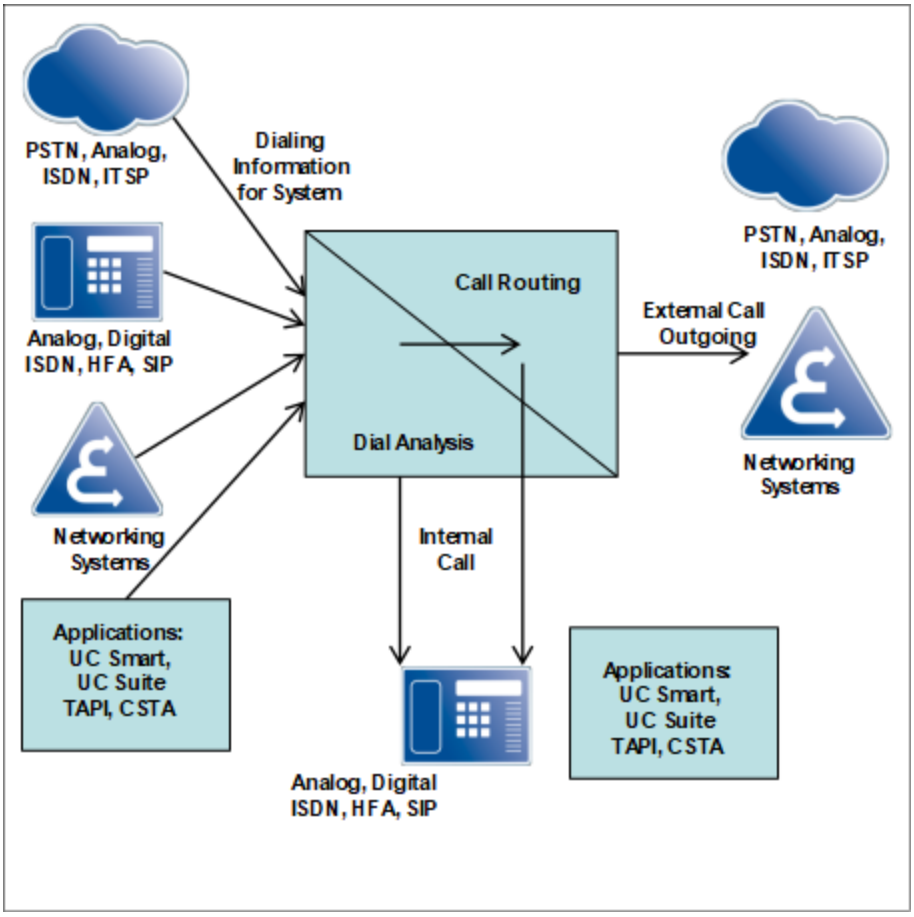
4) Klicken Sie so oft auf **OK & Weiter** bis Sie zum Fenster **Kennzahlen für die gezielte Amtsbelegung** kommen.
5) Im Default sehen Sie die Kennzahl für die gezielte ISDN-Amtsbelegung. Bei konfigurierten ITSPs werden die entsprechenden Kennzahlen angezeigt.
6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

16.3 Wahlbewertung und Call-Routing

In diesem Kapitel wird der Zusammenhang zwischen Wahlbewertung und Call-Routing verdeutlicht. Es erklärt wie das Kommunikationssystem Rufnummern bewertet, die durch Teilnehmer, Leitungen und Applikationen unterschiedlicher Art zur Anwahl eines beliebigen Ziels gewählt werden und wie das Routing nach abgeschlossener Wahlbewertung erfolgt. Die hierfür relevanten Systemfunktionen wurden zum großen Teil bereits in den vorherigen Kapiteln beschrieben. Die Wahl mit öffentlicher Rufnummer innerhalb eines Knotens/einer Vernetzung wird in diesem Abschnitt detailliert beschrieben.

Die Wahlbewertung

- des Kommunikationssystems erfasst und bewertet alle gewählten Rufnummern anhand der Konfigurationsdaten
- prüft Berechtigungen. z.B. anhand von Berechtigungsklassen für Teilnehmer, Teilnehmerflags, Tag/Nacht, erlaubte und verbotene Rufnummern, LCR-Berechtigungen, Zeitplänen, Verbindungsmatrixen, etc.).
- entscheidet, ob eine gewählte Rufnummer intern zugestellt wird oder eine Leitung zu belegen ist. Das gilt sowohl für die Wahl von Internrufnummern als auch für Öffentliche Rufnummern, als auch für netzinterne Rufnummern.
- normiert Rufnummern, d.h. macht Rufnummern für das Kommunikationssystem wählbar. (z.B. kanonisches Format: "+ 49nnn" wird zu "00049nnn", wobei die erste "0" den Hauptzugangscode der Telefonanlage repräsentiert)
- kürzt ggf. Rufnummern (führende Ziffern von Zielrufnummern bei kommender Amtsbelegung werden ggf. abgeschnitten, um DID-Ziele im kurzen Format zu ermitteln)



16.3.1 Überblick Call Routing / LCR

Ein eingehender Anruf wird im Kommunikationssystem verschiedenen Prüfungen unterzogen und entsprechend weitergeleitet.

Prüfung 1 (Internes Rufziel?)

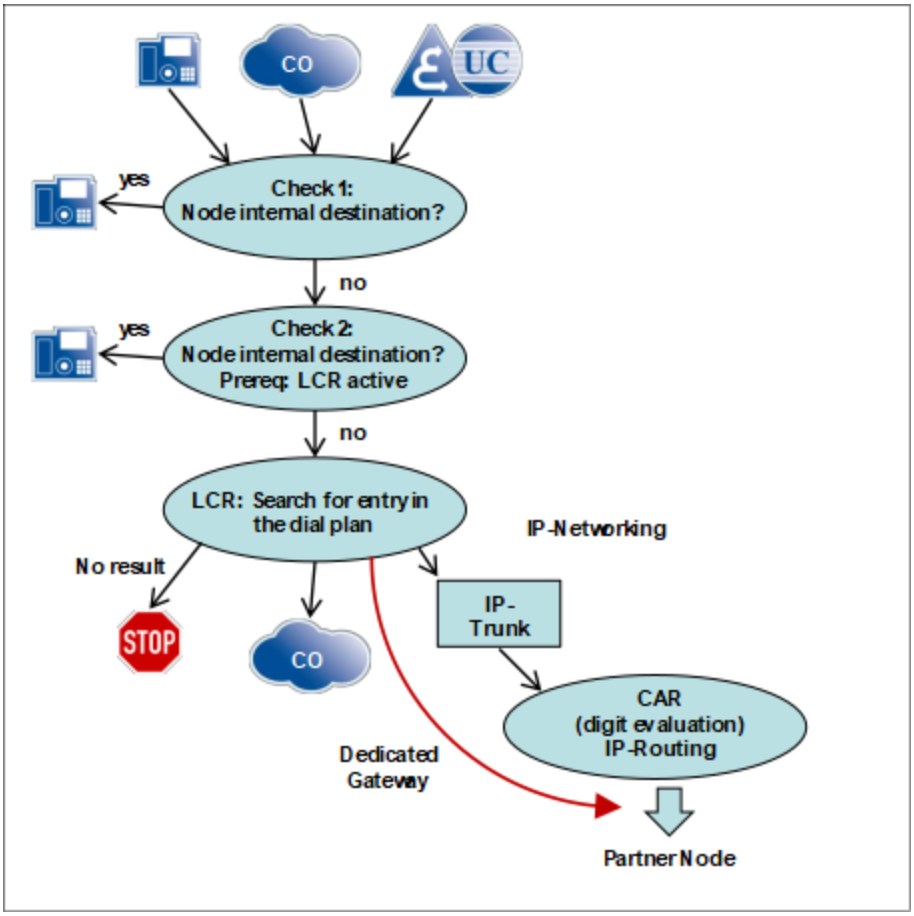
- Ziele mit kanonischer Rufnummer werden zunächst in wählbare Rufnummern (an der Teilnehmer-Schnittstelle) gewandelt, bzw. mit TON=International versehen (ITSP-Schnittstelle).
- Zielrufnummern von Leitung werden ggf. um den Rufnummernanteil der Anlagenrufnummer der entsprechenden Richtung gekürzt.
- Internrufe werden über den internen Wahlplan bewertet, Rufe von Extern durch den Wahlplan der Durchwahlrufnummern.

Prüfung 2 (Internes Rufziel?)

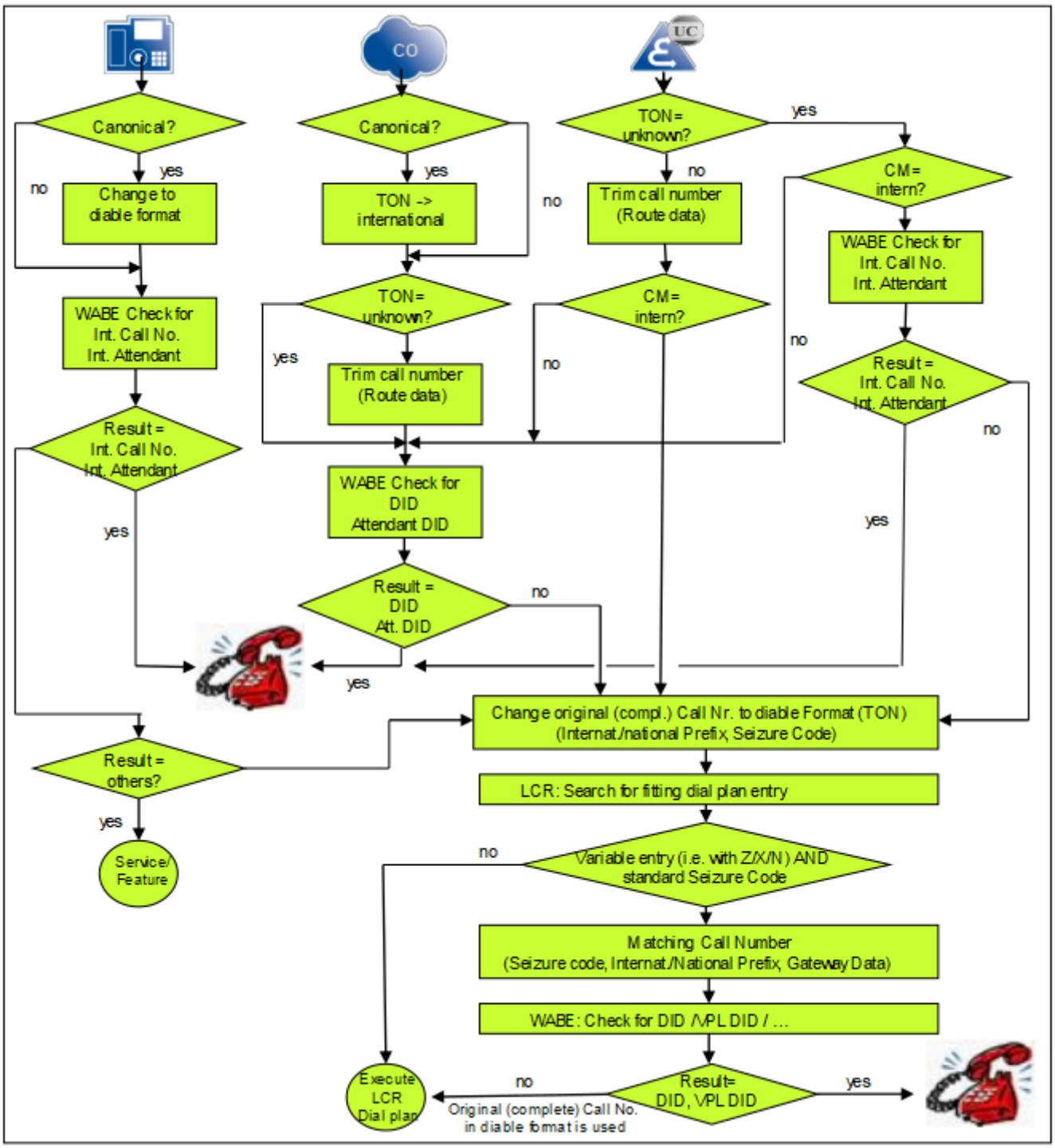
- Teilnehmer, Applikationen, Clients oder andere Kommunikationssysteme wählen Zielrufnummern im öffentlichen Format (z.B. 0 0049nnn)
- Bedingung: Standard-Amtskennzahl (z.B. "0") ist eingerichtet
- Zielrufnunmmer wird entsprechend der Anteile der Standortrufnummer (Gateway Standort) gekürzt und anhand des Wahlplans der Durchwahlrufnummern bewertet, unabhängig davon, ob es sich um einen Intern- oder Externruf handelt.

- Falls kein internes Rufziel gefunden wird, wird die wählbare, ungekürzte (!) Rufnummer im LCR verarbeitet und der Anruf entsprechend über eine Leitung weitergeroutet.

Innerhalb einer IP-Vernetzung ermöglicht der LCR-Wegetabelle-Parameter "Dedicated Gateway" die direkte Adressierung eines Knotens für eine gewählte Rufnummer unter Umgehung der CAR-Wahlbewertung.



16.3.2 Flußdiagramm Wahlbewertung



Erläuterungen zum Flußdiagramm:

Deutsch	Englisch	Erklärung
WABE		Wahlbewertung

Deutsch	Englisch	Erklärung
CM	CM	Classmark, kennzeichnet den Rufer als externen Rufer oder (netz-)internen Rufer
TON	TON	Type Of Number Rufnummerntyp: Unknown, Subscriber (Teilnehmer), National oder International und wird sowohl bei Zielrufnummern als auch bei Ursprungsrufnummern verwendet.
DuWa	DuWa	Durchwahlrufnummer
TNR RNR	Int. Rufnr.	Internrufnummer
Int. Attendant	VPL INT	Vermittlungsplatznummer für Interanrufe
VPL DID	VPL DID	Vermittlungsplatznummer für Externanrufe
SERVICE	SERVICE	Servicekennzahl
LCR	LCR	Least-Cost-Routing

UC-Clients verhalten sich bzgl. der Wahlbewertung wie Teilnehmer, die über CSTA gesteuert werden.

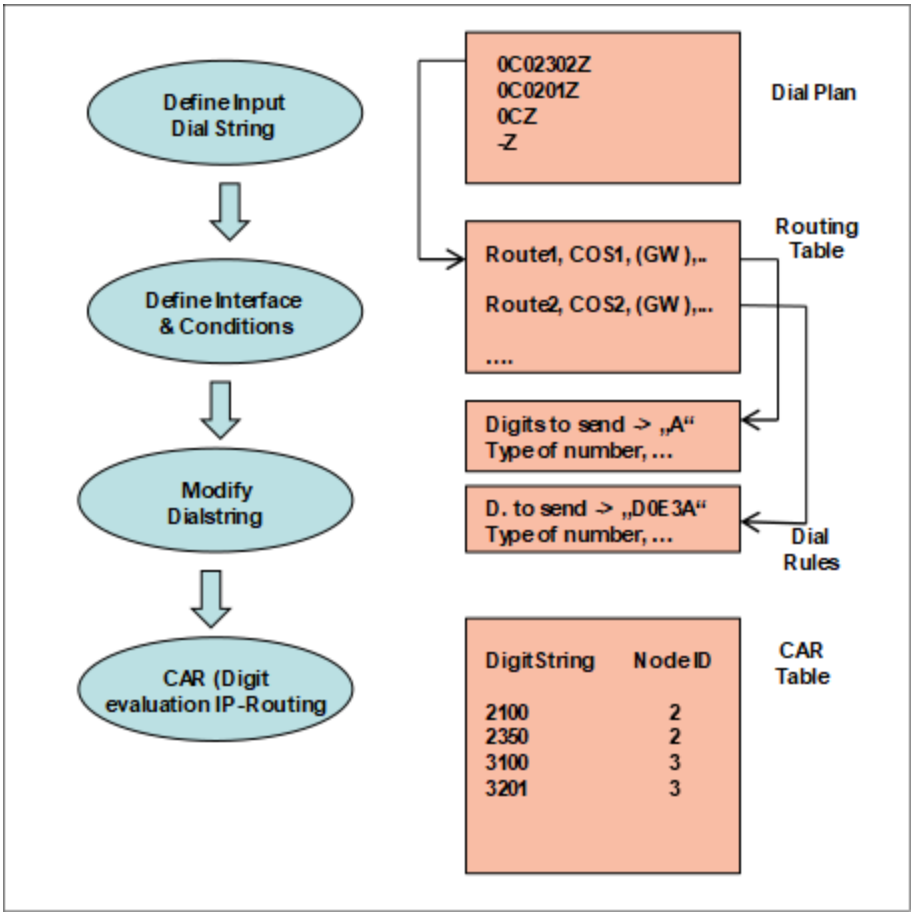
Die UC-Suite verhält sich bzgl. der Wahlbewertung wie ein SIP-Q-Trunk.

16.3.3 Call Routing und LCR im Netzverbund

Bei der Vernetzung spielen Call Routing und LCR eine wichtige Rolle. Über Wahlplan und Wahlregeln werden die Anrufe geroutet. Eine besondere Rolle übernimmt das dedizierte Gateway.

LCR Basics

LCR-Einträge bei der Ersteinrichtung



Die Einträge in der Wegetabelle (Routing table) werden, wenn keine erfolgreiche Leitungsbelegung erfolgt, nacheinander in einer Schleife abgearbeitet.

Anmerkung: Bei Standalone-Systemkonfigurationen muss die Regel -z entfernt werden.

Bei der erstmaligen Inbetriebnahme des Kommunikationssystem erfolgen länderabhängig bestimmte Default-Einträge im LCR-Wahlplan. Bis Wahlplan 35 werden systemseitige Einträge für Notrufe, Auskunft, Sonderrufnummern, Standard-Amtsbelegung für PSTN und ITSPs, UC Suite, Vernetzung und die Berücksichtigung der Wahl im internationen Format auf ISDN-Amtsleitungen vorbelegt.

Dieser Bereich kann durch Konfigurationsänderungen (z.B. Änderungen des Flags **Standortnummer**) beeinflusst werden. Daher ist sicherzustellen, dass die Standard-Amtsbelegung mit der Änderung der Standortnummer weiterhin funktioniert (wichtig bei Wahl mit öffentlichen Rufnummern).

Tipp: Ab LCR-Wahlplan 36 stehen Einträge zur freien Verfügung.

16.3.3.1 Dediziertes Gateway

Das dedizierte Gateway ist nur bei einer IP-Vernetzung relevant.

Warum ein dediziertes Gateway notwendig ist?

Wie können Ziele per Konfiguration, dauerhauft eingerichtet werden?

Anwendungsfälle für ein dediziertes Gateway

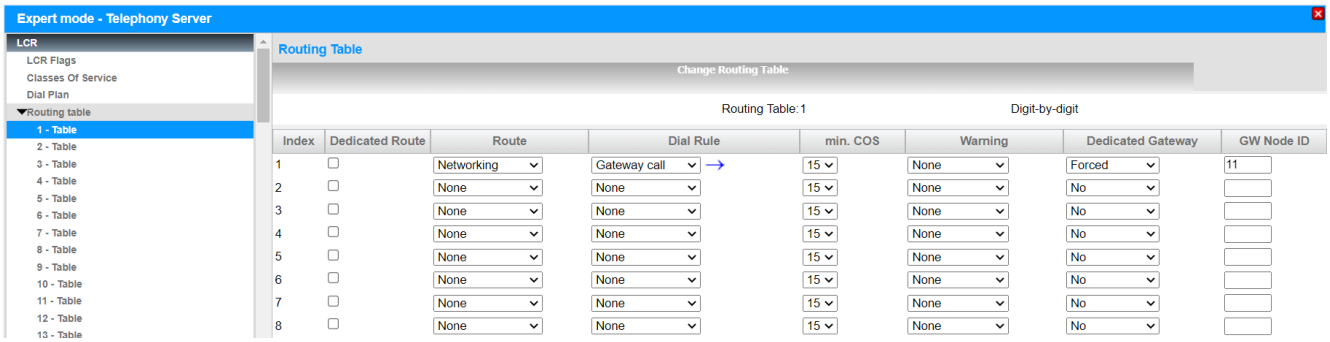
Das dedizierte Gateway im WBM

Folgende Werte können eingestellt werden:

- Die CAR-Tabelle jedes Kommunikationssystems enthält netzweite Rufnummern der jeweils anderen Knoten und wird zyklisch bei Updates automatisch aktualisiert (überschrieben). Daher sind CAR-Tabellen nicht geeignet um manuell hinzugefügte Einträge dauerhaft zu nutzen.
- Es sind netztweit gültige Rufnummern eingetragen, d.h. es ist kein knoten-individuelles Routing möglich (z.B. "0" zum jeweils zugehörigen Gateway-Knoten)
- Durch Verwendung einer direkten Adressierung im LCR
- Das dedizierte Gateway adressiert direkt den Zielknoten anhand der Knoten ID (IP-Adresse)
- Bei Verwendung des dedizierten Gateways werden die CAR-Tabellen übersprungen (siehe vorheriges Bild).

Direktes Adressieren

- von TDM-Gateways um Amtsleitungen zu belegen ("0CZ")
- von TDM-Gateways um Breakouts über separate Kennzahlen zu realisieren
- von netzinternen Knoten, die über öffentliche Rufnummern erreicht werden sollen
- von TDM-Gateways, denen die Teilnehmer einer Multi Gateway Vernetzung (an einer OpenScape Business S) zugewiesen sind (z.B. Teilnehmer 1 gehört per Definition zum Gateway 1 und Teilnehmer 2 gehört zum Gateway 2).
- von Gateways und Anrufen, deren Ursprung in einer Multi Gateway Konfiguration NICHT einem bestimmten Gateway zugeordnet werden können (z.B. die Faxgruppe eines UC Contact Centers)



Nein	Die Rufnummernbewertung erfolgt anhand der CAR-Tabellen (keine **GW Knoten-ID** erforderlich)

Erzwungen	Wird direkt zum entsprechenden Gateway geroutet (GW Knoten-ID = n)
Mehrere Standorte (Multi Location)	Nur bei Multi-Gateway-Konfigurationen zu verwenden: Anhand der Multi-Gateway-Konfiguration der OpenScape Business S-Teilnehmer kennt das Kommunikationssystem die Zuordnung zu deren Gateway und kann daher den gehenden Anruf gezielt zum entsprechenden Gateway routen. In der Konfiguration **Mehrere Standorte** wird die GW Knoten-ID nur dann verwendet, wenn durch die Zuordnung der Teilnehmer kein Gateway identifiziert werden kann (Default).

16.3.4 Szenarien: Wahlbewertung und Call Routing

Anhand von Szenarien werden Abhängigkeiten und erforderliche Konfigurationsparameter beschrieben, um die Abläufe im Kommunikationssystem zu erläutern. Die dargestellten Szenarien können je nach Anwendungsfall aufeinander aufbauen.

Einzelsystem

Vernetztes System als Unteranlage (ohne Amtsleitung)

Netzverbund mit Multi Gateway

1) Teilnehmer A ruft Teilnehmer B über Internrufnummer
2) Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer
3) Teilnehmer A ruft externen Teilnehmer über Amt
4) ISDN-Amt ruft Teilnehmer A
5) Sonderkonfigurationen und entsprechende Auswirkungen:

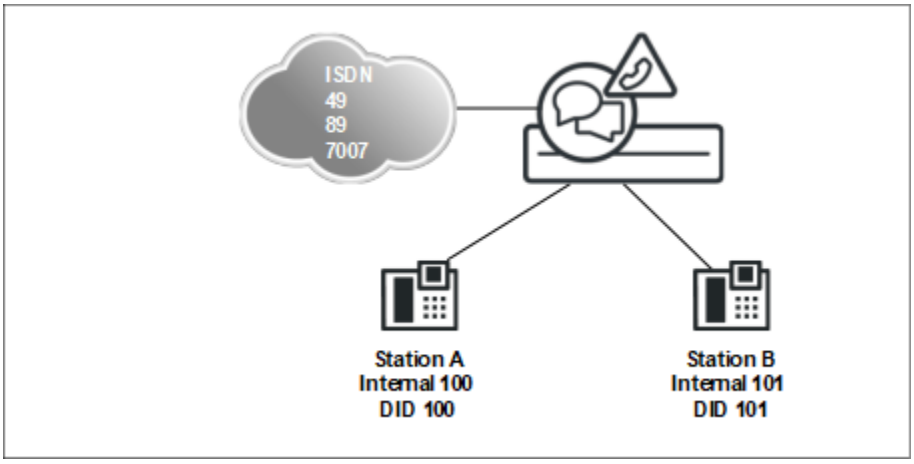
2 Amtsrichtungen

1) Teilnehmer A ruft Teilnehmer C über Internrufnummer
2) Teilnehmer A ruft Teilnehmer C über öffentliche Rufnummer im Netzverbund
3) ISDN-Amt ruft Teilnehmer C

1) ISDN-Amt Gateway 1 ruft Teilnehmer D
2) Teilnehmer D ruft externen Teilnehmer über Amt

16.3.4.1 Teilnehmer A ruft Teilnehmer B über Internrufnummer

Konfiguration der beiden Intern-Rufnummern

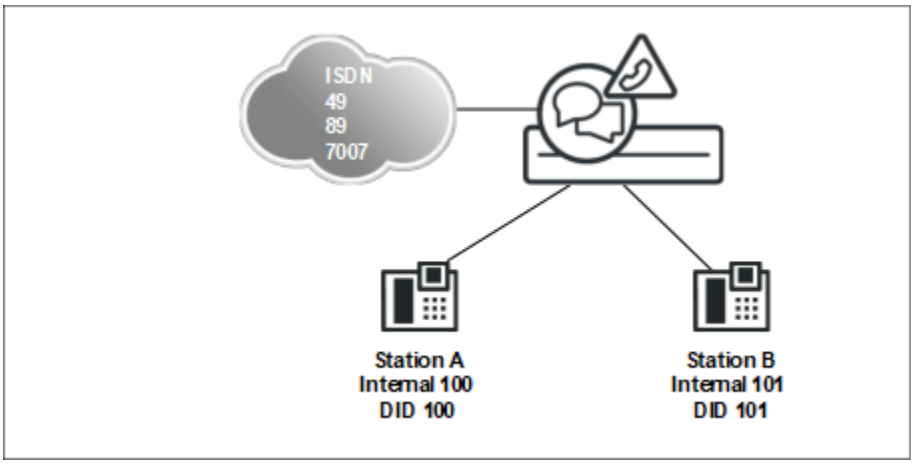


	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

16.3.4.2 Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer

Konfiguration

Abhängigkeiten der "Standortnummer" (Gateway Location)



Der Anruf wird system-intern zugestellt, da die Zielrufnummer ein DID-Teilnehmer des eigenen Systems ist.

	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

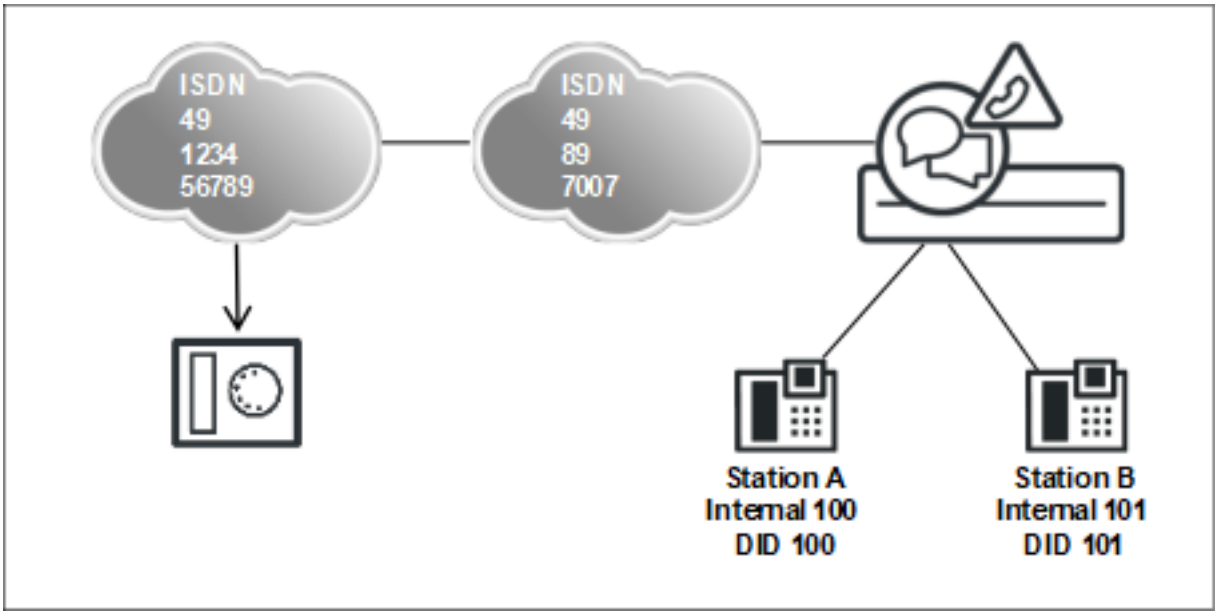
Nachdem die Zielrufnummer anhand der Gateway Location abgestrippt wurde, wird mit der abgestrippten Rufnummer im DID-(DUWA-)Rufnummernplan nach einem Ziel gesucht.

Die Standortnummer (Gateway Location) wird bei der Wahl mittels öffentlicher Rufnummer ausgewertet. Wenn die gewählte Rufnummer in den relevanten Anteilen mit dieser Nummer übereinstimmt, wird die DID-Tabelle ausgewertet und, bei Übereinstimmung, das betreffende interne Ziel gerufen (keine Belegung einer Leitung !). Die Standortdaten werden durch Setzen des Flags Location Number automatisch von den entsprechenden Richtungsdaten (PABX-Number incoming) übernommen und brauchen in Standardszenarien nicht verändert zu werden.

In den DID-Tabellen dürfen daher nur gültige, diesem System zugeordnete Rufnummern eingetragen sein, da sonst Verdeckungseffekte mit Rufnummern im öffentlichen Netz auftreten können. Es würde sonst u. U. das durch eine ungültige DID identifizierte interne Ziel gerufen, obwohl ein Ruf über eine Leitung zu einem externen Ziel beabsichtigt ist.#

Änderungen des Flags "Standortnummer" beeinflussen unter Umständen die vorbelegten Standard-LCR-Einträge. Es ist sicherzustellen, dass die Standard-Amtsbelegung mit der Änderung der Standortnummer weiterhin funktioniert. Dies ist wichtig bei Wahl mit öffentlichen Rufnummern.

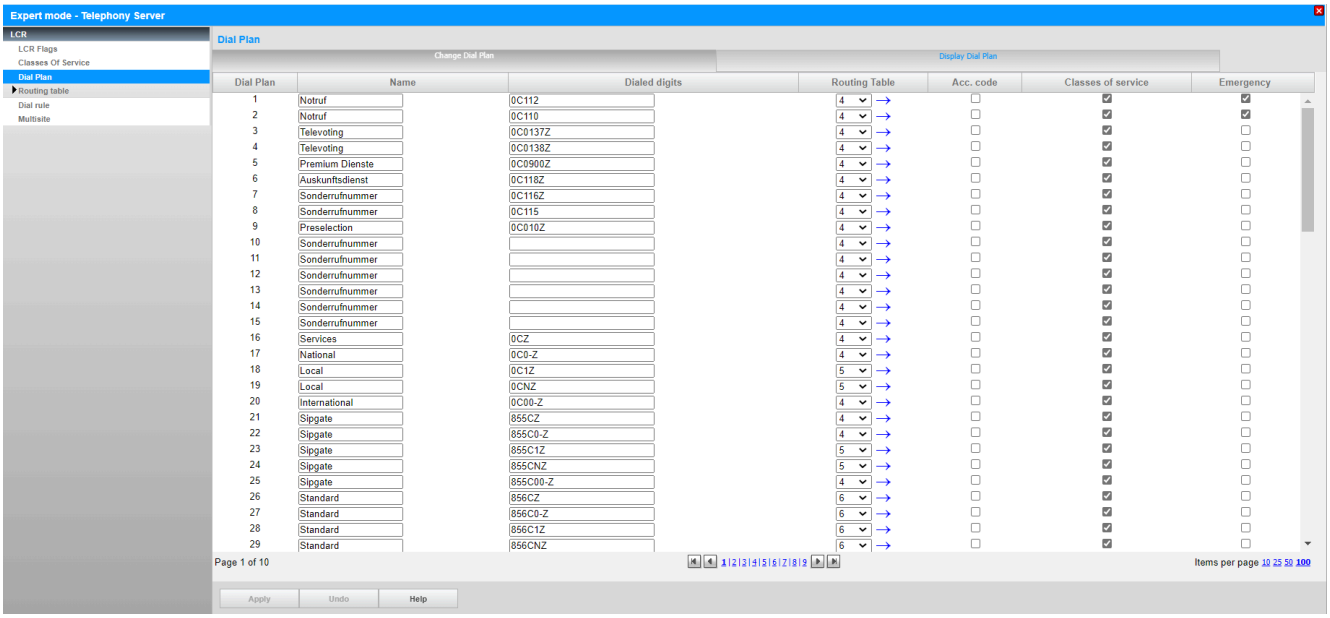
16.3.4.3 Teilnehmer A ruft externen Teilnehmer über Amt



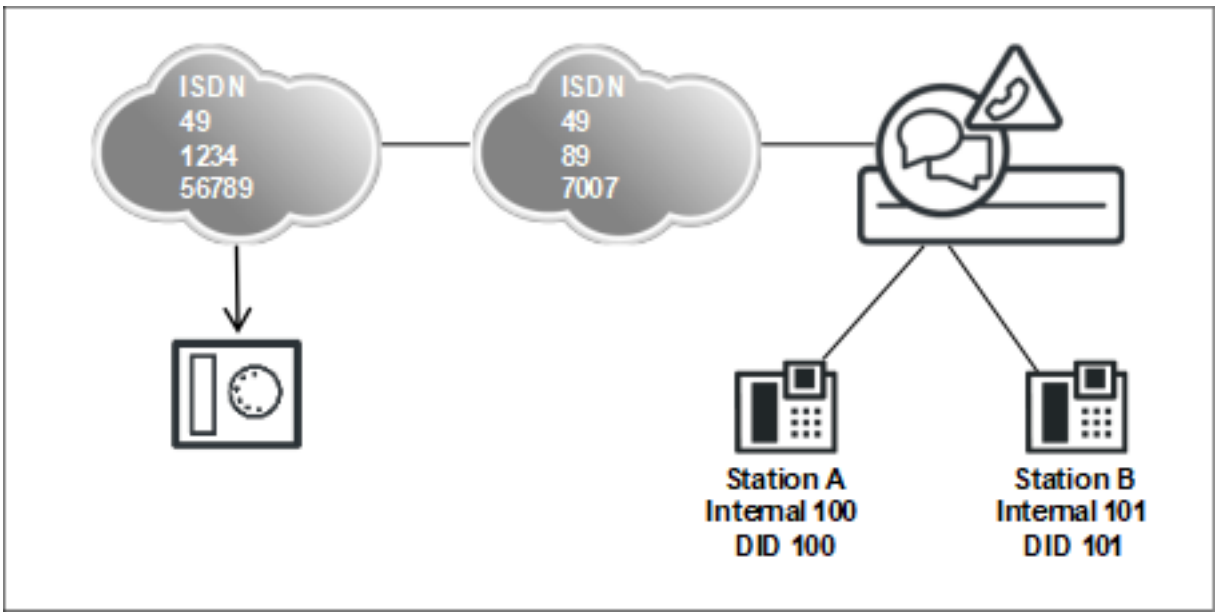
Der Anruf wird per LCR geroutet, da das Ziel nicht im eingenen Kommunikationssystem liegt.

Zusätzlich zu den Daten des vorherigen Szenarios "Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer" muss im LCR ein geeignetet Wahlplan-Eintrag zur Belegung der Amtsleitung vorhanden sein (z.B. "0CZ").

Die LCR-Wegetabelle und der Wahlplan müssen dem entsprechend eingerichtet sein.

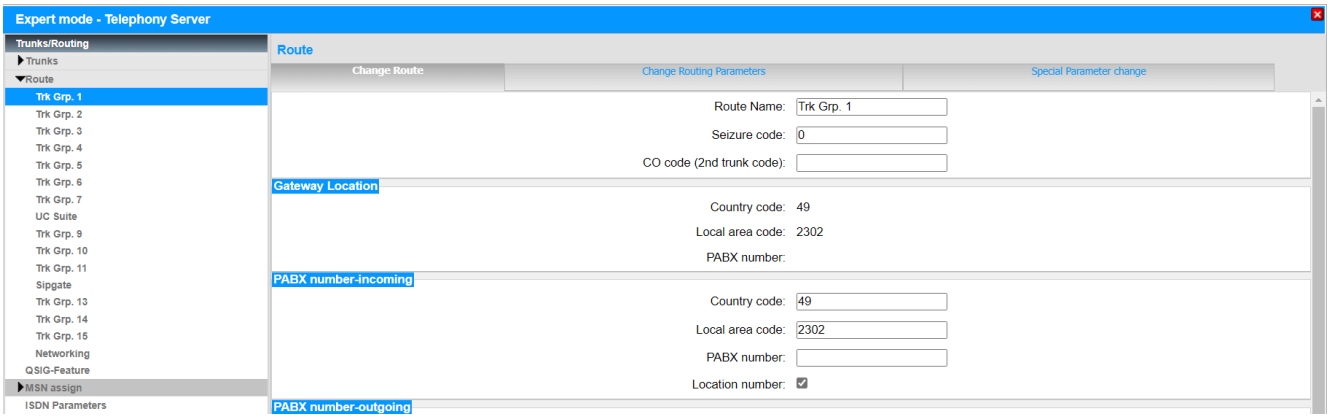


16.3.4.4 ISDN-Amt ruft Teilnehmer A



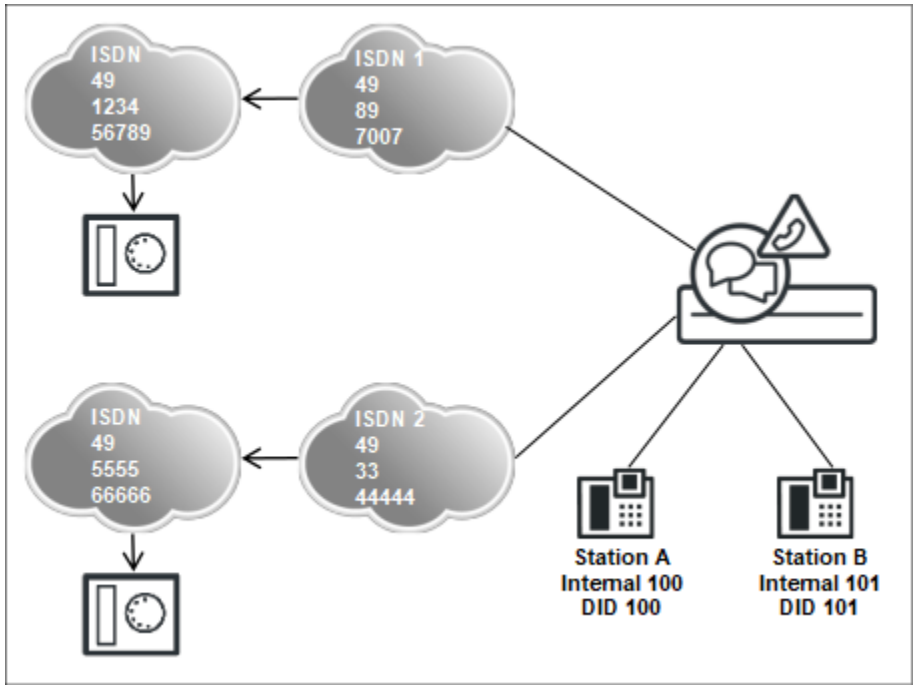
Bei einem kommenden Anruf über ISDN-Trunk wird die Zielrufnummer anhand der Konfigurationsdaten der Anlagenrufnummer kommend (PABX number incoming) der Richtung abgestrippt. Mit dem verbleibenden Rest der Zielrufnummer (Duwa) wird nach einem Ziel im Duwa-Wahlplan gesucht.

Die Parameter des Gateway-Standorts bzw. des Flags **Standort-Nummer** spielen für dieses Szenario keine Rolle.



16.3.4.5 Sonderkonfigurationen

Sonderkonfigurationen und entsprechende Auswirkungen: 2 Amtsrichtungen



Teilnehmer A ruft externen Tln über Amtsanschlus 1 bzw. 2

Beispiel:

- Ein Kunde möchte einen Standard-Anschluß ISDN 1 verwenden. Dieser wird als Standortnummer eingerichtet.
- Additiv wird ein zweiter Anschluß ISDN 2 für besondere Anwendungen verwendet.

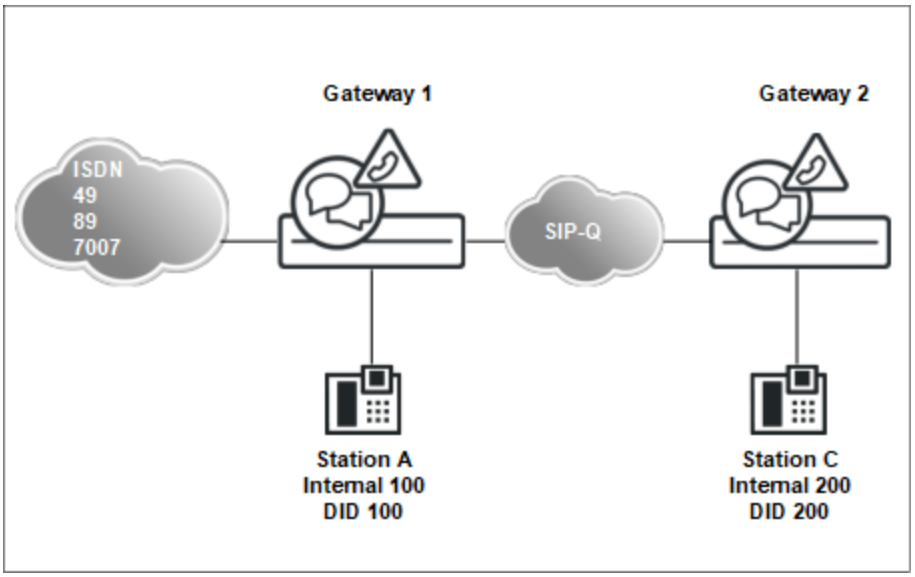
Hinweise bzw. Einschränkungen:

- Nur EINE Amtsrichtung (ISDN 1 = Standort des Systems) wird in vollem Umfang unterstützt, d.h. es kann keine Mehrkundenkonfiguration (Gemeinschaftsanlage) mit gleichberechtigten Amtsanschlüssen eingerichtet werden.

- Der additive Amtsanschluß ISDN 2 kann für Basic Call (kommend/gehend) verwendet werden.
- In komplexen Vermittlungsszenarien kann eine korrekte Rufnummerndarstellung unter Umständen nicht sichergestellt werden.
- Bei Anschaltung von Applikationen wird nur die Standort-Rufnummer unterstützt, ebenso die Wahl von internen Zielen mit öffentlicher Rufnummer.
- Die Konfiguration leitet sich bzgl. Richtungskonfiguration und LCR aus den vorangegangenen Beispielen ab.

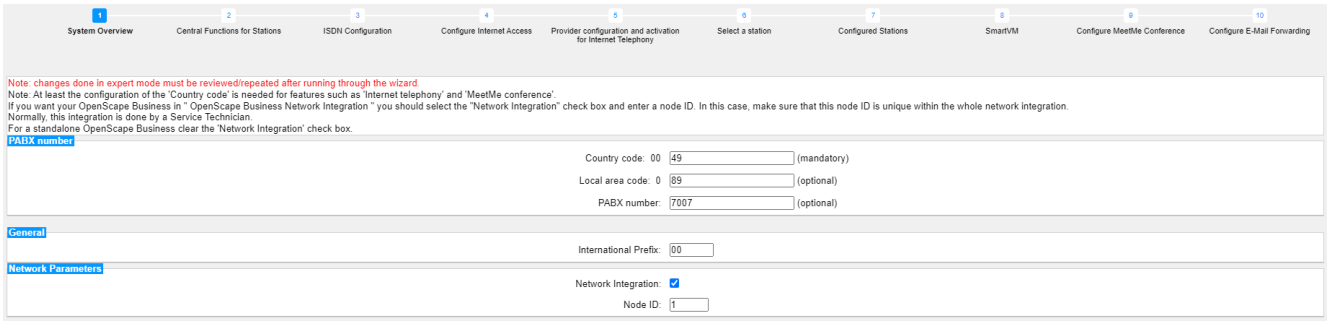
16.3.4.6 Teilnehmer A ruft Teilnehmer C über Internrufnummer

Vernetztes Kommunikationssystem als Unteranlage (ohne Amtsleitung)



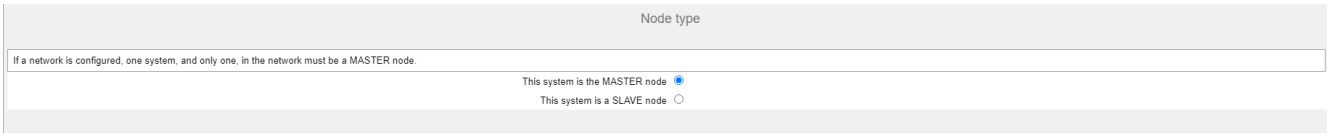
Voraussetzungen der Standalone-Systeme vor der Vernetzung:

- Beide Kommunikationssysteme haben eindeutige IP-Adressen und sind im IP-Netz des Kunden eingebunden.
- Beide Kommunikationssysteme sind per WBM im Kundennetz administrierbar.
- In der Basisinstallation ist je Kommunikationssystem eine eindeutige Knoten-ID für die Vernetzung vergeben (z B. System 1 = Knoten-ID 1 und System 2 = Knoten-ID 2).
- Festlegung der Nummerierung in der Grundinstallation der Systeme 1 und 2: Bei der Nummerierung der Standalone-Systeme muss die geschlossene Nummerierung im zukünftigen Netzverbund berücksichtigt werden.
- Dieses Beispiel geht davon aus, dass eine geschlossene Nummerierung (bei Einsatz von UC-Suite zwingend!) zum Einsatz kommt, Konfiguration über Netzwerk-Wizard. Bei einer offenen Nummerierung (möglich bei UC-Smart) wird der Netzwerk-Wizard nicht verwendet. Bei einer Anbindung von OpenScape Voice und OpenScape 4000 ebenfalls nicht.



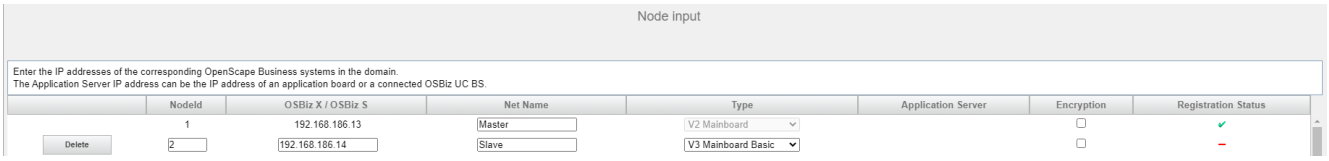
Starten Sie den Netzwerk-Wizard in System 1. Dieses System (dieser Knoten) wird als Master deklariert. Der Master hat verschiedene zentralen Funktionen im Netzverbund (z.B. Administration, Lizenzverwaltung bei zentraler Lizenzierung, CSP netzweit).

Falls sich eine OpenScape Business S im Netzverbund befindet, sollte diese bevorzugt zum Master erklärt werden (Bandbreite, Performance).



Je Knoten werden die IP-Adressen eingetragen, damit sich die Systeme nach Abschluss der Administration selbstständig finden. Unter **Typ** stehen die OpenScape Business Systeme.

Dieser Dialog ist für Knoten 2 (Slave) ebenfalls durchzuführen.



Bei erfolgreicher Konfiguration synchronisieren beide Systeme (Knoten) ihre Rufnummern und tragen die Rufnummern des anderen Knotens in die CAR-Tabelle ein.

Mit der Erstellung der CAR-Tabellen ist netzweite Telefonie mit Internrufnummern möglich. UC-Suite wird ebenfalls netzweit gestartet. Weitere Schritte zur vollständigen Inbetriebnahme des Netzes stehen in den weiteren Szenarien.

Die Kontrolle der CAR-Einträge ist über **Experten-Modus** > **Sprachgateway** > **Networking** > **Routing** möglich.

Die Übersicht über die automatische Synchronisierung im Netzverbund sehen Sie im WBM (Sync-Status).

Weitere Netzknoten können jetzt unter dem Menüpunkt **Networking** in der Navigationsleiste im Direktzugriff administriert werden.

16.3.4.7 Teilnehmer A ruft Teilnehmer C über öffentliche Rufnummer im Netzverbund

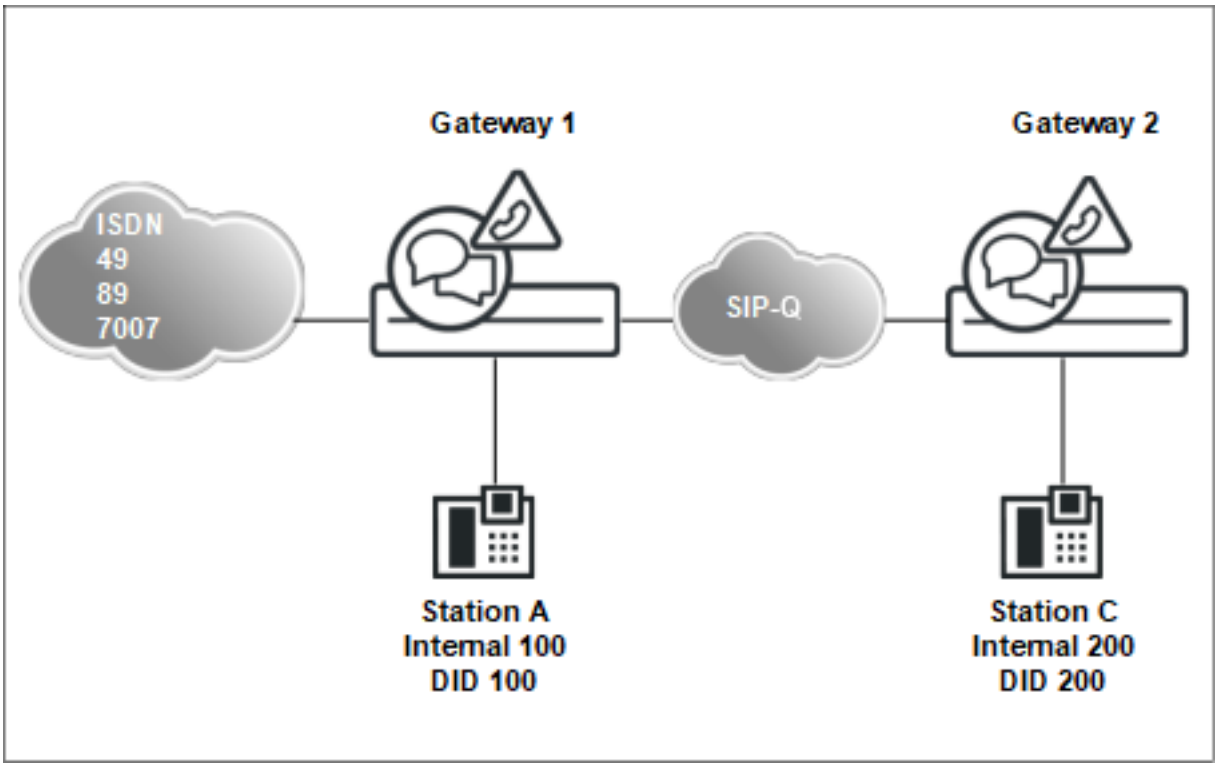
Vernetztes Kommunikationssystem als Unteranlage

Konfiguration von Knoten 1, Einrichtung im LCR über Dediziertes Gateway

Konfiguration von Knoten 2, Einrichtung der Richtung "Networking"

Konfiguration von Knoten 2, Einrichtung der Standortnummer an der "Dummy-Amtsrichtung"

Konfiguration von Knoten 2, Einrichtung im LCR über dediziertes Gateway



Besonderheiten dieses Szenarios:

- System 1 erkennt, dass die Zielrufnummer nicht zum eigenen System gehört. Die weitere Suche erfolgt daher im LCR. Das dedizierte Gateway ist im LCR des Systems 1 zur direkten Adressierung der Knoten-ID des Systems 2 zu verwenden. Die Zielrufnummer ist keine Internrufnummer des Netzes (damit wäre sie in der CAR-Tabelle), sondern eine öffentliche Rufnummer, die vom Teilnehmer in drei unterschiedlichen Längen gewählt werden kann:

  Lang = 00049897007nnn

  Mittellang = 00897007nnn

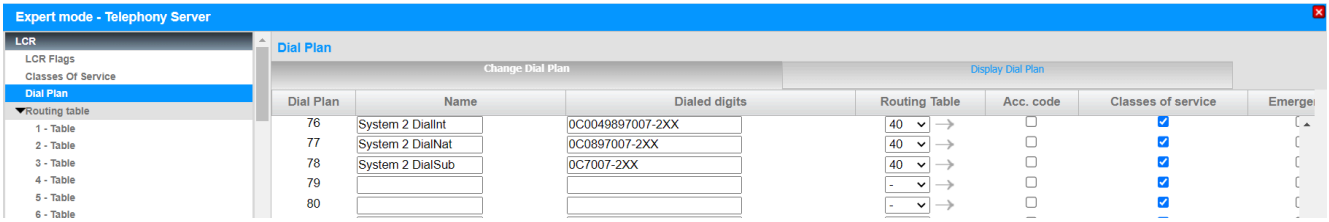
  Kurz = 07007nnn

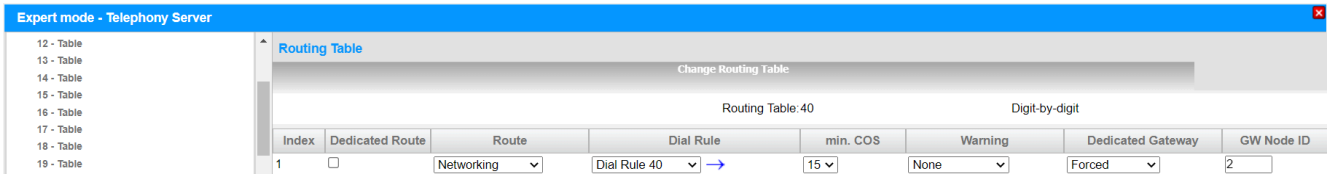
  Das Beispiel geht davon aus, dass alle 2xx-Durchwahlnummern Teilnehmer im System 2 sind.

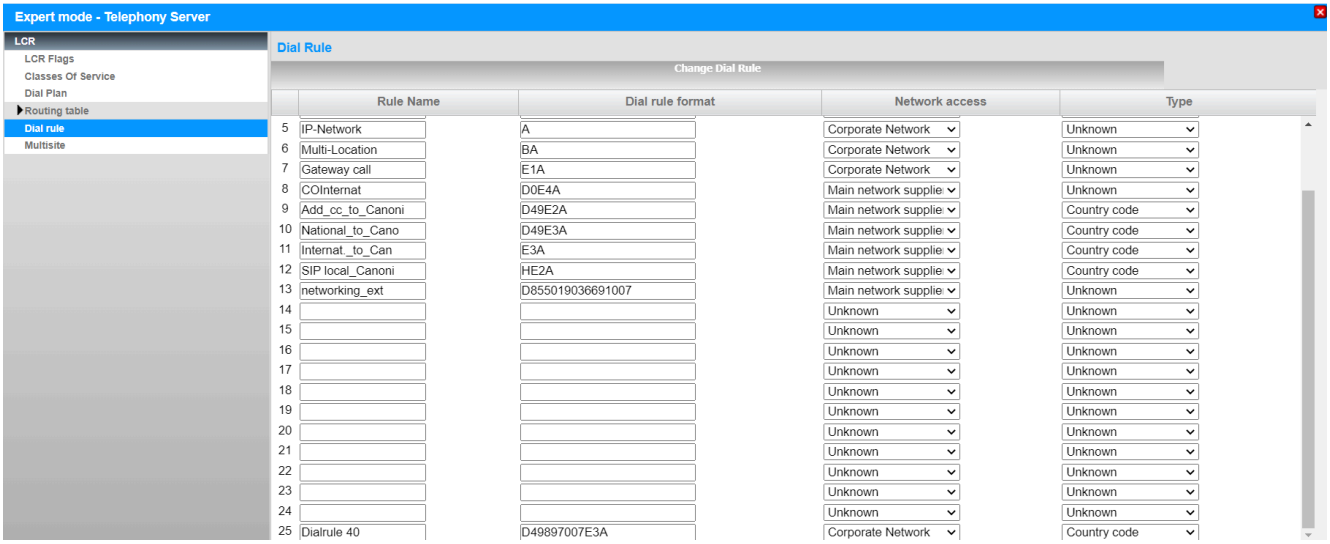
  Anmerkung: Die Wahlplaneinträge müssen so genau konfiguriert werden, dass ALLE getroffenen Rufnummern auch wirklich zum Unterknoten (Netzverbund) gehören. Das kann bei Besonderheiten des Rufnummernplans eine

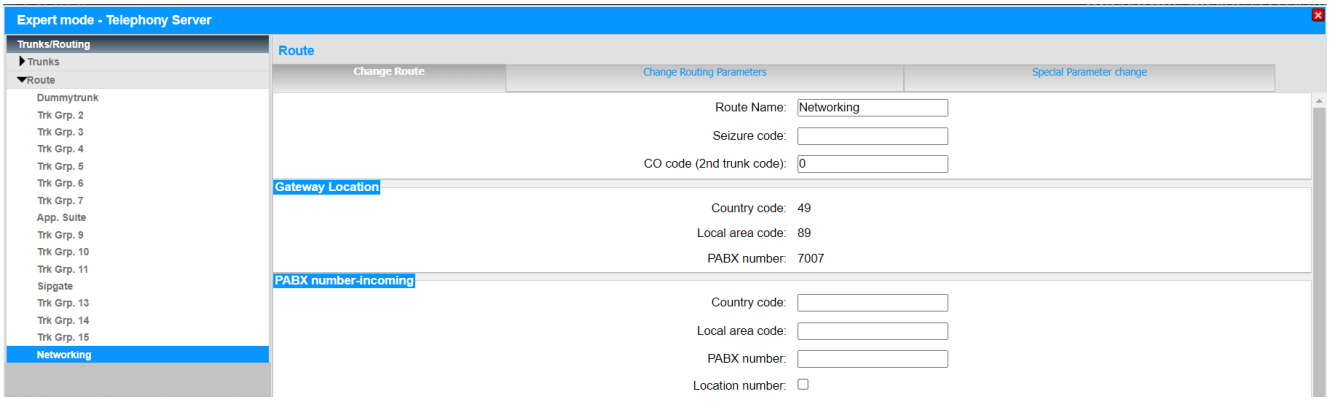
größere Anzahl Einträge erforderlich machen, z.B. bei geteiltem Amtsanschluss oder einer MSN-Konfiguration.

- Im Knoten 2 wird eine Standortnummer mittels "Dummy-Amtsrichtung" mit den Standortdaten von Knoten 1 (Gateway) eingetragen, damit die Zielrufnummer bei der öffentlichen Wahl abgestrippt werden kann, bevor nach einem internen Ziel in Knoten 2 gesucht wird.

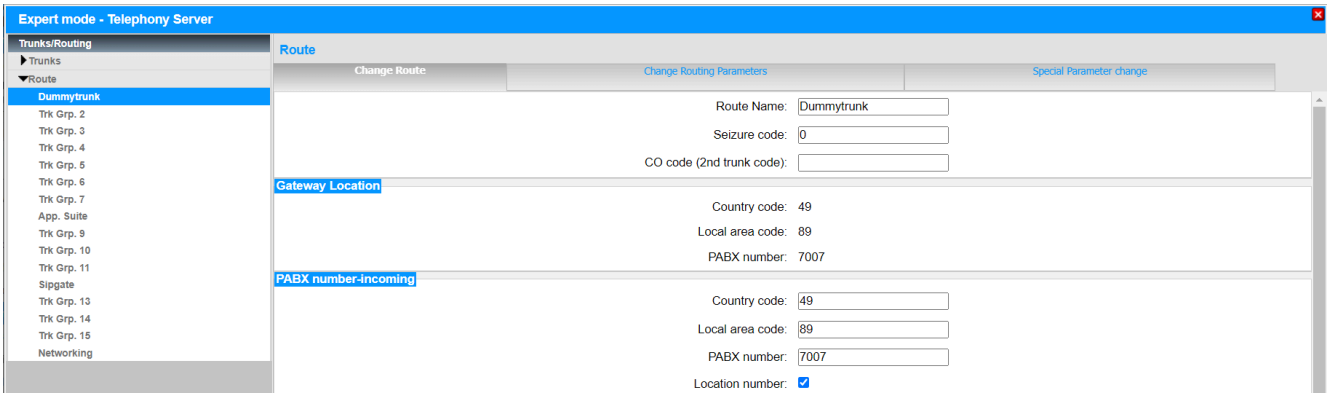








In der Registerkarte **Richtungsparameter ändern** ist die Richtungsart **PABX** einzutragen.



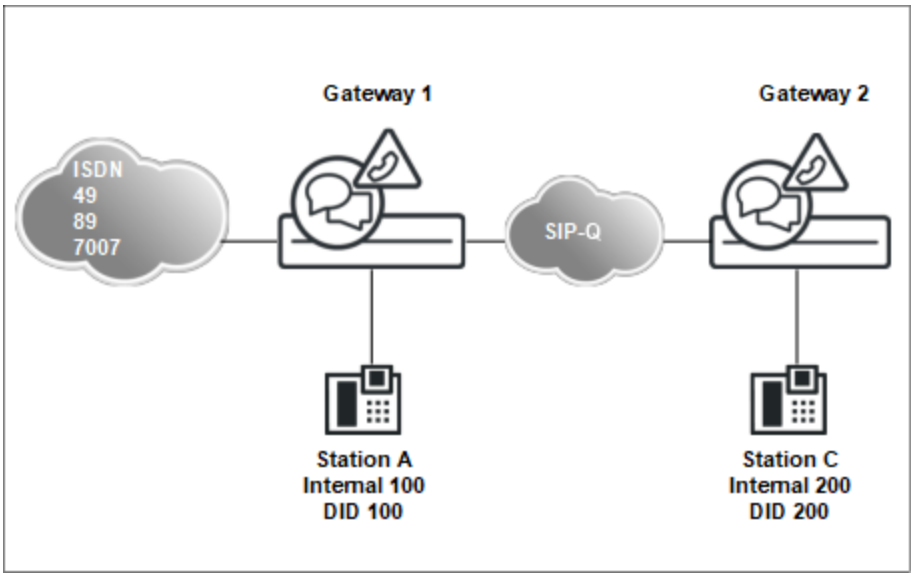
In der Registerkarte **Richtungsparameter ändern** ist die Richtungsart **Amt** einzutragen.

Im Knoten 2 werden alle öffentlichen Rufnummern, die nicht zum eigenen Knoten gehören, zum Knoten 1 geroutet (Standardwahl z.B. 0CZ)

16.3.4.8 ISDN-Amt ruft Teilnehmer C

Vernetztes System als Unteranlage

Besonderheiten dieser Konfiguration



Beispiel: Kommender Anruf mit Zielrufnummer mit TON = Teilnehmer

- Knoten 1 ist, wie im vorherigen Szenario beschrieben, einzurichten.

  Die Adressierung von Knoten 2 erfolgt in beiden Fällen mit der öffentlichen Rufnummer, und zwar unabhängig davon, ob der Ursprung der Verbindung in Knoten 1 (Teilnehmer des Systems 1) oder im öffentlichen Netz liegt.

Tipp: Die Wahlplaneinträge müssen so genau konfiguriert werden, dass ALLE getroffenen Rufnummern auch wirklich zum Unterknoten (Netzverbund) gehören. Das kann bei Besonderheiten des Rufnummernplans eine größere

Anzahl Einträge erforderlich machen, z.B. bei geteiltem Amtsanschluss oder einer MSN-Konfiguration.

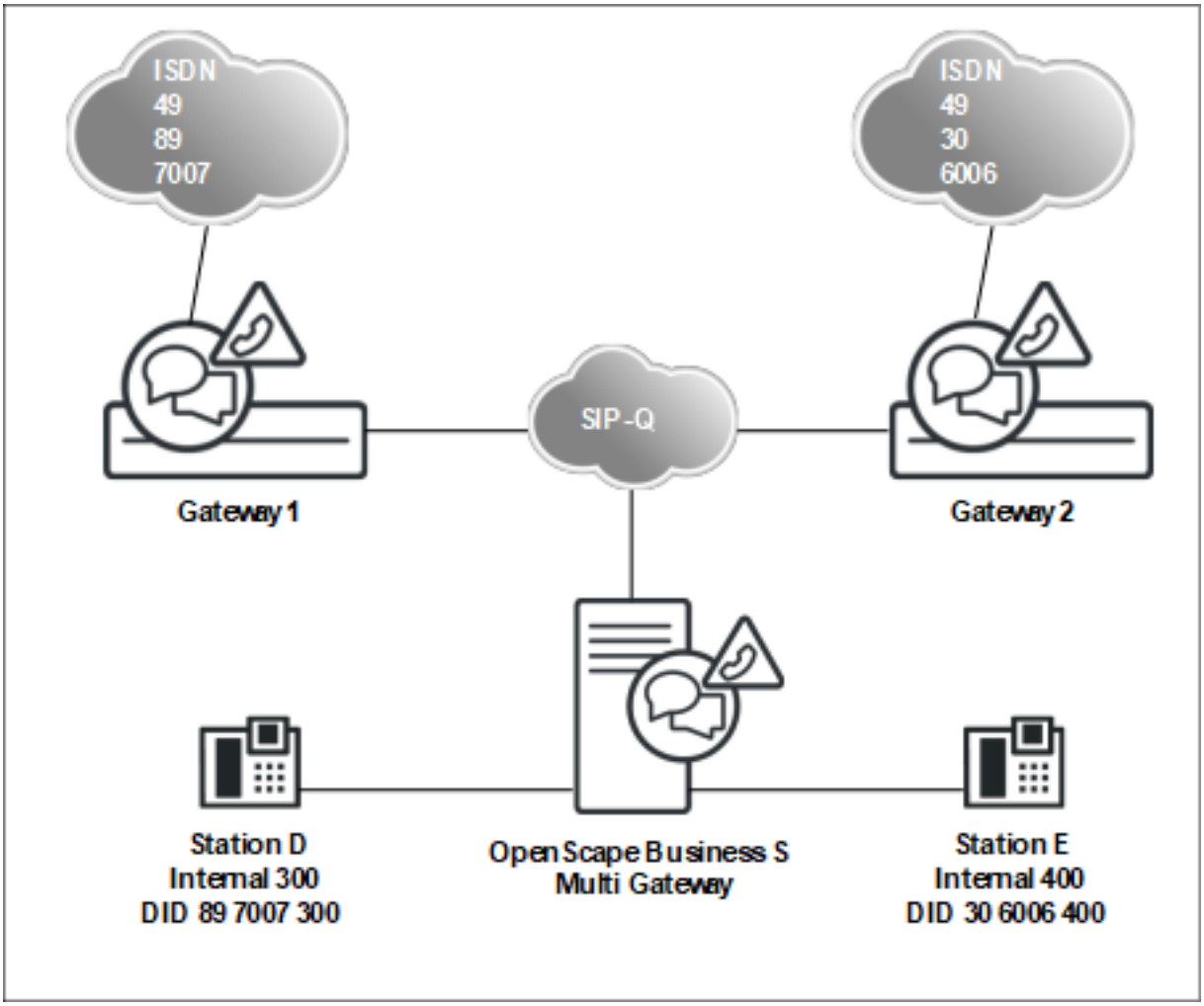
- Knoten 2 ist ebenfalls, wie im vorherigen Szenario beschrieben, einzurichten.

16.3.4.9 ISDN-Amt Gateway 1 ruft Teilnehmer D

Vernetztes System in einer Multi Gateway Konfiguration

Konfiguration

Konfiguration des Multi Gateway, OpenScape Business S



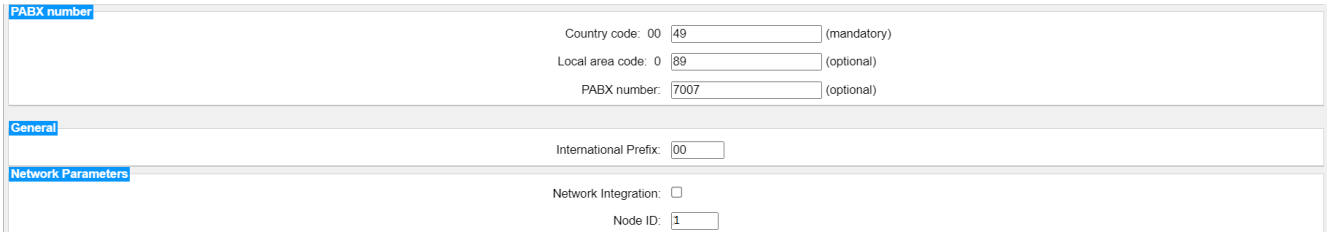
Beispiel: Kommender Anruf mit Zielrufnummer mit TON = Teilnehmer

Besonderheiten in diesem Szenario:

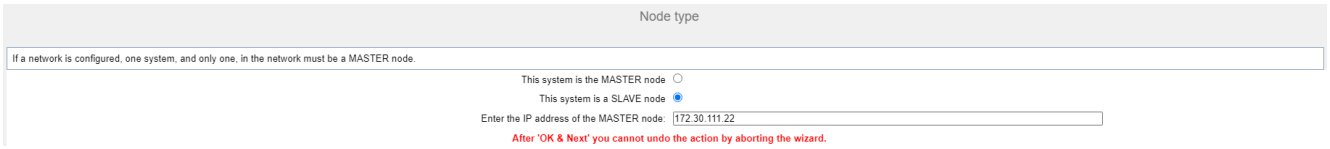
- Das Gateway 1 wird im Prinzip wie im vorherigen Szenario (Gateway 1) eingerichtet, d.h. zunächst Basisinstallation und dann den Netzwerk-Wizard durchlaufen. Wesentlicher Unterschied: Die Gateways werden als Slave, die OpenScape Business S wird als Master eingerichtet (Performance, Bandbreite Lizenzierung).

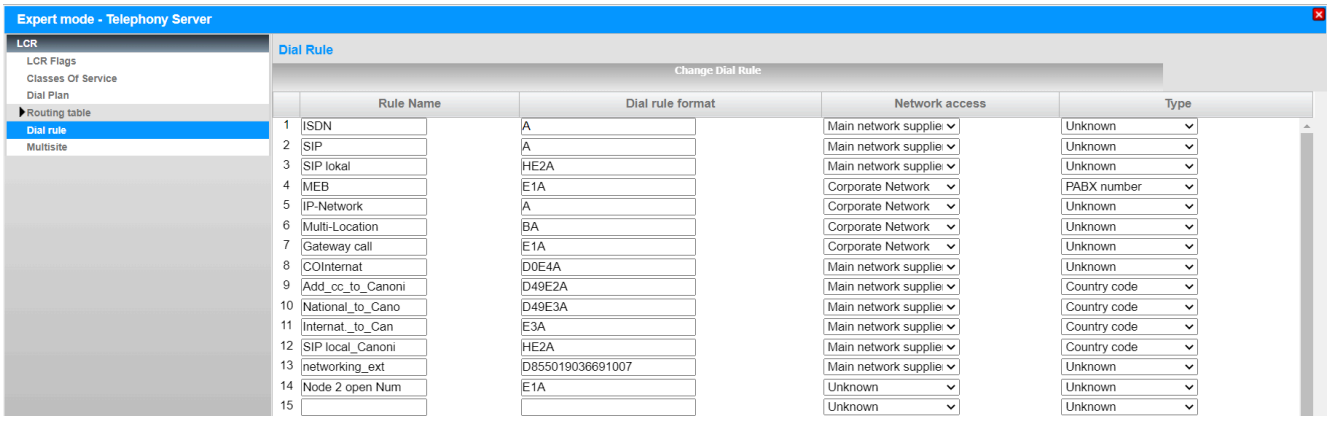
- In diesem Beispiel werden nur die wesentlichen Unterschiede zum vorherigen Szenario genannt.

Basisinstallation von Gateway 1



Netzwerk-Wizard für Gateway 1





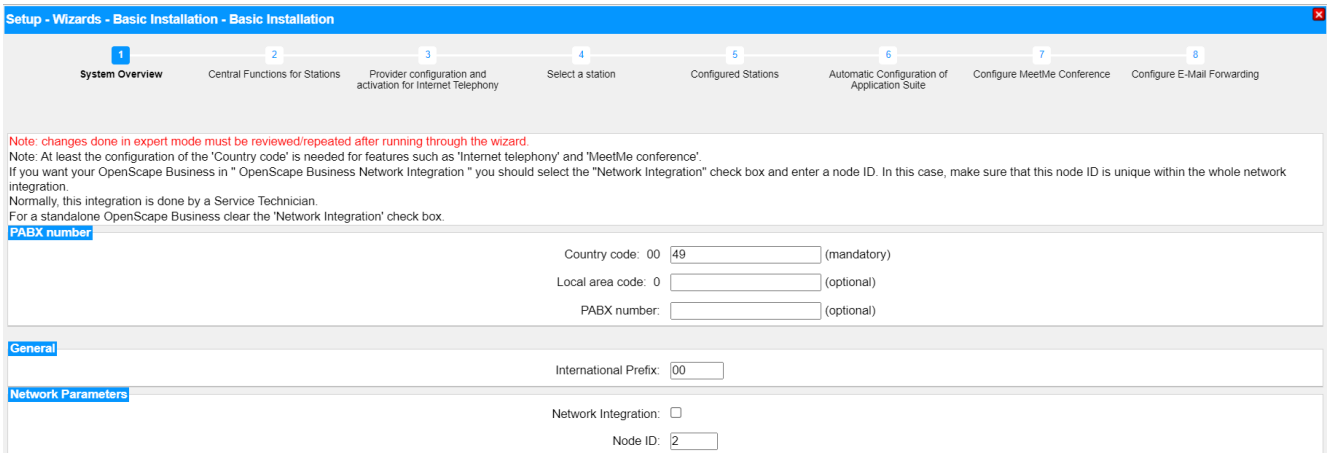
In der OpenScape Business S ist die Zielrufnummer bereits im "National-Format" als DuWa eingetragen.

"BA" (Broaden all) hat nur im Gateway eine Bedeutung.

"BA" wird nur benötigt, wenn die ursprüngliche Zielrufnummer TON unknown empfangen wurde, d.h. nur die "kurze DID" = Nebenstellen-Anteil enthält.

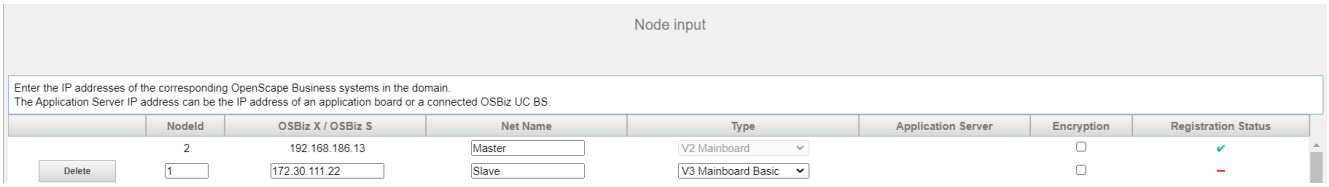
- Erst wird die Basisinstallation, dann der Netzwerk-Wizard durchlaufen.
- Für jeden Teilnehmer der OpenScape Business S werden eingerichtet:
  - Internrufnummer im Kurzformat (z.B. 300)
  - DUWA-Rufnummer im nationalen Format (z.B. 89 7007 300)
  - Zugehörige Gateway Knoten-ID

Basisinstallation der OpenScape Business S, Multi Gateway



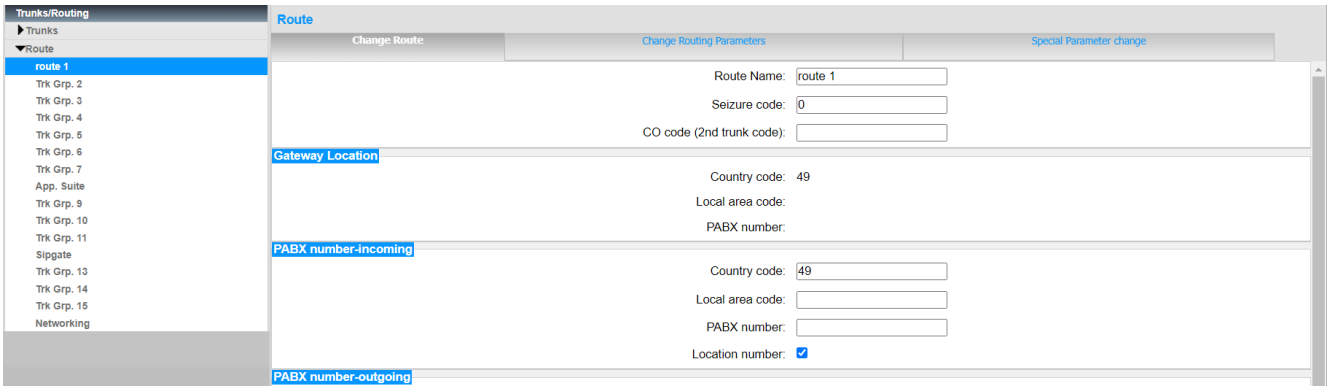
Tipp: Bei Anlagendaten nur den Country Code eintragen, der Rest der Gesamt-Rufnummer steht im DID-Eintrag der Teilnehmer.

Netzwerk-Wizard der OpenScape Business S, Multi Gateway



Wählen Sie Multi Gateway in der Netzwerk-Konfiguration aus.

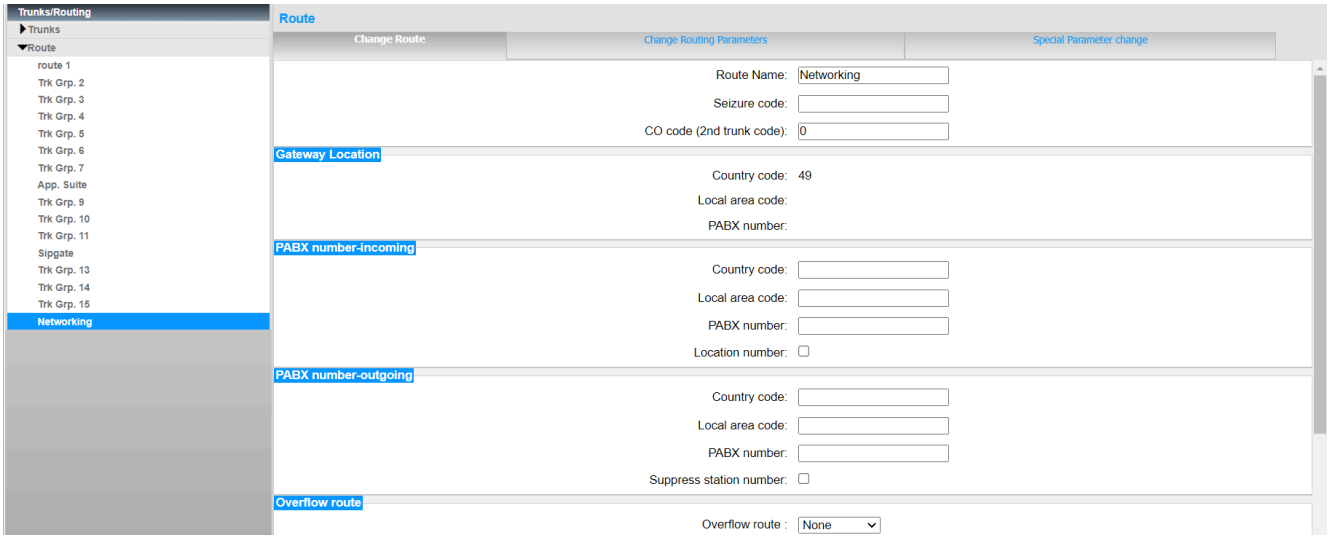
Richtungen der OpenScape Business S, Multi Gateway



Der Country Code wurde bereits im wizard eingetragen.

Richtungsparameter: Richtungsart Amt

Diese Richtung bekommt die Richtungsart "Amt".



Routing Parameter: Rufnummerntyp outgoing=National, Richtungsart PABX

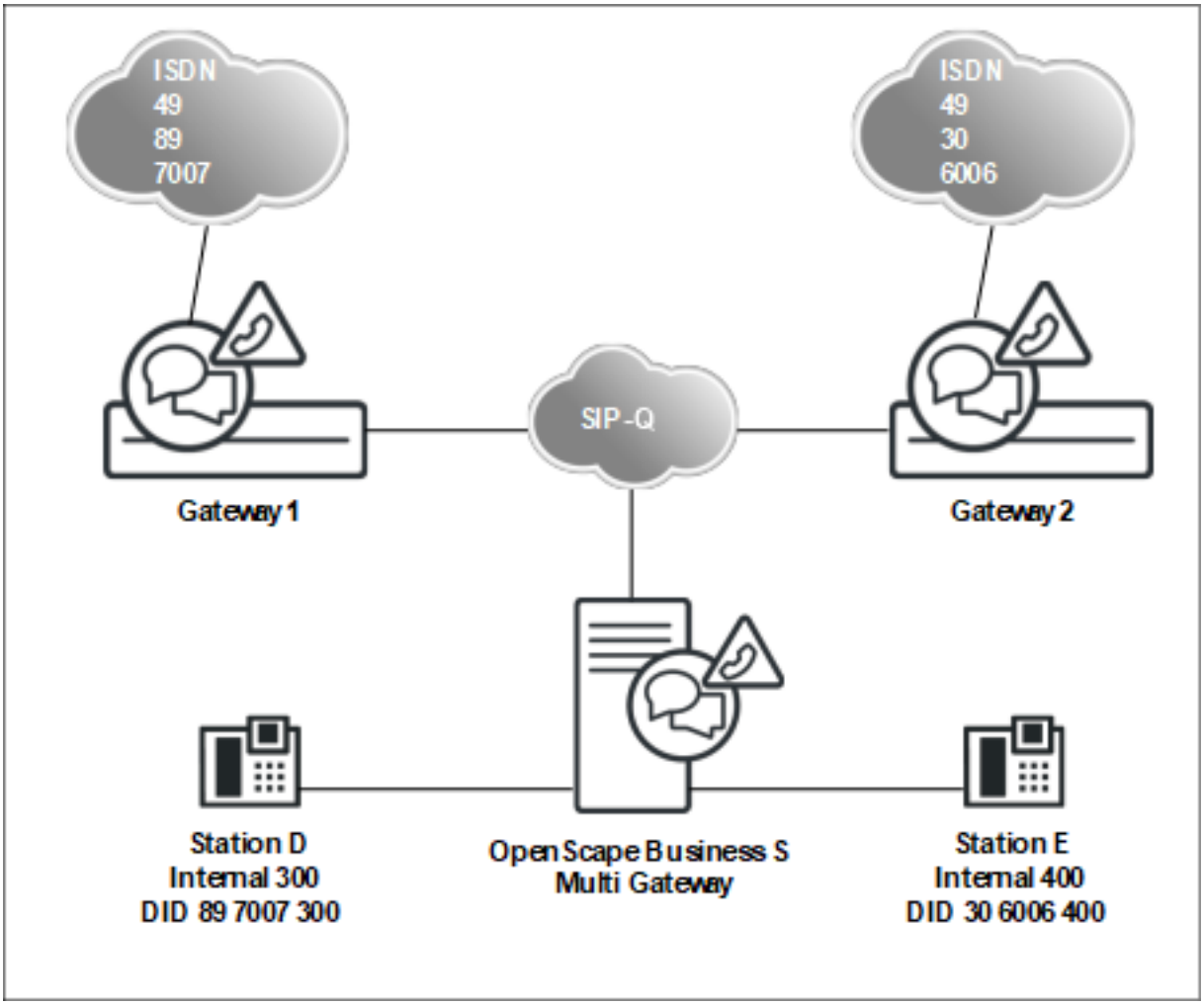
Diese Richtung bekommt die Richtungsart „PABX“ und der NR-Typ gehend ist mit **Ortsnetzkennzahl** einzurichten.

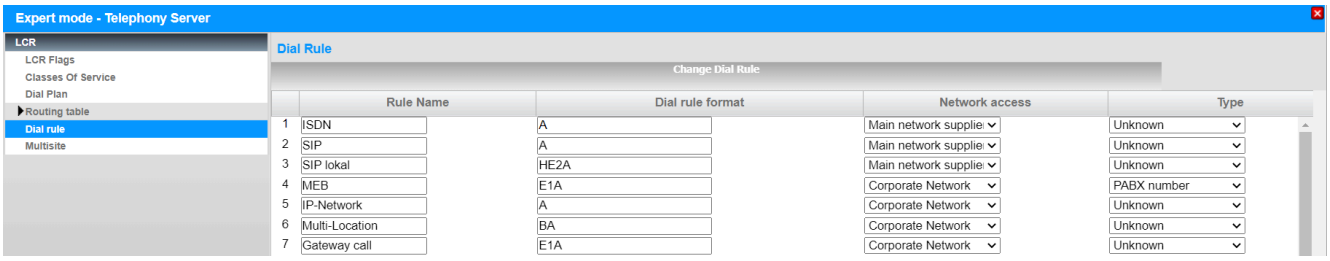
16.3.4.10 Teilnehmer D ruft externen Teilnehmer über Amt

Vernetztes System in Multi Gateway Konfiguration

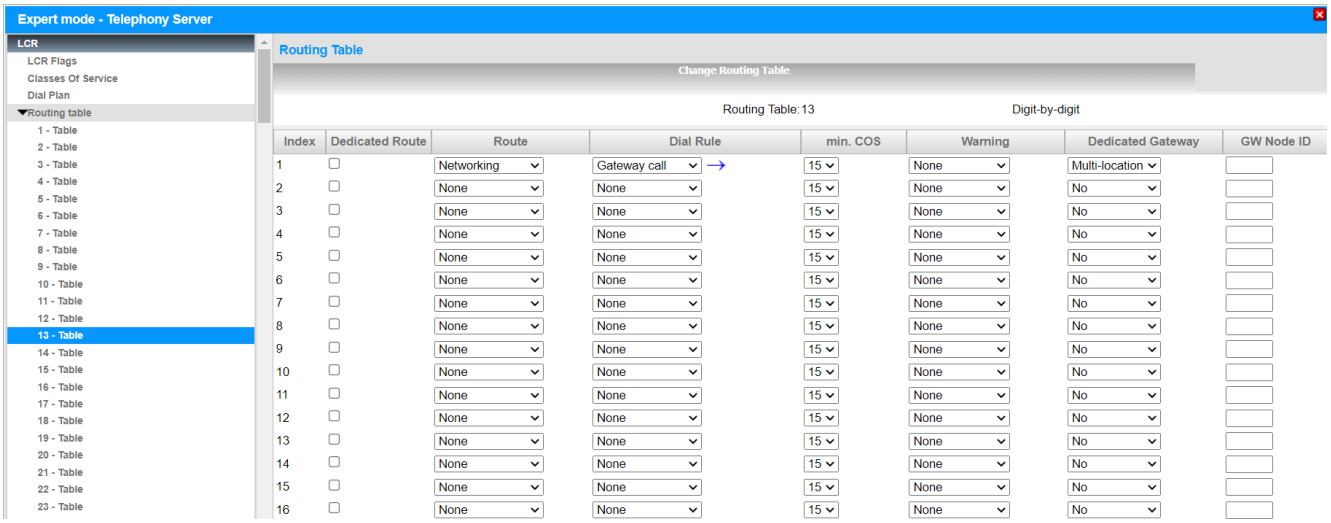
Konfiguration der OpenScape Business S, Multi Gateway

Routing der OpenScape Business S, Multi Gateway, zu den Gateways





	Rule Name	Dial rule format	Network access	Type
1	ISDN	A	Main network supplie	Unknown
2	SIP	A	Main network supplie	Unknown
3	SIP lokal	HE2A	Main network supplie	Unknown
4	MEB	E1A	Corporate Network	PABX number
5	IP-Network	A	Corporate Network	Unknown
6	Multi-Location	BA	Corporate Network	Unknown
7	Gateway call	E1A	Corporate Network	Unknown



Die Einrichtung von Gateway 1 erfolgt wie im vorherigen Beispiel, bei Gateway 2 gilt dies ebenfalls.

16.4 Notrufe

Das Kommunikationssystem und die angeschlossenen Telefone bieten verschiedene Möglichkeiten einen Notruf abzusetzen. Der Administrator kann eine Hotline/Röchelschaltung oder einen Notrufdienst konfigurieren.

Wurde die Activation Period noch nicht gestartet oder befindet sich das Kommunikationssystem in der Failover Period, können Notrufe immer von den beiden ersten aktiven Telefonen abgesetzt werden.

Voraussetzungen

Die Notrufzentrale wird durch Wahl der Amtskennziffer (z.B. 0) und der Notrufnummer (z.B. 112) erreicht. Aus Applikationen muss deshalb die Wahl der Zielrufnummer für Notrufe mit führender Amtskennziffer erfolgen.

Prinzipieller Ablauf

Fall 1: Wahl des Notrufs über PSTN-Leitung

Fall 2: Wahl des Notrufs über ITSP

Fall 3: Spezielle Vereinbarung mit ITSP oder PSTN-Providern

Fall 4: Notrufe bei Mobile Logon (IP-Mobility)

Notrufe werden von einem Teilnehmer des Kommunikationssystems durch die Wahl von Amtskennzahl und Notrufnummer initiiert. Die Notrufnummer wird vom Kommunikationssystem an den jeweiligen Provider (PSTN oder ITSP) übergeben.

Der Notruf wird in dem Ortsnetz abgesetzt, dem der Anschluss des Kommunikationssystems zugeordnet ist. Folgendes ist dabei zu beachten: Alle Teilnehmer, die sich nicht am selben Standort des Kommunikationssystems aufhalten, (z.B. Mobility-Teilnehmer, CallMe-Benutzer (Teleworker) oder

über WAN abgesetzte Telefone) sollten den Notruf über Handy bzw. ein anderes Festnetztelefon wählen, um den Notruf im Ortsnetz ihres Standortes abzusetzen.

Nicht alle ITSPs unterstützen Notrufe. In diesem Fall muss per LCR-Konfiguration dafür gesorgt werden, dass Notrufe über PSTN geroutet werden.

Für den Fall, dass sich nicht alle Teilnehmer des Kommunikationssystems an einem Standort aufhalten, jedoch fest einem Standort ohne eigenes PSTN zugeordnet sind, kann in Zusammenarbeit mit dem Provider eine individuelle Prozedur zur Notrufsignalisierung festgelegt werden. Z.B. Abhängig von der Anrufer-ID des Rufers kann der Notruf durch den Provider zum entsprechenden vereinbarten Ortsnetz geroutet werden. Diese Vereinbarungen sind individuell und unterliegen keiner Richtlinie.

Mobile Logon (IP-Mobility) bedeutet, dass Teilnehmer das Telefon wechseln und dabei ihre Rufnummer mitnehmen.

Notrufe funktionieren in diesem Fall, solange die Telefone an den Standorten der Gateways angemeldet sind. Alle Teilnehmer, die sich nicht am Standort des Gateways aufhalten, (z.B. Mobility Teilnehmer, CallMe user Homeworker, über WAN abgesetzte Endgeräte) sollten den Notruf über Handy bzw. ein anderes Festnetzendgerät wählen, um den Notruf im Ortsnetz ihres Standortes abzusetzen.

Tipp: Für Multigateway-Szenarien, in denen das Leistungsmerkmal Mobile Logon eingesetzt wird, gelten besondere Anforderungen. Die entsprechende Konfiguration wird in Kapitel "Notrufe in Kombination mit Mobile Logon" beschrieben.

16.4.1 Röchelschaltung / Hotline

Für jeden Teilnehmer kann die Hotline-Funktion aktiviert werden. Dabei wird festgelegt, ob beim Abheben des Hörers sofort (Hotline) oder nach einer bestimmten Zeit (Röcheln) die Verbindung zum Hotline-Ziel aufgebaut werden soll.

Röchelschaltung

Wählt der Teilnehmer in der vordefinierten Zeit (Röchelzeit) eine beliebige Ziffer, erfolgt **kein** Verbindungsaufbau zum Hotline-Ziel.

Die Röchelzeit wird vom Administrator zentral konfiguriert und ist individuell für jeden Teilnehmer ein- und ausschaltbar.

Hotline

Bei aktivierter Hotline, hat der Teilnehmer nach Abnehmen des Hörers **keine** Möglichkeit, eine Rufnummer einzugeben. Vor Abnehmen des Hörers kann eine Rufnummer gewählt werden. Der Teilnehmer kommt immer nach Abheben des Hörers automatisch beim vordefinierten internen oder externen Hotline-Ziel an.

Der Teilnehmer wird immer weitergeleitet, wenn das Hotline-Ziel einer Anrufumleitung oder Rufweiterschaltung folgt.

Systemspezifische Informationen

Der Administrator kann 6 Hotline-Ziele und die Länge der Röchelzeit (0-99 Sekunden) konfigurieren. Gibt der Administrator bei der Röchelzeit den Wert 0 an, wird sofort das Hotline-Ziel gerufen.

Abhängigkeiten

Themenbereich	Abhängigkeit
Anrufschutz	Ist beim Ziel der Anrufschutz aktiviert, hört der Anrufer den Besetztton.

16.4.1.1 Wie Sie einen Hotlineziel konfigurieren und ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Navigieren Sie im Menübaum zu **System** > **Abwurf/VPL/Hotline**.
4) Unter **Hotline** können Sie 6 verschiedene Ziele (**Ziel-Ruf-Nr.**) eintragen.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.4.1.2 Wie Sie die Röchelzeit ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System**.
4) Klicken Sie auf **Abwurf/VPL/Hotline**.
5) Unter Hotline können Sie die **Röchelzeit** (Verzögerungszeit in Sekunden,) ändern.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.4.1.3 Wie Sie Röcheln oder Hotline für einen Teilnehmer konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.
4) Klicken Sie z.B. auf **IP Clients**.
5) Klicken Sie z.B. auf **System Clients**.
6) Markieren Sie den entsprechenden Teilnehmer und stellen Sie im Feld **Hotline** Modus **Röcheln** oder **Hotline** ein.
7) Haben Sie Hotline eingestellt, dann müssen Sie im Feld Hotline noch die **Anzahl der Hotline-Ziele** einstellen.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.4.2 Leitungstrennung für einen Notruf

Wird ein Notruf abgesetzt und keine Amtsleitung ist frei, dann wird eine Zwangstrennung ausgelöst. Dem notrufenden Teilnehmer wird automatisch die freie Leitung zugewiesen.

Die Leitungstrennung funktioniert bei ISDN- und ITSP-Amtsanschlüssen.

Der Teilnehmer hat die Möglichkeit, bei besetzten Leitungen eine automatische oder manuelle Leitungstrennung durchzuführen.

- Automatisch: Das Leistungsmerkmal Leitweglenkung (LCR) ist aktiv und es ist eine Notrufnummer im LCR hinterlegt.
- Manuell: Das Leistungsmerkmal "Leitung freischalten" ist für den Vermittlungsplatz immer aktiv und wird über Taste oder Kennzahl ausgeführt.

Systemspezifische Informationen

Der Administrator kann beliebig viele Notrufnummern konfigurieren.

Damit eine automatische Leitungstrennung erfolgt, wenn alle Leitungen belegt sind, muss die Notrufnummer im Wahlplan des LCR hinterlegt sein und das Notruf Flag *Experten Mode* für diese gesetzt sein.

16.4.2.1 Wie Sie die Leitungstrennung für einen Notruf aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Routing**.
3) Navigieren Sie im Menübaum zu **LCR** > **Wahlplan**.
4) Wählen Sie im Fenster **Wahlplan ändern** eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Notrufnummer** für die entsprechende Rufnummer.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Notrufnummer** für die entsprechende Rufnummer.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.4.3 Nur für USA, Kanada: Notrufdienst E911

Durch den erweiterten Notrufdienst E911 werden neben der Rufnummer auch Informationen über den geographischen Standort (hinterlegte Adresse) des Anrufers beim Absetzen eines Notrufs übermittelt.

Die den Notruf entgegennehmende Rettungsleitstelle ist nicht auf die mündliche Übermittlung des Standortes durch den Anrufer angewiesen.

In den USA greift das Leistungsmerkmal nur dann, wenn die Notrufnummer 911 gewählt wird.

Für den Notrufdienst E911 muss jedem Teilnehmeranschluss mit gültiger Durchwahlnummer eine LIN (Location Identification Number) vom Administrator zugeordnet werden. Räumlich nah zusammen liegende Teilnehmeranschlüsse sind mit der gleichen LIN zu versehen. Eine Datenbasis in der Notrufzentrale, in der alle LIN gespeichert sind, identifiziert anhand der übermittelten LIN den Namen und die Adresse des Notrufenden.

Abhängigkeiten

Thema	Abhängigkeit
CLIP	Für USA ist standardmäßig LIN aktiviert. Wenn allerdings CLIP (Calling Line Identification Presentation) für USA aktiviert wird, so ist automatisch LIN deaktiviert.

16.4.3.1 Wie Sie CLIP / Lin bearbeiten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer**.
4) Klicken Sie z.B. auf **IP Clients**.
5) Klicken Sie auf die Registerkarte **Teilnehmer ändern**.
6) Tragen Sie beim entsprechenden Teilnehmer im Feld **CLIP/LIN** die 16-stellige LIN ein.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.4.4 Notrufe in Kombination mit Mobile Logon

Wenn man das Leistungsmerkmal Mobile Logon in einem Multi-Gateway-Netzverbund verwendet, kann bei einem Wechsel des Telefons auch der physikalische Standort wechseln. Daher sind besondere Maßnahmen für das Routing von Notrufen erforderlich.

Algorithmus-Beschreibung für die Wahl eines Notrufs

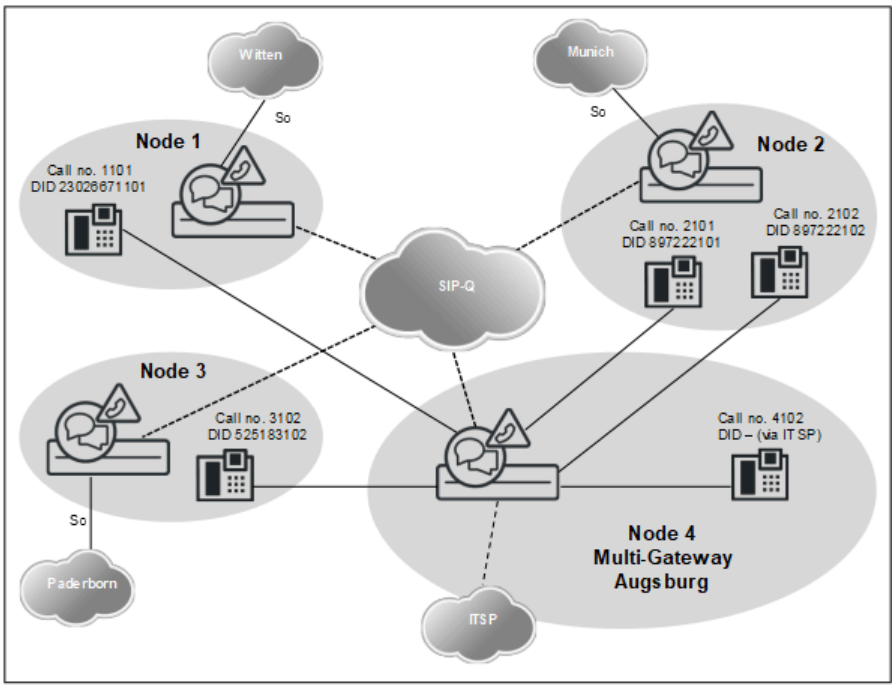
Wenn ein Teilnehmer eine Notrufnummer wählt (Kennung im LCR), überprüft ein Algorithmus, ob für das Telefon eine Notrufnummer konfiguriert wurde. Diese wird dann zur Erzeugung einer abgeleiteten Rufnummer verwendet, die im Netzverbund zum Routen des Anrufs über das richtige Gateway genutzt wird.

Jede Nummer, die im Wahlplan als Notrufnummer gekennzeichnet ist, hat auch einen Verweis auf einen Eintrag in der Wegetabelle. Jeder Eintrag in der Wegetabelle, der zu einer Notrufnummer gehört, muss mit einer geringen Berechtigungsklasse (COS) versehen sein. Geringe Berechtigungsklasse bedeutet, dass jeder Teilnehmer berechtigt ist eine Notrufnummer abzusetzen.

16.4.4.1 Konfiguration des Notrufszenarios

Die Konfiguration des Notrufszenarios zeigt für einen Multi-Gateway-Netzverbund, welche Schritte für die Einrichtung durchzuführen sind.

Behandlung von Notrufnummern



Mobile Logon wird nur innerhalb eines Knotens unterstützt, d.h. Standortwechsel - und damit besondere Anforderungen für Notrufe - sind nur für Telefone relevant, die am Multi-Gateway Knoten (4) betrieben werden. Generell sind alle betroffenen Telefone an Knoten 4 angemeldet, befinden sich physikalisch jedoch an verschiedenen Standorten.

- In allen betroffenen Telefonen ist ein Eintrag für Notruf erforderlich (Anschlussanteil der kanonischen Rufnummer des Standort-Knotens + Belegungskennzahl Notruf-Richtung)
- Der LCR-Eintrag (Knoten_4lokal) in der nachfolgenden Tabelle ist nur erforderlich, wenn am Knoten 4 (Multi-Gateway) Telefone physikalisch vorhanden sind. Es wird ebenfalls die Standort-Nummer vorangestellt, die

hier aber unvollständig ist (nur Landeskennzahl). Die Voraussetzung dafür ist ein ITSP-Zugang an Knoten 4, der Notrufe ins Ortsnetz unterstützt.

- Bei der Wahl am Telefon wird eine mit Notruf gekennzeichnete LCR-Regel (z.B. 0C11x) getroffen.
- Die im Telefon gespeicherte (und bei der Anmeldung ins System übertragene) Notrufnummer wird mit den Standortdaten des Systems (Ländervorwahl, Ortsnetzkennzahl, Anlagenrufnummer) verglichen.

  Falls unterschiedlich wird eine "lange" Notrufnummer gebildet:

  – Entfernen des Access-Codes: 0112 -> 112
  – Einfügen von <LDAP-Belegungskennzahl><InternationalesPräfix><programmierte Notfallrufnummer>: z.B. 112 -> 0 00 49897220 112
- Die "lange" Notrufnummer wird durch das LCR geroutet, durch spezifische LCR-Regeln entweder direkt ins lokale Amt oder per Querleitung zum jeweiligen Partnerknoten und von dort ins Amt.

Tipp: Weil im Telefon nicht genau die vollständige Standort-Nummer des lokalen Knotens eingetragen wird, muss auch für den lokalen Notruf am Multi-Gateway-Standort eine geeignete LCR-Regel eingetragen werden.

Einrichtung der Standortdaten für Knoten 4

Richtungsparameter

Knoten 4, Telefone

Übersicht der für einen Notruf relevanten Einträge im LCR für Knoten 4

Knoten 4	Gateway-Knoten
G.-Standort Land	49
G.-Standort Ortsnetz	
G.-Standort Anlage	
Internationales Präfix	00
Nationales Präfix	0
LDAP-Belegungskennzahl	0

Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	National	Int/Duwa

Richtung Networking	
Amtskennziffer (2. AKZ)	0

Standort Witten	
Rufnummer	1101
Emergency Number (Notrufnummer)	4923026670

Standort München	
Rufnummer	2101
Emergency Number (Notrufnummer)	49897220

Standort Paderborn	
Rufnummer	3102
Emergency Number (Notrufnummer)	49525180

Standort Augsburg	
Rufnummer	4102
Emergency Number (Notrufnummer)	490

Rufnummernplan			Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Not-betrieb	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Notruf [5]	0C112	X	Vernetzung	Multi-Gateway	1	E1A	Corp. Network	Unbekannt
Notruf [5]	0C0110	X						
Amt	0CZ							
Notruf_nach1	0C00492302667-0-11X	X	Vernetzung	Erzwungen	1	E3A	Corp. Network	Unbekannt
Notruf_nach2	0C004989722-0-11X	X			2			
Notruf_nach3	0C004952518-0-11X	X			3			
Notruf_4lokal [6]	0C0049-0-11X	X	ITSP	Nein		E4A	Hauptnetzanbieter	Unbekannt

16.4.5 Notrufdienst E112 (für Europa)

Durch den erweiterten Notrufdienst E112 werden neben der Rufnummer auch Informationen über den geographischen Standort (hinterlegte Adresse) des Anrufers beim Absetzen eines Notrufs übermittelt.

Die geografischen Informationen werden in einem standardisierten XML-Dokument übertragen. Die inhaltliche Definition dieses Dokuments variiert je nach Land und ITSP. Sie müssen daher nur die Teilmenge an Daten eingeben, die Sie von Ihrem ITSP erhalten haben (z. B. in der Schweiz nur den NAM-Parameterwert).

Das Leistungsmerkmal wird durch Einrichtung von Notrufnummern in der LCR-Konfiguration und Angabe von geeigneten Standortinformationen aktiviert.

5 Mit den obigen Regeln wird in diesem Beispiel nur die Notrufsituation erkannt, aber nicht geroutet. Für das Notruf-Routing wird die abgeleitete "lange" Notrufnummer verwendet.

6 Weil am Multi-Gateway-Standort Teilnehmer physikalisch angeschlossen sind, ist eine eigene LCR-Regel für einen lokalen Notrufzugang einzutragen (via ITSP-Richtung).

16.4.5.1 Wie Sie eine ITSP Loc-ID zu einem Teilnehmer hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.
3) Klicken Sie im Menübaum auf **ITSP Loc-ID Einstellungen**.
4) Geben Sie den Pflichtparameter **Loc-ID-Name** und die Standortinformationsparameter Ihres ITSP (z. B. in der Schweiz nur den NAM-Parameterwert) ein.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

   Der **ITSP Loc-ID** wird automatisch eine Index-ID zugewiesen.
6) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
7) Klicken Sie im Menübaum auf **Teilnehmer**.
8) Klicken Sie z.B. auf **IP Clients**.
9) Klicken Sie auf die Registerkarte **Teilnehmer ändern**.
10) Geben Sie die entsprechende Index-ID des Felds ITSP Loc-ID ein.
11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.5 Anrufsteuerungsdienst (Call Admission Control)

Über das Leistungsmerkmal Anrufsteuerungsdienst (Call Admission Control CAC) kann die benutzte Bandbreite über die Anzahl von Gesprächen eingeschränkt werden.

Das Kommunikationssystem bietet drei Möglichkeiten Einfluß auf die benötigte Bandbreite zu nehmen:

- Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP
- Einschränkung des Bandbreitenbedarfs bei Gateway-Gesprächen
- Einschränkung der Anzahl der Gespräche in Vernetzungsszenarien

16.5.1 Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP

Durch die Konfiguration der verfügbaren Upload-Bandbreite wird die maximal mögliche Anzahl von Anrufen über ITSP festgelegt. Durch Herabsetzen der Anzahl dieser Anrufe (Internet-Anrufe) kann der Bandbreitenbedarf weiter reduziert werden.

Die Einstellungen dazu können in den Wizards **Netzwerk/Internet** und **Zentrale Telefonie** vorgenommen werden.

Die Anzahl der möglichen Anrufe über einen ITSP kann im **Expertenmodus** unter **Telephonie** >**Voice Gateway** > **SIP Parameters**angezeigt werden.

Internet-Anrufe sind:

- ITSP-Anrufe
- Unify Phone-Anrufe

- myPortal for Teams-Anrufe
- myPortal@work-Anrufe
- Device@Home-Anrufe

Nur bei LAN myPortal@Work und PureWebRTC-Anrufen wird keine Bandbreite reserviert, da die Nutzdaten direkt sind.

16.5.2 Einschränkung des Bandbreitenbedarfs bei Gateway-Gesprächen

Durch Konfiguration der zulässigen Codecs bei Gateway-Gesprächen kann die Bandbreite beeinflußt werden.

Werden nur komprimierende Codecs eingestellt, so ist der Bandbreitenbedarf geringer. Wenn gemischte Codecs genutzt werden, kann die Priorisierung der nicht komprimierenden Codecs herabgesetzt werden, sodass diese seltener verwendet werden.

Die entsprechenden Einstellungen dazu werden im **Experten-Modus** unter **Telefonie** > **Sprachgateway** > **Codec-Parameter ändern** gemacht.

16.5.3 Einschränkung der Anzahl der Gespräche in Vernetzungszenarien

Das Kommunikationssystem bietet zwei Möglichkeiten die Bandbreite in Vernetzungsszenarien zu kontrollieren.

Beschränkung durch die Anzahl der Leitungen zu anderen Netzknoten

Beschränkung der Bandbreite durch gezielte Codec-Auswahl

Durch Zuordnung einer bestimmten Anzahl von Leitungen zu anderen Netzknoten kann eine Obergrenze aller gleichzeitig möglichen Gespräche von und zu diesen Knoten vorgenommen werden.

Die verfügbare Bandbreite kann durch Konfiguration der verwendeten Codecs vom und zum Partner (Ziel-IP-Adresse) festgelegt werden.

Die entsprechenden Einstellungen dazu werden im **Experten-Modus** unter **Telefonie** > **Sprachgateway** > **Ziel-Codec-Parameter hinzufügen** gemacht.

16.6 Gemeinschaftsanlage

Die gesamte Kapazität des Kommunikationssystems kann organisatorisch in maximal sechs Unteranlagen aufgeteilt werden. Dadurch können z.B. mehrere Firmen ein Kommunikationssystem gemeinsam nutzen.

Das Leistungsmerkmal Gemeinschaftsanlage wird durch Ausnutzung vorhandener Leistungsmerkmale realisiert. Das bedeutet, dass keine explizite Einrichtung von Teilanlagen erfolgt.

Die Steuerung von erlaubten und verbotenen Verbindungen zwischen einzelnen Teilnehmern und Leitungen geschieht über die Verkehrsbeziehungsgruppen.

Leistungsmerkmale in der Gemeinschaftsanlage:

- Abwurf
- Anlagenrufnummer

- Anruferliste
- Aufschalten
- DISA
- Direktansprechen
- Gesprächsdatenerfassung
- Hotline-Ziele
- Infotexte, Abwesenheitstexte
- Interne Anrufe
- Internes Verzeichnis
- KDS-Ausdruck
- Nachtschaltung
- Parkposition
- Verkehrsbeziehungsgruppen
- Voicemail
- Amtsberechtigung

Das Kommunikationssystem kann als Gemeinschaftsanlage eingesetzt und dadurch gleichzeitig von mehreren Firmen genutzt werden. Die Funktionalität aller Leistungsmerkmale bleibt für alle Teilnehmer unverändert erhalten.

Eine Ausnahme bilden bestimmte Ressourcen, die auf die Unterbetreiber (Firmen) aufgeteilt werden müssen. Diese können entweder einem, mehreren oder allen Unterbetreibern zugeordnet werden. Bei den aufzuteilenden Ressourcen handelt es sich um:

- Teilnehmer
- Richtungen
- Vermittlungsplatz
- Abwurfstation
- Ansagegeräte, Voice Mail
- Verkehrsbeziehungsgruppen
- Türöffner
- DISA-Leitungen

Über die VBZ-Gruppen wird die Erreichbarkeit der Unterbetreiber untereinander festgelegt.

Für jeden Teilbereich lassen sich eigene Hotline-Ziele einrichten.

Abhängigkeiten

Thema	Abhängigkeiten
GEZ	Es existiert nur eine zentrale Gebührenerfassung für alle Teilbereiche.
Interne Anrufe	Interne Gespräche zwischen Teilnehmern "unterschiedlicher" Teilbereiche sind möglich, sofern dies die VBZ erlaubt.
LCR	Die automatische Leitungsbelegung ist nur systemweit konfigurierbar.
KDS-Ausdruck	Der Ausdruck der Datenbasis erfolgt nur für das gesamte System.

Thema	Abhängigkeiten
Internes Verzeichnis	Es werden die Namen aller Teilnehmer und Kurzwahlnummern im System angezeigt.
Vermitteln	Das Vermitteln unbewählter Leitungen ist nicht möglich.
Abwurf	Abwurf ist nur systemweit programmierbar.

16.6.1 Kurzwahl zentral in Gemeinschaftsanlagen

Mit Kurzwahl zentral in Gemeinschaftsanlagen können Kurzwahlziele in Abhängigkeit von den Verkehrsbeziehungsgruppen ausgewählt werden. Dazu kann über das WBM ein Bereich von Kurzwahlzielen den entsprechenden Verkehrsbeziehungsgruppen zugeordnet werden.

Abhängigkeiten

Thema	Abhängigkeiten
Ext. Rufnummern	Kurzwahlziele können nur externe Rufnummern enthalten.
	Die externe Rufnummer muss mit Richtungs- bzw. Belegungskennzahl eingegeben werden.
KWZ Namen	Jedem Kurzwahlziel kann ein Name zugewiesen werden.
Türsprechstelle	Die Türsprechstelle kann kein Kurzwahlziel anrufen.
VBZ-Gruppen	Es ist nicht möglich, mehrere Kurzwahlziel-Bereiche einer VBZ-Gruppe zuzuordnen.

17 Attendants

OpenScape Business bietet Vermittlungsfunktionen für jeden Bedarf, wie AutoAttendants, Telefon- und PC-basierte Attendants.

Übersicht über die angebotenen Attendants

	Einsetzbar für	Hardware	Lizenz
AutoAttendants			
Company AutoAttendant (UC Smart)	UC Smart	OpenScape Business X OpenScape Business S	Erforderlich
Company AutoAttendant (UC Suite)	UC Suite	OpenScape Business X3/X5/X8 mit UC Booster Card oder UC Booster Server OpenScape Business S	Erforderlich
Telefon-basierte Attendants			
OpenStage Attendant			
PC-basierte Attendants			
OpenScape Business Attendant	UC Smart	PC und Telefon, UP_{0E}	Erforderlich
- OpenScape Business BLF	UC Smart	IP-Basis	
myAttendant	UC Suite	OpenScape Business X3/X5/X8 mit UC Booster Card oder UC Booster Server OpenScape Business S	Erforderlich

17.1 AutoAttendant

Der AutoAttendant bildet zusammen mit der Voicemail einen integrierten automatischen Vermittlungsdienst und einen Nachrichtenspeicher, z.B. für die Firmenzentrale. Der AutoAttendant spielt Anrufern eine Begrüßungsansage vor. Während oder nach dieser Ansage kann der Anrufer automatisch oder durch Eingabe von Ziffern an eine Nebenstelle oder Mailbox weitervermittelt werden.

Hierzu stehen verschiedenste Funktionen zur Verfügung, die mit Hilfe von Ansagen eine individuelle Vermittlung ermöglichen, wie z.B. "Drücken Sie die 1 für Service und die 2 für Vertrieb". Der Anrufer wird nach Eingabe der gewünschten Ziffer automatisch mit Vertriebs- oder Service-Mitarbeitern verbunden.

Der Company AutoAttendant ist keiner internen Rufnummer zugeordnet, sondern eine zentrale Instanz. Einer Nebenstelle können somit mehrere Company AutoAttendants bzw. Mailboxen zugewiesen werden. Dadurch ist es dem Benutzer möglich, individuell auf den entsprechenden Company AutoAttendant umzuleiten. Dem Anrufer wird je nach Umleitung entweder die Ansage der persönlichen Mailbox angesagt oder die zentrale Firmenansage. Durch den Company AutoAttendant ist es aber auch möglich, pro Nebenstelle individuelle Ansagen abzuspielen, unabhängig von der persönlichen Mailbox.

Funktionsübersicht

- Abwurf nach Ansage zu einem konfigurierten Ziel
- Statusabhängige Ansage - es können je nach Status der Nebenstelle (frei oder besetzt) unterschiedliche Ansagen abgespielt werden.
- Unterschiedliche Tag-/Nacht-Ansage (Umschaltung erfolgt entweder manuell oder automatisch)
- Zentrale Kalendersteuerung über die Automatische Nachtschaltung
- Nachwahl einer beliebigen Rufnummer bis zu einer konfigurierten Länge (deaktivierbar)
- Kurzwahl (= Direktwahl von extern) zu konfigurierten Zielen (beliebige Rufnummer oder Mailbox)

  Insgesamt sind 4 Listen mit insgesamt 10 Zielen und einem Abwurfziel möglich. Die aktive Liste wird durch die gewählte Begrüßung festgelegt.
- Nachwahl einer beliebigen Rufnummer bis zu einer konfigurierten Länge. Die Funktion der Nachwahl kann auch deaktiviert werden um Gebührenmissbrauch zu verhindern.
- Multi Step AutoAttendant

  AutoAttendant-Mailboxen können als Kurzwahlziele (Manuell 1 bis 4, Tag/Nacht) konfiguriert werden. Dies ermöglicht eine Verkettung von Mailboxen.

  Dabei verhält sich der Company AutoAttendant wie bei einer Anrufumleitung, das Gespräch wird von einer verketteten Mailbox auf die nächste weitergeleitet und dabei immer die jeweilige Ansage abgespielt. Insgesamt sind bis zu 100 AutoAttendant-Mailboxen verfügbar.
- Schnellwahl

  Ansagen können deaktiviert werden, um eine schnelle Vermittlung zu garantieren.
- Ansage vor Melden mit Parallelsignalisierung (ohne Kurzwahl)

  Wird dem Anrufer die Begrüßungsansage vorgespielt, wird der Anruf beim Teilnehmer zugleich akustisch (und optisch) signalisiert. Hebt der Teilnehmer ab, wird die Ansage abgebrochen und der Teilnehmer mit dem Anrufer verbunden. Hebt der Teilnehmer nicht ab, wird die Ansage im Endlos-Betrieb abgespielt, bis der Teilnehmer auflegt oder über das Call Management weitervermittelt wird.
- Besetztttonerkennung
- Weiterleitung von Faxanrufen (automatische Faxtonerkennung) an ein vorkonfiguriertes Fax-Ziel.
- Wiederanruf

  Bei einem Wiederanruf (ausgenommen bei einem Faxanruf), wird der Anrufer zur zugehörigen Mailbox weitergeleitet, falls eine solche vorhanden ist und die Nachrichtenaufzeichnung aktiv ist.

Anmerkung: Um einen automatischen Abwurf zum Vermittlungsplatz durch das Voicemailsystem zu gewährleisten ist zwingend die Platzkennzahl intern einzutragen (Default 9, USA 0).

Anmerkung: Die Administration (TUI) einer AutoAttendant-Mailbox kann nur von einem Telefon ausgeführt werden. Deswegen sollte sich das Passwort für die AutoAttendant-

Mailbox sich vom Passwort für die persönliche Mailbox des Telefons unbedingt unterscheiden!

Anwendungsfälle

- Beispiel 1: **Unabhängige Bereitschafts- oder Notdienste Ansagen**

  Außerhalb der Geschäftszeiten leitet der Kunde auf den AutoAttendant um (z.B. per Nachtschaltung). Der AutoAttendant verbindet auf Wunsch zum jeweils diensthabenden Servicetechniker oder bietet die Option, eine Nachricht in einer zentralen Mailbox zu hinterlassen. In diesem Fall führt eine Ansage zur Weiterleitung auf die verschiedenen Mobiltelefon-Nummern der Servicetechniker.
- Beispiel 2: **Unterschiedliche Sonntagsdienste für Arztpraxen**

  Der jeweils aktuelle Sonntagsdienst muss nicht mehr auf den Anrufbeantworter gesprochen bzw. die AB-Kassette gewechselt werden. Der Kunde richtet sich genauso viele AutoAttendants ein, wie er Vertreter hat. Die AutoAttendants werden einmal besprochen und jeweils am Wochenende mit einer Umleitung (Nachtschaltung) zu dem betreffenden AutoAttendant aktiviert. Hier ist es umgekehrt: Mehrere unterschiedliche Ansagen führen auf dieselbe Mailbox.

17.1.1 Company AutoAttendant (UC Smart)

Der Company AutoAttendant (UC Smart) ist der AutoAttendant der UC-Lösung UC Smart. Er kann als persönlicher AutoAttendent und als zentraler AutoAttendant verwendet werden. Die erstmalige Einrichtung erfolgt über das WBM, anschließend kann er über das Telefon gesteuert und konfiguriert werden.

Der Company AutoAttendant (UC Smart) kann in zwei Modi betrieben werden:

- **Persönlicher AutoAttendant**

  Der persönliche AutoAttendant ist einem Teilnehmer oder einer Gruppe zugeordnet und reagiert auf die Rufnummer des ursprünglich angerufenen, umleitenden Teilnehmers oder Gruppe (z.B. `12345678-100`).

  Der persönliche AutoAttendant wird über den Sammelanschluss "Voicemail" (Standardrufnummer: 351) erreicht. Der Betrieb erfolgt über SmartVM-Ports (EVM Ports) vom Typ "PhoneMail", die alle diesem Sammelanschluss zugewiesen sein müssen.

  Der Parallelbetrieb mit UC Suite ist nicht möglich.

- **Zentraler AutoAttendant**

  Der zentrale AutoAttendant wird als zentraler Vermittlungsplatz genutzt und reagiert auf seine eigene Rufnummer (z.B. `12345678-0`). Egal ob der Anruf direkt auf den AutoAttendant erfolgt oder ob der Anruf umgeleitet wurde, das Verhalten ist immer identisch.

  Der zentrale AutoAttendant wird über einen oder mehrere eigene Sammelanschlüsse erreicht (Standardrufnummer: 352). Der Betrieb erfolgt über SmartVM-Ports (EVM Ports) vom Typ "Standard", die einem oder mehreren Sammelanschlüssen (max.100) zugewiesen sein können.

  Im Default ist ein Company Auto Attendant (Gruppenindex 3) mit 2 SmartVM-Ports eingerichtet. Die Namen und die Typen der Ports können mit

dem Wizard **Zentrale Telefonie** > **SmartVM** geändert werden (siehe auch Wie Sie die Sprachbox (SmartVM) konfigurieren).

Die Kurzwahlliste und der Begrüßungs-Upload können im Experten-Modus **Telefonie** > **Anschaltungen** > **SmartVM** geändert werden (siehe Wie Sie einzelne Begrüßungen laden, sichern und löschen). Ebenfalls können weitere (max. 99) Company AutoAttendants (UC Smart) eingerichtet und aktiviert werden.

Der Parallelbetrieb mit UC Suite ist möglich.

Der Company AutoAttendant (UC Smart) ist lizenzpflichtig (Lizenz Company AutoAttendant). Wenn keine Lizenz vorhanden ist, werden die "Regeln" des Company AutoAttendant ignoriert, Anrufe werden zum zentralen Abwurfplatz weitergeleitet.

17.1.1.1 Wie Sie einen eingerichteten Company AutoAttendant konfigurieren

Als Beispiel soll tagsüber eine Ansage vor dem Melden mit Aufnahmemöglichkeit (z.B. Mailbox 100) eingerichtet werden. Nachts soll direkt nach der entsprechenden Ansage ein Abwurf zur Nachtbox mit Aufnahmemöglichkeit (auch Mailbox 100) erfolgen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

UC Smart ist aktiviert.

Standardmäßig erfolgt nach der Ansage im Tag- und Nacht-Betrieb ein Abwurf zum Abwurfplatz.

Standardmäßig sind die Speeddial-Funktion und die Nachwahl nicht aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Anschaltungen**.
3) Klicken Sie im Menübaum auf **Anschaltung** > **SmartVM**.
4) Klicken Sie im Menübaum auf **AutoAttendant**.
5) Deaktivieren Sie in der Zeile des gewünschten AutoAttendant (z.B. `352`) das Kontrollkästchen **Abwurf nach Ansage**, um während der Begrüßungsansage Kurzwahlziffern eingeben zu können.
6) Aktivieren Sie das Kontrollkästchen **keine Nachwahl**. Somit ist nur die Eingabe vom Kurzwahlziffern möglich (keine Eingabe von internen Rufnummern möglich).
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
8) Klicken Sie im Menübaum auf **AutoAttendant** und anschließend auf den Eintrag des gewünschten AutoAttendant (z.B. `352`).
9) Klicken Sie auf die Registerkarte **Kurzwahl-/Abwurfziel (Tag) bearbeiten**.
10) Wählen Sie in der Zeile **Kurzwahl 0** aus der Aufklappliste **Auswählen** den Teilnehmer für den Abwurfplatz aus (z.B. Teilnehmer 100) und in der Aufklappliste **Typ** den Eintrag **Mailbox**.
11) Wählen Sie in der Zeile **Abwurf** aus der Aufklappliste **Auswählen** den Teilnehmer für den Abwurfplatz aus (z.B. Teilnehmer 100).
12) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13) Klicken Sie auf die Registerkarte **Kurzwahl-/Abwurfziel (Tag) bearbeiten**.
14) Wählen Sie in der Zeile **Abwurf** aus der Aufklappliste **Auswählen** den Teilnehmer für den Abwurfplatz aus (z.B. Teilnehmer 100) und in der Aufklappliste **Typ** den Eintrag **Mailbox**.
15) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
16) Klicken Sie im Menübaum auf **SmartVM**.
17) Um bei der Abwurf-Mailbox eine zweifache Begrüßung zu vermeiden, wählen Sie in der Zeile des Abwurfplatzes (z.B. Teilnehmer 100) aus der Aufklappliste **Begrüßung** den Eintrag **Kein** aus. Dann erfolgt direkt nach der Begrüßung des Company AutoAttendant der Signalton für die Aufnahme.
18) Die die Begrüßung des Company AutoAttendant kann über ein Telefon oder über den **Experten-Modus** > **Wartung** > **SmartVM** geändert werden (siehe Konfiguration der Sprachbox (SmartVM)).

17.1.1.2 Wie Sie einen neuen Company AutoAttendant einrichten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

UC Smart ist aktiviert.

Erforderliche Lizenzen

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Konfigurieren Sie zuerst den Sammelanschluss:
   a) Klicken Sie im Navigationsbaum auf **Telefonie** > **Kommende Rufe**.
   b) Klicken Sie im Menübaum auf **Kommende Rufe** > **Gruppen-/ Sammelanschluss**.
   c) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.
   d) Geben Sie im Feld **Rufnummer** die Rufnummer des neuen AutoAttendant ein (z.B.`353`).
   e) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer des neuen AutoAttendant ein (z.B. **353**).

      : Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

   f) Geben Sie im Feld **Name** den Namen des neuen AutoAttendant ein (z.B. `AutoAttendant 353`).
   g) Wählen Sie aus der Aufklappliste **Typ** den Eintrag **Zyklischer Sammelanschluss** aus.
   h) Wählen Sie im Bereich **Gruppenmitglied** aus der Aufklappliste Rufnummer den gewünschten AutoAttendant Port aus (z.B. **745 SmartVM 7**).
   i) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
   j) Um einen weiteren AutoAttendant Port zu dem Sammelanschluss hinzuzufügen, klicken Sie im Menübaum unter **Gruppen-/ Sammelanschluss** auf den gewünschten AutoAttendant und

anschließend auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie dort unter **Rufnummer** einen weiteren AutoAttendant Port aus (z.B. **746 SmartVM 8**) aus.

k) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

3) Konfigurieren Sie die Mailbox des AutoAttendant:

a) Klicken Sie im Navigationsbaum auf **Telefonie** > **Anschaltungen**.
b) Klicken Sie im Menübaum auf **Anschaltungen** > **SmartVM**.
c) Klicken Sie im Menübaum auf **AutoAttendant**.
d) Setzen Sie in der Zeile des gewünschten AutoAttendant (z.B. `353`) die beiden Kontrollkästchen nach Bedarf:

Abwurf nach Ansage: Wenn aktiviert, kann der Anrufer während der Begrüßung eine Kurzwahlziffer für eine Vermittlungsmöglichkeit eingeben.

Keine Nachwahl: Wenn aktiviert, können nur Kurzwahlziffern und keine internen Rufnummern eingegeben werden.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
f) Klicken Sie im Menübaum auf **SmartVM**.
g) Klicken Sie auf die
h) Wählen Sie auf der Registerkarte **SmartVM-Mailboxen bearbeiten** in der Zeile des gewünschten AutoAttendants unter **Begrüßung** die gewünschte Begrüßung aus.
i) Aktivieren Sie in der Zeile des gewünschten AutoAttendants das Kontrollkästchen **AutoAttendant**.
j) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

4) Konfigurieren Sie die Vermittlungsmöglichkeiten (z.B. "0" für Verbinden und "1" für eine Ansage):

a) Klicken Sie im Menübaum auf **SmartVM** und anschließend auf **AutoAttendant**.
b) Klicken Sie im Menübaum unter **AutoAttendant** auf den Eintrag des gewünschten AutoAttendant (z.B. `352`).
c) Klicken Sie auf die Registerkarte **Kurzwahl-/Abwurfziel bearbeiten**. **Tag bearbeiten**.
d) Geben Sie in der Zeile **Kurzwahl 0** unter Rufnummer die**Rufnummer** ein, zu der verbunden werden soll, und wählen Sie in der Aufklappliste **Typ** den Eintrag **Rufnummer**.
e) Wählen Sie in der Zeile **Kurzwahl 1** aus der Aufklappliste **Auswählen** den Teilnehmer für den Abwurfplatz aus (z.B. Teilnehmer 100) und in der Aufklappliste **Typ** den Eintrag **Mailbox**.
f) Wählen Sie in der Zeile **Abwurf** aus der Aufklappliste **Auswählen** den Company AutoAttendant aus (z.B. `353`).
g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
h) Ist das Flag **keine Nachwahl** deaktiviert, können während der Begrüßungsansage auch interne Nummern gewählt werden. Um Gebührenmissbrauch zu vermeiden, sollte die **Rufnummernlängenbegrenzung** überprüft bzw. limitiert werden, damit keine externen Rufnummern gewählt werden können (siehe **Experten-Modus** > **Telefonie** > **SmartVM** > **SmartVM-Parameter bearbeiten**).

17.1.2 Company AutoAttendant (UC Suite)

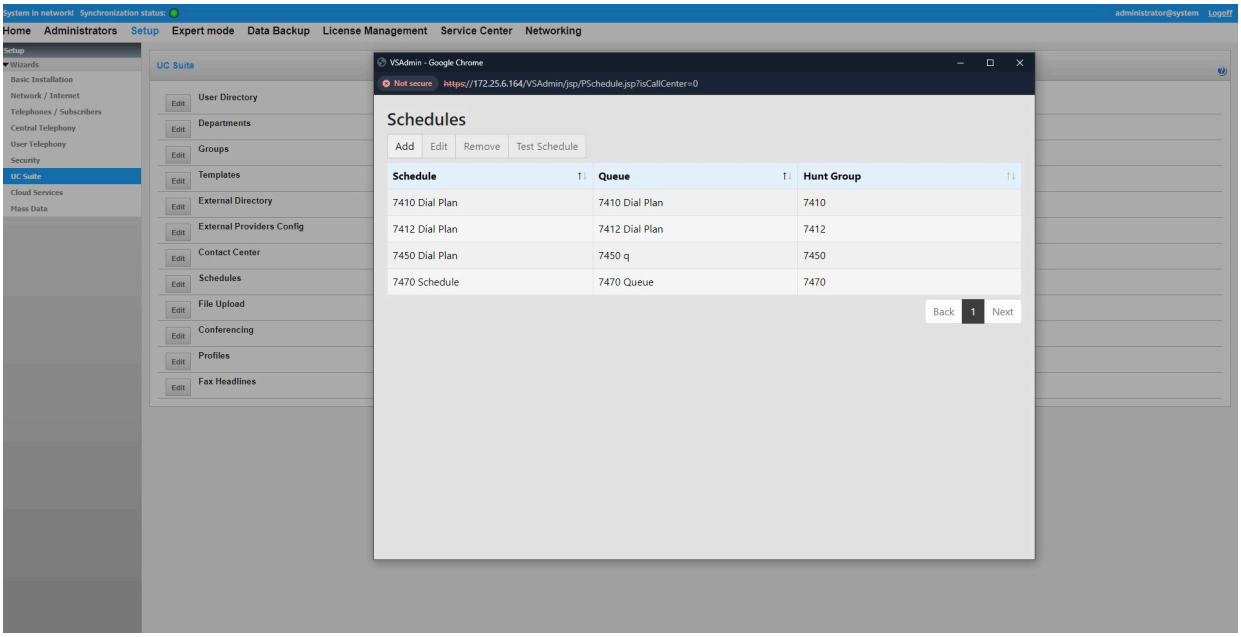
Der zentrale Company AutoAttendant (UC Suite) ist ein Vermittlungsplatz, der ausschließlich vom Administrator konfiguriert werden kann. Um die Installation und Einrichtung zu erleichtern, stehen fünf Templates zur Verfügung, die vom Administrator angepasst werden können.

Der Administrator kann den Company AutoAttendant (UC Suite) mit Hilfe von Zeitplänen regelbasiert konfigurieren. Zeitpläne ermöglichen erweiterte Auswahlmöglichkeiten wie z.B. nach Namen wählen.

17.1.2.1 Zeitpläne

Dieser Zeitplan und die darin enthaltenen Regeln (Call Control Vector CCV) definieren, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.

Beispielsweise kann für Werktage eine Regel für die Frühschicht (von 6:00 Uhr bis 14:00 Uhr), eine für die Mittagschicht (14:00 Uhr bis 22:00 Uhr) und eine für die Nachtschicht (von 22:00 bis 06:00 Uhr) definiert werden. Für das Wochenende kann eine Wochenendregel definiert werden. Für jede dieser Regeln kann zum Beispiel angegeben werden, ob eine Ansage abgespielt und/ oder wohin Anrufe weitergeleitet werden sollen.



Einem Zeitplan muss mindestens eine Regel (Call Control Vector CCV) zugeordnet werden. Die Regeln bestimmen für den Zeitraum für den ein Zeitplan gilt, wie kommende Anrufe behandelt werden. Regeln gelten ausschließlich für Anrufe und nicht für Faxe und E-Mails.

Regeln werden mit dem graphischen Regel-Editor (CCV-Editor) durch die Verknüpfung von vordefinierten CCV-Objekten erstellt und können nach der Fertigstellung unter einem frei definierbaren Namen gespeichert werden.

Gespeicherte Regeln können einem oder auch mehreren Zeitplänen als Standard-Regel (Standard-CCV) oder Ausnahme-Regel (Ausnahme-CCV)

zugeordnet werden. Das Öffnen, Modifizieren und erneute Speichern über den Regel-Editor ist jederzeit möglich.

Wurde einem Zeitplan eine Standard-Regel (Standard-CCV) zugeordnet, kann dieser Zeitplan unter einem frei definierbaren Namen gespeichert werden. Ein Zeitplan mit einer Standard-Regel gilt nach Zuweisung zu einer Warteschlange 24 Stunden am Tag und 365 Tage im Jahr. Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden. Damit kann definiert werden, wie kommende Anrufe beispielsweise während der Urlaubszeit behandelt werden sollen. Urlaubspläne haben hierbei Vorrang vor anderen Zeitplänen und Regeln.

Regel-Editor (CCV-Editor)

Mit dem Regel-Editor können aus vordefinierten CCV-Objekten Regeln gebildet werden. Die Anordnung der CCV-Objekte und deren Eigenschaften bestimmen, wie kommende Anrufe behandelt werden.

Anmerkung: Eine Regel hat eine Obergrenze von 500 CCV-Objekten.

Folgende vordefinierte CCV-Objekte stehen zur Verfügung:

Tipp: Für alle genannten CCV-Objekte gelten zusätzlich die beiden folgenden allgemeinen Eigenschaften:

Beschreibung: Optionale Möglichkeit, das CCV-Objekt zu beschreiben, wie zum Beispiel Begrüßungsansage.

Aktion nach Zifferneingabe: Angabe der benötigten Ziffer(n) ohne Leerzeichen, Kommas oder andere Zeichen. Die Angabe bezieht sich auf das vorherige CCV-Objekt. Wurde dort unter Mögliche Ziffern 9 angegeben, muss auch hier 9 stehen.

- **Nachricht abspielen**

  Bewirkt das Abspielen der gewünschten Ansage. Ausgewählt werden kann eine in der UC Suite vorliegende Audiodatei. Darüber hinaus kann eine neue Audiodatei in die UC Suite importiert werden oder eine neue Ansage aufgezeichnet und anschließend als Audiodatei in die UC Suite importiert werden.

  Durch das Abspielen der Ansage wird jeweils ein Media Stream Channel belegt.

  Eigenschaften:

  – **Dateiname**: Auswahl einer Ansage (Audiodatei im wav-Format)
  – **Abbruchtasten**: Angabe einer Taste oder Tastenkombination auf der Wähltastatur, mit der ein Anrufer das Abspielen der Ansage abbrechen kann.
  – **Datei-Manager**: Über diese Schaltfläche ist es möglich, eine Audio-Datei im wav-Format direkt hochzuladen bzw. mit dem Aufzeichnungsgerät eine neue Sprachdatei zu erzeugen.

- **Verbindung mit Anrufer trennen**

  Bewirkt das Beenden der Verbindung.

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
- **Zu CCV**

  Bewirkt eine Schleife zu einem anderen CCV-Objekt

  Eigenschaft:

  – **Ziel-CCV**: Auswahl des CCV-Objekts
- **Aktion nach Zifferneingabe**

  Bewirkt die Ausführung des oder der nachfolgenden CCV-Objekte in Abhängigkeit von den dort angegebenen Ziffern (Aktion nach Zifferneingabe).

  Eigenschaften:

  – **Dateiname**: Auswahl einer oder mehrerer Ansagen (Audiodatei im wav-Format)
  – **Wiedergabeliste**: Liste der ausgewählten Ansagen (Audiodatei im wav-Format) in der Reihenfolge der Wiedergabe
  – **Zeitüberschreitung bei Zifferneingabe**: Zeit in Sekunden, innerhalb der das Kommunikationssystem auf die Zifferneingabe wartet.

    Erfolgt die vollständige Zifferneingabe nicht innerhalb der angegebenen Zeit, wird die Nachricht (Ansage) erneut abgespielt.
  – **Link an**: Auflistung der Ziffern mit Ziel.

    Die Ziffern und Ziele können hinzugefügt, bearbeitet und entfernt werden.
  – **Datei-Manager**: Über diese Schaltfläche ist es möglich, eine Audio-Datei im wav-Format direkt hochzuladen bzw. mit dem Aufzeichnungsgerät eine neue Sprachdatei zu erzeugen.

  Der Inhalt der Wiedergabeliste wird im Regel-Editor anhand eines Tooltips angezeigt, wenn man mit dem Mauszeiger auf dem CCV-Objekt verweilt.
- **Einzelschritt-Übergabe**

  Die Funktion ist abhängig von der Einstellung **Normales Vermittlungsplatz-SST** (WBM, **Experten-Modus**: **Applikationen** > **OpenScape Business UC Suite** > **Server** > **Allgemeine Einstellungen**):

  – **Normales Vermittlungsplatz-SST** aktiviert (Standardeinstellung, nicht für USA): Bewirkt die Übergabe des Anrufs, unabhängig davon, ob das Ziel frei, besetzt oder nicht verfügbar ist.

    Tipp: Bei einem Teilnehmer mit Anklopfschutz wird der Anruf erst vermittelt, wenn der Zielteilnehmer frei ist. Ein Anklopfen im Besetztfall erfolgt nicht.
  – **Normales Vermittlungsplatz-SST** deaktiviert (Standardeinstellung, nur für USA): Bewirkt die Übergabe des Anrufs wenn das Zeil frei ist.

    Ist das Ziel besetzt und der Anklopfschutz deaktiviert oder ist das Ziel nicht verfügbar, wird dem Anrufer eine Ansage eingespielt. Dabei kann der Anrufer wählen, ob er eine Nachricht auf der Sprachbox des

Teilnehmers hinterlassen möchte oder ob er die Rufnummer eines anderen Ziels wählen möchte.

Ist das Ziel besetzt und der Anklopfschutz aktiviert, erfolgt keine Vermittlung des Anrufs.

Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

Eigenschaft:

– **Zielnebenstelle**: Angabe der internen Rufnummer oder der externen Durchwahl mit Amtsleitungsnummer. Leerzeichen, Kommas oder andere Zeichen sind nicht erlaubt.

Die Rufnummer der Zielnebenstelle wird im CCV-Objekt angezeigt.

Anmerkung: Nach einer Einzelschritt-Übergabe trennt das System die Verbindung nach Klingeln für 5 Minuten.

- **In Mailbox aufzeichnen**

  Bewirkt den Anruf an die gewünschte Sprachbox eines Teilnehmers oder einer Sprachbox-Gruppe

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

  Eigenschaft:

  – **Benutzer-Mailbox**: Angabe der Rufnummer der Sprachbox eines Teilnehmers oder einer Sprachbox-Gruppe

  Die Rufnummer und der Name der Sprachbox oder der Sprachbox-Gruppe werden im Regel-Editor anhand eines Tooltips angezeigt, wenn man mit dem Mauszeiger auf dem CCV-Objekt verweilt.

- **Übergabe nach Melden (Supervised Transfer)**

  Bewirkt die Übergabe des Anrufs an ein internes Ziel. Während der Übergabe wird dem Anrufer Wartemusik (Music On Hold MOH der UC Suite) eingespielt.

  Im Gegensatz zum CCV-Objekt Einzelschritt-Übergabe müssen hier zwei weitere CCV-Objekte eingefügt werden. Es muss nämlich definiert werden, wie sich das Kommunikationssystem verhalten soll, wenn das Anrufziel besetzt ist oder der Anruf nicht angenommen wird. Üblicherweise wird dem Anrufer in diesen Fällen eine Ansage eingespielt.

  Eigenschaften:

  – **Zielnebenstelle**: Angabe der internen Rufnummer.

    Es werden nur interne Rufnummern im eigenen Knoten unterstützt. Das Weiterleiten auf externe Ziele, virtuelle Teilnehmer, weitere AutoAttendants, UCD inkl. Contact Center sowie externe CallMe-Ziele ist

nicht zulässig! Für diese Szenarien ist der SST (Einzelschritt Übergabe) zu verwenden.

– **Zeitüberschreitung beim Klingeln (Sek.)**: Zeit in Sekunden, innerhalb der der Anruf angenommen werden muss.

  Wird der Anruf nicht innerhalb der angegebenen Zeit angenommen, wird dieser zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

  Tipp: Die hier angegebene Zeit muss kürzer sein als die für die Rufweiterschaltung konfigurierte Zeit (Standardeinstellung für die Rufweiterschaltung = 15 Sekunden). Siehe Rufweiterschaltung konfigurieren.

– **Anruf zurücknehmen, wenn Zielgerät weitergeleitet/umgeleitet ist**: Option (gilt nur für interne Rufnummer).

  Bei aktivierter Option erfolgt eine Prüfung des Anrufziels. Wurde für das Anrufziel eine Anrufweiterschaltung oder Anrufumleitung aktiviert, wird der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

– **Anwesenheitsstatus bei Anrufübergabe prüfen**: Option

  Bei aktivierter Option erfolgt eine Prüfung des Anwesenheitsstatus des Anrufziels. Bei einem anderen Anwesenheitsstatus als Büro wird der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

  Anmerkung: Wenn ein eingehender Anruf von einer unterdrückten/unbekannten Nummer kommt und der Anruf vom UC Suite AutoAttendant angenommen und über die überwachte Übertragung weitergeleitet wird, wird als Nummer des Anrufers die UC Suite-Nummer angezeigt.

- **Nach Name wählen**

  Bewirkt die Aufforderung des Anrufers, die ersten drei Buchstaben des gewünschten Teilnehmer-Nachnamens über die Wähltastatur einzugeben.

  Gibt es einen Teilnehmer mit den eingegebenen Anfangsbuchstaben, wird eine Verbindung hergestellt.

  Gibt es mehrere Teilnehmer mit den eingegebenen Anfangsbuchstaben, werden dem Anrufer die Namen dieser Teilnehmer angesagt (maximal 10 Teilnehmer). Hat ein Teilnehmer keine Namensansage aufgezeichnet, wird stattdessen die Rufnummer angesagt. Nach der Auswahl des gewünschten Teilnehmers wird eine Verbindung hergestellt.

  Entspricht kein Teilnehmer den eingegebenen Anfangsbuchstaben, erhält der Anrufer eine entsprechende Meldung.

  Tipp: Die Tasten der Wähltastatur reagieren auf den ersten Tastendruck. Mit jedem Tastendruck wird geprüft, ob es Teilnehmer-Nachnamen mit den der Taste zugeordneten Buchstaben gibt.

  Beispiel: Im internen Verzeichnis gibt es die folgenden fünf Nachnamen mit den Anfangsbuchstaben t, u und v: Taylor,

Taler, Ullrich, Vasquez und Volterra. Um ein Verbindung mit dem Teilnehmer Taylor herzustellen, sind folgende Tasten zu betätigen: 8 2 9

Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

Eigenschaften:

– **Methode**: Auswahl von **An Nebenstelle übergeben** oder **In Mailbox aufzeichnen**.

  Je nach ausgewählter Methode wird eine Verbindung zum gewünschten Teilnehmer oder zu dessen Sprachbox hergestellt. Dabei werden ausschließlich interne Teilnehmer unterstützt, die mit Vor- und Nachnamen im internen Verzeichnis eingetragen sind.

- **Nebenstellenwahl**

  Bewirkt die Aufforderung des Anrufers, die Rufnummer des gewünschten Teilnehmers über die Wähltastatur einzugeben.

  Wählt der Anrufer die Rufnummer eines virtuellen Teilnehmers, wird er aufgefordert eine andere Teilnehmer-Rufnummer einzugeben. Anschließend wird eine Verbindung hergestellt. Meldet sich der gewünschte Teilnehmer nicht, nimmt dessen Sprachbox den Anruf entgegen.

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

  Eigenschaften:

  – **Methode**: Auswahl von **An Nebenstelle übergeben** oder **In Mailbox aufzeichnen**.

    Je nach ausgewählter Methode wird eine Verbindung zum gewünschten Teilnehmer oder zu dessen Sprachbox hergestellt. Dabei werden ausschließlich interne Teilnehmer unterstützt, deren Rufnummer im internen Verzeichnis eingetragen ist.

- **Sprache einstellen**

  Bewirkt die Auswahl der Sprache für die jeweilige Standardansage anhand der Rufnummer des Anrufers. Zu beachten ist, dass ausschließlich

Standardansagen (Systemansagen) und keine persönlichen Ansagen berücksichtigt werden.

Definiert werden kann zum Beispiel, dass für eine Rufnummer mit der Ländervorwahl +49 eine deutsche Ansage und für eine Rufnummer mit der Ländervorwahl +33 eine französische Ansage abgespielt wird.

Eigenschaften:

– **Standardsprache**: Aufklappliste zur Auswahl einer Sprache.

  Die hier ausgewählte Sprache wird für alle Rufnummern verwendet, für die selbst keine Sprache definiert wurde.
– **Muster**: Angabe der Rufnummer, der eine bestimmte Sprache zugeordnet werden soll.

  Folgende Platzhalter können verwendet werden: * = beliebige Zahl, ? = beliebige Ziffer.
– **Sprache**: Aufklappliste zur Auswahl der Sprache, die den zugehörigen (dem **Muster** entsprechenden) Rufnummern zugeordnet werden soll.

Eine Sprache kann beliebig vielen verschiedenen (dem **Muster** entsprechenden) Rufnummern zugeordnet werden.

- **CLI-Routing**

  Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand der Rufnummer des Anrufers.

  Definiert werden kann zum Beispiel, dass für eine Rufnummer mit der Ländervorwahl +49 zuerst eine deutsche Ansage abgespielt werden soll (CCV-Objekt **Nachricht abspielen**) und der Anruf anschließend an eine internes Telefon weitergeleitet werden soll (CCV-Objekt **Einzelschritt-Übergabe**). Es kann auch die Ortsvorwahl verwenden werden (z B. 089 für München).

  Im Kontext von UC Suite und CLI-Routing müssen Benutzer bestimmte Szenarien berücksichtigen, wie z. B. eingehende Anrufe von MS Teams Nativer SIP-Trunk. Wenn Sie beabsichtigen, die Rufnummern von OpenScape Business-Anrufern im kanonischen Format einschließlich der Landesvorwahl zu senden, müssen Sie zusätzliche CLI-Routing-Regeln festlegen.

  Wenn beispielsweise Anrufer von MS Teams Nummern im Format +49777555XXXX haben und 777555 der gemeinsame Teil dieser Nummern ist, sollten Benutzer entsprechende CLI-Routing-Regeln erstellen, die diesen gemeinsamen Teil (777555) enthalten.

  Eigenschaften:

  – **Standard**: Aufklappliste zur Auswahl des CCV-Objekts.

    Das hier ausgewählte CCV-Objekt wird für alle Rufnummern verwendet, für die selbst kein Ziel definiert wurde.
  – **Muster**: Angabe der Rufnummern, denen ein bestimmtes CCV-Objekt als Ziel zugeordnet werden soll.

    Folgende Platzhalter können verwendet werden: * = beliebige Zahl, ? = beliebige Ziffer.

– **Beschreibung**

  Angabe einer Erläuterung.

  Für das **Muster** +49 (=Ländervorwahl Deutschland) kann zum Beispiel Deutschland eingegeben werden.

  Der hier eingegebene Text wird im Regel-Editor angezeigt.
– **Ziel**: Aufklappliste zur Auswahl des CCV-Objekts, das den zugehörigen (dem **Muster** entsprechenden)Rufnummern als Ziel zugeordnet werden soll.

Beliebig vielen verschiedenen (dem **Muster** entsprechenden) Rufnummern kann ein CCV-Objekt als Ziel zugeordnet werden.

• **Bedingte Verzweigung**

Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand einer Bedingung.

Definiert werden kann zum Beispiel, dass Anrufern eine Ansage eingespielt wird (Bitte rufen Sie zu einem späteren Zeitpunkt noch einmal an ...), sobald sich mehr als 20 Anrufe in einer Warteschlange befinden.

Eigenschaften:

– **Variable**: Auswahl von **Anrufe** oder **Verfügbare Agenten**.

  Je nach ausgewählter Variablen wird als Bedingungsvorgabe die Anzahl der wartenden Anrufe in einer Warteschlange oder die Anzahl der verfügbaren Agenten (inklusive Agenten in der Nachbearbeitungszeit) einer Warteschlange verwendet. In der zugehörigen Aufklappliste ist die Bedingung (**kleiner als**, **größer als**, **kleiner oder gleich als**, **größer oder gleich als**, **gleich als**) auszuwählen und in dem zugehörigen Eingabefeld ist der Vergleichswert einzugeben.
– **Bedingung erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei erfüllter Bedingung als Ziel verwendet werden soll.
– **Bedingung nicht erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei nicht erfüllter Bedingung als Ziel verwendet werden soll.

Die Anzahl der verfügbaren Agenten in einer Warteschlange wird durch folgende Statusänderungen der Agenten beeinflusst:

– Anmelden eines Agenten in die Warteschlange über „Anmelden/Login“: --> +1
– Abmelden eines Agenten aus der Warteschlange über „Abmeldung/ Logout“: --> -1
– Agent im Status "Pause":-->-1
– Agent im Status "Verfügbar nach Pause":--> +1

Die Anzahl der verfügbaren Agenten in einer Warteschlange wird durch folgende Statusänderungen der Agenten **nicht** beeinflusst:

– Agent im Zustand "Klingeln"
– Agent im Zustand 'Gespräch'
– Agent in Zustand "Nachbearbeitung"
– Agent im Zustand "Verpasster Anruf"
– Agent im Zustand "Überfällig"

17.1.2.1.1 Ausnahme in CCV hinzufügen

Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden. Damit kann definiert

werden, wie kommende Anrufe beispielsweise während der Urlaubszeit behandelt werden sollen. Urlaubspläne haben hierbei Vorrang vor anderen Zeitplänen und Regeln.

Schritt für Schritt

1) Navigieren Sie zu **Expertenmodus > Anwendungen > OpenScape Business UC Suite**.
2) Klicken Sie auf **Zeitpläne**, wählen Sie einen der verfügbaren Zeitpläne aus und klicken Sie auf **Bearbeiten**.

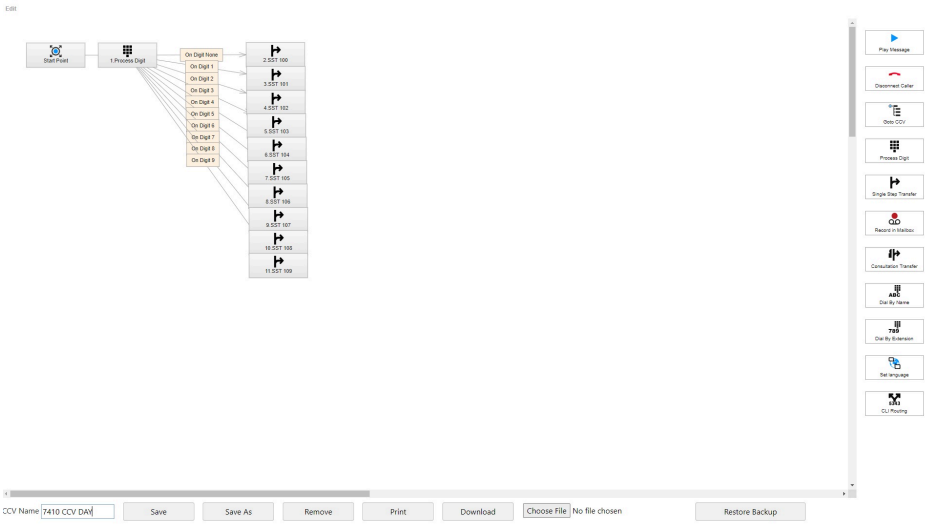
   Sie können auf **Hinzufügen** klicken, um einen neuen Zeitplan zu erstellen.
3) Klicken Sie unter dem Bereich **Zeitplan** auf **Hinzufügen**.
4) Füllen Sie das Feld **Beschreibung** aus, wenn Sie möchten.
5) Wählen Sie die Art der Ausnahme aus einer der verfügbaren Optionen aus:
   - **Im Zeitbereich**: Wählen Sie eine bestimmte Uhrzeit, einen Tag und eine Wiederholung für die Ausnahme aus
   - **Im Zeit-/Datumsbereich**: Wählen Sie ein bestimmtes Datum, eine Uhrzeit, einen Tag und eine Wiederholung für die Ausnahme aus
   - **Urlaubspläne**: Wählen Sie ein bestimmtes Urlaubsdatum für die Ausnahme aus
   - **Jährliche Wiederholung**: Wählen Sie aus, ob die Ausnahme jedes Jahr wiederholt werden soll
6) Klicken Sie auf **Speichern**.

17.1.2.2 Vorlagen (Templates)

Die nachfolgenden Template sind vorbelegte, standardisierte Vorlagen für den Company AutoAttendant (UC Suite), die beliebig verändert und an den speziellen Bedarf angepasst werden können.

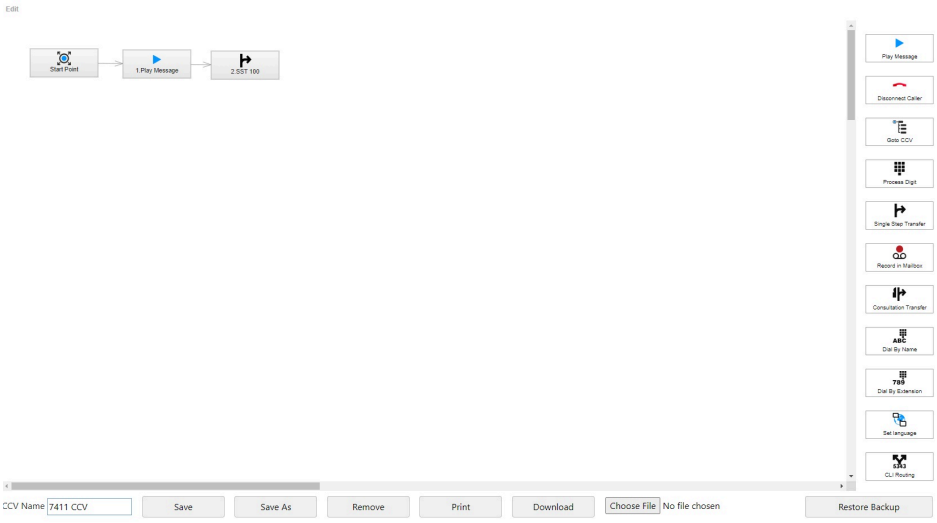
Vorlage 1 – 7410 CCV: Anruf mit Durchschaltung (ohne Mailbox)

Dem Anrufer wird eine Ansage vorgespielt. Anschließend wird er aufgefordert eine (Ziffer) Taste zu drücken und wird zu einem Teilnehmer durchgestellt. Drückt der Anrufer keine Taste, wird er zum Abwurfplatz (Default 100) durchgestellt.



Vorlage 2 – 7411 CCV: Ansage vor Beantwortung

Dem Anrufer wird eine Ansage vorgespielt. Anschließend wird auf den Abwurfplatz 100 vermittelt.

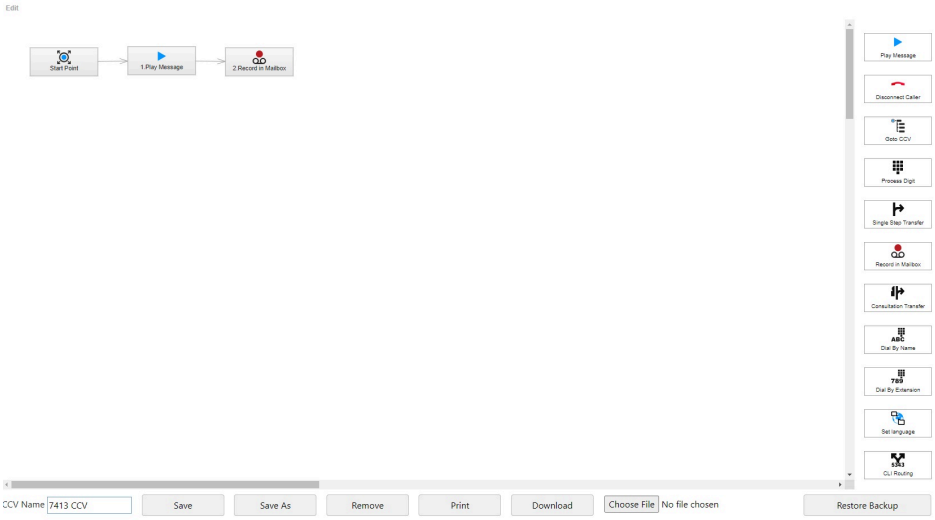


Vorlage 3 – 7412 CCV: Anruf außerhalb der Geschäftszeit

Dem Anrufer wird bei einem eingehenden Anruf außerhalb der Geschäftszeiten eine Ansage vorgespielt. Anschließend wird die Verbindung getrennt.

Vorlage 4 – 7413 CCV: 7413 CCV: Anruf außerhalb der Geschäftszeit mit Rufweiterschaltung auf eine Mailbox

Dem Anrufer wird bei einem eingehenden Anruf außerhalb der Geschäftszeiten eine Ansage vorgespielt. Anschließend wird er aufgefordert auf eine Mailbox zu sprechen und kann eine Nachricht hinterlassen.



17.2 OpenStage Attendant

Vermittlungsfunktionen können mit einem speziell eingerichteten OpenStage-Telefon ausgeführt werden. Der OpenStage Attendant dient gleichzeitig als Abwurfplatz.

Tastenlayout

Am OpenStage Attendant kommen alle Gespräche an, für die keine Durchwahlmöglichkeit besteht, oder für die über die Rufzuordnungkriterien kein Teilnehmer erreicht werden konnte (Abwurf). Die Vermittlungsperson leitet die kommenden Gespräche dann zu den gewünschten Teilnehmern weiter.

Folgende OpenStage Telefone können als Attendant fungieren:

- OpenStage 30
- OpenStage 40
- OpenStage 60
- OpenStage 80

Bei einem als Vermittlungsplatz konfigurierten OpenStage Telefon sind die frei programmierbaren Funktionstasten wie folgt belegt:

- Nachtschaltung
- Telefonbuch
- Wartende Anrufe
- Aufschalten
- Halten
- Extern 1
- Extern 2 (nicht bei OpenStage 40)
- Leere, nicht vorbelegte Taste (nicht bei OpenStage 40)

17.3 OpenScape Business Attendant

Der OpenScape Business Attendant bietet Vermittlungsfunktionen sowie eine Telefonbuchanbindung für OpenScape Business. Der OpenScape Business Attendant kann in einem Netzwerk erweitert werden, um netzweite BLF- und Anwesenheitsinformationen anzuzeigen.

Wesentliche Vermittlungsfunktionen:

- Anstehende bzw. angenommene Anrufe verwalten
- Daten des aktiven Gesprächs
- Geparkte, gehaltene Gespräche
- Anrufliste
- Journal für angenommene, verpasste und gehende Gespräche
- Persönliche VoiceMail

Telefonbuchanwendung:

- Outlook-Kontakte
- LDAP (Anschaltung via OpenDirectory Service)
- Persönliches Verzeichnis

Besetztlampenfeld-Status:

- Frei, Besetzt, Gerufen, Umgeleitet

Sichtbarkeit Präsenzstatus:

- Büro, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zuhause

  Anmerkung: Der Anwesenheitsstatus "krank" ist je nach Systemeinstellung des Administrators möglicherweise nicht verfügbar.

- Ändern des Anwesenheitsstatus für Teilnehmer des eigenen Knotens (derzeit nicht für Teilnehmer aus anderen Knoten)

Für die Darstellung der Benutzeroberfläche von OpenScape Business Attendant stehen zwei unterschiedliche Styles zur Verfügung.

Es können maximal acht OpenScape Business Attendants je Kommunikationssystem angeschlossen werden (maximal acht Lizenzen je OpenScape BusinessX1/X3/X5/X8 und Business OpenScape BusinessS).

Die Lizenzierung des OpenScape Business Attendant geschieht über das WBM.

Technische Voraussetzungen

- Standard Windows-PC
- Möglicher Einsatz eines Terminal Servers bei Verwendung von HFA-Telefonen (Voraussetzungen dazu siehe Voraussetzungen für UC Suite PC-Clients)
- USB-Interface bzw. LAN-Interface, abhängig vom verwendeten Endgerät
- Bildschirm mit einer Auflösung von min. 1024x768, optional zweiter Bildschirm zur Anzeige des zweiten BLF
- Grafikkarte mit 16 Bit Farbtiefe (min. 256 Farben)
- Internetzugang für Support bzw. Updates

Betriebssystem

- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)
- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server

Der Support von OpenScape Business Attendant für Microsoft Windows XP und Microsoft Windows Server 2003 endet zeitgleich mit der Einstellung des Produktsupports durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Unterstützte Telefone

- OpenStage 40/60/80 HFA
- openStage 30T/40T/60T/80T
- OpenScape DeskPhone CP 100/200/205/400/600/600E/700/700X

- OpenScape DeskPhone CP 110/210/410/710

> **Anmerkung:** Beim OpenScape DeskPhone CP 200/205/210 wird bei einem externen Anruf der Name des Benutzers nicht angezeigt.

Ältere Geräte (z. B. optiPoint410/420/500) werden teilweise noch unterstützt. Getestete und freigegebene Geräte entnehmen Sie bitte den jeweiligen Freigabemitteilungen.

Einfaches Plug-and-Play bei der Installation

Der OpenScape Business Attendant wird bei der Ersteinrichtung über einen Wizard konfiguriert. Der Wizard öffnet die erforderlichen Konfigurationsdialoge.

z. B.:

- Abfrage des Endgeräte-Typs
- Abfrage und Überprüfung des Anlagenzugangs
- Abfrage und Überprüfung eines evtl. vorhandenen Netzverbunds
- Automatische Integration des BLFs.

17.3.1 OpenScape Business BLF

Das Besetzttlampenfeld OpenScape Business BLF ist eine eigenständige Applikation zur Anzeige von Belegtzuständen. Optionale Funktionen sind Anzeige und Setzen des Anwesenheitsstatus, sowie der Verbindungsaufbau für das zugeordnete Telefon.

Technische Voraussetzungen

Wesentliche Funktionen:

- OpenScape Business BLF ist skalierbar und individuell einrichtbar
  - 10 bis 350 BLF-Felder (Benutzerschaltflächen), abhängig von der Bildschirmauflösung
- Telefonfunktionen
  - Wählen
  - Rufnannahme
  - Trennen
- Anwesenheitsstatus setzen (für den eigenen Teilnehmer)
- Telefonbuch (Systemtelefonbuch)
- Anrufjournal

Zum Betrieb des OpenScape Business BLF ist eine OpenScape Business BLF-Lizenz plus eine UC User-Lizenz erforderlich.

- Standard Windows-PC
- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)
- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server

- Bildschirm mit einer Auflösung von min. 1024x768
- Grafikkarte mit 16 Bit Farbtiefe (min. 256 Farben)
- LAN-Schnittstelle
- Standard Maus und Tastatur
- Internetzugang für Support bzw. Updates

17.3.2 Einrichtebeispiele für OpenScape Business Attendant, OpenScape Business BLF

In den folgenden Kapiteln finden Sie Einrichtebeispiele für die generelle Konfiguration von OpenScape Business Attendant, OpenScape Business BLF.

17.3.2.1 Szenario 1: OpenScape Business Attendant an ein OpenScape Business Einzelsystem angeschlossen

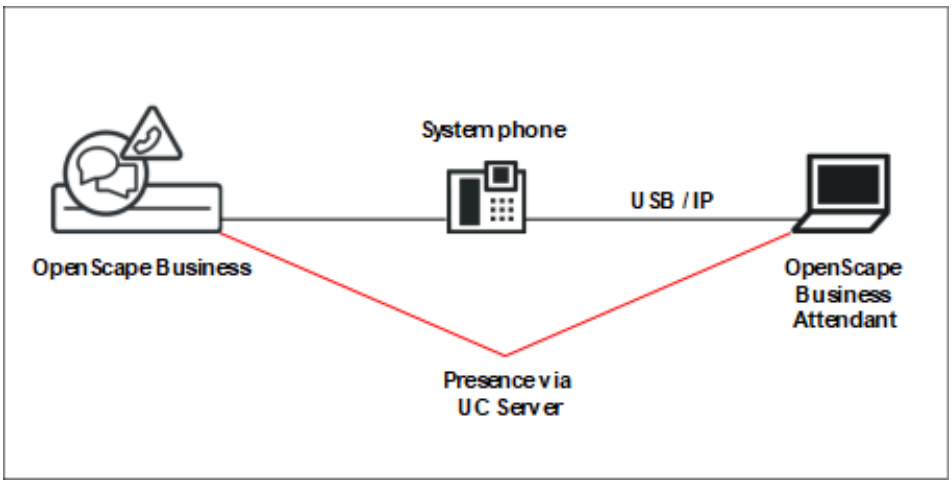
Voraussetzungen

Lizenz für OpenScape Business Attendant ist vorhanden.

Endgerät mit gültiger Lizenz

Lizenz für UC Smart oder UC Suite für Presence-Information (optional)

Die IP-Adresse für das Web Service Interface ist bei Nutzung von UC Smart oder UC Suite unterschiedlich. Bei UC Smart läuft das WSI immer auf dem Kommunikationssystem, bei UC Suite hingegen auf dem Bewerbungsausschuss oder Anwendungsserver (siehe UC Smart und UC Suite). Wenn Booster Server verwendet wird, muss dessen IP-Adresse verwendet werden. Wird eine OCAB verwendet, dann muss die IP-Adresse der OCAB verwendet werden. Nur wenn beide Komponenten nicht verbunden sind, muss die IP des Kommunikationssystems verwendet werden.



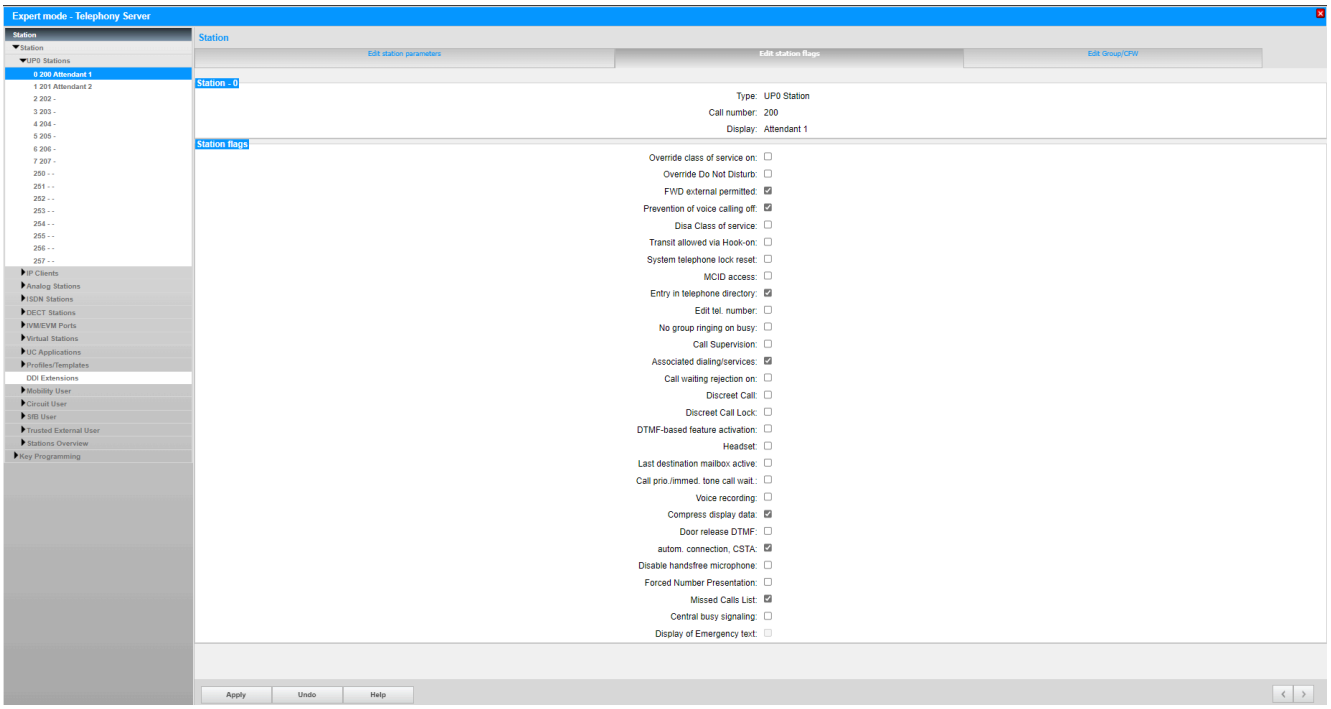
Schritt für Schritt

1) Konfigurieren Sie eine Station als Vermittlung über das WBM oder den Manager E (optiPoint 500, OpenStage 30T, 40T, 60T, 80T oder OpenStage 40HFA, 60HFA, 80 HFA).

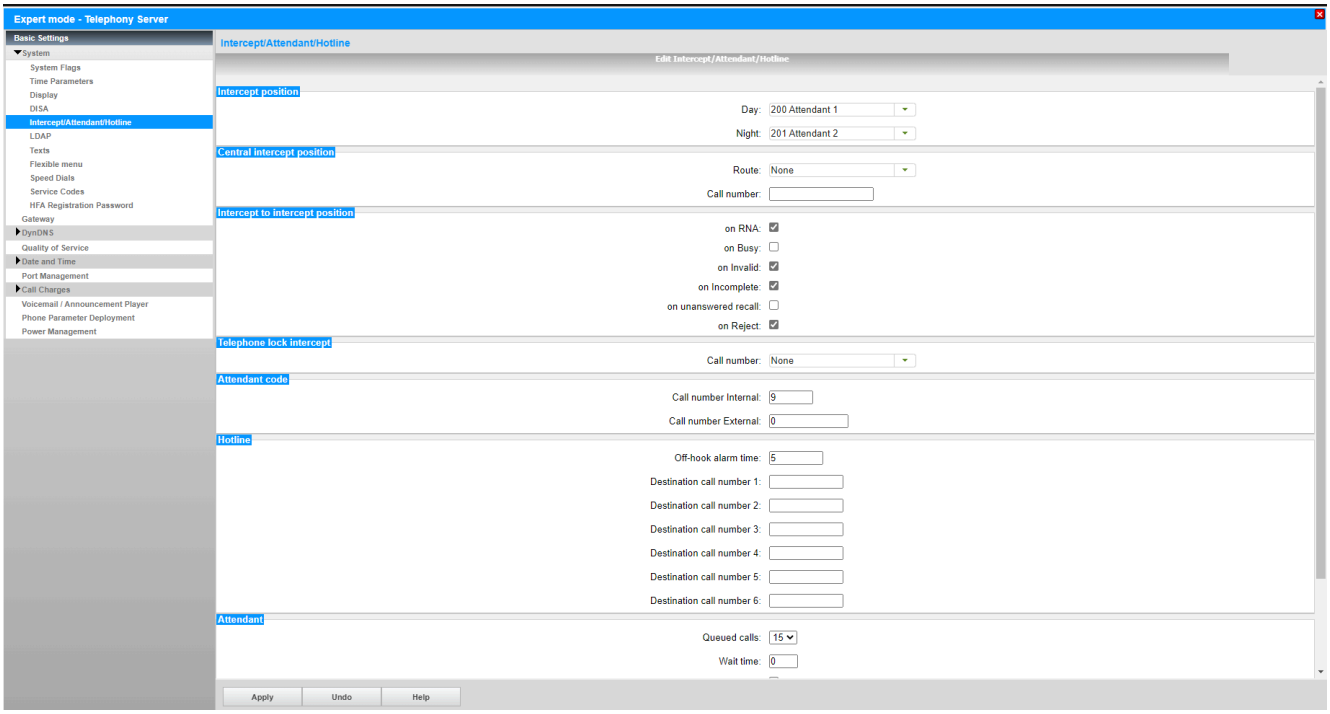
Tipp: SIP- oder CMI-Telefone sind nicht freigegeben.

---

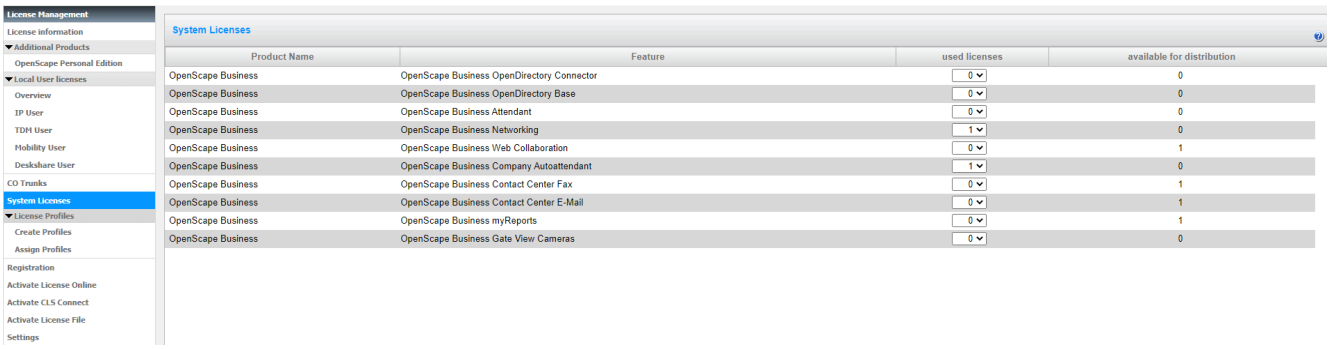
2) Aktivieren Sie das Leistungsmerkmal **Assoziierte Dienste**. Dies ist erforderlich für den OpenScape Business Attendant zum Aktivieren und Deaktivieren von Leistungsmerkmalen für andere Teilnehmer.
3) Aktivieren Sie **Nicht stören aufheben** und deaktivieren Sie **Anklopfen ablehnen Ein**.



4) Konfigurieren Sie die Abwurfkriterien und Platzkennzahlen (Definieren der Abwurfoptionen und der Rufnummern für den Vermittlungsplatz).

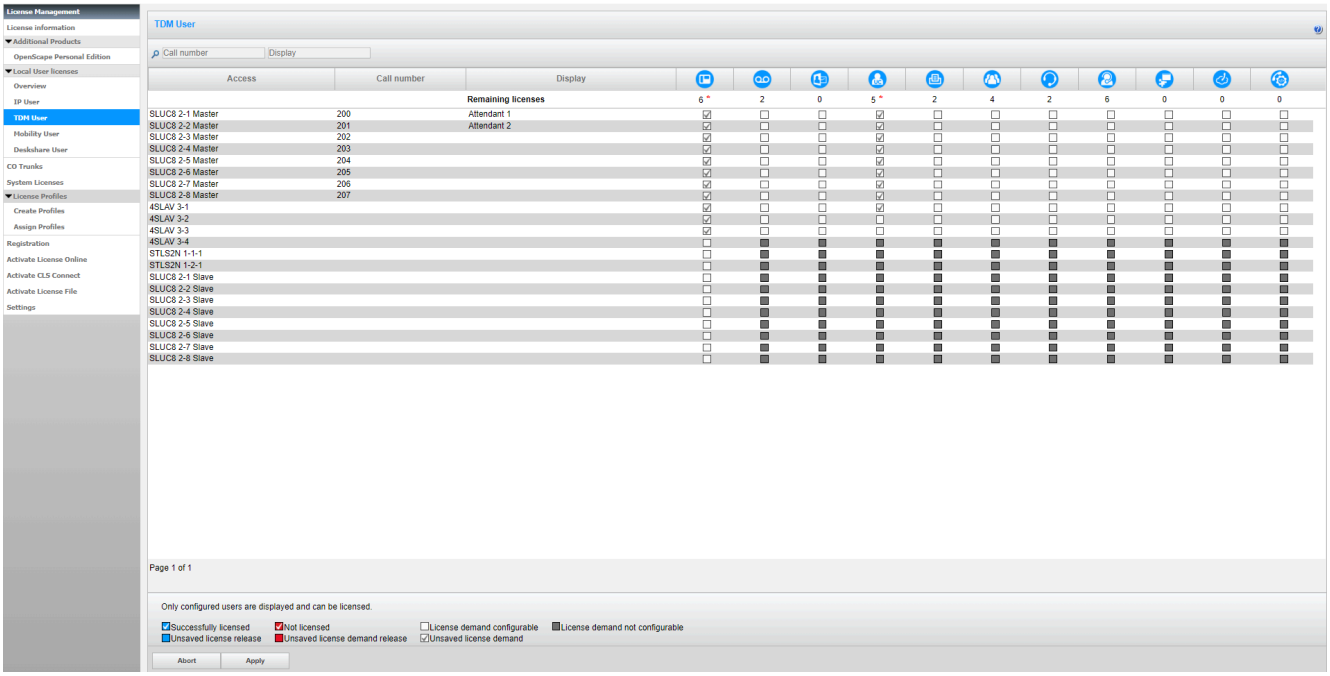


5) Lizenzierung des OpenScape Business Attendant



Product Name	Feature	used licenses	available for distribution
OpenScape Business	OpenScape Business OpenDirectory Connector	0	0
OpenScape Business	OpenScape Business OpenDirectory Base	0	0
OpenScape Business	OpenScape Business Attendant	0	0
OpenScape Business	OpenScape Business Networking	1	0
OpenScape Business	OpenScape Business Web Collaboration	0	1
OpenScape Business	OpenScape Business Company Autoattendant	1	0
OpenScape Business	OpenScape Business Contact Center Fax	0	1
OpenScape Business	OpenScape Business Contact Center E-Mail	0	1
OpenScape Business	OpenScape Business myReports	0	1
OpenScape Business	OpenScape Business Gate View Cameras	0	0

6) Lizenzierung des Präsenzstatus



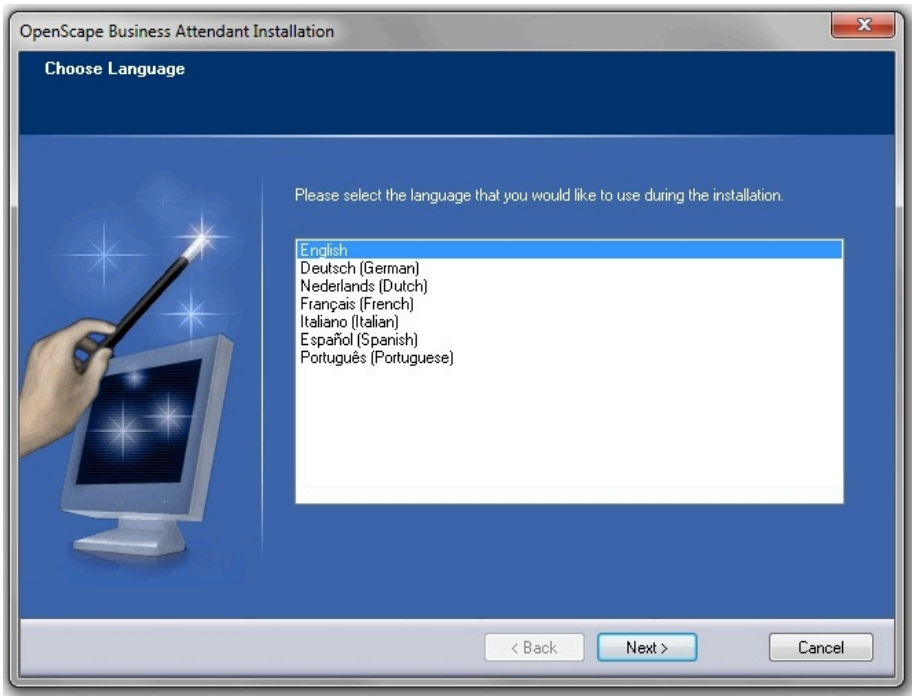
7) Optional: Bei Einrichtung eines Attendants als IP-Teilnehmer muss am Telefon ein Passwort für den Benutzerzugang eingerichtet werden.

8) USB-Treiber installieren

USB - COM-Treiber (CallBridge) für optiPoint 500, OpenStage 30T und OpenStage 40T

USB - RNDIS-Treiber für OpenStage 60T und OpenStage 80T

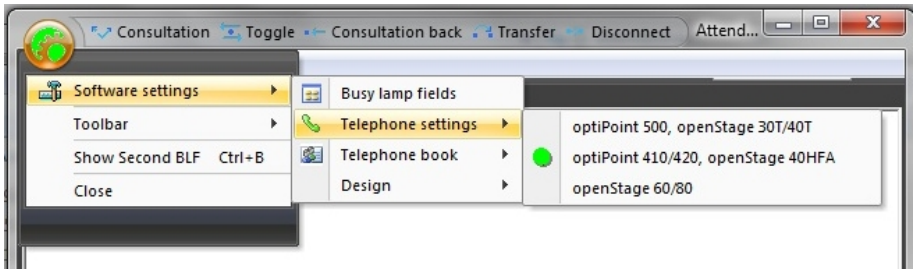
9) OpenScape Business Attendant über die Installationsroutine installieren (Lizenzvereinbarung zustimmen, Angabe des Speicherorts und der Sprache desOpenScape Business Attendants).

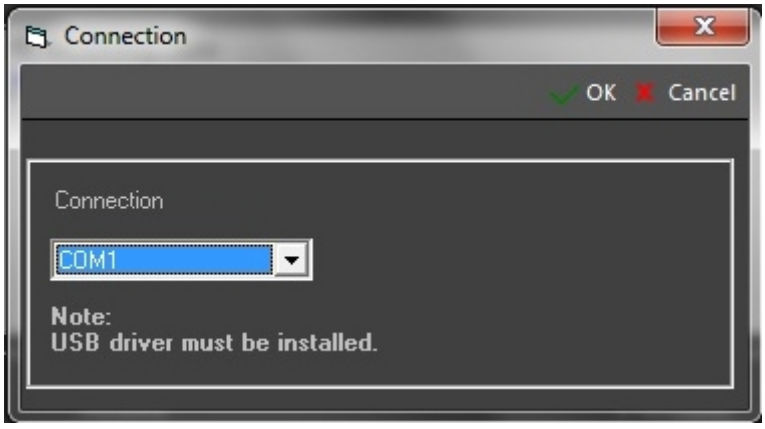


Nach der Installation und dem erstem Start des Programms wird automatisch der Einrichteassistent gestartet, der folgende Einstellungen abfragt:

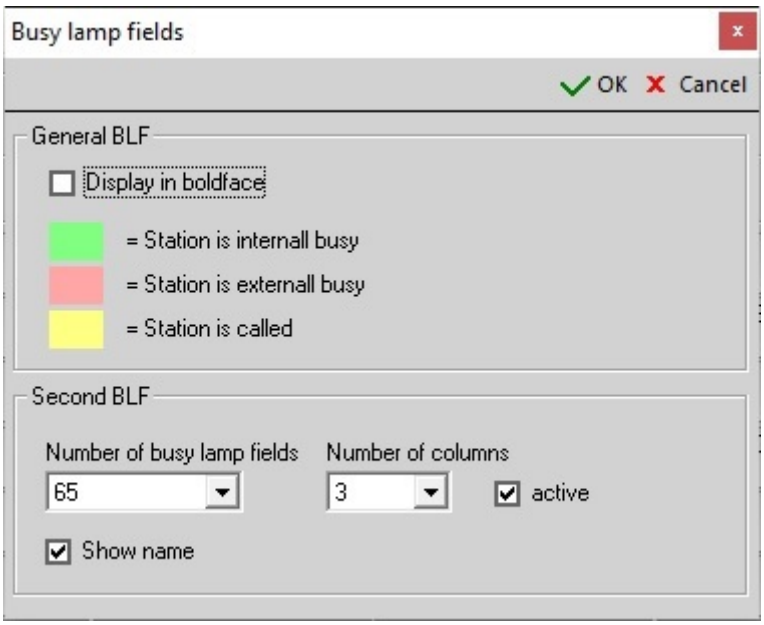
- Art des Telefons
- Soll die Presence-Funktion genutzt werden?

Konfiguration für den Zugang im Attendant:

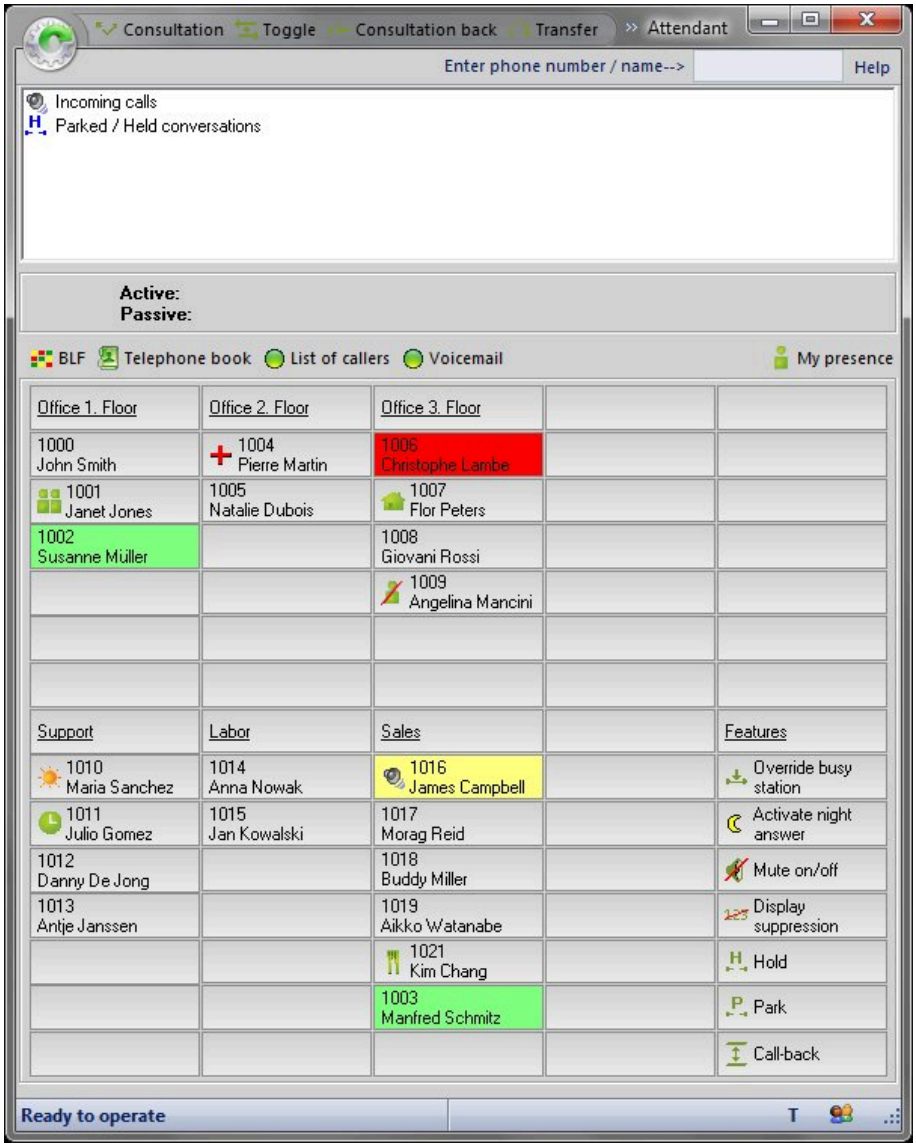




Nach erfolgreicher Anmeldung am Kommunikationssystem besteht die Möglichkeit das BLF automatisch zu füllen.



Tipp: Sicherheitseinstellungen (http oder https) im WBM vergeben bzw. prüfen.



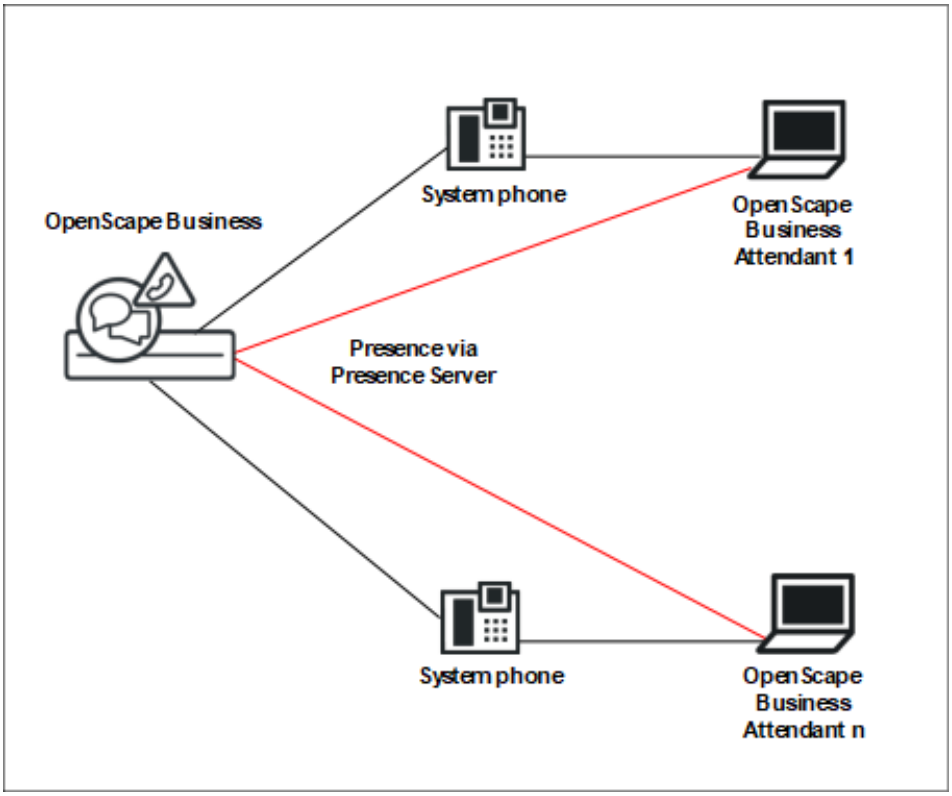
17.3.2.2 Szenario 2: Zwei oder mehr OpenScape Business Attendants, die an ein OpenScape Business Einzelsystem angeschlossen sind

Voraussetzungen

Additiv zum Szenario 1 sind folgende Voraussetzungen erforderlich:

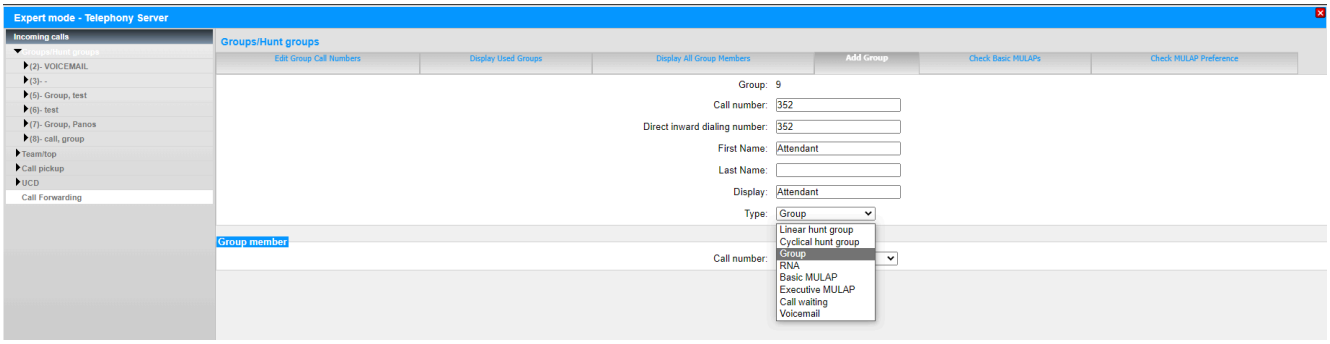
Ausreichende Lizenzen für UC Smart oder UC Suite für Presence-Information (optional)

Gruppenkonfiguration

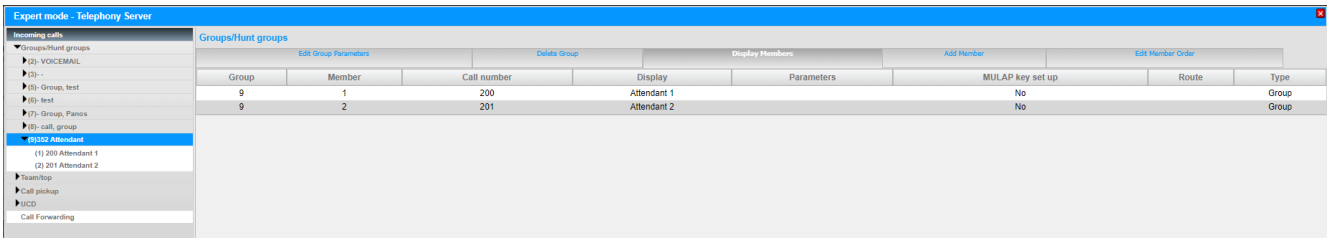


Schritt für Schritt

1) Einrichten eines Teilnehmers als Attendant über WBM (siehe Einrichtebeispiel 1).
2) Definieren einer Gruppe, dabei werden Sammelanschluß (linear und zyklisch) und Rufgruppen unterstützt.



3) Zuweisen der Attendants (der entsprechenden Teilnehmer) zur Gruppe.



Tipp: Konfigurieren Sie die Abwurfkriterien und Platzkennzahlen (Definieren der Abwurfoptionen und der Rufnummern für den Vermittlungsplatz). Der Abwurfplatz ist in diesen Fällen die Gruppen-Rufnummer.

17.3.2.3 Szenario 3: OpenScape Business Vernetzung mit jeweils eigenen OpenScape Business Attendants (netzweite BLF und Anwesenheitsstatus über WSI)

Voraussetzungen

Lizenz für UC Smart für Presence-Information (optional)

Die Verwendung mehrerer OpenScape Business Attendants ist nur in UC Smart-Netzwerken möglich. WSI (Presence Server von OpenScape Business) liefert netzweite Telefoniestatus- und Präsenzinformationen. UC Suite-Netzwerke benötigen myAttendant, um netzweite Funktionen bereitzustellen.

17.3.2.4 Szenario 4: OpenScape Business-Vernetzung mit zentralem OpenScape Business Attendant (netzweite BLF und Anwesenheitsstatus über WSI)

Voraussetzungen

Lizenz für UC Smart für Presence-Information (optional)

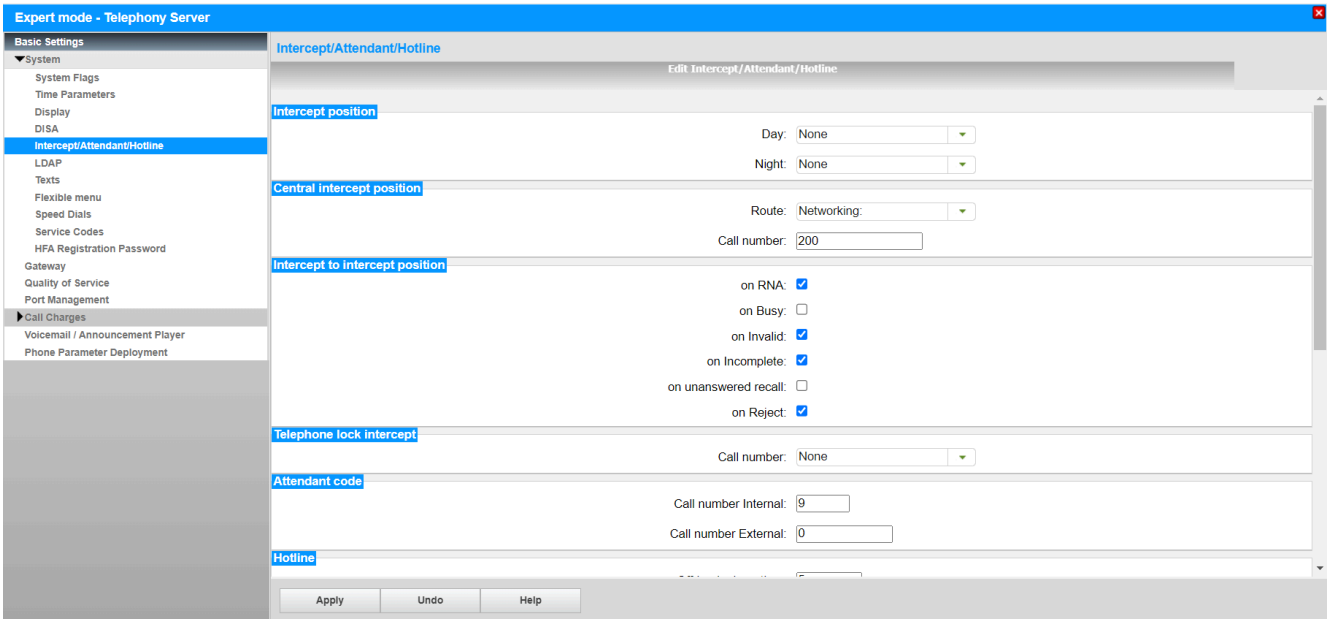
Mehrere OpenScape Business Attendants können nur in UC-Smart-Netzwerken verwendet werden. WSI (Anwesenheitsserver von OpenScape Business) bietet netzweite Informationen zu Telefoniestatus und Anwesenheit. UC-Suite-Netzwerke benötigen myAttendant für netzweite Funktionalität.

Zentraler Abwurfplatz (in dem Knoten, in dem kein OpenScape Business Attendant eingerichtet ist)

Schritt für Schritt

1) Einrichten des OpenScape Business Attendant gemäß Einrichtebeispiel 1.

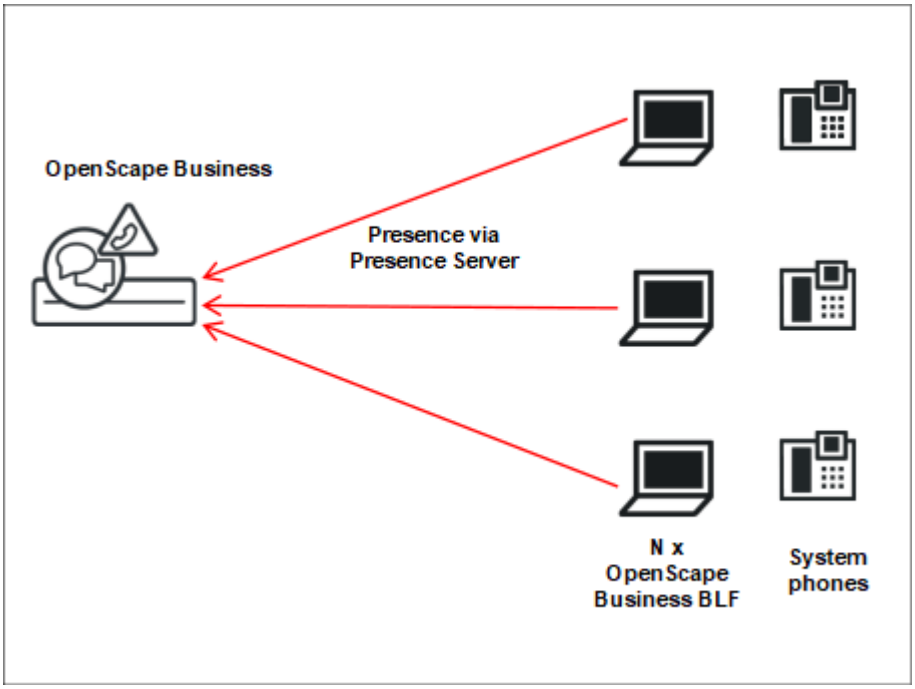
2) In dem Knoten (in dem kein OpenScape Business Attendant eingerichtet ist) den zentralen Abwurfplatz eintragen.



17.3.2.5 Szenario 5: OpenScape Business BLF an einem OpenScape Business Einzelsystem

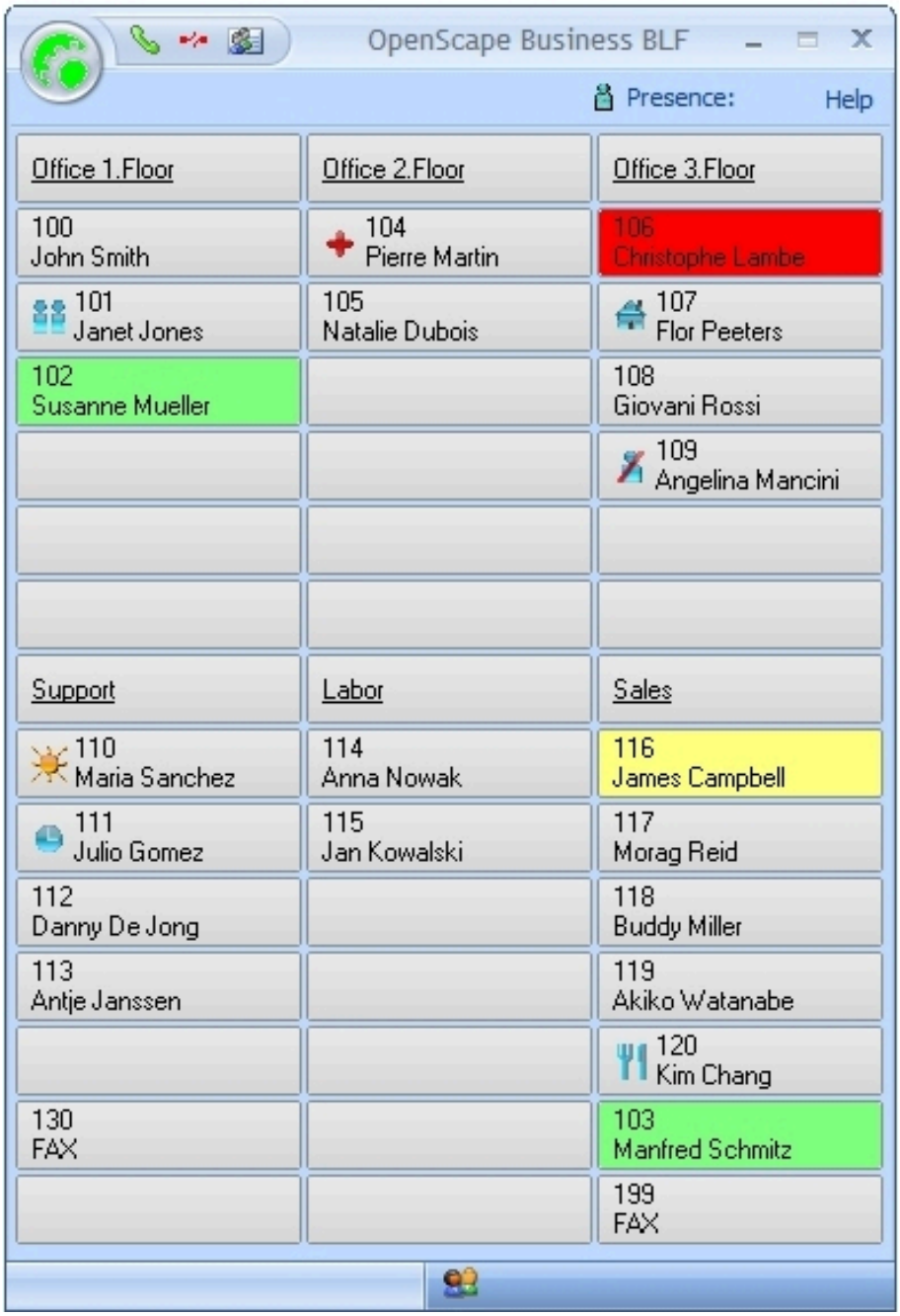
Voraussetzungen

- Eine OpenScape Business BLF Lizenz je Teilnehmer ist vorhanden
- Telefone sind bereits zugeordnet
- Eine UC User-Lizenz je Teilnehmer ist vorhanden



Schritt für Schritt

1) Telefone über WBM einrichten
2) Presence Server über WBM einrichten
3) OpenScape Business BLF installieren und starten
4) Die (optionale) automatische Belegung des OpenScape Business BLF erfolgt nach dem ersten Hochfahren.



17.3.2.6 Szenario 6: OpenScape Business BLF an einem OpenScape Business Netzverbund (BLF und Anwesenheitsstatus über WSI)

Voraussetzungen

- Eine OpenScape Business-BLF-Lizenz je Teilnehmer ist vorhanden
- Telefone sind bereits zugeordnet
- Eine UC User-Lizenz je Teilnehmer ist vorhanden
- OpenScape Business BLF kann in UC-Smart-Netzwerken verwendet werden, nicht in UC Suite-Netzwerken. WSI (Anwesenheitsserver von OpenScape Business) bietet netzweite Informationen zu Telefoniestatus und Anwesenheit.

Schritt für Schritt

1) Telefone über WBM einrichten

2) OpenScape Business BLF installieren und starten

3) Nach dem ersten Hochlauf erfolgt die Anbindung an den WSI sowie die manuelle Belegung des BLF. In diesem Fall kann das BLF mit netzweiten Teilnehmern belegt werden.

17.4 myAttendant

Mit myAttendant stehen Ihnen umfangreiche Vermittlungsfunktionen zur Verfügung. Die Teilnehmer werden komfortabel über Benutzerschaltflächen verwaltet. Für die Nachrichtenvermittlung (Sprach-, Fax- und Sofortnachrichten, SMS, E-Mail) steht Ihnen das Nachrichten-Center zur Verfügung.

Wesentliche Vermittlungsfunktionen

Pro Kommunikationssystem (pro Netzknoten) können maximal 20 myAttendant angeschlossen werden. Der Maximalausbau eines Netzverbunds ist die Summe der Kapazitäten der vernetzten Kommunikationssysteme. Der Anwesenheitszustand und der Telefonstatus werden für alle Teilnehmer im Netzwerk dargestellt. Im Nachrichtencenter von myAttendant werden die Teilnehmer des eigenen Kommunikationssystems dargestellt.

- Anstehende bzw. angenommene Anrufe verwalten
- Daten des aktiven Gesprächs werden angezeigt
- Geparkte, gehaltene Gespräche werden angezeigt
- Anruferliste
- Journal für offene, geplante, interne, extern, angenommene, verpasste und gehende Gespräche
- Telefonbuchanwendung
  - LDAP (z. B. ODS)
  - Persönliches Telefonbuch / Outlook-Kontakte
  - Internes Verzeichnis, bei Vernetzung aller Teilnehmer im Netzwerk.

- Besetztlampenfeld-Status aller internen Teilnehmer des eigenen Systems sowie aller Teilnehmer des Netzwerks
  - Telefonstatus: Frei, Besetzt, Gerufen, Umgeleitet, Anrufschutz
  - Anwesenheitsstatus: Büro, CallMe, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zuhause (netzweit)

  Anmerkung: Der Anwesenheitsstatus "krank" ist je nach Systemeinstellung des Administrators möglicherweise nicht verfügbar.

- Es stehen drei Oberflächen-Styles zur Auswahl.
- Es können maximal 20 myAttendant je Kommunikationssystem angeschlossen werden (max. 20 Lizenzen je OpenScape Business X3/X5/X8 und OpenScape Business S). Die Lizenzierung von myAttendant geschieht über das WBM.

Technische Voraussetzungen (Details hierzu siehe Vertriebsinformation)

- Standard Windows-PC
- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)
- Terminal Server Einsatz möglich

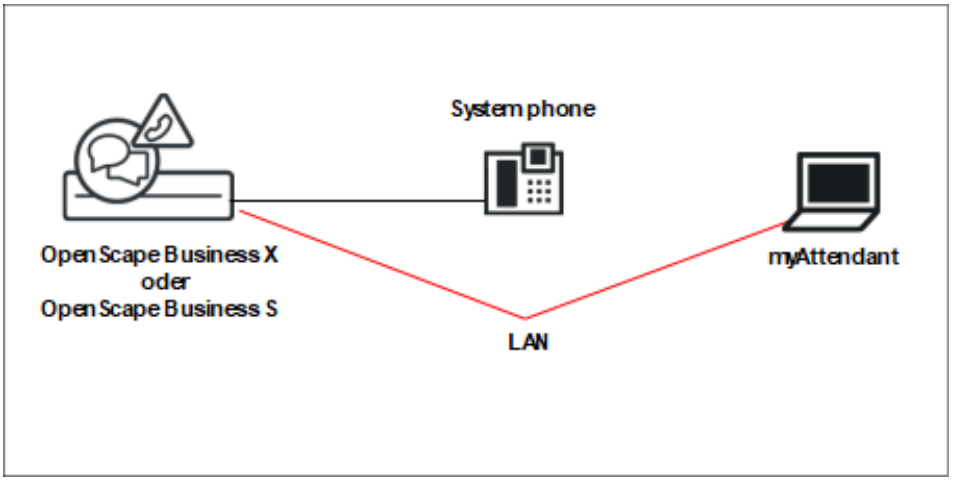
Zusätzliche Software

- Auf einem PC muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein (siehe **Service-Center** > **Software**)

Unterstützte Telefone

- OpenStage 40/60/80 HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- SIP-Telefone mit RFC 3725-Unterstützung, z. B. OpenScape Desk Phone IP 35G/55G SIP, OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X SIP, OpenScape Desk Phone CP 110/210/410/710 SIP
- OpenStage 30T/40T/60T/80T

Einfaches Plug-and-Play bei der Installation, die ersten Schritte für die Installation werden dem Anwender (wenn seine Mail-Adresse konfiguriert wurde) vom System zugeschickt.



17.4.1 Teilnehmerverwaltung

Für die Verwaltung der Teilnehmer in myAttendant stehen die Benutzerschaltflächen, das interne, das externe und das persönliche Verzeichnis zur Verfügung.

Benutzerschaltflächen

Die Benutzerschaltflächen befinden sich in der Registerkarte **Standard** und sind ein Bestandteil des Hauptfensters von myAttendant.

In einer Registerkarte der Benutzerschaltflächen stehen 100 Benutzerschaltflächen zur Verfügung. Sie können die Standardanzahl der Benutzerschaltflächen pro Registerkarte jederzeit ändern.

Die Benutzerschaltflächen sind standardmäßig alphabetisch nach Nachname sortiert.

Es können mehrere Registerkarten für Benutzerschaltflächen eingerichtet werden; für diese Benutzerschaltflächen können Sie die Namen frei wählen.

Den Benutzerschaltflächen können interne, externe und persönliche Kontakte (Benutzer) zugeordnet werden.

17.4.2 Nachrichtencenter

Im **Nachrichten-Center** von myAttendant werden Sprach-, Fax- und Sofortnachrichten, sowie SMS und E-Mails protokolliert und verwaltet.

Nachrichten können für andere Teilnehmer verwaltet werden. Diese müssen dazu die Erlaubnis erteilt haben.

In der Teilnehmerliste sind alle Teilnehmer des Kommunikationssystems mit ihrem An-/Abwesenheitsstatus aufgelistet. An oberster Stelle steht Ihr eigener Status mit aufgeklappter Nachrichtenübersicht. Die weiteren Teilnehmer folgen in alphabetischer Reihenfolge.

Abhängig von der Auswahl in der Nachrichtenübersicht werden Nachrichtendetails angezeigt, die Informationen zu den Nachrichten tabellarisch angezeigt und können dort zur Bearbeitung ausgewählt werden.

Die Nachrichtentypen können wie folgt bearbeitet werden:

- **Sprachnachrichten** können abgehört, gelöscht, weitergeleitet werden,
- **LAN-Nachrichten** können gelesen, geändert und gelöscht werden,
- **Faxnachrichten** können weitergeleitet werden.

LAN-Nachrichten

LAN-Nachrichten können nur von Benutzern von myAttendant erstellt werden. Sie dienen als eine Art "Schwarzes Brett" für den Teilnehmer, auf dem er sich Notizen (zu einzelnen Teilnehmern) macht. Diese Nachrichten können angesehen, geändert oder gelöscht werden; sie können nicht an andere Teilnehmer versendet werden.

17.4.3 Szenario 1: Wie Sie myAttendant an einem OpenScape Business Einzelsystem einrichten

Voraussetzungen

Lizenz für myAttendant ist vorhanden

Telefon mit gültiger Lizenz

Application Server oder Application Board vorhanden

UC Suite ist über den Basisinstallations-Wizard aktiviert

Schritt für Schritt

1) Telefon für den Vermittlungsplatz über WBM konfigurieren

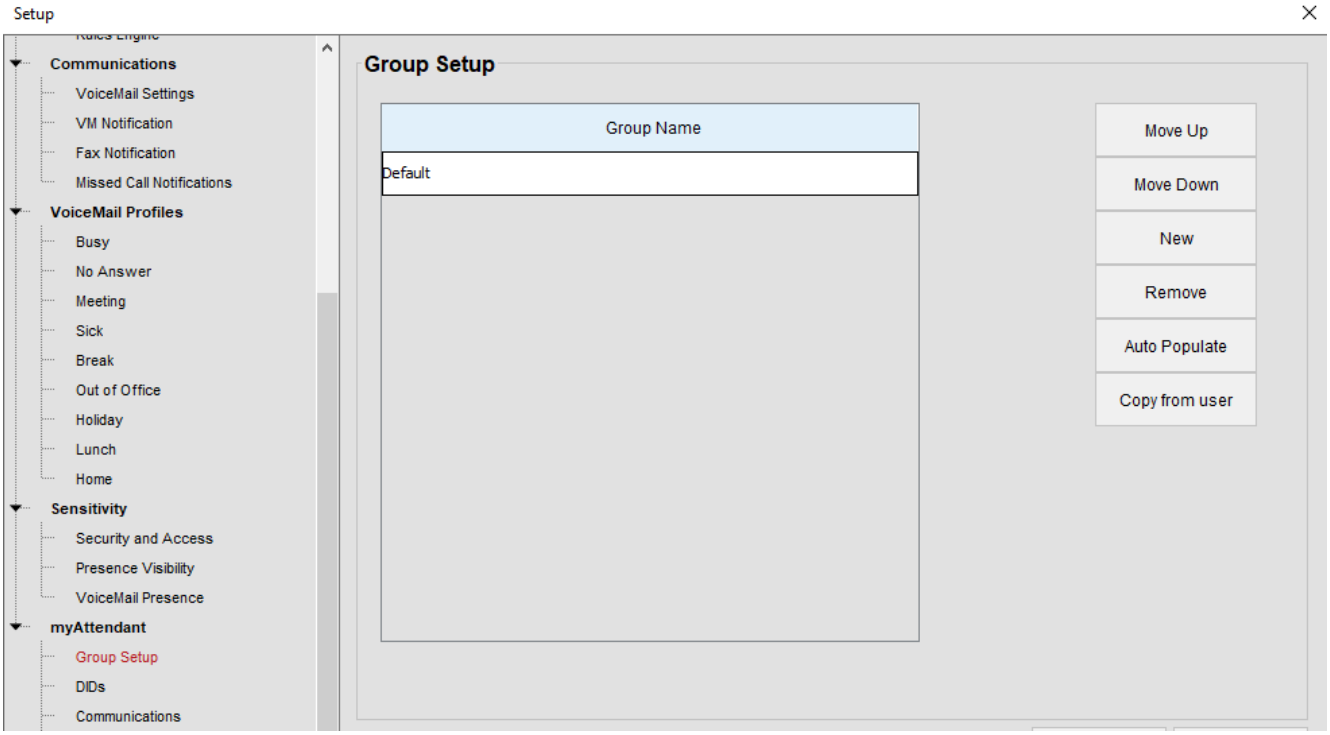
2) Deaktivieren Sie im **Experten-Modus** unter **Teilnehmer**>**IP-Clients**>**System Clients**>**Teilnehmer**>**Teilnehmer Flags ändern** den Anklopfschutz.

3) Aktivieren Sie im **Experten-Modus** unter **Telefonie**>**Grundeinstellungen**>**System> Abwurf**>**VPL**>**Hotline** das Leistungsmerkmal **Sofortiges Anklopfen durch VPL**.

4) Kontrollieren bzw. ändern Sie die Abwurfkriterien und Platzkennzahlen (Definieren der Abwurfoptionen und der Rufnummern für den Vermittlungsplatz).

5) Lizenzierung von myAttendant

6) Nach erfolgreicher Anmeldung am Kommunikationssystem besteht die Möglichkeit das BLF automatisch zu füllen. Dies können Sie in myAttendant unter **Einrichtung > myAttendant > Gruppeneinrichtung** konfigurieren.



17.4.4 Szenario 2: Wie Sie zwei oder mehrere myAttendants an einem OpenScape Business Einzelsystem einrichten

Das Szenario 2 baut auf Szenario 1 auf und wird additiv eingerichtet.

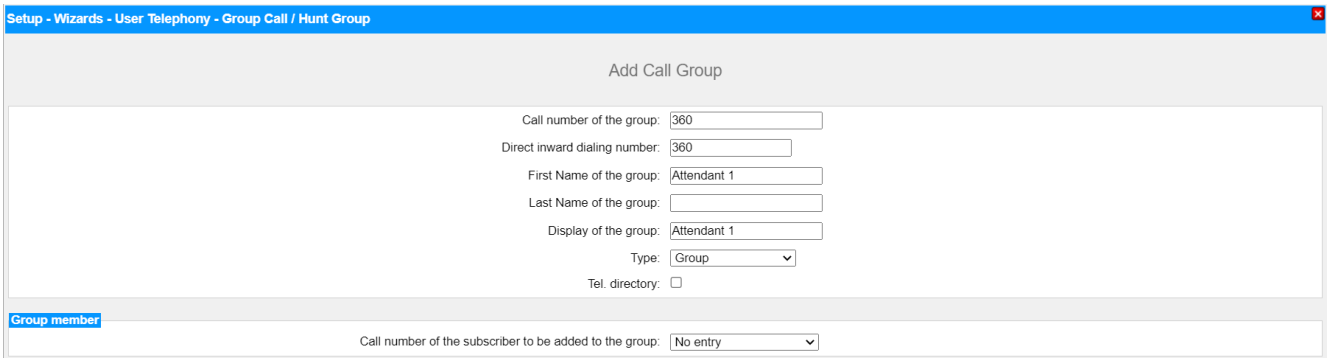
Voraussetzungen

Ausreichende Lizenzen für myAttendant

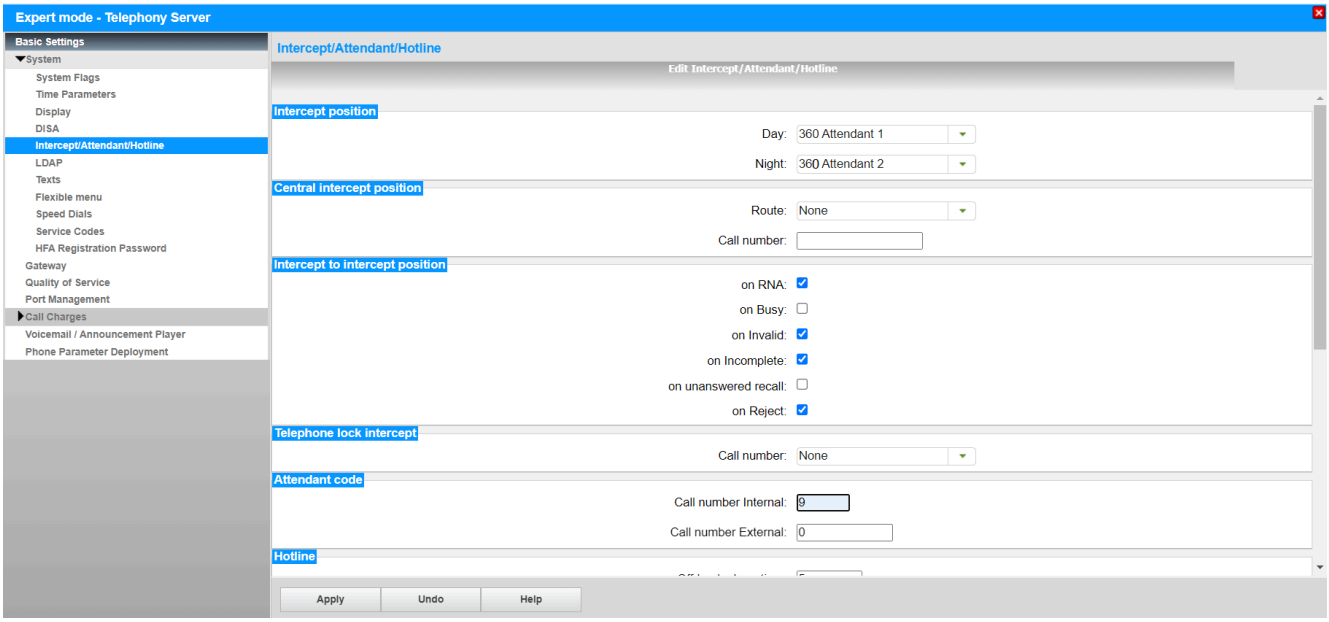
Telefon mit gültiger Lizenz

Schritt für Schritt

1) Konfigurieren Sie eine Gruppe (die nur aus Vermittlungsplätzen besteht) im WBM unter **Einrichtung** > **User-Telefonie** > **Gruppenruf / Sammelanschluss**>**Hinzufügen**.



2) Wählen Sie diese Gruppe bei der Konfiguration der OpenStage Vermittlungsplatz Telefone aus.



17.4.5 Szenario 3: Wie Sie ein OpenScape Business-Netzwerk mit zentralem myAttendant einrichten

Das Szenario 3 baut auf Szenario 1 und 2 auf und wird additiv eingerichtet. Knoten 1 wird mit Knoten 2 verbunden. Die zentrale Vermittlungsplatz befindet sich in Knoten 2.

Voraussetzungen

Ausreichende Lizenzen für myAttendant vorhanden

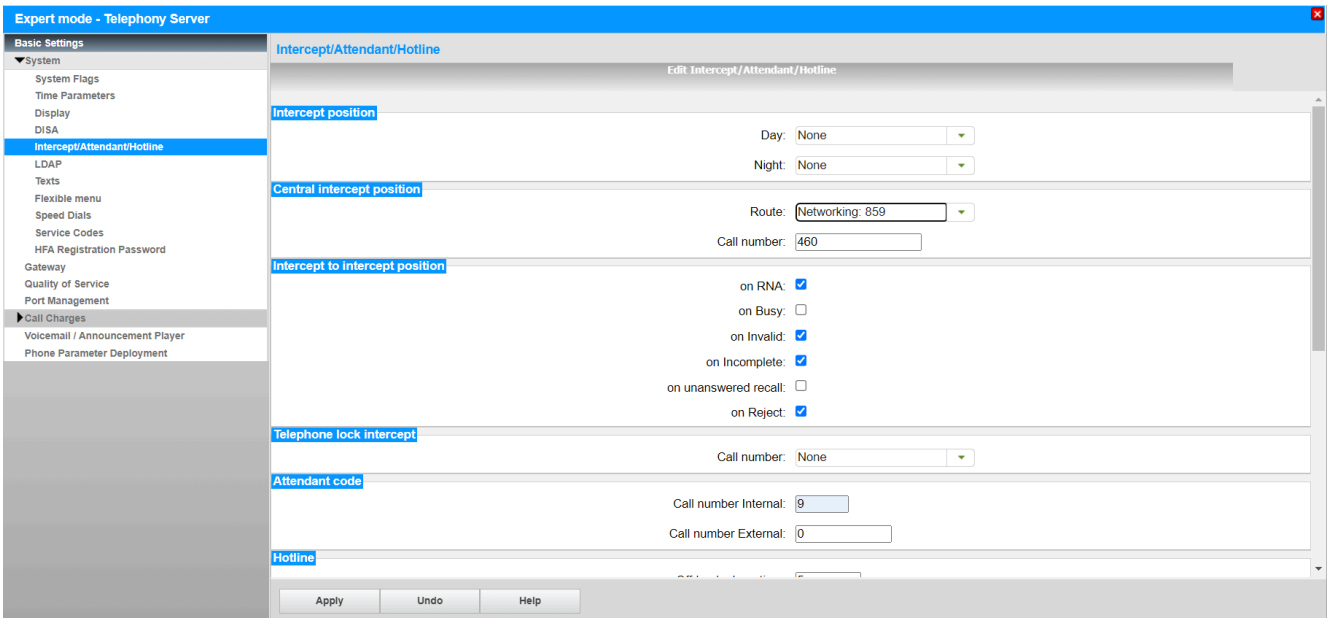
Lizenzen für die Vernetzung sind vorhanden

Telefon mit gültiger Lizenz

LCR ist eingerichtet

Schritt für Schritt

1) Richten Sie einen zentralen Abwurfplatz in Knoten 1 ein. Der zentrale Abwurfplatz muss in einem Knoten angelegt sein, in dem KEIN Vermittlungsplatz eingerichtet ist.



2) Richten Sie den Vermittlungsplatzes für System 2 ein (wie in Szenario 2 beschrieben).
3) Installieren Sie myAttendant mit den Benutzerdaten von Knoten 2.

17.5 Abwurfplatz

Das Kommunikationssystem ermöglicht, externe Anrufe, die keinem Teilnehmer zuzuordnen sind oder nicht beantwortet werden, an einen festzulegenden Abwurfplatz umzuleiten, damit kein Anruf verloren geht. Die Abwurfkriterien können Sie als Administrator konfigurieren.

Der Abwurfplatz kann ein einzelner Teilnehmer, eine Gruppe oder ein Ansagegerät sein:

- Abwurfplatz (Vermittlungsplatz)
- Teilnehmer
- Sammelanschluss
- MULAP-Gruppe
- Gruppenruf
- externes Ansagegerät

Eine UCD-Gruppe darf nicht als Abwurfplatz ausgewählt werden.

Ist ein Abwurfplatz konfiguriert, werden im Abwurffall die Anrufe an diesen Abwurfplatz weitergeleitet. Ist kein Abwurfplatz konfiguriert, so werden abgeworfene Anrufe beim ersten IP-Teilnehmer signalisiert.

Ist ein interner Teilnehmer als Abwurfplatz eingerichtet, wird ihm automatisch die Standard-Tastenbelegung zugewiesen. Zusätzlich kann der Abwurfplatz für das Leistungsmerkmal "Aufschalten" berechtigt werden.

Sie können als Administrator dem Abwurfplatz für intern und extern jeweils eine Platzkennzahl (2-stellig) zuweisen, unter welcher dieser direkt erreichbar ist.

Ein Abwurf wirkt systemweit, d.h. bei Gemeinschaftsanlagen für alle Teilnehmer gleich. Siehe auch "Zentraler Abwurfplatz im Netzverbund" im Kapitel Vernetzung.

Abwurfkriterien

Durch Abwurfkriterien legen Sie als Administrator fest, in welchen Situationen der Abwurf erfolgen soll. Folgende Abwurfkriterien sind möglich:

- Im Freifall

  Der Anruf folgt den Einträgen im Call Management (z.B. einer konfigurierten Rufweiterschaltung). Nimmt kein Teilnehmer den Anruf an, wird er zum Abwurfplatz weitergeleitet.
- Im Besetztfall, falls keine Weiterschaltung mehr möglich ist

  Zunächst wird geprüft, ob angeklopft werden kann. Wenn nicht angeklopft werden kann, so folgt der Anruf den Einträgen im Call Management (z.B. einer konfigurierten Rufweiterschaltung). Nimmt kein Teilnehmer den Anruf an, wird er zum Abwurfplatz weitergeleitet. Abwurf im Besetztfall bezieht sich nur auf den Erstanruf, nicht auf vermittelte oder gehende Verbindungen. Ein Wiederanruf eines externen Teilnehmers wird bei besetztem Zielteilnehmer nicht sofort abgeworfen, sondern es erfolgt Anklopfen.
- Bei Falschwahl

  Falls die gewählte Rufnummer nicht konfiguriert oder nicht aktiv ist.
- Bei unvollständiger Wahl

  Falls die gewählte Rufnummer zu kurz ist. Existiert ein zentraler Abwurfplatz, wird unvollständige Wahl nicht ausgewertet.
- Bei nicht beantwortetem Wiederanruf

  Wird ein externer Anruf nach Übergeben vor Melden nicht abgefragt und erfolgt nach Wiederanruf am ursprünglichen Ziel ebenfalls kein Melden, so erfolgt nach Ablauf der voreingestellten Zeit der Abwurf.
- Bei Ablehnung

  Falls der Anruf von einem internen Teilnehmer abgelehnt wurde, so folgt der Anruf den Einträgen im Call Management (z.B. einer konfigurierten Rufweiterschaltung). Nimmt kein Teilnehmer den Anruf an, wird er zum Abwurfplatz weitergeleitet.
- Bei fehlender Rufnummer

  Wie bei Falschwahl.
- Bei Anrufweiterschaltung mit Verkettung

  Wenn ein umgeleiteter Anruf am Ziel der Umleitung jeweils auf eine weitere Anrufumleitung trifft und dabei die Anzahl der zulässigen Verkettungen überschritten wird, erfolgt Abwurf. Die Anzahl der zulässigen Verkettungen ist abhängig von den Eintragungen in der Rufweiterschaltung, maximal sind drei Verkettungen erlaubt.
- Bei Codeschloss

  Wählt ein Teilnehmer an einem Telefon mit aktiviertem Codeschloss eine Richtungskennzahl, erfolgt Abwurf. Für diesen Fall legt der Administrator ein separates Abwurfziel fest.

- Bei Ansage (nur mit UC Suite)

  Wählt ein Teilnehmer die Platzkennzahl (2-stellig), während er eine Ansage der Sprachbox oder des AutoAttendant hört, erfolgt Abwurf. Für diesen Fall legt der Administrator ein separates Abwurfziel fest.

Abhängigkeiten

Themenbereich	Abhängigkeit
Datenrufe	Datenrufe werden getrennt anstatt abgeworfen.
Sammelanschluss	Aus einem Sammelanschluss erfolgt kein Abwurf, der Ruf wird wieder zum ersten Sammelanschluss-Teilnehmer weitergeschaltet und verbleibt im Sammelanschluss.
Standard-Tastenbelegung	Die Standard-Tastenbelegung enthält auch die Taste **Zahl der Anrufe zeigen**. Diese kann nur an 6 Endgeräte vergeben werden. Wenn die Grenze erreicht ist, werden keine Standard-Tastenbelegungen mehr vergeben. Die vergebene Standard-Tasten werden nicht zurückgenommen, wenn ein Gerät nicht länger als Abwurfplatz definiert ist.
S_0-Leitungen	Eine Auswertung für S_0-Leitungen findet nur dann statt, wenn kein Abwurfplatz für Tag/Nacht eingerichtet ist.
Nachtschaltung	Damit bei aktivierter Nachtschaltung über DuWa- und HKZ-Leitungen jeweils das gleiche Ziel erreicht wird, muss der Eintrag für die Nachtstellen-Nummer unter Abwurf > VPL mit der **NachtRuf-Nr** in **Rufzuordnung Ltg** übereinstimmen.

17.5.1 Wie Sie Abwurfplatz und Abwurfkriterien konfigurieren

Mit dem Wizard **Vermittlungsplatz** können Sie die Rufnummern für den Abwurfplatz sowie Abwurfkriterien konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vermittlungsplatz** zu starten.
4) Legen Sie in den Bereichen **Vermittlungsplatz** und **Platzkennzahl** (2-stellig) die gewünschten Rufnummern für den Abwurfplatz fest.
5) Legen Sie im Bereich **Abwurfkriterien** die gewünschten Werte fest.
6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

17.5.2 Wie Sie einen zentralen Abwurfplatz konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Abwurf/ VPL/Hotline**.
4) Wählen Sie im Bereich **Zentraler Abwurfplatz** in der Aufklappliste **Richtung** den gewünschten Eintrag.
5) Geben Sie im Bereich **Zentraler Abwurfplatz** die gewünschte **Rufnummer** für **Tag** und **Nacht** ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

17.5.3 Wie Sie Abwurf bei Codeschloss konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Abwurf/ VPL/Hotline**.
4) Wählen Sie im Bereich **Abwurf bei Codeschloss** in der Aufklappliste **Rufnummer** den gewünschten Eintrag.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

17.5.4 Abwurf bei Ansage konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie im Menübaum auf **Server**.
4) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.
5) Geben Sie im Bereich **Rufnummer des Abwurfplatzes** im Feld **Zielnummer** die Rufnummer für den Abwurfplatz ein.
6) Klicken Sie auf **Speichern** und schließen Sie das Fenster.

18 Multimedia Contact Center

Das Contact Center ist eine leistungsstarke Lösung zur optimalen Verteilung und Bearbeitung von kommenden Anrufen, Faxen und e-Mails. Die intelligente, fähigkeitsbasierte Verteilung stellt sicher, dass Anrufer unabhängig vom Kontaktmedium mit dem am besten qualifizierten Contact-Center-Agenten verbunden werden. Über die Applikation myAgent stehen den Contact-Center-Agenten komfortable Funktionen für die Bearbeitung und Nachbearbeitung von Anrufen, Faxen und E-Mails zur Verfügung. myReports stellt für die Auswertung des Contact-Center-Betriebs vielfältige Berichtsvorlagen zur Verfügung.

Das Multimedia Contact Center ist vollständig in die UC-Suite-Software integriert. Alle benötigten Software-Komponenten sind enthalten. Die Contact-Center-Funktionen selbst werden über Lizenzen freigeschaltet.

Das Contact Center nutzt die Ressourcen des Kommunikationssystems, wie zum Beispiel Warteschlangen für kommende Anrufe und Unified-Communications-Funktionen für die Aufnahme und die Wiedergabe von Ansagen.

Die zentrale Software-Komponente des Contact Centers steuert alle Routing-Funktionen für kommende Anrufe, Faxe, E-Mails und steuert die über LAN angeschlossenen PC-Arbeitsplätze der Agenten und Wandanzeigen.

Auf den PC-Arbeitsplätzen der Agenten wird die Applikation myAgent installiert. Optional kann auch die Applikation myReports zur Generierung und Versendung von Berichten installiert werden. Die erforderliche Software kann direkt aus dem Downloadbereich des Kommunikationssystems heruntergeladen und auf den Client-PC installiert werden.

Mittels WBM wird die Einrichtung der Contact-Center-Grundfunktionen, der Zeitpläne und Verteilregeln sowie der Agenten vorgenommen. Einstellungen für den täglichen Betrieb des Contact Centers, wie zum Beispiel die Zuordnung von Agenten zu Warteschlangen können auch direkt über myAgent getätigt werden.

Steht das Contact Center aufgrund von Problemen (Absturz, fehlende Verbindung oder ähnliches) nicht zur Verfügung, kann eine Rückfalllösung über die UCD-Funktion des Kommunikationssystems realisiert werden. Verteilregeln für den Notfall müssen bei der Einrichtung der UCD-Gruppen im Rahmen der Ersteinrichtung des Contact Centers berücksichtigt werden.

Tipp: Informationen zur UC Suite und den Unified-Communications-Funktionen können dem Kapitel UC Suite entnommen werden.

18.1 Contact Center Clients

Die Applikation myAgent stellt den Contact Center-Agenten komfortable Funktionen für die Bearbeitung und Nachbearbeitung von Anrufen, Faxen und E-Mails zur Verfügung. Über die Applikation myReports können Berichte (Reports) über Anrufe, Warteschlangen, Agenten, Performance, Servicelevel und Nachbearbeitungscodes des Contact Centers erstellt werden. Mehr als 100 vordefinierte Berichtsvorlagen stehen zur Verfügung.

18.1.1 myAgent

Allen Agenten stehen über myAgent komfortable Funktionen für die Bearbeitung und Nachbearbeitung von Anrufen, Faxen und E-Mails zur Verfügung.

myAgent bietet folgende Leistungsmerkmale:

- Bearbeitung von
  - Anrufen
  - Faxe
  - E-Mails
- Rückruffunktion für Agenten
- Anzeige und Änderung des Agentenstatus
- Anzeige und Änderung des Anwesenheitsstatus interner Teilnehmer des Kommunikationssystems
- Darstellung der Warteschlangen in Echtzeit
- Aufzeichnung von Anrufen, sofern im Kommunikationssystem aktiviert
- Sofortnachricht versenden
- Anforderung um Unterstützung durch
  - Anrufüberwachung (länderabhängig)
  - Aufschalten auf Anrufe
  - Sofortnachricht versenden
- Einbindung des internen Verzeichnisses, des externen Verzeichnisses, des externen Offline-Verzeichnisses (LDAP) und der Outlook-Kontakte für die Suche nach Namen
- Erstellung von Berichten auf Basis vordefinierter Berichtsvorlagen

Je nach zugewiesener Berechtigungsstufe stehen einem Agenten Standardfunktionen (Agent) oder erweiterte Funktionen (Supervisor oder Administrator) in myAgent zur Verfügung (siehe Berechtigungsunabhängige Funktionen für Agenten).

Die Zuordnung von Agenten zu Warteschlangen erfolgt mit Hilfe der Applikation myAgent. Diese Zuordnung kann ein Agent mit dem Berechtigungs-Level Supervisor oder Administrator durchführen. Dabei können den Agenten folgende Eigenschaften zugewiesen werden (Agentenzuweisung), die Einfluss auf die Verteilung der Anrufe, Faxe und E-Mails in einer Warteschlange haben:

- **Hauptagent** oder **Agent bei Überlauf**

  An Hauptagenten werden Anrufe gleichmäßig verteilt. Ein Agent bei Überlauf erhält einen Anruf nur dann, wenn die Anrufe eine bestimmte Anzahl überschritten haben oder ein Anruf eine bestimmte Wartezeit überschritten hat.
- **Agentenrückruf aktivieren**

  Agentenrückruf ermöglicht einem Anrufer in der Warteschlange eine Sprachnachricht für Agenten zu hinterlassen. Sobald ein entsprechender Agent verfügbar wird, erhält dieser einen Anruf, hört die Sprachnachricht des Anrufers und kann ihn zurückrufen.
- **Fähigkeits-Level**

  Das Fähigkeits-Level steuert die Verteilung der Anrufe auf die Agenten in einer Warteschlange. Agenten mit höherem Fähigkeits-Level werden bei

der Anrufverteilung bevorzugt. Haben alle Agenten den gleichen Fähigkeits-Level, erhält der am längsten freie Agent den Anruf.

- **Nachbearbeitung**

  Während der Nachbearbeitung kann ein Agent nach Beenden eines Gesprächs zum Beispiel Verwaltungsaufgaben erledigen, bevor er den nächsten Anruf erhält.
- **Überlauf nach Anrufen in Warteschlange**

  Anrufe, die über diese Maximalzahl hinausgehen, erhält ein Agent bei Überlauf.
- **Überlauf nach Sekunden in Warteschlange**

  Anrufe, die diese Wartezeit überschreiten, erhält ein Agent bei Überlauf.

Die **Liste der Agentenzuweisungen** zeigt Agenten mit der Berechtigungsstufe Supervisor oder Administrator, welche Agenten welchen Warteschlangen zugeordnet sind. Agenten mit der Berechtigungsstufe Agent sehen nur die Warteschlangen, denen sie selbst zugeordnet sind.

18.1.2 Voraussetzungen für myAgent

Um myAgent nutzen zu können, muss der Client-PC des Teilnehmers eine geeignete Hardware- und Softwareausstattung haben.

Tipp: Beachten Sie bitte unbedingt die aktuellen Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Telefone

myAgent kann in Verbindung mit folgenden Telefonen genutzt werden:

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- OpenStage T
- OpenScape Personal Edition HFA
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)

Ältere Geräte (z. B. optiPoint 410/420/500 und Gigaset M2/SL3/S4/SL4/S5) werden unterstützt. Optiset E-Geräte können nicht betrieben werden. myAgent kann nicht verwendet werden mit SIP-Teilnehmern, Mobility Teilnehmern, virtuellen Teilnehmern, Gruppen oder MULAP-Teilnehmern. Getestete und freigegebene Telefone entnehmen Sie bitte der Freigabemitteilung.

Betriebssysteme

myAgent kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)

Tipp: Das verwendete Betriebssystem benötigt stets den aktuellen Stand aller verfügbaren Updates (Service Packs und Patches).

Der Support von myReports für Microsoft Windows XP und Microsoft Windows Server 2003 endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Zusätzliche Software

- Auf einem PC muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein (siehe **Service-Center** > **Software**)
- Adobe Reader 9 oder höher (für Berichte im PDF-Format)

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbit/s LAN
- XGA (1024x768) Bildschirmauflösung, myPortal for Outlook: SVGA (800x600) Bildschirmauflösung

Microsoft Terminalserver, Citrix XenApp Server

myAgent kann unter den nachfolgend genannten Voraussetzungen in Microsoft Terminalserver- und Citrix-Server-Umgebungen eingesetzt werden:

Tipp: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

Tipp: Citrix-Server-Umgebungen können einige regionale Buchstaben (z. B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssysteme:

- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) mit Citrix XenApp 6.5 Server (Desktop Mode)

Der Support von myAgent für Microsoft Windows XP und Microsoft Windows Server 2003 endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Hardware-Voraussetzungen: Die Anzahl der installierbaren Clients hängt von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher ab. Werden auf dem Server weitere Applikationen genutzt, ist deren Arbeitsspeicherbedarf zu berücksichtigen.

Weitere Informationen über die Konfiguration unter Citrix XenApp Server finden Sie unter:

`http://wiki.unify.com/wiki/OpenScape_Business`.

Installationsdateien

Für die Bereitstellung der Installationsdateien an die Benutzer bestehen folgende Möglichkeiten:

- Der Administrator lädt die Installationsdateien aus dem **Service-Center** herunter und stellt diese den Benutzern bereit, z. B. über ein Netzlaufwerk.

Beachten Sie die Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Tipp: Die automatische Verteilung der MSI-Datei über einen Deployment-Dienst mit Microsoft Windows Server wird nicht unterstützt.

18.1.3 myReports

Agenten mit dem Berechtigungs-Level Supervisor oder Administrator können mit myReports Berichte über Agenten und deren Aktivitäten, über Anrufe, Warteschlangen, Leistung, Servicelevel und Nachbearbeitungscodes erstellen.

myReports bietet folgende Leistungsmerkmale:

- Mehr als 100 vordefinierte und nach Themengebieten (Berichtgruppen) sortierte Berichtsvorlagen für die Erstellung von Berichten
- Zeitpläne für die zeitgesteuerte Erstellung von Berichten
- Sofortiger oder zeitgesteuerter Versand von Berichten per E-Mail
- Zeitgesteuerter Export von Berichten
- Ausgabeformate für die Berichtsvorschau, den E-Mail-Versand und den Export von Berichten: Excel, PDF und Word
- Berichtsvorschau für die Prüfung eines zu erstellenden Berichts im gewünschten Ausgabeformat

Benutzerrollen

myReports besitzt eine eigene Benutzerverwaltung, die den Zugriff auf die Funktionen von myReports durch Benutzerrollen regelt. Dabei wird zwischen dem myReports-Benutzer (Standardbenutzer) und dem myReports-Administrator unterschieden.

Die aktuelle Benutzerrolle wird bei der Anmeldung an myReports festgelegt.

Die Unterschiede zwischen den Benutzerrollen sind in der folgenden Tabelle zusammengefasst.

myReports:	**Benutzerrolle**	
Aktivität	myReports Benutzer	myReports Administrator
Berichte		

myReports: Aktivität	Benutzerrolle	
	myReports Benutzer	myReports Administrator
Berichtsvorschau anzeigen	X	X
Bericht sofort per E-Mail senden	X	X
Berichtsvorlage hinzufügen	X	X
Hinzugefügte Berichtsvorlage löschen	X	X
Neue Berichtsvorlage definieren		X
Vordefinierte Berichtsvorlagen aktualisieren		X
Zeitpläne		
Zeitplan hinzufügen	X	X
Details eines Zeitplans anzeigen	X	X
Zeitplan bearbeiten	X	X
Zeitplan löschen	X	X
Konfiguration		
Sprache der Benutzeroberfläche ändern	X	X
Farbe der Benutzeroberfläche ändern	X	X
E-Mail-Vorlage konfigurieren	X[7]	X
Serveradresse ändern	X	X
Administrator-Kennwort ändern		X
Vorwahlen für externe Rufnummern konfigurieren		X
Datenschutz aktivieren/deaktivieren		X
Speicherort für den Export zeitgesteuerter Berichte konfigurieren		X
Sprache einrichten		X[8]
Standard-Sprache einrichten		X[8]

7 Für die Konfiguration der E-Mail-Vorlage ist die Eingabe des Administrator-Kennworts erforderlich.

8 Für die Einrichtung der Sprache und der Standard-Sprache ist die Anmeldung als myReports-Administrator mit einem speziellen Kennwort erforderlich.

18.1.3.1 Wie Sie myReports-Administrator-Kennwort zurücksetzen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Wartung**.
5) Klicken Sie unter dem Bereich **Berichte** auf **Kennwort zurücksetzen**.

Nächste Schritte

Informieren Sie den oder die myReports-Administrator(en) über das Zurücksetzen des Administrator-Kennworts auf das Standardkennwort `reports`.

18.1.4 Voraussetzungen für myReports

Um myReports zu nutzen, muss der Client-PC des Teilnehmers über eine geeignete Hardware- und Softwareausstattung verfügen.

Tipp: Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Betriebssysteme

myReports kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)

Tipp: Das verwendete Betriebssystem benötigt stets den aktuellen Stand aller verfügbaren Updates (Service Packs und Patches).

Der Support von myReports für Microsoft Windows XP und Microsoft Windows Server 2003 endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Zusätzliche Software

- Auf einem PC muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein (siehe **Service-Center** > **Software**)
- Adobe Reader 9 oder höher (für Berichte im PDF-Format)
- Microsoft Excel 16 / 2013 / 2010 (für Berichte im Excel-Format)
- Microsoft Word 16 / 2013 / 2010 (für Berichte im Word-Format)

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbit/s LAN (1 Gbit/s LAN empfohlen)
- XGA (1024x768) Bildschirmauflösung, myPortal for Outlook: SVGA (800x600) Bildschirmauflösung

Multi-User PC

Unter Microsoft Windows 7 mit Multiuser-PC und Microsoft Windows Vista mit Multiuser-PC kann jeder lokale Benutzer myReports mit seinen individuellen Einstellungen verwenden, wenn der erste lokale Benutzer mit lokalen Administrationsrechten dieses installiert. Nur der erste lokale Benutzer mit lokalen Administrationsrechten kann Updates per AutoUpdate durchführen.

Microsoft Terminalserver, Citrix XenApp Server

myReports kann unter den nachfolgend genannten Voraussetzungen in Microsoft Terminalserver- und Citrix-Server-Umgebungen eingesetzt werden.

Tipp: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

Tipp: Citrix-Server-Umgebungen können einige regionale Buchstaben (z. B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssysteme:

- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) mit Citrix XenApp 6.5 Server (Desktop Mode)

Hardware-Voraussetzungen: Die Anzahl der installierbaren Clients hängt von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher ab. Werden auf dem Server weitere Applikationen genutzt, ist deren Arbeitsspeicherbedarf zu berücksichtigen.

Weitere Informationen über die Konfiguration unter Citrix XenApp Server finden Sie unter:

`http://wiki.unify.com/wiki/OpenScape_Business`.

Installationsdateien

Für die Bereitstellung der Installationsdateien an die Benutzer bestehen folgende Möglichkeiten:

- Der Administrator lädt die Installationsdateien aus dem **Service-Center** herunter und stellt diese den Benutzern bereit, z. B. über ein Netzlaufwerk.

Beachten Sie die Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Tipp: Die automatische Verteilung der MSI-Datei über einen Deployment-Dienst mit Microsoft Windows Server wird nicht unterstützt.

18.1.5 Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients

Bei gleichzeitiger Nutzung von myAgent und UC Suite Clients über ein UC Suite-Benutzerkonto ist eine gegenseitige Beeinflussung nicht ausgeschlossen.

Der Begriff myPortal wird in diesem Abschnitt stellvertretend für myPortal for Desktop, myPortal for Outlook, myPortal @work und myPortal to go verwendet.

Beispiele gegenseitiger Beeinflussung:

- Änderung des Anwesenheitsstatus über myPortal

  Die Beispiele gelten für die Standardeinstellung **Sprachnachrichten** für alle Anrufumleitungsziele.

  – myAgent: Agent ist angemeldet.

    myPortal: Das automatische Zurücksetzen des Anwesenheitsstatus auf Büro ist deaktiviert.

    Eine Änderung des Anwesenheitsstatus über myPortal bewirkt ein sofortiges Abmelden des Agenten von der oder den Warteschlange(n). Nach dem Anmelden des Agenten über myAgent wird der Anwesenheitsstatus in myPortal wieder auf **Büro** zurückgesetzt.

    Eine Änderung des Agentenstatus über myAgent (zum Beispiel **Pause**) wird durch myPortal registriert, mit Ausnahme von **Anmelden**, **Abmelden** und **Nachbearbeitung**.

  – myAgent: Agent ist angemeldet.

    myPortal: Das automatische Zurücksetzen des Anwesenheitsstatus auf Büro ist aktiviert.

    Ändert der Agent seinen Status über myAgent in **Pause**, ist er nach Ablauf der Pausenzeit automatisch wieder verfügbar.

    Eine Änderung des Anwesenheitsstatus über myPortal in **Pause** bewirkt ein sofortiges Abmelden des Agenten von der oder den Warteschlange(n).

  – myAgent: Agent ist angemeldet.

    Eine Änderung des Anwesenheitsstatus über myPortal in **Anrufschutz** bewirkt ein sofortiges Abmelden des Agenten von der oder den Warteschlange(n).

- Gehende Anrufe über myPortal

  Der Anwesenheitsstatus des Teilnehmers ist über myAgent sichtbar.

  Die Anrufe erscheinen ausschließlich im Journal von myPortal. Eine Übernahme in die Statistik des Contact Centers erfolgt nicht, da es sich nicht um Contact Center-Anrufe handelt.

- Kommende Anrufe an die Teilnehmerrufnummer des Agenten

  Der Anwesenheitsstatus des Teilnehmers ist über myAgent sichtbar.

  Die Anrufe erscheinen ausschließlich im Journal von myPortal. Eine Übernahme in die Statistik des Contact Centers erfolgt nicht, da es sich nicht um Contact Center-Anrufe handelt.
- Anruf aufzeichnen

  Das Aufzeichnen von Anrufen über myPortal wird nicht durch myAgent registriert. myAgent bietet diese Funktion an, auch wenn die Aufzeichnung eines Anrufs bereits über myPortal erfolgt.

18.2 Agenten

Die zu einer Warteschlange gehörenden Agenten (Teilnehmer) bilden eine Arbeitsgruppe, die zum Beispiel bei technischen Hotlines oder in der Auftrags- und Bestellannahme zum Einsatz kommen kann. Die kommenden Anrufe, Faxe und E-Mails werden gleichmäßig auf die verfügbaren Agenten einer Warteschlange verteilt.

Um einen Teilnehmer des Kommunikationssystems als Agent zu verwenden, muss dieser Teilnehmer als Agent konfiguriert werden. Die Rechte des Agenten werden dabei durch Auswahl des Berechtigungs-Levels definiert (Agent, Supervisor oder Administrator). Ein Agent mit dem Berechtigungs-Level Supervisor oder Administrator verfügt über erweiterte Berechtigungen (siehe Berechtigungsabhängige Funktionen für Agenten).

Ein Agent kann als dauerverfügbarer Agent definiert werden. Er bleibt dadurch auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

18.2.1 Berechtigungsabhängige Funktionen für Agenten

Bei der Konfiguration eines Teilnehmers als Agent werden die Rechte des Agenten durch Auswahl des Berechtigungs-Levels definiert (Agent, Supervisor oder Administrator). Ein Agent mit dem Berechtigungs-Level Supervisor oder ein Administrator verfügt über erweiterte Berechtigungen.

Die Unterschiede zwischen den Berechtigungsstufen sind in der folgenden Tabelle zusammengefasst.

myAgent:	**Berechtigungsstufe (Serviceklasse)**		
Aktivität	**Agent**	**Supervisor**	**Administrator**
Agent einer Warteschlange zuordnen	–	X	X
Agent zu anderer Warteschlange verschieben	–	X	X
Agent aus Warteschlange entfernen	–	X	X
Status eines Agenten ändern	–	X	X
Liste der Agentenzuweisungen einblenden/ausblenden	Zugeordnete Warteschlangen	Alle Warteschlangen	Alle Warteschlangen
Agentenzuweisung bearbeiten	–	X	X

myAgent: Aktivität	Berechtigungsstufe (Serviceklasse)		
	Agent	**Supervisor**	**Administrator**
Liste der Live-Anrufe anzeigen	Zugeordnete Warteschlangen	Alle Warteschlangen	Alle Warteschlangen
myAgent bei Alarm automatisch im Vordergrund aktivieren	–	X	X
Alarmton aktivieren	–	X	X
Wandanzeige (Wallboard) anzeigen	Zugeordnete Warteschlangen	Alle Warteschlangen	Alle Warteschlangen
Diagramm Servicegrad anzeigen	Zugeordnete Warteschlangen	Alle Warteschlangen	Alle Warteschlangen
Diagramm Durchschnittszeiten anzeigen	Zugeordnete Warteschlangen	Alle Warteschlangen	Alle Warteschlangen
Anruf an die erste Position in einer Warteschlange verschieben	–	X	X
Anruf aufzeichnen	Aktueller Anruf	Alle Anrufe	Alle Anrufe
Aufzeichnung eines Anruf als WAV-Datei speichern oder als WAV-Datei per E-Mail versenden	–	X	X
Fax als TIFF-Datei speichern oder per E-Mail versenden	–	X	X
E-Mail als EML-Datei speichern oder als EML-Datei per E-Mail versenden	–	X	X
Call Supervision (länderabhängig)	–	X	X
Anruf aufschalten	–	X	X
Unterstützungsanfrage annehmen	–	X	X
Berichte erstellen	–	X	X
WBM öffnen	–	X	X

18.2.2 Bevorzugte Agenten

Jedem Anrufer (beispielsweise jedem anrufenden Kunden) können ein oder mehrere bevorzugte Agenten einer Warteschlange zugeordnet werden.
In diesem Fall versucht das Kommunikationssystem, den Anrufer und die Rückrufwünsche dieses Anrufers zunächst an einen bevorzugten Agenten zu vermitteln. Wurden mehrere bevorzugte Agenten festgelegt, kann eine Priorität (Reihenfolge) definiert werden, mit der die bevorzugten Agenten vermittelt werden.

Ist kein bevorzugter Agent verfügbar, wird der Anruf an einen beliebigen verfügbaren Agenten weitergeleitet.

18.2.3 Agent in mehreren Warteschlangen

Ein Agent kann mehreren Warteschlangen mit unterschiedlichem Fähigkeits-Level zugeordnet werden. Dabei ist zu definieren, ob der Agent als Hauptagent oder als Agent bei Überlauf fungieren soll.

18.2.4 Contact Center Pausen

Um jedem Agenten definierte Pausen zu ermöglichen, können unterschiedlich lange Contact Center-Pausen festgelegt werden (zum Beispiel Mittagspause, Zigarettenpause). Contact Center-Pausen stehen systemweit zur Verfügung und können bei Bedarf von einem Agenten über myAgent ausgewählt werden.

18.2.5 An- und Abmeldung des Agenten per Telefon

Anmeldung/Abmeldung beim Contact Center wird auch über Telefon unterstützt; dabei besteht keine Notwendigkeit zur Ausführung von myAgent, um die Contact Center-Funktionen nutzen zu können. Wenn ein Agent über Telefon angemeldet wurde, können nur Sprachanrufe verarbeitet werden. Popup-Fenster und die Eingabe von Nachbearbeitungscodes werden in diesem Fall nicht unterstützt. Dies gilt auch, wenn der Agent sich bei aktivem myAgent über Telefon beim Contact Center anmeldet. Um die volle Funktionalität von myAgent wiederherzustellen, muss der Agent sich über Telefon abmelden und anschließend über myAgent wieder anmelden.

Voraussetzungen und Einschränkungen

- OpenScape Business Contact Center Leistungsmerkmale funktionieren über Telefon nur für Agenten, denen in OpenScape Business eine myAgent-Lizenz zugeordnet ist
- Alle Funktionen werden nur auf Telefonen unterstützt, die für die Verwendung mit OpenScape Business Contact Center freigegeben sind
- Wenn die Anmeldung über Telefon erfolgreich war und der zugehörige myAgent-Client nicht aktiv ist, werden nur Sprachanrufe an den Agenten weitergeleitet
- Wenn die Anmeldung über Telefon erfolgreich war und der zugehörige myAgent-Client aktiv ist, werden E-Mails/Faxe und Rückrufe nicht an den Agenten weitergeleitet, wenn dieser über Telefon angemeldet ist. In diesem Fall funktionieren Popup-Fenster und Nachbearbeitung wie gewohnt, aber nur Sprachanrufe werden an den Agenten weitergeleitet. Um die volle Funktionalität wiederherzustellen, muss sich der Agent zunächst über Telefon abmelden und dann erneut über myAgent anmelden

Anmeldung über Telefon beim Contact Center

Wenn die Agenten sich beim OpenScape Business Contact Center über Telefon anmelden (unabhängig davon, ob der myAgent-Client und das Contact Center aktiv ist):

- Am Telefon werden die UCD-Funktionen für die Anmeldung verwendet

- Die Anmeldung kann entweder per Leistungsmerkmal-Code oder über eine programmierte Taste erfolgen
- Der Agent wird bei allen Warteschlangen angemeldet, denen er innerhalb der Contact Center-Konfiguration zugeordnet ist
- Am Telefondisplay wird der Anmeldestatus des Agenten angezeigt
- Bei Bedarf können nur die UCD-Warteschlangeninformationen (z. B. Informationen zu Anrufen in der Warteschlange) angezeigt werden

Der Agent kann folgende Funktionen verwenden:

- Anmeldung/Abmeldung (mit UCD Agenten-ID)
- Nachbearbeitung
- Verfügbar/Nicht verfügbar
- Anzeige der in der UCD-Warteschlange eingereihten Anrufe mit zugeordneter UCD-Agenten-ID

Anmerkung: Die UCD-Nachtschaltung darf nicht vom Agenten verwendet werden.

Anmerkung: Das Flag für „myAgent permanent verfügbar“ wird für die Anmeldung über das Telefon unterstützt.
Das bedeutet, dass, wenn ein Agent mit seinem Telefon angemeldet ist und ein Anruf verpasst wurde, dieser Agent für den nächsten Anruf verfügbar bleibt. Dies ist das gleiche Verhalten wie bei der Verwendung des myAgent Client.

Fällt das Contact Center aus, während der Agent angemeldet ist, bleibt der Agent bei UCD angemeldet und Sprachanrufe werden entsprechend der UCD-Routing-Konfiguration weitergeleitet. Wenn der Agent nicht angemeldet war, kann er sich über Telefon bei UCD anmelden.

Abmeldung über Telefon beim Contact Center

Wenn die Agenten sich beim OpenScape Business Contact Center über Telefon abmelden (unabhängig davon, ob der myAgent-Client und das Contact Center aktiv ist):

- Am Telefon werden die UCD-Funktionen für die Abmeldung verwendet
- Die Abmeldung kann entweder per Leistungsmerkmal-Code oder über eine programmierte Taste erfolgen
- Der Agent wird bei allen Warteschlangen abgemeldet, denen er innerhalb der Contact Center-Konfiguration zugeordnet ist
- Am Telefondisplay wird der Abmeldestatus des Agenten angezeigt
- Zusätzliche Contact Center / UC-Informationen (z.B. Informationen zu Anrufen in der Warteschlange) werden nicht angezeigt

Agent per Telefon als verfügbar/nicht verfügbar einstellen

Wenn ein Agent seinen Status für OpenScape Business Contact Center Kontaktrouting über Telefon auf Verfügbar / Nicht Verfügbar setzt (unabhängig davon, ob der myAgent-Client und das Contact Center aktiv ist):

- Am Telefondisplay wird der Anmeldestatus des Agenten angezeigt
- Wenn myAgent nicht aktiv ist, werden nur Sprachanrufe an den Agenten weitergeleitet

Bearbeitung nach Anruf (Nachbearbeitung) über Telefon setzen/ rücksetzen

Wenn ein Agent seinen Status über Telefon auf "Bearbeiten nach Anruf" (Nachbearbeitung) setzt (unabhängig davon, ob der myAgent-Client und das Contact Center aktiv ist), werden keine Anrufe zum Agenten weitergeleitet, bis die im OpenScape Contact Center konfigurierte Nachbearbeitungszeit des Agenten abgelaufen ist oder der Agent die Nachbearbeitung über Telefon zurückgesetzt hat.

Statuszuordnung

Über Telefon geänderte Agentenstatus werden myAgent-Agentenstatus wie folgt zugeordnet:

Telefongerät			myAgent			
Leistungsm Code	**Leistungsm Code**	**Beschreibung**	Telefondispl	**Status**	**Zusatztext**	Bemerkung
*401	UCD Agenten-ID	UCD-Agenten einloggen	Verfügbar	Verfügbar	-	Der Status des Agenten wird in allen zugeordneten Warteschlangen auf "Verfügbar" gesetzt
#401	–	UCD-Agenten ausloggen	Nicht verfügbar	Nicht verfügbar	-	Der Status des Agenten wird in allen zugeordneten Warteschlangen auf "Nicht verfügbar" gesetzt
*402	–	UCD-Agent verfügbar	Verfügbar	-	-	Verfügbar (Ende der Nachbearbeitung)
#402	–	UCD-Agent nicht verfügbar	Nicht verfügbar	Nachbearbeitung	Countdown von 999.999 Sekunden	-

Telefongerät			myAgent			
Leistungsm Code	**Leistungsm Code**	**Beschreibung**	Telefondispl	**Status**	**Zusatztext**	Bemerkung
*403	–	UCD-Nachbearbeitung ein	Nachbearbeitung	Nachbearbeitung	Countdown der konfigurierten Nachbearbeitungszeit	Die Nachbearbeitung muss abgeschlossen sein, bevor sie erneut gestartet werden kann. Eine Kumulierung der Nachbearbeitungszeit wie bei myAgent gibt es nicht. Nach Ablauf der Nachbearbeitungszeit wird der Agentenstatus automatisch auf Verfügbar gesetzt.
#403	–	UCD-Nachbearbeitung aus	Verfügbar	Verfügbar	-	-
*404	Nachtschaltung Ziel	UCD-Nachtschaltung ein	–	Nicht unterstützt	-	UCD-Nachtschaltung darf nicht verwendet werden
#404	–	UCD-Nachtschaltung aus	–	Nicht unterstützt	-	UCD-Nachtschaltung darf nicht verwendet werden
*405	–	UCD-Rufqueue-Status abfragen	-	-	-	Nur die Warteschlange mit zugeordneter UCD-Agenten-ID wird angezeigt, unabhängig davon, ob der Agent mehreren Warteschlangen im Contact Center zugeordnet ist

18.3 Warteschlangen und Zeitpläne

Warteschlangen sind die Basis des Contact Centers. Anrufe, Faxe und E-Mails für eine Warteschlange können in Abhängigkeit vom Fähigkeits-Level der Agenten, von der Priorität und der Wartezeit behandelt werden. Anrufern, die sich im Wartezustand befinden, können Ansagen eingespielt werden. Über einen Zeitplan wird definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.

18.3.1 Warteschlangen

Im Regelfall erfolgt die Anrufverteilung so, dass ein kommender Anruf, ein Fax oder eine E-Mail an eine Warteschlange an denjenigen Teilnehmer in der Gruppe (Agent) weitergeleitet wird, dessen letztes Gespräch am längsten zurückliegt. Es ist ebenfalls möglich andere Verteilungsregeln festzulegen (zum Beispiel anhand der verschiedenen Fähigkeits-Level der Agenten). Sind alle Agenten belegt, werden zusätzliche Anrufe, Faxe und E-Mails in Wartestellung gebracht und anschließend in Abhängigkeit von Priorität und Wartezeit an die frei werdenden Agenten verteilt.

Anhand von Zeitplänen und den darin enthaltenen Regeln (= CCV, Call Control Vector) kann definiert werden, wie ein Anruf an eine Warteschlange zu einer bestimmten Zeit oder an einem bestimmten Tag behandelt werden soll. Die Regeln definieren beispielsweise, welche Ansage Anrufern eingespielt wird oder wohin ein Anruf weitergeleitet wird.

Faxe, E-Mails und Agentenrückrufe werden unabhängig von Zeitplänen den Warteschlangen direkt zugeordnet.

Bei der Zuordnung von Agenten zu Warteschlangen können den Agenten verschiedene Eigenschaften zugewiesen werden (Agentenzuweisung), die Einfluss auf die Verteilung der Anrufe in einer Warteschlange haben (zum Beispiel Hauptagent oder Agent bei Überlauf, Fähigkeits-Level). Die Zuordnung von Agenten zu Warteschlangen ist möglich

- über das WBM durch einen Administrator mit dem Profil **Advanced**.
- über die Applikation myAgent durch einen Agenten mit dem Berechtigungs-Level Supervisor oder Administrator.

Ist ein Agent mehreren Warteschlangen zugeordnet, kann über die Warteschlangen-Priorität festgelegt werden, ob die Anrufe für eine Warteschlange mit höherer Priorität an diesen Agenten weitergeleitet werden sollen als die Anrufe für andere Warteschlangen.

Für Warteschlangen können folgende wesentlichen Einstellungen über das WBM vorgenommen werden:

- Warteschlangen aktivieren, deaktivieren, löschen

  Hinweis: Nach dem Löschen einer Warteschlangen können keine Berichte über vergangene Zeiträume erstellt werden. Nicht mehr benötigte Warteschlangen sollten deaktiviert werden.
- Warteschlangen-Alarme konfigurieren

  Sie haben die folgenden Möglichkeiten:

  – Anzahl Warteschlangen-Alarme (Alarm-Schwellwertanzahl): Wird die hier angegebene Anzahl wartender Anrufe in der Warteschlange überschritten, wechselt das Warteschlangensymbol bei den Agenten von

grün auf orange. Agenten mit dem Berechtigungs-Level Supervisor oder Administrator können einstellen, ob sie durch einen Alarmton gewarnt werden sollen und ob myAgent automatisch im Vordergrund erscheinen soll.

– Zeit Warteschlangen-Alarm (Alarm-Schwellwertzeit): Wird die hier angegebene Wartezeit eines Anrufs in der Warteschlange überschritten, wechselt der betreffende Eintrag in der Liste der Contact-Center-Anrufe bei den Agenten auf rot. Agenten mit dem Berechtigungs-Level Supervisor oder Administrator können einstellen, ob sie durch einen Alarmton gewarnt werden sollen und ob myAgent automatisch im Vordergrund erscheinen soll.

- Zeitüberschreitung für entgangene Anrufe, Faxe und E-Mails definieren

  Wird ein Anruf, ein Fax oder eine E-Mail nach Ablauf der hier angegebenen Zeit vom Agenten nicht angenommen, wird der Anruf, das Fax oder die E-Mail zum nächsten freien Agenten weitergeleitet.
- Schwellwert für abgebrochene Anrufe definieren

  Die hier angegebene Zeit legt fest, ob ein abgebrochener Anruf in die Statistik (in einen Bericht) aufgenommen wird oder nicht. Statistisch erfasst werden Anrufe, die nach Ablauf der angegebenen Zeit abgebrochen werden.
- Warteschlangen-Tiefe konfigurieren

  Kontrolle über die maximale Anzahl von aktiven und wartenden Anrufen in einer bestimmten Warteschlange. Das Contact Center weist das System darauf hin, wenn der definierte Schwellwert für die Warteschlangengröße erreicht ist. In der Folge weist das System jeden neuen bei der entsprechenden Warteschlange eingehenden Anruf zurück, bevor dieser mit dem System verbunden wird; dies geschieht solange, bis die Anzahl der Anrufe unter den Schwellwert fällt.

  Die maximale Warteschlangengröße hängt von folgenden Parametern ab:

  – Maximale Anzahl an Warteposition in der Warteschlange. (WLS = Waiting Loop Size, Warteschlangengröße)
  – Maximale Anzahl aktiver und wartender Anrufe in der Warteschlange. (Warteschlangentiefe-Größe).
- Pilots für eingehende Faxnachrichten einrichten

  Falls eingerichtet, können Rufnummern für eingehende Faxnachrichten ausgewählt werden. Faxe an diese Rufnummern werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
- Dienst für eingehende E-Mails einrichten

  Für eine Warteschlange können mehrere E-Mail-Adressen eingerichtet werden. E-Mails an diese Adressen werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
- Absender-E-Mail-Adresse einrichten

  E-Mail-Adresse der Warteschlange, die beim Versenden einer E-Mail durch einen Agenten beim Empfänger angezeigt wird.
- Intelligente Anrufweiterleitung aktivieren

  Ein kommender Anruf wird an den Agenten weitergeleitet, der zuletzt mit dem Anrufer verbunden war. Vorausgesetzt, für diesen Anrufer wurden keine bevorzugten Agenten definiert.

18.3.2 Zeitpläne

Für jede Warteschlange wird über einen Zeitplan und die darin enthaltenen Regeln (Call Control Vector CCV) definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.

Beispielsweise kann für Werktage eine Regel für die Frühschicht (von 6:00 Uhr bis 14:00 Uhr), eine für die Mittagschicht (14:00 Uhr bis 22:00 Uhr) und eine für die Nachtschicht (von 22:00 bis 06:00 Uhr) definiert werden. Für das Wochenende kann eine Wochenendregel definiert werden. Für jede dieser Regeln kann zum Beispiel angegeben werden, ob eine Ansage abgespielt und/ oder wohin Anrufe weitergeleitet werden sollen.

Zeitpläne sind das Kernstück der Contact-Center-Einrichtung. Ohne die Definition mindestens eines Zeitplans kann die Einrichtung eines Contact Centers nicht erfolgreich beendet werden. Jeder Warteschlange muss mindestens ein Zeitplan zugewiesen worden sein. Das kann auch immer derselbe Zeitplan sein.

Einem Zeitplan muss mindestens eine Regel (Call Control Vector CCV) zugeordnet werden. Die Regeln bestimmen für den Zeitraum für den ein Zeitplan gilt, wie kommende Anrufe in einer Warteschlange behandelt werden. Regeln gelten ausschließlich für Anrufe und nicht für Faxe und E-Mails.

Regeln werden mit dem graphischen Regel-Editor (CCV-Editor) durch die Verknüpfung von vordefinierten CCV-Objekten erstellt und können nach der Fertigstellung unter einem frei definierbaren Namen gespeichert werden.

Gespeicherte Regeln können einem oder auch mehreren Zeitplänen als Standard-Regel (Standard-CCV) oder Ausnahme-Regel (Ausnahme-CCV) zugeordnet werden. Das Öffnen, Modifizieren und erneute Speichern über den Regel-Editor ist jederzeit möglich.

Wurde einem Zeitplan eine Standard-Regel (Standard-CCV) zugeordnet, kann dieser Zeitplan unter einem frei definierbaren Namen gespeichert werden. Ein Zeitplan mit einer Standard-Regel gilt nach Zuweisung zu einer Warteschlange 24 Stunden am Tag und 365 Tage im Jahr. Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden. Damit kann definiert werden, wie kommende Anrufe beispielsweise während der Urlaubszeit behandelt werden sollen. Urlaubspläne haben Vorrang vor anderen Zeitplänen und Regeln einer Warteschlange.

Regel-Editor (CCV-Editor)

Mit dem Regel-Editor können aus vordefinierten CCV-Objekten Regeln gebildet werden. Die Anordnung der CCV-Objekte und deren Eigenschaften bestimmen, wie kommende Anrufe behandelt werden.

Anmerkung: Eine Regel hat eine Obergrenze von 500 CCV-Objekten.

Folgende vordefinierte CCV-Objekte stehen zur Verfügung:

Tipp: Für alle genannten CCV-Objekte gelten zusätzlich die beiden folgenden allgemeinen Eigenschaften:

Beschreibung: Optionale Möglichkeit, das CCV-Objekt zu beschreiben, wie zum Beispiel Begrüßungsansage.

Aktion nach Zifferneingabe: Angabe der benötigten Ziffer(n) ohne Leerzeichen, Kommas oder andere Zeichen. Die Angabe bezieht sich auf das vorherige CCV-Objekt. Wurde dort unter Mögliche Ziffern 9 angegeben, muss auch hier 9 stehen.

- **Nachricht abspielen**

  Bewirkt das Abspielen der gewünschten Ansage. Ausgewählt werden kann eine in der UC Suite vorliegende Audiodatei. Darüber hinaus kann eine neue Audiodatei in die UC Suite importiert werden oder eine neue Ansage aufgezeichnet und anschließend als Audiodatei in die UC Suite importiert werden.

  Durch das Abspielen der Ansage wird jeweils ein Media Stream Channel belegt.

  Eigenschaften:

  – **Dateiname**: Auswahl einer Ansage (Audiodatei im wav-Format)
  – **Abbruchtasten**: Angabe einer Taste oder Tastenkombination auf der Wähltastatur, mit der ein Anrufer das Abspielen der Ansage abbrechen kann.
  – **Datei-Manager**: Über diese Schaltfläche ist es möglich, eine Audio-Datei im wav-Format direkt hochzuladen bzw. mit dem Aufzeichnungsgerät eine neue Sprachdatei zu erzeugen.

- **Wartemusik**

  Bewirkt das Einspielen von Wartemusik (Music On Hold MOH des Kommunikationssystems) für externe Anrufer für eine einstellbare Zeit

  Eigenschaft:

  – **Zeitwert**: Zeit in Sekunden, über die die Wartemusik eingespielt werden soll.

- **Verbindung mit Anrufer trennen**

  Bewirkt das Beenden der Verbindung.

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

- **Anrufer über Warteschlangenposition informieren**

  Bewirkt die Information des Anrufers über seine aktuelle Warteschlangenposition

- **Geschätzte Wartezeit**

  Bewirkt die Information des Anrufers über seine geschätzte Wartezeit.

  Die Berechnung der geschätzten Wartezeit erfolgt auf der Grundlage von:

  1) Durchschnittliche Wartezeit in allen Warteschlangen in der Vergangenheit
  2) Durchschnittliche Wartezeit in einer bestimmten Warteschlange in der Vergangenheit
  3) Durchschnittliche Gesprächszeit für den bestimmten Agent in der Vergangenheit

- **Zu CCV**

  Bewirkt eine Schleife zu einem anderen CCV-Objekt

  Eigenschaft:

  – **Ziel-CCV**: Auswahl des CCV-Objekts
- **Callback aufzeichnen**

  Ermöglicht einem Anrufer in einer Warteschlange einen Agentenrückruf zu aktivieren (Aufnahme einer Sprachnachricht). Der Agentenrückruf bleibt anstelle des eigentlichen Anrufers in der Warteschlange. Agenten mit dem Merkmal **Agentenrückruf aktivieren** wird der Agentenrückruf in der Liste der Contact-Center-Anrufe angezeigt.

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

  Eigenschaften:

  – **Typ**: Auswahl von **Einfacher Rückruf** oder **Extensiver Rückruf**.

    Im Gegensatz zu einem einfachen Rückruf stehen einem Anrufer bei einem extensiven Rückruf zusätzliche Möglichkeiten und Informationen zur Verfügung (Bestätigung oder Änderung der Rufnummer an die der Rückruf erfolgen soll, Bestätigung der Sprachnachricht).
  – **Max. Nachrichtenlänge**: Zeit in Sekunden, die einem Anrufer für die Aufnahme einer Sprachnachricht zur Verfügung steht.
- **Aktion nach Zifferneingabe**

  Bewirkt die Ausführung des oder der nachfolgenden CCV-Objekte in Abhängigkeit von den dort angegebenen Ziffern (Aktion nach Zifferneingabe).

  Eigenschaften:

  – **Dateiname**: Auswahl einer oder mehrerer Ansagen (Audiodatei im wav-Format)
  – **Wiedergabeliste**: Liste der ausgewählten Ansagen (Audiodatei im wav-Format) in der Reihenfolge der Wiedergabe
  – **Zeitüberschreitung bei Zifferneingabe**: Zeit in Sekunden, innerhalb der das Kommunikationssystem auf die Zifferneingabe wartet.

    Erfolgt die vollständige Zifferneingabe nicht innerhalb der angegebenen Zeit, wird die Nachricht (Ansage) erneut abgespielt.
  – **Link an**: Auflistung der Ziffern mit Ziel.

    Die Ziffern und Ziele können hinzugefügt, bearbeitet und entfernt werden.
  – **Datei-Manager**: Über diese Schaltfläche ist es möglich, eine Audio-Datei im wav-Format direkt hochzuladen bzw. mit dem Aufzeichnungsgerät eine neue Sprachdatei zu erzeugen.

  Der Inhalt der Wiedergabeliste wird im Regel-Editor anhand eines Tooltips angezeigt, wenn man mit dem Mauszeiger auf dem CCV-Objekt verweilt.

- **Einzelschritt-Übergabe**

  Die Funktion ist abhängig von der Einstellung **Normales Vermittlungsplatz-SST** (WBM, **Experten-Modus**: **Applikationen** > **OpenScape Business UC Suite** > **Server** > **Allgemeine Einstellungen**):

  – **Normales Vermittlungsplatz-SST** aktiviert (Standardeinstellung, nicht für USA): Bewirkt die Übergabe des Anrufs, unabhängig davon, ob das Ziel frei, besetzt oder nicht verfügbar ist.

  > **Tipp:** Bei einem Teilnehmer mit Anklopfschutz wird der Anruf erst vermittelt, wenn der Zielteilnehmer frei ist. Ein Anklopfen im Besetztfall erfolgt nicht.

  – **Normales Vermittlungsplatz-SST** deaktiviert (Standardeinstellung, nur für USA): Bewirkt die Übergabe des Anrufs wenn das Zeil frei ist.

    Ist das Ziel besetzt und der Anklopfschutz deaktiviert oder ist das Ziel nicht verfügbar, wird dem Anrufer eine Ansage eingespielt. Dabei kann der Anrufer wählen, ob er eine Nachricht auf der Sprachbox des Teilnehmers hinterlassen möchte oder ob er die Rufnummer eines anderen Ziels wählen möchte.

    Ist das Ziel besetzt und der Anklopfschutz aktiviert, erfolgt keine Vermittlung des Anrufs.

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

  Eigenschaft:

  – **Zielnebenstelle**: Angabe der internen Rufnummer oder der externen Durchwahl mit Amtsleitungsnummer. Leerzeichen, Kommas oder andere Zeichen sind nicht erlaubt.

  Die Rufnummer der Zielnebenstelle wird im CCV-Objekt angezeigt.

  > **Anmerkung:** Nach einer Einzelschritt-Übergabe trennt das System die Verbindung nach Klingeln für 5 Minuten.

- **An Warteschlange übergeben**

  Bewirkt die Übergabe des Anrufs an eine Warteschlange

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

  Eigenschaft:

  – **Warteschlange**: Auswahl der Warteschlange

- **In Mailbox aufzeichnen**

  Bewirkt den Anruf an die gewünschte Sprachbox eines Teilnehmers oder einer Sprachbox-Gruppe

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

  Eigenschaft:

  – **Benutzer-Mailbox**: Angabe der Rufnummer der Sprachbox eines Teilnehmers oder einer Sprachbox-Gruppe

  Die Rufnummer und der Name der Sprachbox oder der Sprachbox-Gruppe werden im Regel-Editor anhand eines Tooltips angezeigt, wenn man mit dem Mauszeiger auf dem CCV-Objekt verweilt.
- **Überwachter Weiterleitung (auch als Abgeschirmte Weiterleitung genannt)**

  Bewirkt die Übergabe des Anrufs an ein internes Ziel. Während der Übergabe wird dem Anrufer Wartemusik (Music On Hold MOH der UC Suite) eingespielt.

  Im Gegensatz zum CCV-Objekt Einzelschritt-Übergabe müssen hier zwei weitere CCV-Objekte eingefügt werden. Es muss nämlich definiert werden, wie sich das Kommunikationssystem verhalten soll, wenn das Anrufziel besetzt ist oder der Anruf nicht angenommen wird. Üblicherweise wird dem Anrufer in diesen Fällen eine Ansage eingespielt.

  Eigenschaften:

  – **Zielnebenstelle**: Angabe der internen Rufnummer.

    Es werden nur interne Rufnummern im eigenen Knoten unterstützt. Die Weiterleitung an externe Ziele, virtuelle Stationen, zusätzliche AutoAttendants, Mobility-Benutzer sowie externe CallMe-Ziele ist nicht erlaubt!

    Für diese Szenarien sollte der SST (einstufige Weiterleitung) verwendet werden. Um einen Anruf an ein anderes UCD, das Teil von Contact Center ist, weiterzuleiten, sollte das CCV-Objekt **Weiterleitung an die Warteschlange** verwendet werden.

  – **Zeitüberschreitung beim Klingeln**: Zeit in Sekunden, innerhalb der der Anruf angenommen werden muss.

    Wird der Anruf nicht innerhalb der angegebenen Zeit angenommen, wird dieser zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

    Tipp: Die hier angegebene Zeit muss kürzer sein als die für die Rufweiterschaltung konfigurierte Zeit (Standardeinstellung für die Rufweiterschaltung = 15 Sekunden). Siehe Rufweiterschaltung konfigurieren.

  – **Anruf zurücknehmen, wenn Zielgerät weitergeleitet/umgeleitet ist**: Option (gilt nur für interne Rufnummer).

    Bei aktivierter Option erfolgt eine Prüfung des Anrufziels. Wurde für das Anrufziel eine Anrufweiterschaltung oder Anrufumleitung aktiviert, wird

der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

– **Anwesenheitsstatus bei Anrufübergabe prüfen**: Option

Bei aktivierter Option erfolgt eine Prüfung des Anwesenheitsstatus des Anrufziels. Bei einem anderen Anwesenheitsstatus als Büro wird der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

- **Nach Name wählen**

Bewirkt die Aufforderung des Anrufers, die ersten drei Buchstaben des gewünschten Teilnehmer-Nachnamens über die Wähltastatur einzugeben.

Gibt es einen Teilnehmer mit den eingegebenen Anfangsbuchstaben, wird eine Verbindung hergestellt.

Gibt es mehrere Teilnehmer mit den eingegebenen Anfangsbuchstaben, werden dem Anrufer die Namen dieser Teilnehmer angesagt (maximal 10 Teilnehmer). Hat ein Teilnehmer keine Namensansage aufgezeichnet, wird stattdessen die Rufnummer angesagt. Nach der Auswahl des gewünschten Teilnehmers wird eine Verbindung hergestellt.

Entspricht kein Teilnehmer den eingegebenen Anfangsbuchstaben, erhält der Anrufer eine entsprechende Meldung.

Tipp: Die Tasten der Wähltastatur reagieren auf den ersten Tastendruck. Mit jedem Tastendruck wird geprüft, ob es Teilnehmer-Nachnamen mit den der Taste zugeordneten Buchstaben gibt.

Beispiel: Im internen Verzeichnis gibt es die folgenden fünf Nachnamen mit den Anfangsbuchstaben t, u und v: Taylor, Taler, Ullrich, Vasquez und Volterra. Um ein Verbindung mit dem Teilnehmer Taylor herzustellen, sind folgende Tasten zu betätigen: 8 2 9

Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

Eigenschaften:

– **Methode**: Auswahl von **An Nebenstelle übergeben** oder **In Mailbox aufzeichnen**.

Je nach ausgewählter Methode wird eine Verbindung zum gewünschten Teilnehmer oder zu dessen Sprachbox hergestellt. Dabei werden ausschließlich interne Teilnehmer unterstützt, die mit Vor- und Nachnamen im internen Verzeichnis eingetragen sind.

- **Nebenstellenwahl**

Bewirkt die Aufforderung des Anrufers, die Rufnummer des gewünschten Teilnehmers über die Wähltastatur einzugeben.

Wählt der Anrufer die Rufnummer eines virtuellen Teilnehmers, wird er aufgefordert eine andere Teilnehmer-Rufnummer einzugeben. Anschließend

wird eine Verbindung hergestellt. Meldet sich der gewünschte Teilnehmer nicht, nimmt dessen Sprachbox den Anruf entgegen.

Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

Eigenschaften:

– **Methode**: Auswahl von **An Nebenstelle übergeben** oder **In Mailbox aufzeichnen**.

  Je nach ausgewählter Methode wird eine Verbindung zum gewünschten Teilnehmer oder zu dessen Sprachbox hergestellt. Dabei werden ausschließlich interne Teilnehmer unterstützt, deren Rufnummer im internen Verzeichnis eingetragen ist.

- **Sprache einstellen**

  Bewirkt die Auswahl der Sprache für die jeweilige Standardansage anhand der Rufnummer des Anrufers. Zu beachten ist, dass ausschließlich Standardansagen (Systemansagen) und keine persönlichen Ansagen berücksichtigt werden.

  Definiert werden kann zum Beispiel, dass für eine Rufnummer mit der Ländervorwahl +49 eine deutsche Ansage und für eine Rufnummer mit der Ländervorwahl +33 eine französische Ansage abgespielt wird.

  Eigenschaften:

  – **Standardsprache**: Aufklappliste zur Auswahl einer Sprache.

    Die hier ausgewählte Sprache wird für alle Rufnummern verwendet, für die selbst keine Sprache definiert wurde.
  – **Muster**: Angabe der Rufnummer, der eine bestimmte Sprache zugeordnet werden soll.

    Folgende Platzhalter können verwendet werden: * = beliebige Zahl, ? = beliebige Ziffer.
  – **Sprache**: Aufklappliste zur Auswahl der Sprache, die den zugehörigen (dem **Muster** entsprechenden) Rufnummern zugeordnet werden soll.

  Eine Sprache kann beliebig vielen verschiedenen (dem **Muster** entsprechenden) Rufnummern zugeordnet werden.

- **CLI-Routing**

  Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand der Rufnummer des Anrufers.

  Definiert werden kann zum Beispiel, dass für eine Rufnummer mit der Ländervorwahl +49 zuerst eine deutsche Ansage abgespielt werden soll (CCV-Objekt **Nachricht abspielen**) und der Anruf anschließend an eine internes Telefon weitergeleitet werden soll (CCV-Objekt **Einzelschritt-Übergabe**). Es kann auch die Ortsvorwahl verwenden werden (z B. 089 für München).

  Im Kontext von UC Suite und CLI-Routing müssen Benutzer bestimmte Szenarien berücksichtigen, wie z. B. eingehende Anrufe von MS Teams Nativer SIP-Trunk. Wenn Sie beabsichtigen, die Rufnummern von OpenScape Business-Anrufern im kanonischen Format einschließlich der Landesvorwahl zu senden, müssen Sie zusätzliche CLI-Routing-Regeln festlegen.

  Wenn beispielsweise Anrufer von MS Teams Nummern im Format +49777555XXXX haben und 777555 der gemeinsame Teil dieser Nummern

ist, sollten Benutzer entsprechende CLI-Routing-Regeln erstellen, die diesen gemeinsamen Teil (777555) enthalten.

Eigenschaften:

– **Standard**: Aufklappliste zur Auswahl des CCV-Objekts.

  Das hier ausgewählte CCV-Objekt wird für alle Rufnummern verwendet, für die selbst kein Ziel definiert wurde.
– **Muster**: Angabe der Rufnummern, denen ein bestimmtes CCV-Objekt als Ziel zugeordnet werden soll.

  Folgende Platzhalter können verwendet werden: * = beliebige Zahl, ? = beliebige Ziffer.
– **Beschreibung**

  Angabe einer Erläuterung.

  Für das **Muster** +49 (=Ländervorwahl Deutschland) kann zum Beispiel Deutschland eingegeben werden.

  Der hier eingegebene Text wird im Regel-Editor angezeigt.
– **Ziel**: Aufklappliste zur Auswahl des CCV-Objekts, das den zugehörigen (dem **Muster** entsprechenden)Rufnummern als Ziel zugeordnet werden soll.

Beliebig vielen verschiedenen (dem **Muster** entsprechenden) Rufnummern kann ein CCV-Objekt als Ziel zugeordnet werden.

• **Bedingte Verzweigung**

Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand einer Bedingung.

Definiert werden kann zum Beispiel, dass Anrufern eine Ansage eingespielt wird (Bitte rufen Sie zu einem späteren Zeitpunkt noch einmal an ...), sobald sich mehr als 20 Anrufe in einer Warteschlange befinden.

Eigenschaften:

– **Variable**: Auswahl von **Anrufe** oder **Verfügbare Agenten**.

  Je nach ausgewählter Variablen wird als Bedingungsvorgabe die Anzahl der wartenden Anrufe in einer Warteschlange oder die Anzahl der verfügbaren Agenten (inklusive Agenten in der Nachbearbeitungszeit) einer Warteschlange verwendet. In der zugehörigen Aufklappliste ist die Bedingung (**kleiner als**, **größer als**, **kleiner oder gleich als**, **größer**

oder gleich als, **gleich als**) auszuwählen und in dem zugehörigen Eingabefeld ist der Vergleichswert einzugeben.

– **Bedingung erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei erfüllter Bedingung als Ziel verwendet werden soll.
– **Bedingung nicht erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei nicht erfüllter Bedingung als Ziel verwendet werden soll.

Die Anzahl der verfügbaren Agenten in einer Warteschlange wird durch folgende Statusänderungen der Agenten beeinflusst:

– Anmelden eines Agenten in die Warteschlange über „Anmelden/Login“: --> +1
– Abmelden eines Agenten aus der Warteschlange über „Abmeldung/ Logout“: --> -1
– Agent im Zustand "Pause": --> -1
– Agent im Zustand "Verfügbar nach Pause": --> +1

Die Anzahl der verfügbaren Agenten in einer Warteschlange wird durch folgende Statusänderungen der Agenten **nicht** beeinflusst:

– Agent im Zustand "Klingeln"
– Agent im Zustand 'Gespräch'
– Agent in Zustand "Nachbearbeitung"
– Agent im Zustand "Verpasster Anruf"
– Agent im Zustand "Überfällig"

• **Datenverzweigung**

Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand einer Bedingung.

Definiert werden kann zum Beispiel, dass Anrufern eine Ansage eingespielt wird (Bitte rufen Sie zu einem späteren Zeitpunkt noch einmal an ...), sobald sich mehr als 20 Anrufe in einer Warteschlange befinden.

Eigenschaften:

– **Variable**: Auswahl von **LDAP-Daten1 (XMPP)** oder **LDAP-Daten2 (Pager)**.

  Die Datenabfrage erfolgt über LDAP entweder direkt an eine LDAP-fähige Datenbank oder indirekt über den Directory Service (ODS) an eine SQL / ODBC-Datenbank. Die Abfrageergebnisse werden über die Zuordnung des LDAP-Feldes der UC Suite den entsprechenden Kriterien des Contact Centers zugewiesen. In der zugehörigen Aufklappliste ist die Bedingung (**kleiner als**, **größer als**, **kleiner oder gleich als**, **größer oder gleich als**, **gleich als**) auszuwählen und in dem zugehörigen Eingabefeld ist der Vergleichswert einzugeben. Die Stichworte „Pager“ und „Info“ müssen unbedingt zugewiesen werden.
– **Zeitüberschreitung**: Zeitüberschreitung in Sekunden.
– **Verzweigung nach Zeitüberschreitung**: Aufklappliste zur Auswahl des CCV-Objekts, das bei einer Zeitüberschreitung als Ziel verwendet werden soll.
– **Bedingung erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei erfüllter Bedingung als Ziel verwendet werden soll.
– **Bedingung nicht erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei nicht erfüllter Bedingung als Ziel verwendet werden soll.
– **Beschreibung**: Angabe einer Erläuterung.

18.3.3 Nachbearbeitung

Anhand von Nachbearbeitungsgründen können kommende Anrufe bestimmten Themen (Bestellung, Reklamation, Service usw.) zugeordnet werden. Die Zuweisung erfolgt durch einen Agenten nach Beendigung des Anrufs (während der Arbeitszeit) durch Eingabe des entsprechenden Nachbearbeitungsgrundes über myAgent.

Nachbearbeitungsgründe können für jede Warteschlange individuell definiert werden.

Dabei wird unterschieden zwischen

- Einfache Nachbearbeitung

  Für Warteschlangen mit dem Nachbearbeitungsmodus "Einfache Nachbearbeitung" können ein oder mehrere Nachbearbeitungsgründe definiert werden.

  Beispiel: Für eine Warteschlange wurden die beiden Nachbearbeitungsgründe "Hardwareproblem" und "Softwareproblem"definiert. Jedem Anruf wird von einem Agenten während der Arbeitszeit einer dieser Nachbearbeitungsgründe zugewiesen. So kann beispielsweise ein Bericht erstellt werden, der eine Übersicht aller Anrufe zum Thema Hardware-Problem enthält.

- Mehrfache Nachbearbeitung

  Für Warteschlangen mit dem Nachbearbeitungsmodus "Mehrfache Nachbearbeitung" können ein oder mehrere Nachbearbeitungsgründe definiert und in Gruppen und Untergruppen zusammengefasst werden.

  Unterhalb jeder Gruppe oder Untergruppe (falls vorhanden) sollte ebenfalls mindestens ein Element konfiguriert werden, damit der Agent einen Anruf abschließen kann. Der Abbruch eines Anrufs ist nicht möglich, wenn eine Gruppe oder Untergruppe leer ist. Dies gilt nur für Warteschlangen, bei denen die Konfiguration „Multiple Wrapup“ aktiviert ist.

  Beispiel: Für eine Warteschlange wurden eine Hardware-Gruppe mit den Nachbearbeitungsgründen Hauptplatine und Stromversorgung und eine Software-Gruppe mit den Nachbearbeitungsgründen Betriebssystem und Treiber definiert. Jedem Anruf wird von einem Agenten während der Arbeitszeit einer dieser Nachbearbeitungsgründe zugewiesen. So kann beispielsweise ein Bericht mit einer Übersicht über alle Anrufe zu Hardware-Problemen oder auch über alle Anrufe zu Motherboard-Hardware-Problemen erstellt werden.

18.3.4 Servicegrad

Anhand des Servicegrads können Aussagen über die Beantwortungsqualität einer Warteschlange getroffen werden. Ermöglicht wird dies durch den Vergleich der Anruferwartezeiten in einer Warteschlange mit Sollwerten, die individuell für jede Warteschlange vorgegeben werden können.

Die Sollwerte für den Servicegrad (Grade Of Service GOS) können in Abhängigkeit von der Anruferwartezeit in einer Warteschlange frei bestimmt werden. Für jeden Anruf an eine entsprechende Warteschlange wird der Servicegrad nach Beendigung des Anrufs ermittelt und in die Datenbank

übernommen. Eine Auswertung des Servicegrads können Agenten mit dem Berechtigungs-Level Supervisor oder Administrator über die Applikation myAgent vornehmen.

18.3.5 Wandanzeige (Wallboard)

Über myAgent kann die Anzeige der Warteschlangendetails aufgerufen werden. Diese enthält eine Tabelle mit statistischen Informationen zu Warteschlangen in Echtzeit für den aktuellen 24-Stunden-Zeitraum. Die Anzeige kann zum Beispiel über einen großen LCD-Monitor oder über einen Beamer erfolgen (Wallboard).

Ein Agent mit dem Berechtigungs-Level Agent erhält Informationen über die Warteschlangen, denen er zugeordnet ist. Ein Agent mit dem Berechtigungs-Level Supervisor oder Administrator erhält Informationen über alle Warteschlangen.

Für die Wandanzeige sollte ein separater Teilnehmer eingerichtet werden. Dafür ist eine Teilnehmer-Lizenz (IP User oder TDM User) und eine myAgent-Lizenz erforderlich.

18.3.6 Agentenrückruf

Ist einem Anrufer die Wartezeit in der Warteschlange zu lang und enthält der zugehörige Zeitplan das CCV-Objekt **Callback aufzeichnen**, kann er einen Rückrufwunsch hinterlassen. Dieser Rückrufwunsch behält die Position des ursprünglichen Anrufers in der Warteschlange und wird den Agenten in Form einer Sprachnachricht zugestellt. Nach Abhören der Sprachnachricht kann der Agent den Anrufer über ein PopUp-Fenster zurückrufen.

Wurde für einen Anrufer ein bevorzugter Agent festgelegt, wird zunächst versucht die Rückrufwünsche dieses Anrufers an den bevorzugten Agenten zu vermitteln. Ist der bevorzugte Agent nicht verfügbar, wird der Rückrufwunsch an einen beliebigen verfügbaren Agenten weitergeleitet.

18.4 VIP-Betreuung

Für jede Warteschlange kann individuell definiert werden, ob bestimmte Anrufer oder Anrufer, die einstellbaren Rufnummernmustern entsprechen, bevorzugt behandelt werden sollen und dadurch schneller einen freien Agenten erreichen sollen.

Sind alle Agenten einer Warteschlange belegt, werden VIP-Anrufer bevorzugt mit dem nächsten freien Agenten verbunden.

18.4.1 VIP-Anruferpriorität

Anhand der VIP-Anruferpriorität kann für jede Warteschlange individuell definiert werden, ob die in der VIP-Rufliste enthaltenen Anrufer (beispielsweise Kunden) bevorzugt behandelt werden sollen.

Die Werte für die VIP-Anruferpriorität können in Abhängigkeit von der Anruferwartezeit in einer Warteschlange frei bestimmt werden. Damit wird der Grad der Bevorzugung von VIP-Anrufern gegenüber normalen Anrufern festgelegt.

Aktiviert ein VIP-Anrufer einen Agentenrückruf (Aufnahme einer Sprachnachricht mit Rückrufwunsch) verbleibt der Agentenrückruf anstelle des VIP-Anrufers in der Warteschlange. Die VIP-Anruferpriorität wird dabei nicht übernommen.

VIP-Anrufer müssen in der VIP-Rufliste verzeichnet sein (siehe VIP-Rufliste).

18.4.2 VIP-Rufliste

Bereits im Kommunikationssystem erfasste Anrufer (externes Verzeichnis) können in die VIP-Rufliste übernommen werden. Hierzu kann entweder die Mehrfachauswahl oder die Funktion "**Alle auswählen**" verwendet werden. Darüber hinaus ist die Eingabe von Rufnummernmustern möglich. Rufnummernmuster setzen sich aus einer bestimmten Ziffernfolge und einer Wildcard (Platzhalter) zusammen. Damit können beispielsweise alle Mitarbeiter eines Unternehmens in die VIP-Rufliste übernommen werden.

Für jede Warteschlange kann über die VIP-Anruferpriorität definiert werden, ob

- die in der VIP-Rufliste enthaltenen Anrufer und
- die zu einem in der VIP-Rufliste enthaltenen Rufnummernmuster passenden Anrufer bevorzugt behandelt werden sollen.

Die Eingabe von Rufnummernmustern im kanonischen Rufnummernformat ist nicht möglich. Auch die Verwendung von Abkürzungszeichen für Ländervorwahlen (zum Beispiel +49 statt 0049) ist nicht möglich. Rufnummernmuster sind immer ohne Amtskennziffer anzugeben.

Beispiele für Rufnummernmuster:

- 089 7577* (089 = Ortskennzahl München, 7577 = Anlagenrufnummer eines Unternehmens, * = Wildcard für eine beliebige Zahl). Durch den Eintrag dieses Rufnummernmusters in die VIP-Rufliste können alle Anrufer aus München, deren Rufnummer mit 7577 beginnt, bevorzugt behandelt werden.
- 0039* (0039 = Ländervorwahl Italien, * = Wildcard für eine beliebige Zahl). Durch den Eintrag dieses Rufnummernmusters in die VIP-Rufliste können alle Anrufer aus Italien bevorzugt behandelt werden.

Folgende Zeichen können als Wildcards (Platzhalter) in einem Rufnummernmuster verwendet werden:

- * = Wildcard für eine beliebige Zahl
- ? = Wildcard für eine beliebige Ziffer

18.5 Rückfalllösung (Fallback-Lösung)

Steht das Contact Center aufgrund von Problemen (Absturz, fehlende Verbindung oder ähnliches) nicht zur Verfügung, wird automatisch auf das Leistungsmerkmal "Uniform Call Distribution UCD" des Kommunikationssystems umgeschaltet. Das Leistungsmerkmal dient damit als Rückfalllösung für das Contact Center.

Bei einem Ausfall des Contact Centers werden die kommenden Anrufe entsprechend der Rückfalllösung verteilt. Das Verteilung von Faxen und E-Mails ist nicht möglich.

Je nach Anforderung kann eine der nachfolgend beschriebenen Rückfalllösungen konfiguriert werden.

Standard-Rückfalllösung

In diesem Fall basiert die Rückfalllösung auf den UCD-IDs (Agenten-IDs) der Agenten:

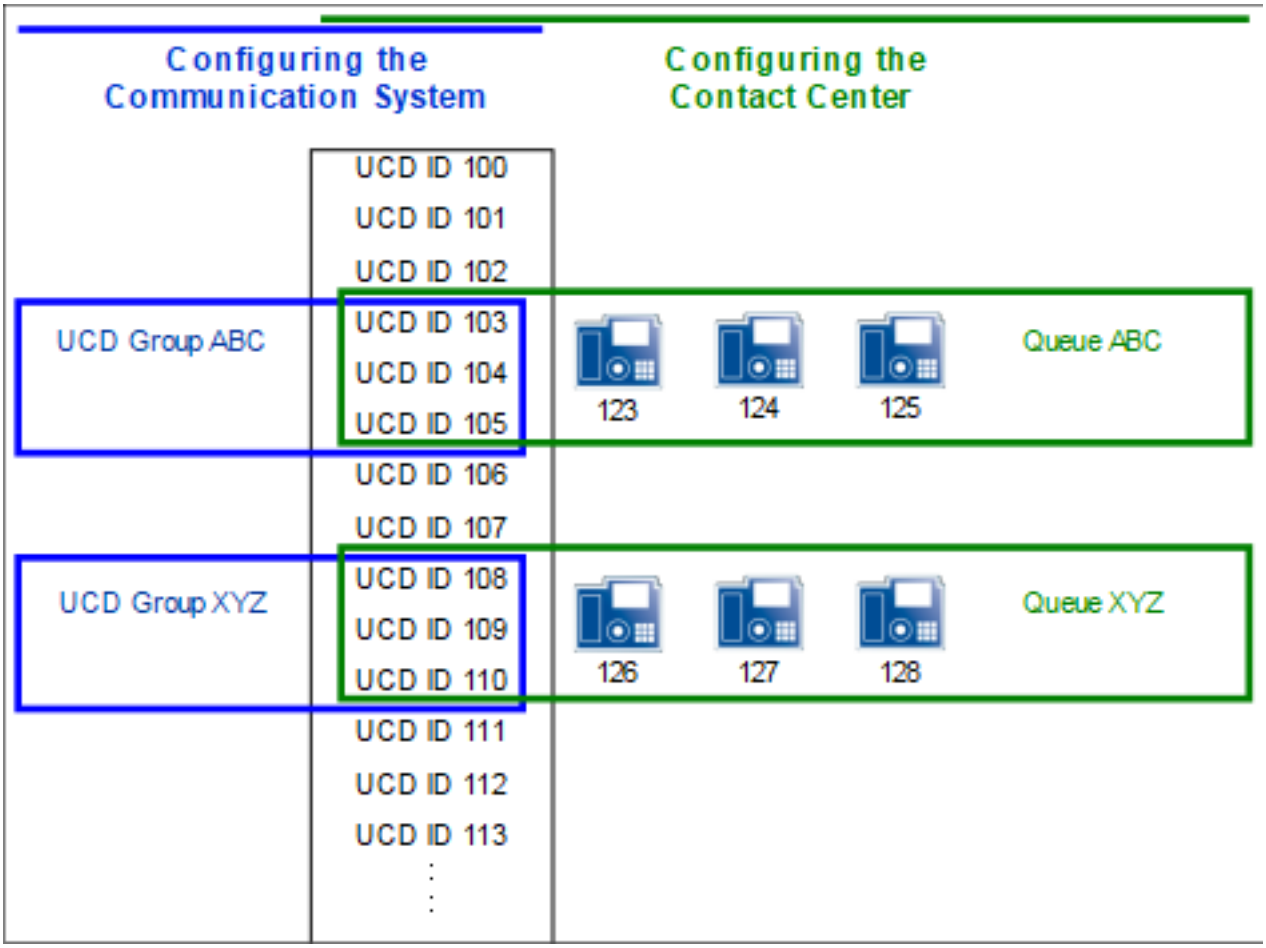
- Den UCD-Gruppen des Kommunikationssystems werden Agenten anhand von UCD-IDs zugeordnet. Die UCD-ID bestimmt, welcher UCD-Gruppe dieser Agent bei einem Ausfall des Contact Centers zugeordnet wird.

Für eine korrekte Funktion der Standard-Rückfalllösung müssen jeder Warteschlange die Contact-Center-Agenten mit den UCD-IDs zugeordnet werden, die den entsprechenden UCD-Gruppen zugeordnet wurden.

Bei einem Ausfall des Contact Centers werden die kommenden Anrufe über die verschiedenen UCD-Gruppen auf die angemeldeten Agenten verteilt.

Beispiel:

- UCD-Gruppe ABC werden die UCD-IDs 103, 104 und 105 zugeordnet. UCD-Gruppe XYZ wurden die UCD-IDs 108, 109 und 110 zugeordnet.
- Die Teilnehmer 123, 124 und 125 sind als Agenten mit den UCD-IDs 103, 104 und 105 konfiguriert. Die Teilnehmer 126, 127 und 128 sind als Agenten mit den UCD-IDs 108, 109 und 110 konfiguriert.
- Bei der Zuordnung von Agenten zu Warteschlangen müssen die Teilnehmer 123, 124 und 125 der Warteschlange ABC und die Teilnehmer 126, 127 und 128 der Warteschlange XYZ zugeordnet werden.



Basis-Rückfalllösung

In diesem Fall werden alle Agenten des Contact Centers anhand ihrer UCD-IDs nur der Backup-UCD-Gruppe zugeordnet. Durch die Zuordnung der entsprechenden Agenten werden diese UCD-IDs dann auch in den Warteschlangen des Contact Centers verwendet. Damit ist gewährleistet, dass bei Ausfall des Contact Centers sich die Agenten nicht mit einer anderen ID manuell an ihrem Telefon neu anmelden müssen. Für alle UCD-Gruppen des Kommunikationssystems wird diese Backup-UCD-Gruppe als Rufweiterschaltungsziel definiert.

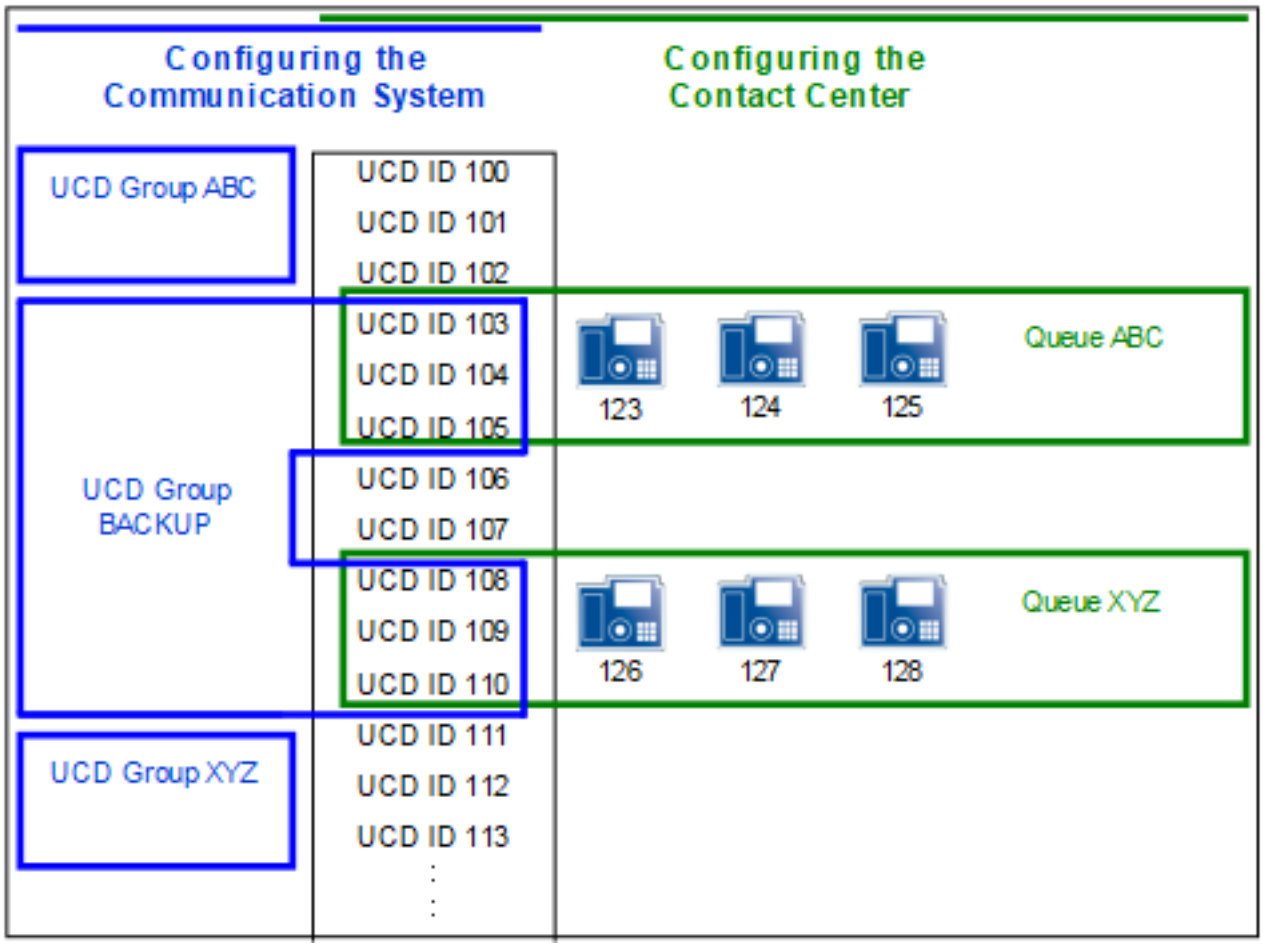
Anmerkung: Die konfigurierte Backup-UCD-Gruppe muss auch als Gruppe im Contact Center konfiguriert werden. Nur so ist sichergestellt, dass diese Gruppe ebenfalls überwacht wird.

Bei einem Ausfall des Contact Centers werden die kommenden Anrufe dann auf alle Agenten der Backup-UCD-Gruppe verteilt.

Beispiel:

- Den UCD-Gruppe ABC und XYZ wurden keine UCD-IDs zugeordnet. Der UCD-Gruppe BACKUP werden die UCD-IDs 103 bis 105 und 108 bis 110 zugeordnet.

- Die Teilnehmer 123, 124 und 125 sind als Agenten mit den UCD-IDs 103, 104 und 105 konfiguriert. Die Teilnehmer 126, 127 und 128 sind als Agenten mit den UCD-IDs 108, 109 und 110 konfiguriert.
- Bei der Zuordnung von Agenten zu Warteschlangen werden die Teilnehmer 123, 124 und 125 der Warteschlange ABC und die Teilnehmer 126, 127 und 128 der Warteschlange XYZ zugeordnet.



Kundenspezifische Rückfalllösung

In diesem Fall wird die kundenspezifische Konfiguration des Contact Centers über mehrere UCD-Gruppen nachgebildet.

Bei einem Ausfall des Contact Centers wird damit ein ähnliches Verhalten der Rückfalllösung erzielt.

Informationen zur Konfiguration einer Anrufverteilung über das Leistungsmerkmal „Uniform Call Distribution UCD“ des Kommunikationssystems siehe UCD (Uniform Call Distribution) (Anrufverteilung).

Wesentlicher Vorteil der kundenspezifischen Rückfalllösung ist die genaue Abbildung des Contact Centers auf die Rückfalllösung.

Nachteil der kundenspezifischen Rückfalllösung ist der hohe Konfigurationsaufwand. Darüber hinaus müssen alle Änderungen an der Contact Center-Konfiguration auch bei der Rückfalllösung nachgebildet werden, um ein ähnliches Verhalten der Anrufverteilung zu gewährleisten.

Wesentlicher Vorteil der Standard- und Basis-Rückfalllösung ist die einfache Konfiguration.

18.6 Konfiguration des Contact Centers

Bei der Konfiguration des Contact Centers sind zuerst die UCD-Gruppen zu definieren. Die Warteschlangen des Contact Centers sind Arbeitsgruppen, die auf den UCD-Gruppen des Kommunikationssystems basieren. Anschließend kann die eigentliche Konfiguration des Contact Centers (Zeitpläne, Warteschlangen usw.) durchgeführt werden.

Vor der Konfiguration des Contact Centers sind die Abläufe für die Anrufverteilung im Normal- und im Notfallbetrieb mit dem Kunden abzustimmen.

Tipp: Die Konfiguration des Contact Centers sollte erst erfolgen, nachdem die Einrichtung des Kommunikationssystems und der UC Suite vollständig abgeschlossen ist.

Werden Änderungen an der Konfiguration der UCD-Gruppen durchgeführt, muss anschließend die UC Suite über das Service Center des WBM neu gestartet werden.

Folgende Lizenzen sind Voraussetzung für den Betrieb eines Contact Centers:

- Eine entsprechende Anzahl Lizenzen für Agenten (myAgent)
- Contact-Center-Fax-Lizenz (für das Empfangen und Senden von Faxen), falls erforderlich
- Contact-Center-E-Mail-Lizenz (für das Empfangen und Senden von E-Mails), falls erforderlich

18.6.1 Beispiel für eine Contact-Center-Konfiguration

Anhand eines Beispiels wird das Funktionsprinzip des Contact Centers mit OpenScape Business dargestellt. Aufbau und Konfiguration des Beispiels basieren auf einem fiktiven Kundenszenario mit Contact-Center-Standardfunktionen.

Beispielszenario für ein Contact-Center

Die Firma XYZ betreibt ein Contact Center mit folgenden Rufnummern (Warteschlangen):

- Rufnummer 440 für den Bereich Service
- Rufnummer 444 für den Bereich Sales
- Rufnummer 456 für kostenlose Anrufe (Hotline). Anrufer erhalten eine Ansage und können anschließend durch Wahl der entsprechenden Ziffer den Bereich Service oder den Bereich Sales erreichen.

Das Contact Center besteht aus sechs Mitarbeitern (Agenten), wobei drei Mitarbeiter für den Bereich Service und drei Mitarbeiter für den Bereich Sales arbeiten.

Die Warteschlangen für die Bereiche Service und Sales sollen innerhalb der Geschäftszeiten von 09:00 Uhr bis 17:00 Uhr direkt erreichbar sein. Beide Warteschlangen verfügen über eine Faxbox und eine E-Mail-Adresse.

Sind alle Agenten im Gespräch oder nicht verfügbar, soll ein Anrufer darauf hingewiesen werden und Musik hören. Ist nach einer bestimmten Zeit kein Agent frei, kann ein Anrufer einen Rückrufwunsch hinterlassen oder durch Wahl einer bestimmten Ziffer zum Vermittlungsplatz gelangen. Wird keine Ziffer gewählt, soll der Anrufer automatisch in die Warteschlange zurückgeschaltet werden.

Außerhalb der Geschäftszeiten soll eine Ansage erfolgen, die eine Aufzeichnung mit Rückrufwunsch (Agentenrückruf) ermöglicht.

Anmerkung: Das Abspielen von Ansagen ist nur über Amtsleitungen möglich. Um die Ansage abzuspielen, muss der Anruf von einer Amtsleitung kommen oder der Anrufer sollte von OpenScape Contact Center überwacht werden.

Während der Mittagspause von 12:00 Uhr bis 13:00 Uhr soll für die Warteschlangen der Bereiche Service und Sales eine Ansage erfolgen, die eine Aufzeichnung mit Rückrufwunsch ermöglicht.

Rückfalllösung (Fallback-Lösung) über Backup-UCD-Gruppe: Steht das Contact Center aufgrund von Problemen (Absturz, fehlende Verbindung oder ähnliches) nicht zur Verfügung, soll automatisch auf das Leistungsmerkmal "Uniform Call Distribution UCD" des Kommunikationssystems umgeschaltet werden. Dafür müssen alle Agenten des Contact Centers einer einzelnen Backup-UCD-Gruppe zugeordnet werden. Für alle UCD-Gruppen des Kommunikationssystems ist diese Backup-UCD-Gruppe als Rufweiterschaltungsziel zu definieren. Bei einem Ausfall des Contact Centers werden die kommenden Anrufe dann auf die Agenten der Backup-UCD-Gruppe verteilt.

Konfiguration des Beispielszenarios

Folgende Tätigkeiten sind für das Beispielszenario durchzuführen:

- Konfiguration von UCD-Gruppen

  Die Warteschlangen des Contact Centers sind Arbeitsgruppen, die auf den UCD-Gruppen des Kommunikationssystems basieren. Vor der eigentlichen Konfiguration des Contact Centers, müssen die UCD-Gruppen definiert werden.

  Für das vorliegende Beispiel des Contact Centers der Firma XYZ sind drei UCD-Gruppen (Service, Sales, Hotline) zu konfigurieren.
- Konfiguration der Rückfalllösung (Fallback-Lösung)

  Für das vorliegende Beispiel ist eine Backup-UCD-Gruppe zu konfigurieren und diese als Rufweiterschaltungsziel aller UCD-Gruppen des Kommunikationssystems zu definieren.
- Konfiguration von Teilnehmern als Agenten

  Für das vorliegende Beispiel sind sechs Teilnehmer als Agenten zu konfigurieren.

- Aufnehmen von individuellen Ansagen

  Für das vorliegende Beispiel sind verschiedene Ansagen aufzunehmen. Das sind beispielsweise Ansagen für den Fall, dass alle Agenten nicht verfügbar sind oder um einen Anrufer über mögliche Optionen (**Aktion nach Zifferneingabe ausführen**) zu informieren.
- Laden von individuellen Ansagen

  Für das vorliegende Beispiel sind die aufgenommenen Ansagen in das Kommunikationssystem zu laden.
- Definition von Zeitplänen

  Für jeden Zeitabschnitt innerhalb eines Zeitplans wird über Regeln (Call Control Vector CCV) definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.

  Für das vorliegende Beispiel ist ein Zeitplan (Standard Schedule XYZ) mit einer Regel für die Zeiten außerhalb der Geschäftszeiten und Ausnahmen für die Geschäftszeiten und die Mittagspause zu definieren. Darüber hinaus ist ein zweiter Zeitplan (Standard Schedule Hotline) mit einer Regel für kostenlose Anrufe (Hotline) zu definieren.

Zeitplan	Regel (CCV)	
Standard Schedule XYZ	Out Of The Office	Zeiten außerhalb der Geschäftszeiten
	Open	Geschäftszeit 08:00 Uhr bis 11:59 Uhr = Open1
		Geschäftszeiten 13:00 Uhr bis 17:00 Uhr = Open2
	Mittagspause	Mittagspause 12:00 Uhr bis 12:59 Uhr
Standard Schedule Hotline	Hotline	24 Stunden

- Hinzufügen von drei Warteschlangen

  Für das vorliegende Beispiel ist eine Warteschlange für den Bereich Service und eine für den Bereich Sales zu konfigurieren. Eine weitere Warteschlange (Hotline) ist für kostenlose Anrufe zu konfigurieren.
- Agenten den Warteschlangen zuordnen

  Für das vorliegende Beispiel sind drei Agenten der Warteschlange Service und drei Agenten der Warteschlange Sales zuzuweisen.

Informationen über die Konfiguration aller Contact-Center-Funktionen finden Sie unter Vorgehensweise bei der Konfiguration .

18.6.1.1 Wie Sie UCD-Gruppen für das Beispiel-Contact-Center konfigurieren

Mit dem Wizard **Anrufverteilung** definieren Sie die drei UCD-Gruppen (Service, Sales, Hotline) mit den Rufnummern 440, 444 und 456 für das Beispiel-Contact-Center der Firma XYZ.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UCD** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.
4) Um eine UCD-Gruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer `440` der UCD-Gruppe Service ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer `440` der UCD-Gruppe Service ein.
7) Geben Sie im Feld **Name** den Namen `Service` ein.
8) Klicken Sie auf **OK & Weiter**. Das Fenster **Zuweisung der UCD-Agenten** wird angezeigt.
9) Klicken Sie auf **OK & Weiter**, da für die UCD-Gruppe Service keine UCD-IDs zugewiesen werden dürfen.

   Da für das Beispiel-Contact-Center der Firma XYZ eine Rückfalllösung über eine Backup-UCD-Gruppe eingerichtet werden soll, dürfen den drei UCD-Gruppen Service, Sales und Hotline keine UCD-IDs zugewiesen werden.
10) Klicken Sie auf **OK & Weiter**. Das Fenster **Ansagen / Überlauf bearbeiten** wird angezeigt.
11) Klicken Sie auf **OK**, da die angezeigten Parameter für die Konfiguration der UCD-Gruppe nicht relevant sind.
12) Wiederholen Sie die Schritte 4 bis 11 für die UCD-Gruppe Sales mit der Rufnummer 444 und für die UCD-Gruppe Hotline mit der Rufnummer 456.
13) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

18.6.1.2 Wie Sie eine Rückfalllösung (Fallback-Lösung) für das Beispiel-Contact-Center konfigurieren

Mit dem Wizard **Anrufverteilung** konfigurieren Sie die Backup-UCD-Gruppe mit der Rufnummer 400 für das Beispiel-Contact-Center der Firma XYZ. Für das Beispiel werden die UCD-Agenten-IDs 101 bis 106 verwendet. Darüber hinaus definieren Sie die Backup-UCD-Gruppe als Rufweiterschaltungsziel aller UCD-Gruppen des Beispiel-Contact-Center der Firma XYZ.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Backup-UCD-Gruppe mit der Rufnummer 400 muss in den Warteschlangen des UC Suite Contact Center konfiguriert werden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufverteilung** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.

4) Um eine UCD-Gruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf Bearbeiten.
5) Geben Sie im Feld **Rufnummer** die Rufnummer `400` der UCD-Gruppe Backup ein.
6) Geben Sie im Feld `Durchwahlnummer` die Durchwahlnummer **400** der UCD-Gruppe Backup ein.
7) Geben Sie im Feld **Name** den Namen `Backup` ein.
8) Klicken Sie auf **OK & Weiter**. Das Fenster **Zuweisung der UCD-Agenten** wird angezeigt.
9) Markieren Sie die gewünschten UCD-Agenten-IDs in der **Auswahl** und weisen Sie diese der UCD-Gruppe Backup durch Klicken auf **Hinzufügen** zu.
10) Klicken Sie auf **OK & Weiter**. Das Fenster **Teilnehmer zuweisen** wird angezeigt.
11) Weisen Sie allen UCD-Agenten-IDs die gewünschten Teilnehmer zu.
12) Klicken Sie auf **OK & Weiter**. Das Fenster **Ansagen / Überlauf bearbeiten** wird angezeigt.
13) Klicken Sie auf **OK**, da die angezeigten Paramater für die Konfiguration der UCD-Gruppe Backup nicht relevant sind.
14) Um die neue UCD-Gruppe Backup als Rufweiterschaltungsziel der UCD-Gruppe Service zu konfigurieren, klicken Sie in der Zeile der UCD-Gruppe Service auf **Bearbeiten**.
15) Klicken Sie so oft auf **OK & Weiter**, bis das Fenster **Ansagen / Überlauf bearbeiten** angezeigt wird.
16) Wählen Sie in der Aufklappliste **Überlauf-Ziel** die UCD-Gruppe Backup mit der Rufnummer 400 als Rufweiterschaltungsziel aus.
17) Klicken Sie auf **OK**.
18) Wiederholen Sie die Schritte 14 bis 17, um die neue UCD-Gruppe Backup als Rufweiterschaltungsziel der UCD-Gruppen Sales und Hotline zu konfigurieren.
19) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

18.6.1.3 Wie Sie einen Teilnehmer als Agent für das Beispiel-Contact-Center konfigurieren

Mit dem Wizard **Benutzerverzeichnis** konfigurieren Sie Teilnehmer als Agenten für das Beispiel-Contact-Center der Firma XYZ. Für das Beispiel werden die Teilnehmer mit den Rufnummern 101 bis 106 als Agenten konfiguriert. Die Teilnehmer mit den Rufnummern 101 und 104 erhalten das Berechtigungs-Level **Supervisor**, die anderen Teilnehmer das Berechtigungs-Level **Agent**.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten.
4) Markieren Sie den Teilnehmer mit der **Nebenstelle** 101 und klicken Sie auf **Bearbeiten**.
5) Klicken Sie im Menübaum auf **Persönliche Daten** > **Benutzerebene**.
6) Aktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.
7) Wählen Sie in der Aufklappliste **Level** das Berechtigungs-Level **Supervisor** aus.
8) Klicken Sie auf **Speichern**.
9) Wiederholen Sie die Schritte 4 bis 8, um die Teilnehmer mit den Rufnummern 102 bis 106 als Agenten zu konfigurieren.

18.6.1.4 Ansagen für das Beispiel-Contact-Center aufnehmen

Mit dem Wizard **Aufzeichnungsgerät** können Sie Ansagen für das Beispiel-Contact-Center der Firma XYZ aufnehmen. Unter anderem ist für den Fall eine Ansage erforderlich, dass alle Agenten nicht erreichbar sind.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.
4) Aktivieren Sie das Optionsfeld **Aufzeichnungsgerät**.
5) Wählen Sie in der Aufklappliste **Nebenstelle** die Rufnummer des Telefons aus, über das die Aufnahme durchgeführt werden soll.
6) Klicken Sie auf **Anrufen**. Die ausgewählte Rufnummer wird angerufen.
7) Nehmen Sie den Hörer ab und geben Sie im Feld **Dateiname** den Namen für Ihre Ansage ein.
8) Klicken Sie auf **Aufzeichnen**, um die Aufnahme der Ansage zu starten.
9) Klicken Sie auf **Anhalten**, sobald Sie die Ansage komplett aufgesprochen haben.
10) Wenn Sie sich Ihre neue Ansage anhören möchten, klicken Sie auf **Wiedergabe**.
11) Klicken Sie auf **Schließen**, um die Ansage zu speichern.

Tipp:

Nach dem Aufnehmen und Speichern ist das Löschen einer Ansage nicht mehr möglich. Durch Verwenden des gleichen Dateinamens kann eine bereits gespeicherte Ansage aber überschrieben werden. Beispielsweise wird durch das Speichern der Audiodatei `ansage1.wav` die bereits vorhandene Datei `ansage1.wav` überschrieben.

---

12) Wiederholen Sie die Schritte 3 bis 10, um weitere Ansagen für das Beispiel-Contact-Center der Firma XYZ aufzunehmen.

18.6.1.5 Ansagen für das Beispiel-Contact-Center laden

Mit dem Wizard **Datei-Upload** können Sie Ansagen für das Beispiel-Contact-Center der Firma XYZ laden.

Voraussetzungen

Eine Audiodatei im wav-Format mit folgenden Eigenschaften liegt vor: Mono, Abtastrate 8 kHz, Abtastgröße 16 Bit, Framelänge 2.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.
4) Klicken Sie auf die Registerkarte **Audiodatei-Manager**.
5) Wählen Sie in der Aufklappliste **Upload-Ziel** das Ziel **Automatischer Vermittlungsplatz** aus.
6) Wählen Sie das Optionsfeld **Uploader** und klicken Sie auf **Datei auswählen**, navigieren Sie zum gewünschten Speicherort der Audiodatei und klicken Sie auf **Öffnen**.
7) Klicken Sie auf **Upload**.

Tipp:

Nach dem Datei-Upload ist das Löschen einer Audiodatei nicht mehr möglich. Durch Verwenden des gleichen Dateinamens kann eine bereits geladene Audiodatei aber überschrieben werden. Beispielsweise wird durch das Laden der Audiodatei `ansage1.wav` die bereits vorhandene Datei `ansage1.wav` überschrieben.

---

8) Wiederholen Sie die Schritte 4 bis 7, um weitere Ansagen für das Beispiel-Contact-Center der Firma XYZ zu laden.

18.6.1.6 Den Zeitplan Standard Schedule XYZ für das Beispiel-Contact-Center hinzufügen

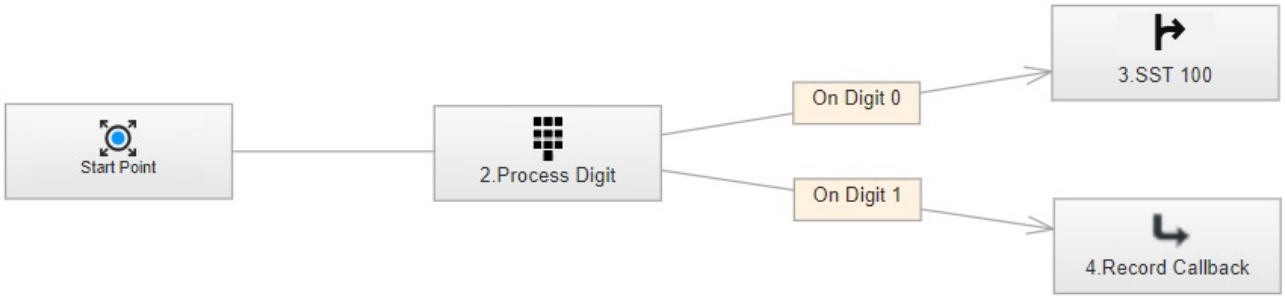
Mit dem Wizard **Contact Center** definieren Sie den Zeitplan mit Regeln für die Pausen- und die Geschäftszeiten für das Beispiel-Contact-Center der Firma XYZ. Dazu ist ein Zeitplan (Standard Schedule XYZ) mit einer Regel für die Zeiten außerhalb der Geschäftszeiten (Out Of The Office) und Ausnahmen für die Geschäftszeiten (08:00 Uhr bis 11:59 Uhr = Open1, 13:00 Uhr bis 17:00 Uhr = Open2) und die Mittagspause (12:00 Uhr bis 12:59 Uhr = Lunch Break) zu definieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.
5) Klicken Sie auf **Hinzufügen**.
6) Klicken Sie unter dem Bereich **Zeitplan** auf **Hinzufügen** .
7) Definieren Sie die abgebildete Regel für Zeiten außerhalb der Geschäftszeiten.



Klicken Sie in der Liste der CCV-Tools auf eins der in der abgebildeten Regel enthaltenen CCV-Objekte und ziehen Sie es in den Regel-Editor. Geben Sie die nachfolgend genannten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **Speichern**. Wiederholen Sie den Vorgang für alle weiteren CCV-Objekte. Verbinden Sie die CCV-Objekte, indem Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte klicken. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte. Wiederholen Sie den Vorgang für alle weiteren zu verbindenden CCV-Objekte.

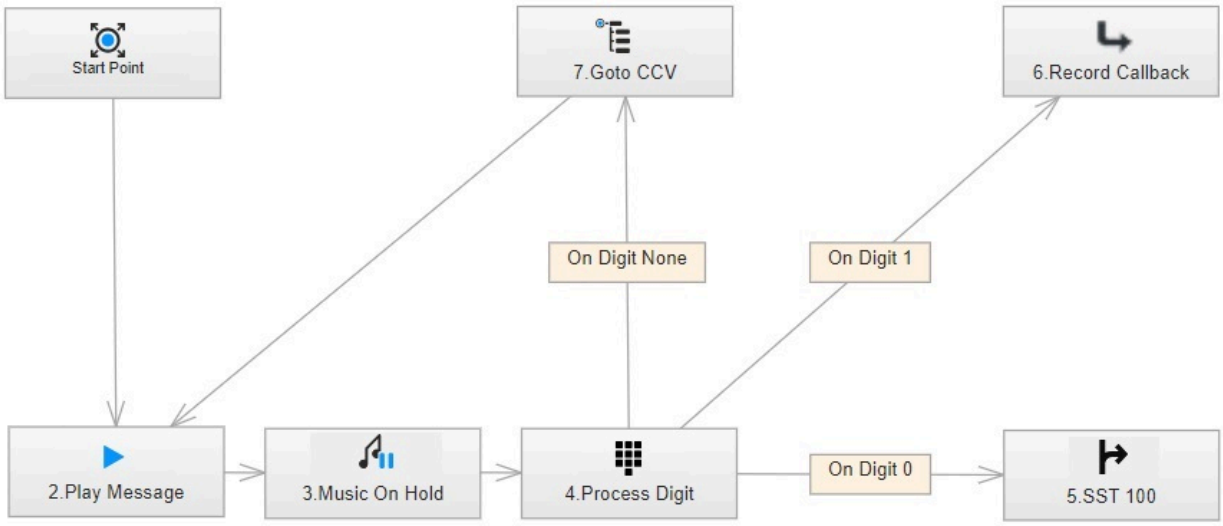
Eigenschaft	Wert
1. CCV-Objekt: **Aktion nach Zifferneingabe ausführen**	
Wiedergabeliste	Audiodatei im wav-Format
Zeitüberschreitung bei Zifferneingabe	5
Beschreibung	Ansage: "Drücken Sie Ziffer 0 bis ...; Drücken Sie Ziffer 1 bis ...
2. CCV-Objekt: **Einzelschritt-Übergabe**	
Zielnebenstelle	100
Beschreibung	Weiter zum Vermittlungsplatz
Aktion nach Zifferneingabe	0
3. CCV-Objekt: **Callback aufzeichnen**	

Eigenschaft	Wert
Typ	Extensiver Rückruf
Max. Nachrichtenlänge	20
Beschreibung	Rückrufwunsch (Agentenrückruf)
Aktion nach Zifferneingabe	1

Klicken Sie auf **Speichern ...**. Geben Sie `Out of the Office` als **CCV-Namen** der Regel ein und klicken Sie anschließend auf **Speichern**. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

Wählen Sie in der Aufklappliste **Standard-CCV** die Regel `Out of the Office` aus.

8) Geben Sie im Feld **Name des Zeitplans** den Namen `Standard Schedule XYZ` ein.
9) Klicken Sie auf **Speichern**.
10) Klicken Sie unter dem Bereich **Zeitplan** auf **Hinzufügen** .
11) Definieren Sie die abgebildete Regel für die Geschäftszeiten.



Klicken Sie in der Liste der CCV-Tools auf eins der in der abgebildeten Regel enthaltenen CCV-Objekte und ziehen Sie es in den Regel-Editor. Geben Sie die nachfolgend genannten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **Speichern**. Wiederholen Sie den Vorgang für alle weiteren CCV-Objekte. Verbinden Sie die CCV-Objekte, indem Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte klicken. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte. Wiederholen Sie den Vorgang für alle weiteren zu verbindenden CCV-Objekte.

Eigenschaft	Wert
1. CCV-Objekt: **Nachricht abspielen**	

Eigenschaft		Wert
	Dateiname	Audiodatei im wav-Format
	Abbruchtasten	5
	Beschreibung	Ansage: Agenten nicht erreichbar
2. CCV-Objekt: **Wartemusik**		
	Zeitwert	30
	Beschreibung	Wartemusik für 30 Sekunden
3. CCV-Objekt: **Aktion nach Zifferneingabe ausführen**		
	Wiedergabeliste	Audiodatei im wav-Format
	Zeitüberschreitung bei Zifferneingabe	5
	Beschreibung	Ansage: "Drücken Sie Ziffer 0 bis ...; Drücken Sie Ziffer 1 bis ...
4. CCV-Objekt **Einzelschritt-Übergabe**		
	Zielnebenstelle	100
	Beschreibung	Weiter zum Vermittlungsplatz
	Aktion nach Zifferneingabe	0
5. CCV-Objekt: **Callback aufzeichnen**		
	Typ	Extensiver Rückruf
	Max. Nachrichtenlänge	20
	Beschreibung	Rückrufwunsch (Agentenrückruf)
	Aktion nach Zifferneingabe	1
6. CCV-Objekt: **Zu CCV**		
	Ziel-CCV	1. Nachricht abspielen
	Beschreibung	Zurück zur Ansage

Klicken Sie auf **Speichern ...**. Geben Sie `Open` als **CCV-Namen** der Regel ein und klicken Sie anschließend auf **Speichern**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

Wählen Sie in der Aufklappliste für die Ausnahme Open1 die Regel `Open` aus.

12) Klicken Sie im Fensterbereich **Ausnahmen** auf **Hinzufügen**, um die erste Ausnahme für die Geschäftszeiten zu definieren.

13) Geben Sie im Feld `Beschreibung` **Open1** ein.

14) Definieren Sie, zu welcher Zeit die Ausnahme Open1 gelten soll:

Aktivieren Sie das Optionsfeld **Im Zeitbereich**. Wählen Sie in der Auswahlliste `Startzeit` **08:00** als Anfang und in der Auswahlliste `Endezeit` **11:59** als Ende des Tageszeitraums aus.

Wählen Sie im Fenster **Tage auswählen** die Wochentage aus, an denen die Regel gelten soll. Klicken Sie anschließend auf **Speichern**.

15) Klicken Sie im Bereich **Ausnahmen** auf **Hinzufügen**, um die zweite Ausnahme für die Geschäftszeiten zu definieren.

16) Geben Sie im Feld **Beschreibung** `Open2` ein.

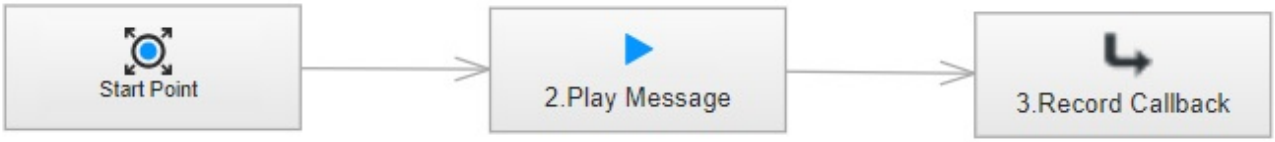
17) Wählen Sie in der Aufklappliste für die Ausnahme Open2 die Regel `Open` aus.

18) Definieren Sie, zu welcher Zeit die Ausnahme Open2 gelten soll:

    Wählen Sie in der Aufklappliste **Typ** die Option **Im Zeitbereich**. Wählen Sie in der Auswahlliste `Startzeit` **13:00** als Anfang und in der Auswahlliste `Endezeit` **17:00** als Ende des Tageszeitraums aus.

    Wählen Sie im Fenster **Tage auswählen** die Wochentage aus, an denen die Regel gelten soll. Klicken Sie anschließend auf **Speichern**.

19) Definieren Sie die abgebildete Regel für die Mittagspause.



Klicken Sie in der Liste der CCV-Tools auf eins der in der abgebildeten Regel enthaltenen CCV-Objekte und ziehen Sie es in den Regel-Editor. Geben Sie die nachfolgend genannten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **Speichern**. Wiederholen Sie den Vorgang für alle weiteren CCV-Objekte. Verbinden Sie die CCV-Objekte, indem Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte klicken. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte. Wiederholen Sie den Vorgang für alle weiteren zu verbindenden CCV-Objekte.

Eigenschaft	Wert
1. CCV-Objekt: **Nachricht abspielen**	
Dateiname	Audiodatei im wav-Format
Abbruchtasten	Service auswählen
Beschreibung	Ansage: Agenten nicht erreichbar
2. CCV-Objekt: **Callback aufzeichnen**	
Typ	Extensiver Rückruf
Max. Nachrichtenlänge	20
Beschreibung	Rückrufwunsch (Agentenrückruf)
Aktion nach Zifferneingabe	1

Klicken Sie auf **Speichern ...**. Geben Sie `Lunch Break` als **CCV-Name** der Regel ein. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

Wählen Sie in der Aufklappliste für die Ausnahme Mittagspause die Regel `Lunch Break` aus.

20) Klicken Sie im Bereich **Ausnahmen** auf **Hinzufügen**, um die Ausnahme für die Mittagspause zu definieren.

21) Geben Sie im Feld `Beschreibung` **Lunch Break** ein.

22) Definieren Sie, zu welcher Zeit die Ausnahme Lunch Break gelten soll:

Wählen Sie in der Aufklappliste **Typ** die Option **Im Zeitbereich**. Wählen Sie in der Auswahlliste **Startzeit** `12:00` als Anfang und in der Auswahlliste **Endezeit** `12:59` als Ende des Tageszeitraums aus.

Wählen Sie im Fenster **Tage auswählen** die Wochentage aus, an denen die Regel gelten soll. Klicken Sie anschließend auf **Speichern**.

23) Wenn Sie testen möchten, welche Regel (CCV) des Zeitplans an einem bestimmten Zeitpunkt ausgeführt wird, klicken Sie auf **Zeitplan testen**. Wählen Sie in der Aufklappliste **Datum** den gewünschten Tag und in der Auswahlliste **Zeit** die gewünschte Uhrzeit aus. Klicken Sie auf **Zeitplan testen**. Anschließend wird angezeigt, welche Regel (CCV) an diesem Tag und zu dieser Uhrzeit aktiv ist. Klicken Sie auf **Schließen**, um das Fenster **Zeitplan testen** zu schließen.

24) Klicken Sie auf **Speichern**.

25) Schließen Sie das Fenster.

18.6.1.7 Den Zeitplan Standard Schedule Hotline für das Beispiel-Contact-Center hinzufügen

Mit dem Wizard **Contact Center** definieren Sie den Zeitplan mit einer Regel für kostenlose Anrufe (Hotline) für das Beispiel-Contact-Center der Firma XYZ.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

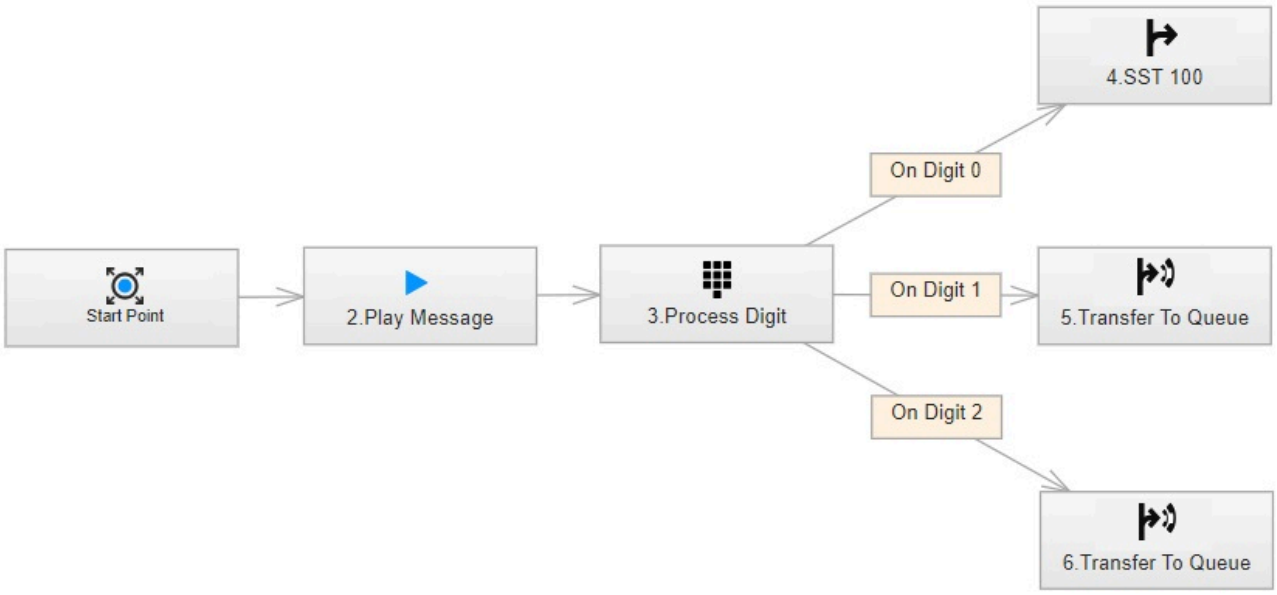
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.

5) Klicken Sie auf **Hinzufügen**.

6) Klicken Sie unter dem Bereich **Zeitplan** auf **Hinzufügen** .

7) Definieren Sie die abgebildete Regel für kostenlose Anrufe (Hotline).



Klicken Sie in der Liste der CCV-Tools auf eins der in der abgebildeten Regel enthaltenen CCV-Objekte und ziehen Sie es in den Regel-Editor. Geben Sie die nachfolgend genannten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **Speichern**. Wiederholen Sie den Vorgang für alle weiteren CCV-Objekte. Verbinden Sie die CCV-Objekte, indem Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte klicken. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte. Wiederholen Sie den Vorgang für alle weiteren zu verbindenden CCV-Objekte.

Eigenschaft	Wert
1. CCV-Objekt: **Nachricht abspielen**	
Dateiname	Audiodatei im wav-Format
Abbruchtasten	5
Beschreibung	Ansage: Begrüßung
2. CCV-Objekt: **Aktion nach Zifferneingabe ausführen**	
Wiedergabeliste	Audiodatei im wav-Format
Zeitüberschreitung bei Zifferneingabe	5
Beschreibung	Ansage: "Drücken Sie Ziffer 0 bis ...; Drücken Sie Ziffer 1 bis ...
3. CCV-Objekt: **Einzelschritt-Übergabe**	
Zielnebenstelle	100
Beschreibung	Weiter zum Vermittlungsplatz
Aktion nach Zifferneingabe	0

Eigenschaft	Wert
4. CCV-Objekt **An Warteschlange übergeben**	
Warteschlange	440
Beschreibung	Weiter zur Warteschlange Service
Aktion nach Zifferneingabe	1
5. CCV-Objekt **An Warteschlange übergeben**	
Warteschlange	444
Beschreibung	Weiter zur Warteschlange Sales
Aktion nach Zifferneingabe	2

Klicken Sie auf **Speichern ...**. Geben Sie `Hotline` als **CCV-Namen** der Regel ein und klicken Sie anschließend auf **Speichern**. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

Wählen Sie in der Aufklappliste `Standard-CCV` die Regel **Hotline** aus.

8) Geben Sie im Feld **Name des Zeitplans** den Namen `Standard Schedule Hotline` ein.
9) Klicken Sie auf **Zeitplan speichern**.

18.6.1.8 Warteschlangen für das Beispiel-Contact-Center hinzufügen

Mit dem Wizard **Contact Center** konfigurieren Sie die Warteschlangen für das Beispiel-Contact-Center der Firma XYZ. Für das Beispiel ist eine Warteschlange für den Bereich Service (Rufnummer 440) und eine für den Bereich Sales (Rufnummer 444) zu konfigurieren. Eine weitere Warteschlange (Hotline, Rufnummer 456) ist für kostenlose Anrufe zu konfigurieren.

Voraussetzungen

Die UCD-Gruppen **Service**, **Sales** und **Hotline** für das Beispiel-Contact-Center wurden eingerichtet.

Die Zeitpläne **Standard Schedule XYZ** und **Standard Schedule Hotline** für das Beispiel-Contact-Center wurden eingerichtet.

Mindestens ein E-Mail-Account für den E-Mail-Empfang steht zur Verfügung.

Der E-Mail-Versand im Kommunikationssystem ist konfiguriert.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Warteschlange**.
5) Klicken Sie auf **Hinzufügen**.
6) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

7) Geben Sie im Feld **Name der Warteschlange** den Namen `Service` ein.
8) Wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Aktiv** aus.
9) Geben Sie im Feld `Gruppennummer` die Rufnummer **440** ein.
10) Wählen Sie in der Aufklappliste **Telefonanlage** den Eintrag **CSP** aus.
11) Wählen Sie in der Aufklappliste **Zeitplan** den Eintrag **Standard Schedule XYZ** aus.
12) Geben Sie im Feld **Anzahl Warteschlangen-Alarme** beispielsweise `20` ein.

    Sind mehr als 20 wartende Anrufe in der Warteschlange, wechselt das Warteschlangensymbol bei den Agenten von grün auf orange.
13) Geben Sie im Feld **Zeit Warteschlangen-Alarm** beispielsweise `300` ein.

    Sobald die Wartezeit eines Anrufs in der Warteschlange 300 Sekunden übersteigt, wechselt der betreffende Eintrag in der Liste der Contact-Center-Anrufe bei den Agenten auf rot.
14) Geben Sie im Feld **Zeitüberschreitung für entgangene Anrufe** beispielsweise `100` ein, damit ein nicht angenommener Anruf nach 100 Sekunden zum nächsten freien Agenten weitergeleitet wird.
15) Geben Sie im Feld **Schwellwert für abgebrochene Anrufe** beispielsweise `120` ein. Damit werden Anrufe in die Statistik (in einen Bericht) aufgenommen, die nach 120 Sekunden abgebrochen werden.
16) Aktivieren Sie das Kontrollkästchen **Pop-up-Fenster aktiviert**, damit bei kommenden Anrufen in myAgent ein Pop-up-Fenster zur Anzeige und Eingabe von Kundendaten erscheint.
17) Aktivieren Sie die Option **Keine Nachbearbeitung**.
18) Wählen Sie in der Aufklappliste **Warteschlangentiefe-Modus** den Eintrag **Statisch**.
19) Geben Sie eine Zahl in das Feld **Warteschlangentiefe** ein, z. B. `5`.
20) Klicken Sie auf die Registerkarte **Warteschlangen-Pilots**.
21) Wählen Sie in der Aufklappliste **Pilots für eingehende Faxnachrichten** die Optionen(en) des/der gewünschten Pilots (Rufnummer(n)), damit Faxe in die Warteschlange übernommen werden.

    Faxe an diese Rufnummer(n) werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.

22) Wählen Sie eine der folgenden Möglichkeiten im Bereich **Dienst für eingehende E-Mails**, damit E-Mails in die Warteschlange übernommen werden:

- Wenn Sie eine neue E-Mail-Adresse einrichten möchten, klicken Sie auf **Hinzufügen**. Das Fenster **Hinzufügen** wird angezeigt.

  Wählen Sie die Authentifizierungsmethode für Ihren E-Mail-Server aus der Aufklappliste **Auth-Methode** aus. Sie können zwischen **Einfach** und **OAuth 2.0**wählen.

  Geben Sie im Feld **Server** die Bezeichnung des E-Mail-Servers ein, der für das Abholen der E-Mails verwendet werden soll (zum Beispiel `pop3.web.de`).

  Geben Sie im Feld **Port** die Portnummer des E-Mail-Servers ein (zum Beispiel `110`, die Standardportnummer für POP3).

  Wenn die Authentifizierungsmethode **Einfach** ausgewählt ist, geben Sie die Zugangsdaten für den E-Mail-Server in die Felder **Benutzername** und **Kennwort** ein.

  Wenn als Authentifizierungsmethode **OAuth 2.0** ausgewählt wurde, geben Sie den Benutzernamen für den Zugriff auf den E-Mail-Server in die Felder **Benutzername**, **Mandanten-ID**, **Anwendungs-ID** und **Client Secret** ein. Mandanten-ID, Anwendungs-ID und Client Secret entsprechen der Anwendung, die in Azure AD für die E-Mail-Warteschlangen registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator. Geben Sie den Geltungsbereich für die Anwendung in das Feld **Umfang** ein (Standardwert: https://outlook.office365.com/.default).

  Wählen Sie aus, ob der E-Mail-Versand über eine SSL (Secure Socket Layer)-Verbindung erfolgen soll: Wenn Sie eine SSL-Verbindung nutzen möchten, aktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**. (Dadurch ändert sich gegebenenfalls die Portnummer des E-Mail-Servers. Standardportnummer für POP3 via SSL = 995). Wenn Sie keine SSL-Verbindung nutzen möchten, deaktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**.

  Klicken Sie auf **Speichern**. Die neue E-Mail-Adresse wird anschließend im Bereich **Dienst für eingehende E-Mails** angezeigt.
- Wenn Sie eine bestehende E-Mail-Adresse ändern möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **Bearbeiten**. Das Fenster **Bearbeiten** wird angezeigt.

  Ändern Sie die gewünschten Parameter und klicken Sie anschließend auf **Speichern**.
- Wenn Sie eine bestehende E-Mail-Adresse löschen möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **E-Mail entfernen**.

23) Klicken Sie auf die Registerkarte **Verschiedenes**.

24) Geben Sie im Feld **Absender-E-Mail-Adresse** die E-Mail-Adresse ein, die beim Versenden einer E-Mail durch einen Agenten beim Empfänger angezeigt werden soll.

25) Wenn Sie das Kontrollkästchen **Intelligente Anrufweiterleitung** aktivieren, werden eingehende Anrufe automatisch an den Agenten weitergeleitet, mit dem der Anrufer zuletzt verbunden war.

26) Klicken Sie auf **Speichern**.

27) Wiederholen Sie die Schritte 5 bis 23, um die Warteschlange Sales zu konfigurieren. Wiederholen Sie die Schritte 5 bis 17 und 23, um die Warteschlange Hotline zu konfigurieren.

18.6.1.9 Agenten den Warteschlangen des Beispiel-Contact-Centers zuordnen

Mit dem Wizard **Contact Center** ordnen Sie die Agenten den Warteschlangen für das Beispiel-Contact-Center der Firma XYZ zu. Für das Beispiel sind drei Agenten der Warteschlange Service und drei Agenten der Warteschlange Sales zuzuordnen.

Voraussetzungen

Die Warteschlangen **Service** und **Sales** für das Beispiel-Contact-Center wurden eingerichtet.

Sechs Agenten für das Beispiel-Contact-Center wurden konfiguriert.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlangen-Bindungen**. Die Warteschlangen für **Service** und **Sales** werden angezeigt.

5) Wählen Sie die Warteschlange aus, der Sie einen Agenten zuweisen möchten, und klicken Sie auf **Bearbeiten**. Alle bereits zugeordneten Agenten werden angezeigt.

6) Wählen Sie in der Tabelle den ersten Agenten für die **Service**-Warteschlange aus und klicken Sie auf **Bearbeiten**. Daraufhin wird das Fenster **Bearbeiten** angezeigt.

7) Wählen Sie eine der folgenden Optionen:

- Wenn der Agent Anrufe unabhängig von der Auslastung der **Service**-Warteschlange entgegennehmen soll, wählen Sie in der Aufklappliste **Typ** den **Hauptagenten** aus.
- Wenn der Agent nur dann Anrufe erhalten soll, wenn die **Service**-Warteschlange überläuft, wählen Sie in der Aufklappliste **Typ** den **Agent bei Überlauf** aus.

8) Wenn Sie **Agent bei Überlauf** gewählt haben:

a) Geben Sie im Feld **Überlauf nach Sekunden in Wartes.** die Zeit ein, nach deren Ablauf ein Anruf an einen Agenten bei Überlauf weitergeleitet werden soll.

b) Geben Sie im Feld **Überlauf nach Anrufen in Wartes.** die Maximalzahl von Anrufen ein. Ein Agent bei Überlauf erhält Anrufe, die über diese Maximalzahl hinausgehen.

9) Stellen Sie einen Prozentwert für das **Fähigkeits-Level** des Agenten ein.

Durch das Fähigkeits-Level steuern Sie die Verteilung der Anrufe auf die Agenten in der Warteschlange **Service**. Agenten mit höherem Fähigkeits-Level werden bei der Anrufverteilung bevorzugt. Haben alle Agenten das gleiche Fähigkeits-Level, erhält der am längsten freie Agent den Anruf.

10) Wählen Sie eine der folgenden Optionen:
    - Wenn der Agent Rückrufwünsche in Form von Sprachnachrichten erhalten soll, aktivieren Sie das Kontrollkästchen **Agentenrückruf aktivieren**.
    - Wenn der Agent keine Rückrufwünsche erhalten soll, deaktivieren Sie das Kontrollkästchen **Agentenrückruf aktivieren**.
11) Geben Sie im Feld **Nachbearbeitung** die automatische Nachbearbeitungszeit in Sekunden für den Agenten in der Warteschlange **Service** ein.
12) Klicken Sie auf **OK**.
13) Wiederholen Sie die Schritte 5 bis 12, um alle Agenten den Warteschlangen des Beispiel-Contact-Centers zuzuordnen.

18.6.2 Vorgehensweise bei der Konfiguration

Hier erhalten Sie einen Überblick über die bei der Konfiguration des Contact Centers durchzuführenden Tätigkeiten.

- Konfiguration von UCD-Gruppen

  Die Warteschlangen des Contact Centers sind Arbeitsgruppen, die auf den UCD-Gruppen des Kommunikationssystems basieren. Vor der eigentlichen Konfiguration des Contact Centers, müssen die UCD-Gruppen definiert werden.
- Konfiguration einer Rückfalllösung (Fallback-Lösung)

  Steht das Contact Center aufgrund von Problemen (Absturz, fehlende Verbindung oder ähnliches) nicht zur Verfügung, wird automatisch auf das Leistungsmerkmal "Uniform Call Distribution UCD" des Kommunikationssystems umgeschaltet. Das Leistungsmerkmal dient damit als Rückfalllösung für das Contact Center (siehe Rückfalllösung (Fallback-Lösung)).
- Konfiguration von Teilnehmern als Agenten
- Aufnehmen von individuellen Ansagen für das Contact Center
- Laden von individuellen Ansagen für das Contact Center

  Anmerkung: Das Abspielen von Ansagen ist nur über Amtsleitungen möglich. Um die Ansage abzuspielen, muss der Anruf von einer Amtsleitung kommen oder der Anrufer sollte von OpenScape Contact Center überwacht werden.
- Hinzufügen von Zeitplänen
- Hinzufügen von Warteschlangen
- Festlegen von Sollwerten für den Servicegrad
- Festlegen der VIP-Anruferpriorität
- Bearbeiten der VIP-Rufliste
- Festlegen von bevorzugten Agenten
- Hinzufügen von Contact Center-Pausen
- Hinzufügen von Nachbearbeitungscodes
- Zuordnen von Agenten zu Warteschlangen

18.6.2.1 Wie Sie UCD-Gruppen für das Contact Center konfigurieren

Mit dem Wizard **Anrufverteilung** können Sie UCD-Gruppen für das Contact Center konfigurieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufverteilung** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.
4) Um eine UCD-Gruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer der UCD-Gruppe ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der UCD-Gruppe ein.
7) Geben Sie im Feld **Name** den Namen der UCD-Gruppe ein.
8) Klicken Sie auf **OK & Weiter**. Das Fenster **Zuweisung der UCD-Agenten** wird angezeigt.
9) Markieren Sie die gewünschten UCD-Agenten-IDs in der **Auswahl** und weisen Sie diese der UCD-Gruppe durch Klicken auf **Hinzufügen** zu.
10) Klicken Sie auf **OK & Weiter**. Das Fenster **Teilnehmer zuweisen** wird angezeigt.
11) Weisen Sie allen UCD-Agenten-IDs die gewünschten Teilnehmer zu.
12) Klicken Sie auf **OK & Weiter**. Das Fenster **Ansagen / Überlauf bearbeiten** wird angezeigt.
13) Klicken Sie auf **OK**, da die angezeigten Parameter für die Konfiguration der UCD-Gruppe nicht relevant sind.
14) Wenn Sie weitere UCD-Gruppen für das Contact Center konfigurieren möchten, wiederholen Sie die Schritte 4 bis 11.
15) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

18.6.2.2 Wie Sie einen Teilnehmer als Agent konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten.
4) Markieren Sie den gewünschten Teilnehmer im Benutzerverzeichnis und klicken Sie auf **Bearbeiten**.
5) Klicken Sie im Menübaum auf **Persönliche Daten** > **Benutzerebene**.

6) Wählen Sie eine der folgenden Möglichkeiten:

   Wenn der Agent dauerverfügbar sein soll, aktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

   Wenn der Agent nicht dauerverfügbar sein soll, deaktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent erhält den Zustand nicht verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

7) Wählen Sie in der Aufklappliste **Level** das Berechtigungs-Level aus.

8) Klicken Sie auf **Speichern**.

9) Wenn Sie einen weiteren Teilnehmer als Agent konfigurieren möchten, wiederholen Sie Schritt 4 bis Schritt 8.

18.6.2.3 Individuelle Ansage für das Contact Center aufnehmen

Mit dem Wizard **Aufzeichnungsgerät** können Sie individuelle Ansagen für das Contact Center aufnehmen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.
4) Aktivieren Sie das Optionsfeld **Aufzeichnungsgerät**.
5) Wählen Sie in der Aufklappliste **Nebenstelle** die Rufnummer des Telefons aus, über das die Aufnahme durchgeführt werden soll.
6) Klicken Sie auf **Anrufen**. Die ausgewählte Rufnummer wird angerufen.
7) Nehmen Sie den Hörer ab und geben Sie im Feld **Dateiname** den Namen für Ihre Ansage ein.
8) Klicken Sie auf **Aufzeichnen**, um die Aufnahme der Ansage zu starten.
9) Klicken Sie auf **Anhalten**, sobald Sie die Ansage komplett aufgesprochen haben.
10) Wenn Sie sich Ihre neue Ansage anhören möchten, klicken Sie auf **Wiedergabe**.
11) Klicken Sie auf **Schließen**, um die Ansage zu speichern.

Tipp:

Nach dem Aufnehmen und Speichern ist das Löschen einer Ansage nicht mehr möglich. Durch Verwenden des gleichen Dateinamens kann eine bereits gespeicherte Ansage aber überschrieben werden. Beispielsweise wird durch das Speichern der Audiodatei `ansage1.wav` die bereits vorhandene Datei `ansage1.wav` überschrieben.

18.6.2.4 Individuelle Ansage für das Contact Center laden

Mit dem Wizard **Datei-Upload** können Sie individuelle Ansagen für das Contact Center laden.

Voraussetzungen

Eine Audiodatei im wav-Format mit folgenden Eigenschaften liegt vor: Mono, Abtastrate 8 kHz, Abtastgröße 16 Bit, Framelänge 2.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.
4) Klicken Sie auf die Registerkarte **Audiodatei-Manager**.
5) Wählen Sie in der Aufklappliste **Upload-Ziel** das Ziel **Automatischer Vermittlungsplatz** aus.
6) Wählen Sie das Optionsfeld **Uploader** und klicken Sie auf **Datei auswählen**, navigieren Sie zum Speicherort der gewünschten Audiodatei und klicken Sie auf **Öffnen**.
7) Klicken Sie auf **Upload**.

Tipp: Nach dem Datei-Upload ist das Löschen einer Audiodatei nicht mehr möglich. Durch Verwenden des gleichen Dateinamens kann eine bereits geladene Audiodatei aber überschrieben werden. Beispielsweise wird durch das Laden der Audiodatei `ansage1.wav` die bereits vorhandene Datei `ansage1.wav` überschrieben.

18.6.2.5 Zeitplan hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.
5) Klicken Sie auf **Hinzufügen**.

6) Wählen Sie für die Auswahl der Regel (CCV) eine der folgenden Möglichkeiten aus:

- Wenn Sie dem Zeitplan eine bereits definierte Regel zuweisen möchten, wählen Sie in der Aufklappliste **Standard-CCV** die gewünschte Regel aus.
- Wenn Sie dem Zeitplan eine neue, noch nicht definierte Regel zuweisen möchten, klicken Sie im Bereich **Zeitplan** auf **Bearbeiten** und gehen Sie wie folgt vor:

  Klicken Sie in der Liste der CCV-Tools auf das gewünschte CCV-Objekt und ziehen Sie es in den Regel-Editor. Geben Sie die gewünschten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und klicken Sie auf **Speichern**. Falls erforderlich, ziehen Sie weitere CCV-Objekte in den Regel-Editor und definieren Sie deren Eigenschaften. Um zwei CCV-Objekte zu verbinden, klicken Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte.

  Wenn Sie ein CCV-Objekt aus dem Regel-Editor löschen möchten, klicken Sie mit der rechten Maustaste auf das betreffende CCV-Objekt und wählen Sie im Aufklappmenü **Entfernen**.

  Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **Speichern**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert.

  Wählen Sie in der Aufklappliste **Standard-CCV** die neue, soeben gespeicherte Regel aus.
- Wenn Sie dem Zeitplan eine neue Regel zuweisen möchten, die auf einer bereits definierten Regel basiert, gehen Sie wie folgt vor:

  Wählen Sie in der Aufklappliste **Standard-CCV** die gewünschte Regel aus und klicken Sie auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt. Ändern Sie die Regel.

  Klicken Sie in der Liste der CCV-Tools auf das gewünschte CCV-Objekt und ziehen Sie es in den Regel-Editor. Geben Sie die gewünschten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und klicken Sie auf **Speichern**. Falls erforderlich, ziehen Sie weitere CCV-Objekte in den Regel-Editor und definieren Sie deren Eigenschaften. Um zwei CCV-Objekte zu verbinden, klicken Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte.

  Klicken Sie auf **Speichern ...**. Geben Sie einen **CCV-Namen** für die neue Regel ein und klicken Sie anschließend auf **Speichern**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert.

  Wählen Sie in der Aufklappliste **Standard-CCV** die neue, soeben gespeicherte Regel aus.

7) Wenn Sie die Regel ausdrucken oder per E-Mail verschicken möchten, können Sie die Regel als PDF-Datei speichern. Klicken Sie dafür auf **Drucken**. Das Fenster **Drucken** öffnet sich.

Geben Sie den Namen der Datei ein und wählen Sie das Verzeichnis aus, in dem die Datei gespeichert werden soll. Klicken Sie auf **Speichern**.

8) Geben Sie im Feld **Name des Zeitplans** den Namen des neuen Zeitplans ein.

9) Klicken Sie auf **Speichern**.

10) Wenn Sie einem bestimmten Zeitraum innerhalb des Zeitplans eine andere Regel (CCV) zuweisen möchten, klicken Sie im Fensterbereich **Ausnahmen** auf **Hinzufügen**. Anschließend werden die Felder für diese Ausnahme angezeigt.

11) Geben Sie im Feld **Beschreibung** den Namen der Ausnahme ein.

12) Wählen Sie für die Auswahl der Regel (CCV) eine der folgenden Möglichkeiten aus:

- Wenn Sie dem Zeitraum innerhalb des Zeitplans eine bereits definierte Regel zuweisen möchten, wählen Sie in der Aufklappliste für diese Ausnahme die gewünschte Regel aus.
- Wenn Sie dem Zeitraum innerhalb des Zeitplans eine neue, noch nicht definierte Regel zuweisen möchten, gehen Sie wie folgt vor:

  Klicken Sie unter dem Bereich **Zeitplan** auf **Hinzufügen** .

  Klicken Sie in der Liste der CCV-Tools auf das gewünschte CCV-Objekt und ziehen Sie es in den Regel-Editor. Geben Sie die gewünschten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und klicken Sie auf **Speichern**. Falls erforderlich, ziehen Sie weitere CCV-Objekte in den Regel-Editor und definieren Sie deren Eigenschaften. Um zwei CCV-Objekte zu verbinden, klicken Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte.

  Wenn Sie ein CCV-Objekt aus dem Regel-Editor löschen möchten, klicken Sie mit der rechten Maustaste auf das betreffende CCV-Objekt und wählen Sie im Aufklappmenü **Entfernen**.

  Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **Speichern**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert.

  Wählen Sie in der Aufklappliste für diese Ausnahme die neue, soeben gespeicherte Regel aus.
- Wenn Sie dem Zeitraum innerhalb des Zeitplans eine neue Regel zuweisen möchten, die auf einer bereits definierten Regel basiert, gehen Sie wie folgt vor:

  Wählen Sie in der Aufklappliste für diese Ausnahme die gewünschte Regel aus und klicken Sie auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt. Ändern Sie die Regel.

  Klicken Sie in der Liste der CCV-Tools auf das gewünschte CCV-Objekt und ziehen Sie es in den Regel-Editor. Geben Sie die gewünschten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und klicken Sie auf **Speichern**. Falls erforderlich, ziehen Sie weitere CCV-

Objekte in den Regel-Editor und definieren Sie deren Eigenschaften. Um zwei CCV-Objekte zu verbinden, klicken Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte.

Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **Speichern**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert.

Wählen Sie in der Aufklappliste für diese Ausnahme die neue, soeben gespeicherte Regel aus.

13) Wählen Sie eine der folgenden Möglichkeiten, um festzulegen, zu welcher Zeit die Ausnahme gelten soll:

- Wenn die Ausnahme für einen unbegrenzten Zeitraum im Jahr gelten soll, wählen Sie in der Aufklappliste **Typ** die Option **Im Zeitbereich**. Wählen Sie in der Auswahlliste **Startzeit** den Anfang und in der Auswahlliste **Endezeit** das Ende des Tageszeitraums aus.

  Wählen Sie die Wochentage aus, an denen die Ausnahme gelten soll. Klicken Sie anschließend auf **Speichern**.
- Wenn die Ausnahme nur für einen begrenzten Zeitraum im Jahr gelten soll, wählen Sie in der Aufklappliste **Typ** die Option **Im Zeitbereich**. Geben Sie im Feld **Startdatum** das Datum für den Beginn und im Feld **Endedatum** das Datum für das Ende des Jahreszeitraums ein (Format tt.mm.jjjj). Wählen Sie das genaue Start- und Endedatum in den Listenfeldern **Startzeit** und **Endezeit** aus. Die Ausnahme gilt zwischen Startdatum/Startzeit und Enddatum/Endzeit des Erfassungszeitraums.

  Wählen Sie die Wochentage aus, an denen die Ausnahme gelten soll. Klicken Sie anschließend auf **Speichern**.
- Wenn die Ausnahme an Feiertagen gelten soll, wählen Sie in der Aufklappliste **Typ** die Option **Urlaubspläne**. Geben Sie im Feld **Startdatum** das Datum für den Beginn und im Feld **Endedatum** das Datum für das Ende der Urlaubszeit ein. Wählen Sie in der Auswahlliste **Startzeit** die Tageszeit für den Anfang und in der Auswahlliste **Endezeit** die Tageszeit für das Ende der Urlaubszeit aus.

  Tipp: Urlaubspläne haben Vorrang vor anderen Zeitplänen und Regeln einer Warteschlange.
- Wenn die Ausnahme jedes Jahr gelten soll, wählen Sie in der Aufklappliste **Typ** die Option **Jährliche Wiederholung**. Geben Sie im Feld **Startdatum** das Datum für den Beginn und im Feld **Endedatum** das Datum für das Ende der jährlichen Wiederholung ein. Wählen Sie in der Auswahlliste **Startzeit** die Tageszeit für den Anfang und in der Auswahlliste **Endezeit** die Tageszeit für das Ende der jährlichen Wiederholung aus.

14) Klicken Sie auf **Speichern**.

15) Wiederholen Sie die Schritte 10 bis 14, wenn Sie für bestimmte Zeiträume weitere Ausnahmen definieren möchten.

16) Wenn Sie testen möchten, welche Regel (CCV) des Zeitplans an einem bestimmten Zeitpunkt ausgeführt wird, klicken Sie auf **Zeitplan testen**. Wählen Sie in der Aufklappliste **Datum** den gewünschten Tag und in der

Auswahlliste **Zeit** die gewünschte Uhrzeit aus. Klicken Sie auf **Zeitplan testen**. Anschließend wird angezeigt, welche Regel (CCV) an diesem Tag und zu dieser Uhrzeit aktiv ist. Klicken Sie auf **Schließen**, um das Fenster **Zeitplan testen** zu schließen.

17) Wenn Sie diesen Zeitplan einer oder mehreren Warteschlangen zuordnen möchten, aktivieren Sie das/die Kontrollkästchen für die gewünschte(n) Warteschlange(n) im Bereich **Warteschlangen**.

Anmerkung: Eine ausgewählte Warteschlange kann nur einem Zeitplan zugewiesen werden, aber mehrere verschiedene Warteschlangen können einem ausgewählten Zeitplan zugewiesen werden.

---

18) Schließen Sie das Fenster.

18.6.2.6 Zeitplan ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.

5) Markieren Sie den zu ändernden Zeitplan und klicken Sie auf **Bearbeiten**.

6) Ändern Sie die gewünschten Einstellungen für die Standard-CCV:

- Wenn Sie eine andere als die in der Aufklappliste **Standard-CCV** angezeigte Regel (CCV) zuweisen möchten, wählen Sie in der Aufklappliste **Standard-CCV** die gewünschte Regel aus.
- Wenn Sie die in der Aufklappliste Standard-CCV angezeigte Regel (CCV) ändern möchten, klicken Sie im Bereich **Zeitplan** auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt. Ändern Sie die Regel. Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **Speichern**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

  Wählen Sie in der Aufklappliste **Standard-CCV** die neue, soeben gespeicherte Regel aus.

7) Klicken Sie auf **Speichern**.

8) Ändern Sie die gewünschten Einstellungen im Bereich **Ausnahmen**:

- Wenn Sie einem bestimmten Zeitraum innerhalb des Zeitplans eine andere Regel (CCV) zuweisen möchten, klicken Sie im Bereich **Ausnahmen** auf **Hinzufügen**. Wählen Sie in der Aufklappliste dieser Ausnahme die gewünschte Regel aus. Wählen Sie anhand der Optionsfelder und Aufklapplisten, zu welcher Zeit diese Ausnahme gelten soll. Geben Sie im Feld **Beschreibung** den Namen der Ausnahme ein. Klicken Sie auf **Speichern**.

- Wenn Sie diese Ausnahme oder eine der angezeigten Ausnahmen bearbeiten möchten, klicken Sie nach der Auswahl der gewünschten Ausnahme auf die Schaltfläche **Bearbeiten** unter dem Bereich **Ausnahme** und geben dann über Optionsfelder, Aufklapplisten und Felder an, wann diese Ausnahme gelten soll und auf welche Regel (CCV). Zusätzlich können Sie unter dem Bereich **Ausnahmen** auf **CCV bearbeiten** klicken, um die zugehörige Regel (CCV) zu bearbeiten. Die Regel wird im Regel-Editor angezeigt. Ändern Sie die Regel. Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **Speichern**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

  Wählen Sie in der Aufklappliste die neue, soeben gespeicherte Regel aus. Wählen Sie anhand der Optionsfelder und Aufklapplisten, zu welcher Zeit diese Regel (CCV) gelten soll. Klicken Sie auf das grüne Speichern-Symbol.
- Wenn Sie diese Ausnahme oder eine der angezeigten Ausnahmen löschen möchten, klicken Sie nach der Auswahl der gewünschten Ausnahme auf **Entfernen**.

9) Wenn Sie testen möchten, welche Regel (CCV) des Zeitplans an einem bestimmten Zeitpunkt ausgeführt wird, klicken Sie auf **Zeitplan testen**. Wählen Sie in der Aufklappliste **Datum** den gewünschten Tag und in der Auswahlliste **Zeit** die gewünschte Uhrzeit aus. Klicken Sie auf **Zeitplan testen**. Anschließend wird angezeigt, welche Regel (CCV) an diesem Tag und zu dieser Uhrzeit aktiv ist. Klicken Sie auf **Schließen**, um das Fenster **Zeitplan testen** zu schließen.

10) Wenn Sie diesen Zeitplan einer oder mehreren Warteschlangen zuordnen möchten, aktivieren Sie das/die Kontrollkästchen für die gewünschte(n) Warteschlange(n) im Bereich **Warteschlangen**.

Anmerkung: Eine ausgewählte Warteschlange kann nur einem Zeitplan zugewiesen werden, aber mehrere verschiedene Warteschlangen können einem ausgewählten Zeitplan zugewiesen werden.

---

11) Schließen Sie das Fenster.

18.6.2.7 Zeitplan löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle vorhandenen Zeitpläne werden angezeigt.

5) Markieren Sie den gewünschten Zeitplan und klicken Sie auf **Entfernen**.

Tipp: Ein Zeitplan kann nicht gelöscht werden, solange er einer Warteschlange zugeordnet ist. Vor dem Löschen

muss die Zuordnung des Zeitplans zu der oder den Warteschlangen entfernt werden.

18.6.2.8 Regel (CCV) als PDF-Datei speichern

Der Wizard **Contact Center** ermöglicht Ihnen das Speichern von Regeln (CCV) als PDF-Datei. Die PDF-Datei kann anschließend beispielsweise ausgedruckt oder per E-Mail verschickt werden.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.
5) Markieren Sie den Zeitplan, der die gewünschte Regel enthält und klicken Sie auf **Bearbeiten**.
6) Wählen Sie in der Aufklappliste die gewünschte Regel aus und klicken Sie auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt.
7) Klicken Sie auf **Drucken**. Das Speichern-Fenster erscheint.
8) Geben Sie den Namen der Datei ein und wählen Sie das Verzeichnis aus, in dem die Datei gespeichert werden soll.
9) Klicken Sie auf **Speichern**.
10) Schließen Sie das Fenster und bestätigen Sie das Schließen mit **Ja**.

18.6.2.9 Regel (CCV) als Backup-Datei herunterladen

Mit dem Wizard **Contact Center** können Sie Regeln (CCV) als Backup-Datei herunterladen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.
5) Markieren Sie den Zeitplan, der die gewünschte Regel enthält und klicken Sie auf **Bearbeiten**.
6) Wählen Sie die gewünschte Regel aus der Aufklappliste **CCV** aus und klicken Sie unter dem Bereich **Zeitplan** auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt.

7) Klicken Sie auf **Download**.

Die gewünschte Regel (CCV) wird nun als Backup-Datei heruntergeladen.

18.6.2.10 Heruntergeladene Regel (CCV) in einem Sicherungsdateiformat hochladen

Mit dem Wizard **Contact Center** können Sie Regeln (CCV) hochladen, die zuvor in einem Sicherungsdateiformat heruntergeladen wurden.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Laden Sie eine Regel (CCV) in einem Sicherungsdateiformat herunter.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.
5) Markieren Sie den Zeitplan, der die gewünschte Regel enthält und klicken Sie auf **Bearbeiten**.
6) Wählen Sie die gewünschte Regel aus der Aufklappliste **CCV** aus und klicken Sie unter dem Bereich **Zeitplan** auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt.
7) Klicken Sie auf **Datei auswählen**, navigieren Sie zum Ablageort der Backup-Datei der gewünschten Regel und klicken Sie auf **Öffnen**.

   Wenn Sie eine Datei auswählen, die nicht in einem Sicherungsformat vorliegt, tritt ein Fehler auf.
8) Klicken Sie auf **Backup wiederherstellen**.

Die gewünschte Regel (CCV) wird nun in das System hochgeladen.

18.6.2.11 Warteschlange hinzufügen

Voraussetzungen

Mindestens eine UCD-Gruppe wurde eingerichtet.

Mindestens ein Zeitplan wurde eingerichtet.

Mindestens ein E-Mail-Account für den E-Mail-Empfang steht zur Verfügung, falls E-Mails in die Warteschlange übernommen werden sollen.

Der E-Mail-Versand im Kommunikationssystem ist konfiguriert, falls E-Mails durch Agenten der Warteschlange versandt werden sollen.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Warteschlange**.
5) Klicken Sie auf **Hinzufügen**.
6) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.
7) Geben Sie im Feld **Name der Warteschlange** den Namen der Warteschlange ein.

   Empfehlung: Verwenden Sie den Namen einer der von Ihnen konfigurierten UCD-Gruppen.

   Tipp: Damit der Name der Warteschlange bei einer Auswertung (Bericht) komplett angezeigt wird, sollten Sie kurze und nicht zusammengesetzte Bezeichnungen wählen. Beispiel: Einkauf Inland Gruppe 1 (nicht: Inlandseinkaufsgruppe 1)

8) Wählen Sie eine der folgenden Möglichkeiten für den Zustand der Warteschlange:

   - Wenn Sie die neue Warteschlange aktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Aktiv** aus.
   - Wenn Sie die neue Warteschlange deaktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Nicht aktiv** aus.

     Die Deaktivierung einer Warteschlange führt zur Aktivierung der Rückfalllösung durch die zugehörige UCD-Gruppe. Ist kein Agent bei der UCD-Gruppe angemeldet und kein weiteres Rufweiterschaltungsziel für die UCD-Gruppe eingetragen, wird Anrufern besetzt signalisiert.

9) Geben Sie im Feld **Gruppennummer** die Rufnummer einer UCD-Gruppe ein, die Sie bei der Grundkonfiguration des Contact Centers eingerichtet haben.
10) Wählen Sie in der Aufklappliste **Telefonanlage** den Eintrag **CSP** aus.
11) Wählen Sie in der Aufklappliste **Zeitplan** den gewünschten Zeitplan aus.
12) Geben Sie im Feld **Anzahl Warteschlangen-Alarme** die Alarm-Schwellwertanzahl ein.

    Wird die hier angegebene Anzahl wartender Anrufe in der Warteschlange überschritten, wechselt das Warteschlangensymbol bei den Agenten von grün auf orange.
13) Geben Sie im Feld **Zeit Warteschlangen-Alarm** die Alarm-Schwellwertzeit in Sekunden ein.

    Wird die hier angegebene Wartezeit eines Anrufs in der Warteschlange überschritten, wechselt der betreffende Eintrag in der Liste der Contact-Center-Anrufe bei den Agenten auf rot.
14) Geben Sie im Feld **Zeitüberschreitung für entgangene Anrufe** die Zeit in Sekunden ein, nach deren Ablauf ein nicht angenommener Anruf zum nächsten freien Agenten weitergeleitet werden soll.
15) Geben Sie im Feld **Schwellwert für abgebrochene Anrufe** die Zeit in Sekunden ein, die festlegt, ob ein abgebrochener Anruf in die Statistik (in einen Bericht) aufgenommen wird oder nicht.

    Statistisch erfasst werden Anrufe, die nach Ablauf der angegebenen Zeit abgebrochen werden.

16) Wählen Sie eine der folgenden Möglichkeiten für die Anzeige von PopUp-Fenstern in der Applikation myAgent aus:

> **Tipp:** PopUp-Fenster sind erforderlich, um Rückrufe anzunehmen und auszuführen und um Faxe und E-Mails anzunehmen.

- Wenn bei kommenden Anrufen in myAgent ein Pop-up-Fenster zur Anzeige und Eingabe von Kundendaten erscheinen soll, aktivieren Sie das Kontrollkästchen **Pop-up-Fenster aktiviert**.
- Wenn bei kommenden Anrufen in myAgent kein Pop-up-Fenster erscheinen soll, deaktivieren Sie das Kontrollkästchen **Pop-up-Fenster aktiviert**.

17) Wählen Sie eine der folgenden Möglichkeiten für den Nachbearbeitungsmodus:

Bei Warteschlangen mit Nachbearbeitungsmodus können Agenten ihre Anrufe anhand von Nachbearbeitungscodes bestimmten Themen zuordnen (Bestellung, Reklamation, Service usw.).

- Wenn Sie eine Warteschlange mit dem Nachbearbeitungsmodus einfache Nachbearbeitung einrichten möchten, aktivieren Sie die Option **Einfache Nachbearbeitung**.
- Wenn Sie eine Warteschlange mit dem Nachbearbeitungsmodus mehrfache Nachbearbeitung einrichten möchten, aktivieren Sie die Option **Mehrfache Nachbearbeitung**.
- Wenn Sie eine Warteschlange ohne Nachbearbeitungsmodus einrichten möchten, aktivieren Sie die Option **Keine Nachbearbeitung**.

18) Wenn Sie die Priorität der Warteschlange ändern möchten, klicken Sie auf **Prioritäten**.

Klicken und ziehen Sie die roten Punkte im Bereich **Warteschlangen-Priorität im Verlauf der Zeit** auf die gewünschten Positionen. Die horizontale Achse zeigt die Wartezeit in der Warteschlange, die vertikale Achse die Priorität der ausgewählten Warteschlange gegenüber anderen Warteschlangen. Ist ein Agent mehreren Warteschlangen zugeordnet, kann über die Warteschlangen-Priorität festgelegt werden, ob die Anrufe für eine Warteschlange mit höherer Priorität an diesen Agenten weitergeleitet werden sollen als die Anrufe für andere Warteschlangen.

Ziehen Sie die Scrollbalken im Bereich **Anruftyp-Prioritäten** auf die gewünschte Position. Damit legen Sie die Priorität der Anruftypen innerhalb der ausgewählten Warteschlange fest. Je weiter rechts sich der Scrollbalken befindet, desto höher ist die Priorität.

> **Tipp:** Für Sprachanrufe sollte eine höhere Priorität als für die anderen Anruftypen gewählt werden. Ansonsten könnten wartende Anrufer durch Rückrufe, Faxe oder E-Mails verdrängt werden.

19) Wählen Sie eine der folgenden Möglichkeiten für den Warteschlangentiefe-Modus:

Die Warteschlangentiefe kann für jede Warteschlange einzeln im Warteschlangenkonfigurationsdialog eingestellt werden.

- Falls der **Warteschlangentiefe-Modus** auf **Statisch** gesetzt wurde, können **WLS** und **Warteschlangentiefe** konfiguriert werden.
- Falls die **Warteschlangentiefe-Modus** auf **Keine** gesetzt wurde, kann dennoch der Parameter **WLS** konfiguriert werden. Dies beeinflusst auch die UCD-Konfiguration, aber die **Warteschlangentiefe** kann nicht eingestellt werden.

20) Geben Sie die Größe der Warteschleife in das Feld **WLS** ein. Der **WLS**-Wert, d. h. die Anzahl der Anrufe, die darauf warten, mit einem Agenten verbunden zu werden, wirkt sich direkt auf die Konfiguration des Parameters Warteschlangen der zugewiesenen UCD-Gruppe aus.

21) Wenn der **Warteschlangentiefe-Modus** auf **Statisch** eingestellt ist, geben Sie die Quantität der Warteschlangentiefe in das Feld **Warteschlangentiefe** ein. Die Warteschlangentiefe ist die Zusammenfassung der Warteschleifengröße (WLS) und die Anrufe bei Agenten.

22) Klicken Sie auf die Registerkarte **Warteschlangen-Pilots**.

23) Wenn Faxe in die Warteschlange übernommen werden sollen, wählen Sie im Bereich **Pilots für eingehende Faxnachrichten** die entsprechende(n) Option(en) des oder der gewünschten Pilots (Rufnummer(n)).

Faxe an diese Rufnummer(n) werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.

24) Wählen Sie eine der folgenden Möglichkeiten im Bereich **Dienst für eingehende E-Mails**, damit E-Mails in die Warteschlange übernommen werden:

- Wenn Sie eine neue E-Mail-Adresse einrichten möchten, klicken Sie auf **Hinzufügen**. Das Fenster **Hinzufügen** wird angezeigt.

  Wählen Sie die Authentifizierungsmethode für Ihren E-Mail-Server aus der Aufklappliste **Auth-Methode** aus. Sie können zwischen **Einfach** und **OAuth 2.0**wählen.

  Geben Sie im Feld **Server** die Bezeichnung des E-Mail-Servers ein, der für das Abholen der E-Mails verwendet werden soll (zum Beispiel `pop3.web.de`).

  Geben Sie im Feld **Port** die Portnummer des E-Mail-Servers ein (zum Beispiel `110`, die Standardportnummer für POP3).

  Wenn die Authentifizierungsmethode **Einfach** ausgewählt ist, geben Sie die Zugangsdaten für den E-Mail-Server in die Felder **Benutzername** und **Kennwort** ein.

  Wenn als Authentifizierungsmethode **OAuth 2.0** ausgewählt wurde, geben Sie den Benutzernamen für den Zugriff auf den E-Mail-Server in die Felder **Benutzername**, **Mandanten-ID**, **Anwendungs-ID** und **Client Secret** ein. Mandanten-ID, Anwendungs-ID und Client Secret entsprechen der Anwendung, die in Azure AD für die E-Mail-Warteschlangen registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator. Geben Sie den Geltungsbereich

für die Anwendung in das Feld **Umfang** ein (Standardwert: https://outlook.office365.com/.default).

Wählen Sie aus, ob der E-Mail-Versand über eine SSL (Secure Socket Layer)-Verbindung erfolgen soll: Wenn Sie eine SSL-Verbindung nutzen möchten, aktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**. (Dadurch ändert sich gegebenenfalls die Portnummer des E-Mail-Servers. Standardportnummer für POP3 via SSL = 995). Wenn Sie keine SSL-Verbindung nutzen möchten, deaktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**.

Klicken Sie auf **Speichern**. Die neue E-Mail-Adresse wird anschließend im Bereich **Dienst für eingehende E-Mails** angezeigt.

- Wenn Sie eine bestehende E-Mail-Adresse ändern möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **Bearbeiten**. Das Fenster **Bearbeiten** wird angezeigt.

  Ändern Sie die gewünschten Parameter und klicken Sie anschließend auf **Speichern**.
- Wenn Sie eine bestehende E-Mail-Adresse löschen möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **Entfernen**.

25) Klicken Sie auf die Registerkarte **Verschiedenes**.

26) Geben Sie im Feld **Absender-E-Mail-Adresse** die E-Mail-Adresse ein, die beim Versenden einer E-Mail durch einen Agenten beim Empfänger angezeigt werden soll.

27) Wählen Sie eine der folgenden Möglichkeiten für die intelligente Anrufweiterleitung innerhalb der Warteschlange aus:

- Wenn kommende Anrufe automatisch an den Agenten weitergeleitet werden sollen, der zuletzt mit dem Anrufer verbunden war, aktivieren Sie das Kontrollkästchen **Nach letztem Agenten des Kunden suchen, wenn kein bevorzugter Agent gefunden wird**. Voraussetzung ist, dass für den Anrufer keine bevorzugten Agenten festgelegt wurden.
- Wenn kommende Anrufe nicht automatisch an den Agenten weitergeleitet werden sollen, der zuletzt mit dem Anrufer verbunden war, deaktivieren Sie das Kontrollkästchen **Nach letztem Agenten des Kunden suchen, wenn kein bevorzugter Agent gefunden wird**.

28) Klicken Sie auf **Speichern**.

18.6.2.12 Warteschlange ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlange**.

5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.

6) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

7) Ändern Sie die gewünschten Einstellungen.

8) Wählen Sie eine der folgenden Möglichkeiten für den Zustand der Warteschlange:

- Wenn Sie die Warteschlange aktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Aktiv** aus.
- Wenn Sie die Warteschlange deaktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Nicht aktiv** aus.

  Die Deaktivierung einer Warteschlange führt zur Aktivierung der Rückfalllösung durch die zugehörige UCD-Gruppe. Ist kein Agent bei der UCD-Gruppe angemeldet und kein weiteres Rufweiterschaltungsziel für die UCD-Gruppe eingetragen, wird Anrufern besetzt signalisiert.

9) Wählen Sie eine der folgenden Möglichkeiten für die Anzeige von PopUp-Fenstern in der Applikation myAgent aus:

Tipp: PopUp-Fenster sind erforderlich, um Rückrufe anzunehmen und auszuführen und um Faxe und E-Mails anzunehmen.

- Wenn bei kommenden Anrufen in myAgent ein Pop-up-Fenster zur Anzeige und Eingabe von Kundendaten erscheinen soll, aktivieren Sie das Kontrollkästchen **Pop-up-Fenster aktiviert**.
- Wenn bei kommenden Anrufen in myAgent kein Pop-up-Fenster erscheinen soll, deaktivieren Sie das Kontrollkästchen **Pop-up-Fenster aktiviert**.

10) Wählen Sie eine der folgenden Möglichkeiten für den Nachbearbeitungsmodus:

Bei Warteschlangen mit Nachbearbeitungsmodus können Agenten ihre Anrufe anhand von Nachbearbeitungscodes bestimmten Themen zuordnen (Bestellung, Reklamation, Service usw.).

- Wenn Sie für die Warteschlange den Nachbearbeitungsmodus einfache Nachbearbeitung einstellen möchten, aktivieren Sie die Option **Einfache Nachbearbeitung**.
- Wenn Sie für die Warteschlange den Nachbearbeitungsmodus mehrfache Nachbearbeitung einstellen möchten, aktivieren Sie die Option **Mehrfache Nachbearbeitung**.
- Wenn Sie für die Warteschlange keinen Nachbearbeitungsmodus einstellen möchten, aktivieren Sie die Option **Keine Nachbearbeitung**.

11) Wenn Sie die Priorität der Warteschlange ändern möchten, klicken Sie auf **Prioritäten**.

Klicken und ziehen Sie die roten Punkte im Bereich **Warteschlangen-Priorität im Verlauf der Zeit** auf die gewünschten Positionen. Die horizontale Achse zeigt die Wartezeit in der Warteschlange, die vertikale Achse die Priorität der ausgewählten Warteschlange gegenüber anderen Warteschlangen. Ist ein Agent mehreren Warteschlangen zugeordnet, kann über die Warteschlangen-Priorität festgelegt werden, ob die Anrufe für

eine Warteschlange mit höherer Priorität an diesen Agenten weitergeleitet werden sollen als die Anrufe für andere Warteschlangen.

Ziehen Sie die Scrollbalken im Bereich **Anruftyp-Prioritäten** auf die gewünschte Position. Damit legen Sie die Priorität der Anruftypen innerhalb der ausgewählten Warteschlange fest. Je weiter rechts sich der Scrollbalken befindet, desto höher ist die Priorität.

Tipp: Für Sprachanrufe sollte eine höhere Priorität als für die anderen Anruftypen gewählt werden. Ansonsten könnten wartende Anrufer durch Rückrufe, Faxe oder E-Mails verdrängt werden.

---

12) Klicken Sie auf die Registerkarte **Warteschlangen-Pilots**.

13) Wählen Sie die gewünschten Einstellungen im Bereich **Pilots für eingehende Faxnachrichten**:

- Wenn Faxe in die Warteschlange übernommen werden sollen, aktivieren Sie im Bereich **Pilots für eingehende Faxnachrichten** das oder die Kontrollkästchen des oder der gewünschten Pilots (Rufnummer(n)).
- Wenn keine Faxe in die Warteschlange übernommen werden sollen, deaktivieren Sie das oder die Kontrollkästchen im Bereich **Pilots für eingehende Faxnachrichten**.

14) Wählen Sie die gewünschten Einstellungen im Bereich **Dienst für eingehende E-Mails**:

- Wenn Sie eine neue E-Mail-Adresse einrichten möchten, klicken Sie auf **Hinzufügen**. Das Fenster **Hinzufügen** wird angezeigt.

  Wählen Sie die Authentifizierungsmethode für Ihren E-Mail-Server aus der Aufklappliste **Auth-Methode** aus. Sie können zwischen **Einfach** und **OAuth 2.0**wählen.

  Geben Sie im Feld **Server** die Bezeichnung des E-Mail-Servers ein, der für das Abholen der E-Mails verwendet werden soll (zum Beispiel `pop3.web.de`).

  Geben Sie im Feld **Port** die Portnummer des E-Mail-Servers ein (zum Beispiel `110`, die Standardportnummer für POP3).

  Wenn die Authentifizierungsmethode **Einfach** ausgewählt ist, geben Sie die Zugangsdaten für den E-Mail-Server in die Felder **Benutzername** und **Kennwort** ein.

  Wenn als Authentifizierungsmethode **OAuth 2.0** ausgewählt wurde, geben Sie den Benutzernamen für den Zugriff auf den E-Mail-Server in die Felder **Benutzername**, **Mandanten-ID**, **Anwendungs-ID** und **Client Secret** ein. Mandanten-ID, Anwendungs-ID und Client Secret entsprechen der Anwendung, die in Azure AD für die E-Mail-Warteschlangen registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator. Geben Sie den Geltungsbereich für die Anwendung in das Feld **Umfang** ein (Standardwert: https://outlook.office365.com/.default).

  Wählen Sie aus, ob der E-Mail-Versand über eine SSL (Secure Socket Layer)-Verbindung erfolgen soll: Wenn Sie eine SSL-Verbindung nutzen möchten, aktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**. (Dadurch ändert sich gegebenenfalls die Portnummer

des E-Mail-Servers. Standardportnummer für POP3 via SSL = 995). Wenn Sie keine SSL-Verbindung nutzen möchten, deaktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**.

Klicken Sie auf **Speichern**. Die neue E-Mail-Adresse wird anschließend im Bereich **Dienst für eingehende E-Mails** angezeigt.

- Wenn Sie eine bestehende E-Mail-Adresse ändern möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **Bearbeiten**. Das Fenster **Bearbeiten** wird angezeigt.

  Ändern Sie die gewünschten Parameter und klicken Sie anschließend auf **Speichern**.
- Wenn Sie eine bestehende E-Mail-Adresse löschen möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **Entfernen**.

15) Klicken Sie auf die Registerkarte **Verschiedenes**.

16) Ändern Sie die gewünschten Einstellungen.

17) Klicken Sie auf **Speichern**.

18.6.2.13 Wie Sie eine Warteschlange aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlange**.

5) Klicken Sie auf **Bearbeiten**.

6) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

7) Wählen Sie eine der folgenden Möglichkeiten für den Zustand der Warteschlange:

- Wenn Sie die Warteschlange aktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Aktiv** aus.
- Wenn Sie die Warteschlange deaktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Nicht aktiv** aus.

  Die Deaktivierung einer Warteschlange führt zur Aktivierung der Rückfalllösung durch die zugehörige UCD-Gruppe. Ist kein Agent bei der UCD-Gruppe angemeldet und kein weiteres Rufweiterschaltungsziel für die UCD-Gruppe eingetragen, wird Anrufern besetzt signalisiert.

8) Klicken Sie auf **Speichern**.

18.6.2.14 Wie Sie einen Pilot für eingehende Faxnachrichten in Warteschlangen konfigurieren

Voraussetzungen

Mindestens eine Faxrufnummer für den Empfang von Faxen liegt vor.

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer** > **UC Applications** > **Contact Center Fax**. Angezeigt werden die für Faxboxen vorgesehenen logischen Portnummern.
4) Klicken Sie im Menübaum auf die gewünschte Portnummer.
5) Klicken Sie auf die Registerkarte **Teilnehmer-Parameter ändern**.
6) Geben Sie im Feld **Rufnummer** die Rufnummer des neuen Pilots für eingehende Faxnachrichten ein.
7) Geben Sie im Feld **Name** den Namen des neuen Pilots für eingehende Faxnachrichten ein.
8) Geben Sie im Feld **Durchwahl** die Durchwahlnummer des neuen Pilots für eingehende Faxnachrichten ein.
9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Der Pilot für eingehende Faxnachrichten kann jetzt für die gewünschte Warteschlange aktiviert werden.

18.6.2.15 Wie Sie Sollwerte für Servicegrad festlegen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Servicegrad**.
5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.
6) Klicken und ziehen Sie die roten Punkte auf die gewünschten Positionen.

   Die horizontale Achse zeigt die Wartezeit in der Warteschlange in Intervallen von 10 Sekunden, die vertikale Achse den Sollwert für den Servicegrad in Prozentwerten.

   Damit geben Sie die Sollwerte für die Vermittlungsqualität der Warteschlange vor. Durch den Vergleich der Sollwerte mit den tatsächlichen Anruferwartezeiten können Qualitätsaussagen getroffen werden.
7) Klicken Sie auf **Speichern**.

18.6.2.16 Wie Sie die VIP-Anruferpriorität festlegen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **VIP-Anruferprioritäten**.
5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.
6) Klicken und ziehen Sie die roten Punkte auf die gewünschten Positionen.

   Damit definieren Sie die Priorität normaler Anrufer gegenüber VIP-Anrufern.

   Die horizontale Achse zeigt die Wartezeit in der Warteschlange in Intervallen von 30 Sekunden, die vertikale Achse die Priorität normaler Anrufer, die nicht in der VIP-Rufliste verzeichnet sind.

   Beispielsweise können Sie die roten Punkte so festlegen, dass nach 180 Sekunden eine Priorität von 100 Prozent erreicht wird. In diesem Fall werden normale Anrufer erst ab einer Wartezeit von 180 Sekunden gleichberechtigt gegenüber VIP-Anrufern behandelt. Zuvor eingehende Anrufe von VIP-Anrufern werden in der Warteschlange bevorzugt behandelt.

   Alternativ können Sie die Werte für die einzelnen Wartezeit-Intervalle auch in die Eingabefelder rechts neben dem Diagramm eingeben.
7) Klicken Sie auf **Speichern**.

18.6.2.17 Wie Sie eine VIP-Rufliste bearbeiten

Voraussetzungen

Der für die VIP-Rufliste vorgesehene Anrufer steht im externen Verzeichnis.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **VIP-Rufliste**.
5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.
6) Wählen Sie eine der folgenden Möglichkeiten:

   - Wenn Sie einen Anrufer in die VIP-Rufliste übernehmen möchten, klicken Sie im oberen Bereich des Fensters auf **Hinzufügen**. Markieren Sie den gewünschten Eintrag. Legen Sie die Priorität dieses VIP-Anrufers gegenüber anderen VIP-Anrufern fest, indem Sie den Scrollbalken auf die gewünschte Position ziehen. Je weiter rechts sich der Scrollbalken befindet, desto höher ist die Priorität.
   - Wenn Sie ein Rufnummernmuster in die VIP-Rufliste übernehmen möchten, klicken Sie im unteren Bereich des Fensters auf **Hinzufügen**. Geben Sie im Feld Muster das gewünschte Rufnummernmuster ein (zum Beispiel `089 7577*`). Legen Sie die Priorität aller VIP-Anrufer dieses Rufnummernmusters gegenüber anderen VIP-Anrufern fest, indem Sie

den Scrollbalken auf die gewünschte Position ziehen. Je weiter rechts sich der Scrollbalken befindet, desto höher ist die Priorität.

Die Eingabe von Rufnummernmustern im kanonischen Rufnummernformat ist nicht möglich. Auch die Verwendung von Abkürzungszeichen für Ländervorwahlen (zum Beispiel +49 statt 0049) ist nicht möglich. Rufnummernmuster sind immer ohne Amtskennziffer anzugeben.

Beispiel für ein Rufnummernmuster: `089 7577*` (089 = Ortskennzahl München, 7577 = Anlagenrufnummer eines Unternehmens, * = Wildcard für eine beliebige Zahl). Durch den Eintrag dieses Rufnummernmusters in die VIP-Rufliste können alle Anrufer aus München, deren Rufnummer mit 7577 beginnt, bevorzugt behandelt werden.

Folgende Zeichen können als Wildcards (Platzhalter) in einem Rufnummernmuster verwendet werden:

  - * = Wildcard für eine beliebige Zahl
  - ? = Wildcard für eine beliebige Ziffer

- Wenn Sie einen Eintrag in der VIP-Rufliste bearbeiten möchten, markieren Sie den gewünschten Eintrag und klicken Sie auf **Bearbeiten**. Ändern Sie die gewünschten Einstellungen.
- Wenn Sie einen Eintrag aus der VIP-Rufliste entfernen möchten, markieren Sie den gewünschten Eintrag und klicken Sie auf **Entfernen**.

7) Klicken Sie auf **Speichern**.

18.6.2.18 Bevorzugten Agenten festlegen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Bevorzugte Agenten**.

5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.

6) Markieren Sie den gewünschten Anrufer im Bereich **Kunden**, d. h. in der oberen der beiden Tabellen.

7) Klicken Sie auf **Agent hinzufügen**.

8) Wählen Sie den gewünschten Agenten aus und klicken Sie auf **Speichern**.

Anschließend wird der Name des ausgewählten Agenten im Bereich **Bevorzugte Agenten** angezeigt.

9) Wenn Sie einen weiteren Agenten als bevorzugten Agenten festlegen möchten, wiederholen Sie die Schritte 7 und 8.

10) Definieren Sie die Priorität der bevorzugten Agenten, falls mehrere bevorzugte Agenten festgelegt wurden. Sie haben folgende Möglichkeiten:
    - Wenn Sie eine höhere Priorität vergeben möchten, markieren Sie den gewünschten Agenten und verschieben Sie diesen über die Schaltfläche **Nach oben** auf eine höhere Listenposition.
    - Wenn Sie eine niedrigere Priorität vergeben möchten, markieren Sie den gewünschten Agenten und verschieben Sie diesen über die Schaltfläche **Nach unten** auf eine tiefere Listenposition.

18.6.2.19 Wie Sie einen bevorzugten Agenten löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Bevorzugte Agenten**.
5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.
6) Markieren Sie im Bereich **Bevorzugte Agenten** den oder die zu löschenden Agenten.
7) Klicken Sie auf **Agent entfernen**.

18.6.2.20 Contact Center-Pause hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center-Pausen**.
5) Klicken Sie auf **Hinzufügen**.
6) Geben Sie im Feld **Name** den Namen der neuen Contact Center-Pause ein.
7) Geben Sie im Feld **Dauer (Minuten)** die Dauer der neuen Contact Center-Pause in Minuten ein.
8) Aktivieren Sie das Kontrollkästchen **Aktiv**, um die neue Contact Center-Pause systemweit zu aktivieren.
9) Klicken Sie auf **Speichern**.
10) Wenn Sie eine weitere Contact Center-Pause hinzufügen möchten, wiederholen Sie die Schritte 5 bis 9.

18.6.2.21 Wie Sie eine Contact Center-Pause ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center Pausen**.
5) Markieren Sie die gewünschte Contact Center-Pause und klicken Sie auf **Bearbeiten**.
6) Ändern Sie die gewünschten Parameter.
7) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Contact Center-Pause den Agenten zur Verfügung stehen soll, aktivieren Sie das Kontrollkästchen **Aktiv**.
   - Wenn die Contact Center-Pause den Agenten nicht zur Verfügung stehen soll, deaktivieren Sie das Kontrollkästchen **Aktiv**.
8) Klicken Sie auf **Speichern**.

18.6.2.22 Contact Center-Pause löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center-Pausen**.
5) Markieren Sie die gewünschte Contact Center-Pause und klicken Sie auf **Entfernen**.

18.6.2.23 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Contact Center Nachbearbeitungs-Codes**. Angezeigt werden alle Warteschlangen für die ein Nachbearbeitungsgrund für "Einfache Nachbearbeitung" definiert wurde.
5) Klicken Sie auf **Hinzufügen**.
6) Wählen Sie in der Aufklappliste **Warteschlange** die Warteschlange aus, für die Sie einen Nachbearbeitungsgrund hinzufügen möchten.
7) Geben Sie im Feld **Beschreibung** eine Bezeichnung für den neuen Nachbearbeitungsgrund ein.
8) Klicken Sie auf **Speichern**.
9) Wenn Sie einen weiteren Nachbearbeitungsgrund hinzufügen möchten, wiederholen Sie die Schritte 5 bis 8.

18.6.2.24 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center Nachbearbeitungs-Codes**. Angezeigt werden alle Warteschlangen für die ein Nachbearbeitungsgrund für "Einfache Nachbearbeitung" definiert wurde.
5) Markieren Sie den gewünschten Eintrag und klicken Sie auf **Bearbeiten**.
6) Wenn Sie dem Nachbearbeitungsgrund einer anderen Warteschlange zuweisen möchten, wählen Sie in der Aufklappliste **Warteschlange** die neue Warteschlange aus.
7) Wenn Sie die Bezeichnung des Nachbearbeitungsgrunds ändern möchten, geben Sie im Feld **Beschreibung** die neue Bezeichnung ein.
8) Klicken Sie auf **Speichern**.

18.6.2.25 Nachbearbeitungsgrund für "Einfache Nachbearbeitung" löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center Nachbearbeitungs-Codes**. Angezeigt werden alle Warteschlangen für die ein Nachbearbeitungsgrund für "Einfache Nachbearbeitung" definiert wurde.
5) Markieren Sie die gewünschte Regel und klicken Sie auf **Entfernen**.

18.6.2.26 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Mehrfache Nachbereitungscode**.
5) Wählen Sie die gewünschte Warteschlange in der Dropdown-Liste **Contact Center-Warteschlange** aus. Angezeigt werden die für diese Warteschlange bereits definierten Gruppen und Untergruppen.

   Anmerkung: Unterhalb jeder Gruppe oder Untergruppe (falls vorhanden) sollte ebenfalls mindestens ein Element konfiguriert werden, damit der Agent einen Anruf abschließen kann. Der Abbruch eines Anrufs ist nicht möglich, wenn eine Gruppe oder Untergruppe leer ist.

   ---

6) Wenn Sie den neuen Nachbearbeitungsgrund in einer Gruppe mit weiteren Nachbearbeitungsgründen zusammenfassen möchten, wählen Sie eine der folgenden Möglichkeiten:

   - Wenn Sie den neuen Nachbearbeitungsgrund einer bestehenden Gruppe oder Untergruppe zuweisen möchten, wählen Sie die gewünschte Gruppe oder Untergruppe aus und klicken Sie auf **Element hinzufügen**. Geben Sie im Feld **Neues Nachbearbeitungselement** eine Bezeichnung für den neuen Nachbearbeitungsgrund ein und klicken Sie auf **OK**.
   - Wenn Sie den neuen Nachbearbeitungsgrund einer neuen Gruppe zuweisen möchten, klicken Sie auf **Gruppe hinzufügen**. Geben Sie im Feld **Gruppenname** eine Bezeichnung für die neue Gruppe ein und klicken Sie auf **OK**.

     Wählen Sie die neue Gruppe aus und klicken Sie auf **Element hinzufügen**. Geben Sie im Feld **Neues Nachbearbeitungselement** eine Bezeichnung für den neuen Nachbearbeitungsgrund ein und klicken Sie auf **OK**.
   - Wenn Sie den neuen Nachbearbeitungsgrund einer neuen Untergruppe zuordnen möchten, wählen Sie die gewünschte Gruppe aus und klicken Sie auf **Gruppe hinzufügen**. Geben Sie im Feld **Gruppenname** eine Bezeichnung für die neue Untergruppe ein und klicken Sie auf **OK**.

     Wählen Sie die neue Untergruppe aus und klicken Sie auf **Element hinzufügen**. Geben Sie im Feld **Neues Nachbearbeitungselement** eine Bezeichnung für den neuen Nachbearbeitungsgrund ein und klicken Sie auf **OK**.

7) Wenn Sie einen weiteren Nachbearbeitungsgrund hinzufügen möchten, wiederholen Sie die Schritte 5 und 6.

18.6.2.27 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Mehrfach-Nachbearbeitung Code**.
5) Wählen Sie in der Aufklappliste **Contact Center-Warteschlange** die gewünschte Warteschlange aus. Angezeigt werden die für diese Warteschlange bereits definierten Gruppen und Untergruppen.
6) Markieren Sie die Gruppe oder Untergruppe, der der zu ändernde Nachbearbeitungsgrund zugeordnet ist. Angezeigt werden alle Nachbearbeitungsgründe (Elemente), die dieser Gruppe zugeordnet sind.
7) Markieren Sie den zu ändernden Nachbearbeitungsgrund und klicken Sie auf **Element umbenennen**.
8) Geben Sie im Feld **Nachbearbeitungscode umbenennen** eine neue Bezeichnung für den Nachbearbeitungsgrund ein und klicken Sie auf **OK**.
9) Wenn Sie die Bezeichnung der Gruppe oder Untergruppe ändern möchten, klicken Sie auf **Gruppe umbenennen**.
10) Geben Sie im Feld **Gruppenname** eine neue Bezeichnung für die Gruppe oder Untergruppe ein und klicken Sie auf **OK**.

18.6.2.28 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Mehrfach-Nachbearbeitung Code**.
5) Wählen Sie in der Aufklappliste **Contact Center-Warteschlange** die gewünschte Warteschlange aus. Angezeigt werden die für diese Warteschlange bereits definierten Gruppen und Untergruppen.
6) Markieren Sie die Gruppe oder Untergruppe, der der zu löschende Nachbearbeitungsgrund zugeordnet ist. Angezeigt werden alle Nachbearbeitungsgründe (Elemente), die dieser Gruppe zugeordnet sind.
7) Markieren Sie den zu löschenden Nachbearbeitungsgrund und klicken Sie auf **Element entfernen**.
8) Wenn Sie die Gruppe oder Untergruppe löschen möchten, klicken Sie auf **Gruppe entfernen**.

18.6.2.29 Warteschlange einen Agenten zuordnen

Mit dem Wizard **Contact Center** können Sie Agenten einer oder mehreren Warteschlangen zuordnen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Warteschlangen-Bindungen**. Alle vorhandenen Warteschlangen werden angezeigt.
5) Wählen Sie die Warteschlange aus, der Sie einen Agenten zuweisen möchten, und klicken Sie auf **Bearbeiten**. Alle bereits zugeordneten Agenten werden angezeigt.
6) Klicken Sie auf **Hinzufügen**, um den entsprechenden Agenten der gewünschten Warteschlange hinzuzufügen. Daraufhin wird das Fenster **Hinzufügen** angezeigt.
7) Wählen Sie eine der folgenden Optionen:
   - Wenn der Agent Anrufe unabhängig von der Auslastung der Warteschlange entgegennehmen soll, wählen Sie in der Aufklappliste **Typ** die Option **Hauptagent**.
   - Wenn der Agent nur dann Anrufe erhalten soll, wenn die Warteschlange überläuft, wählen Sie in der Aufklappliste **Typ** die Option **Agent bei Überlauf**.
8) Wenn Sie **Agent bei Überlauf** gewählt haben:
   a) Geben Sie im Feld **Überlauf nach Sekunden in Wartes.** die Zeit ein, nach deren Ablauf ein Anruf an einen Agenten bei Überlauf weitergeleitet werden soll.
   b) Geben Sie im Feld **Überlauf nach Anrufen in Wartes.** die Maximalzahl von Anrufen ein. Ein Agent bei Überlauf erhält Anrufe, die über diese Maximalzahl hinausgehen.
9) Stellen Sie einen Prozentwert für das **Fähigkeits-Level** des Agenten ein.

   Durch das Fähigkeits-Level steuern Sie die Verteilung der Anrufe auf die Agenten in einer Warteschlange. Agenten mit höherem Fähigkeits-Level werden bei der Anrufverteilung bevorzugt. Haben alle Agenten das gleiche Fähigkeits-Level, erhält der am längsten freie Agent den Anruf.
10) Wählen Sie eine der folgenden Optionen:
    - Wenn der Agent Rückrufwünsche in Form von Sprachnachrichten erhalten soll, aktivieren Sie das Kontrollkästchen **Agentenrückruf aktivieren**.
    - Wenn der Agent keine Rückrufwünsche erhalten soll, deaktivieren Sie das Kontrollkästchen **Agentenrückruf aktivieren**.
11) Geben Sie im Feld **Nachbearbeitung** die automatische Nachbearbeitungszeit in Sekunden für den Agenten in dieser Warteschlange ein.
12) Klicken Sie auf **Speichern**.

13) Wenn Sie den Warteschlangen weitere Agenten zuordnen möchten, wiederholen Sie die Schritte 5 bis 12.

18.6.2.30 Agenten aus einer Warteschlange entfernen

Mit dem Wizard **Contact Center** können Sie Agenten aus einer oder mehreren Warteschlangen entfernen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Warteschlangen-Bindungen**. Alle vorhandenen Warteschlangen werden angezeigt.
5) Wählen Sie die Warteschlange aus, aus der Sie einen Agenten entfernen möchten, und klicken Sie auf **Bearbeiten**. Alle bereits zugeordneten Agenten werden angezeigt.
6) Wählen Sie den gewünschten Agenten aus und klicken Sie auf **Entfernen**.
7) Wenn Sie weitere Agenten aus Warteschlangen entfernen möchten, wiederholen Sie die Schritte 5 und 6.

18.7 Hinweise zum Einsatz des Contact Centers

Hier erhalten Sie Informationen über Besonderheiten und mögliche Einschränkungen beim Einsatz des Contact Centers.

18.7.1 Einschränkungen beim Betrieb des Contact Centers

Für den Betrieb des Contact Centers gelten bestimmte Bedingungen. Darüber hinaus kommt es zu Einschränkungen bei der Nutzung von System-Leistungsmerkmalen durch Agenten.

Bedingungen für den Betrieb des Contact Centers

Folgende Bedingungen für den Betrieb des Contact Centers sind zu beachten:

- Leitungen

  Das Contact Center unterstützt keine analogen Amtsleitungen (HKZ). Alle externen Verbindungen des Contact Centers müssen über ISDN oder über IP-Telefonie erfolgen. Zu beachten ist, dass die Anbindung über IP-Telefonie ausschließlich über zertifizierte Internet-Telefonie-Service-Provider ITSP möglich ist.
- Vernetzung

  Bei einer Vernetzung müssen alle Agenten an dem Kommunikationssystem angeschlossen sein, in dem das Contact Center konfiguriert ist.

- Agententelefone

  Agenten können alle Systemtelefone (IP-Telefone (HFA), wie zum Beispiel OpenStage 40 oder $U_{P0/E}$-Telefone, wie zum Beispiel OpenStage 40 T) und DECT-Telefone nutzen. Zu beachten ist, dass ausschließlich die aktuell für den Betrieb mit OpenScape Business Cordless freigegeben DECT-Telefone eingesetzt werden dürfen.

  Die Verwendung von analogen, ISDN- und SIP-Telefonen ist nicht möglich.

  Agenten dürfen nicht Mitglied einer Gruppe (Gruppenruf, Sammelanschluss) oder eine MULAP sein. Diese Einschränkung gilt auch für die in Verbindung mit MULAPs genutzten System-Leistungsmerkmale "Teamschaltung (Team-Gruppe)", "Chef/Sekretär (Top-Gruppe)" und "Mobility Entry".
- myAgent

  myAgent sollte nicht simultan mit anderen UC-Clients genutzt werden, da eine gegenseitige Beeinflussung des Anwesenheitsstatus nicht ausgeschlossen ist (siehe Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients). Im Normalbetrieb des Contact Centers verwenden Agenten ausschließlich myAgent, um ihren Status zu ändern (Anmelden, Abmelden, Verfügbar usw.).
- Anschaltung von Applikationen über die CSTA-Schnittstelle

  Sofern die folgende Bedingungen eingehalten werden, ist eine Anschaltung von Applikationen über die CSTA-Schnittstelle möglich:

  – Die Applikation darf keine nennenswerte Zusatzlast auf der CSTA-Schnittstelle erzeugen.

    Dementsprechend ist die Anschaltung von Unified-Communications- oder Anrufverteil-Lösungen, CTI-Power-Dialern oder auch CTI-Lösungen mit vielen intensiv genutzten CTI-Einzel-Clients nicht zugelassen.
  – Die Applikation darf über die CSTA-Schnittstelle keine Agententelefone steuern oder Umleitungen für die Agententelefone einrichten.

    Dementsprechend ist die Anschaltung von CTI-Applikationen für Agenten, Regelassistenten oder Personal Assistants nicht zugelassen.

  Die Anschaltung von TAPI 120/170 ist prinzipiell freigegeben. Für die Belastung des Kommunikationssystems gelten die gleichen Bedingungen, wie für die Anschaltung anderer Applikationen über die CSTA-Schnittstelle. In Verbindung mit dem Contact Center sollte TAPI 120/170 vorzugsweise zur Anbindung von CRM (Customer Relationship Management)-/ERP (Enterprise Ressource Planning)-Systemen verwendet werden, sofern diese TAPI unterstützen.

Einschränkungen bei der Nutzung von System-Leistungsmerkmalen

Die nachfolgend genannten System-Leistungsmerkmale stehen für Agenten nicht oder nur mit Einschränkungen zur Verfügung. Diese Leistungsmerkmale sind aber für Agenten nicht zwingend notwendig, da die Zuteilung von Anrufen automatisch durch das Contact Center erfolgt. Die Zuteilung ist abhängig von den eingestellten Regeln und der Verfügbarkeit der Agenten.

- Gesperrte Leistungsmerkmale

  Die Aktivierung von System-Leistungsmerkmalen über myAgent und über das zugehörige Agententelefon wird für verfügbare Agenten des Contact

Centers nicht unterstützt. Agenten können System-Leistungsmerkmale ausschließlich über myAgent aktivieren.

Die folgenden System-Leistungsmerkmale werden deshalb in Verbindung mit myAgent nicht unterstützt:

- Anklopfen
- Zweitanruf
- Parken
- Gruppenruf
- Anrufschutz (für angemeldete Agenten)
- Aufschalten auf ein Agentengespräch (Ausnahme: Agenten mit dem Berechtigungs-Level Supervisor oder Administrator)
- Leistungsmerkmale, die das Anruf-Routing betreffen und aktive Gesprächsverbindungen

• Leistungsmerkmale mit Auswirkungen auf das Anruf-Routing

Folgende Leistungsmerkmale können zu einer Veränderung des Anruf-Routings im Contact Center führen und sollten deshalb von Agenten nicht ausgeführt werden.

- Anrufumleitung

  Aktiviert ein angemeldeter Agent eine Anrufumleitung, erfolgt eine Abmeldung.

  Eine Anrufumleitung wird deaktiviert, sobald sich ein Agent an einer Warteschlange anmeldet.
- Anrufschutz

  Aktiviert ein angemeldeter Agent den Anrufschutz über einen UC Client, erfolgt eine Abmeldung.

  Anrufschutz wird deaktiviert, sobald sich ein Agent an einer Warteschlange anmeldet.
- Relocate/Rufnummerntausch

  Durch das Umziehen eines Telefons wird die logische Zuordnung der Rufnummern verändert. Die neue Rufnummernzuordnung wird erst nach einem Restart (Neustart) des Contact Centers übermittelt.
- Nachtschaltung

  Bei der Einrichtung einer Nachtschaltung im Kommunikationssystem ist darauf zu achten, dass die Konfiguration der Contact-Center-relevanten Parameter (Agenten, Warteschlangen usw.) für den Tag- und Nachtbetrieb identisch ist.

- Leistungsmerkmale mit Auswirkungen auf Berichte

  Die Ausführung folgender Leistungsmerkmale von einem Agenten-Telefon kann zu einer Verfälschung von Berichten führen:

  – Anrufübernahme von Contact-Center-Anrufen durch Nicht-Agenten
  – Anrufübergabe (zum Beispiel über Direktruftaste) von Contact-Center-Anrufen an Nicht-Agenten
  – Konferenz
  – Makeln
  – Parken

  Tipp: Das Leistungsmerkmal "Rückfrage" ist für die Darstellung von Contact-Center-Anrufen in Berichten neutral und kann durch Agenten genutzt werden, unabhängig vom Rückfrageziel.

- Für Agenten nicht sinnvolle Funktionen

  Folgende Funktionen sind nicht sinnvoll, da für Agenten das Leistungsmerkmal "Anklopfen" gesperrt ist.

  – Vermittlungsplatz
  – Hotline-Ziel

18.8 Hinweise zum Einsatz von DECT-Telefonen

DECT-Telefone können als Telefone für Contact-Center-Agenten eingesetzt werden. Unterschiede bei der Bedienprozedur gegenüber schnurgebundenen Telefonen sind dabei zu beachten.

Voraussetzungen für den Einsatz von DECT-Telefonen

- Ausschließlich die aktuell für den Betrieb mit HiPath Cordless Office und OpenScape Business Cordless freigegeben DECT-Telefone dürfen verwendet werden.
- Der Bereich, in dem sich die Contact-Center-Agenten bewegen, muss eine lückenlose Funkabdeckung bieten.
- Die Anzahl der Basisstation muss so bemessen sein, dass genügend B-Kanäle für die DECT-Telefone der Contact-Center-Agenten zur Verfügung stehen.
- Ein Contact-Center-Agent sollte den Funkbereich möglichst nicht verlassen, während er an einer Warteschlange des Contact Centers angemeldet ist.

Unterschiede bei der Bedienprozedur gegenüber schnurgebundenen Telefonen

- Das Anmelden an einer Warteschlange des Contact Centers ist ausschließlich über myAgent möglich.
- Im Display eines DECT-Telefons werden keine Meldungen angezeigt, wie zum Beispiel **Verfügbar** oder **Pause**.
- Die Steuerung eines DECT-Telefons über myAgent (zum Beispiel über den Bereich **Telefonie** des myAgent-Hauptfensters oder über das PopUp-Fenster des ankommenden myAgent-Anrufs) ist nicht möglich.

- Die Annahme eines ankommenden Anrufs ist ausschließlich über das DECT-Telefon möglich.
- Ein gehender Anruf muss über das DECT-Telefon initiiert werden.

Zu berücksichtigende Effekte beim Einsatz von DECT-Telefonen:

- Suchzeit

  Bei einem ankommenden Anruf kann die Zeit bis zum Finden des DECT-Telefons mehrere Sekunden (im ungünstigsten Fall bis zu 20 Sekunden) betragen, bevor ein Anruf am DECT-Telefon signalisiert wird. Während der Suchzeit hört der Anrufer den Rufton.

  Das Contact Center wertet diese Zeit als Zeit bis zur Anrufannahme. Die eigentliche Zeit bis zur Anrufannahme durch einen Contact-Center-Agenten setzt sich damit aus der Suchzeit und der Klingeldauer zusammen.

  Verlässt ein Contact-Center-Agent mit seinem DECT-Telefon den Funkbereich, können sich längere Suchzeiten ergeben.
- DECT-Telefon nicht auffindbar

  Überschreitet ein Contact-Center-Anruf die vorgegebene Zeit bist zur Rufannahme durch den Agenten (Contact-Center-Agent befindet sich beispielsweise außerhalb des Funkbereichs), wird der Agent automatisch von der oder den Warteschlangen abgemeldet. Das Wiederanmelden ist ausschließlich über myAgent möglich.

18.9 Berichte

Anhand von Berichten kann der aktuelle Status des Contact Centers ermittelt und die Stärken und Schwächen der zugehörigen Komponenten analysiert werden. Das ermöglicht beispielsweise eine Optimierung der Contact-Center-Konfiguration und einen effizienteren Einsatz der Contact-Center-Ressourcen. Das Contact Center stellt Anwendern sowohl Echtzeit-Berichte als auch historische Berichte zur Verfügung.

Echtzeit-Berichte

Echtzeit-Berichte werden ständig aktualisiert. Sie liefern wichtige Informationen, wie zum Beispiel Angaben zur Agenten-Auslastung, zum Servicegrad, zu Abbruchraten und zu durchschnittlicher Bearbeitungszeiten. Anhand der fortwährend aktualisierten und filterbaren Anruferlisten kann der Verlauf eines Kundenkontakts schrittweise untersucht werden. Darüber hinaus ist die Prüfung der Aktivitäten aller Agenten möglich. Diese Informationen können beispielsweise für Schulungszwecke, Kontaktprüfungs- und Nachverfolgungsaktivitäten eingesetzt werden.

Agenten mit dem Berechtigungs-Level Supervisor oder Administrator können akustisch und visuell darüber informiert werden, wenn definierbare Betriebsmessgrößen überschritten werden. Die Festlegung der entsprechenden Schwellwerte ist für jede Warteschlange individuell möglich.

Historische Berichte

Durch die Auswahl von Datenelementen und benutzerspezifischen Berichtsparametern können historische Berichte schnell eingerichtet und in Grafik- oder Tabellenform abgerufen werden.

Über die Applikation myAgent können mehr als 20 vordefinierte Berichtsvorlagen für Standardberichte genutzt werden.

Der optional einsatzbare Applikation myReports erweitert die Möglichkeiten zur Erstellung historischer Berichte durch über 100 vordefinierte Berichtsvorlagen. Die Berichtserstellung kann individuell geplant und die erstellten Berichte können zu festgelegten Zeiten in gängigen Exportformaten automatisch an zuvor festgelegte E-Mail-Empfänger versendet oder an einem vom myReports-Administrator konfigurierten Speicherort abgelegt werden.

Tipp: Berichte basieren auf der im Kommunikationssystem gespeicherten Anrufhistorie. Die maximale Aufbewahrungsdauer der Anrufhistorie beträgt 365 Tage (Standardeinstellung). Ein Administrator mit dem Profil **Expert** kann die Aufbewahrungsdauer der Anrufhistorie systemweit einstellen.

Beispiel: Die Aufbewahrungsdauer wurde auf 100 Tage eingestellt. Für die Erstellung von Berichten kann damit auf Daten zurückgegriffen werden, die maximal 100 Tage alt sind.

Datenschutz

Hat der myReports-Administrator bei der Konfiguration von myReports den Datenschutz aktiviert, werden in allen betreffenden Berichten die letzten vier Stellen der Rufnummern (Spalte CLI) durch **** ersetzt.

Hat ein interner Teilnehmer seine private Rufnummer, Mobilrufnummer, externe Rufnummer 1 und/oder externe Rufnummer 2 als nicht sichtbar gekennzeichnet, werden diese Rufnummern in allen betreffenden Berichten nicht angezeigt.

18.9.1 Vordefinierte Berichtsvorlagen

myReports stellt mehr als 100 vordefinierte Berichtsvorlagen zur Verfügung, um Berichte zu erstellen.

Diese Vorlagen sind folgenden Themengebieten (Berichtgruppen) zugeordnet:

- **Agententätigkeit**
- **Agenten**
- **CLI**
- **Anrufhistorie**
- **Anrufe**
- **Fax / E-Mail**
- **Andere**
- **Leistung**
- **Warteschlangen**
- **Benutzer-Anwesenheitsstatus**
- **Nachbearbeitungscodes**

19 Mobility

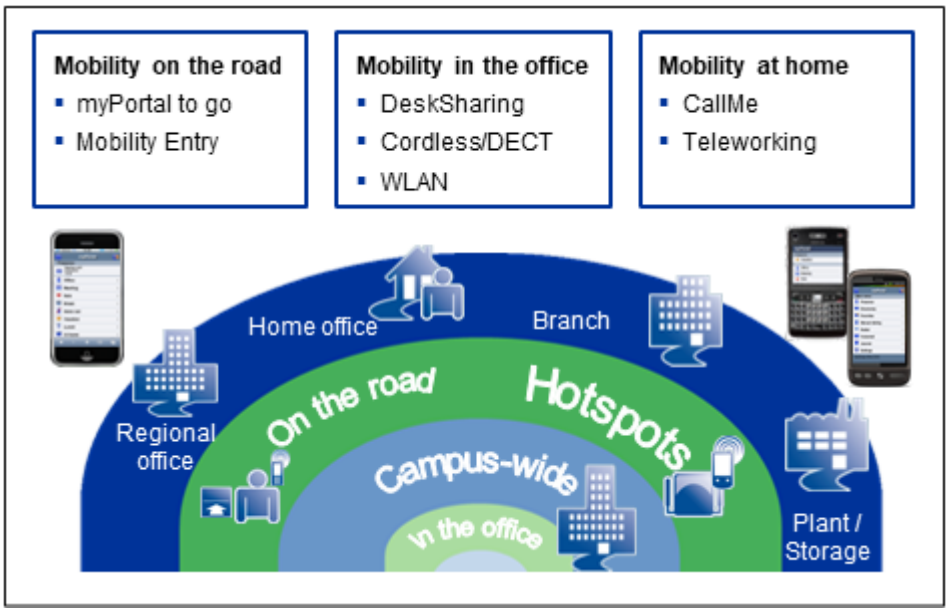
OpenScape Business bietet integrierte Mobilitätslösungen für jedes Unternehmen. Dies beinhaltet z.B. die Einbindung von Mobiltelefonen/ Smartphones, die Nutzung von Cordless/DECT- und WLAN-Telefonen bis hin zu DeskSharing und Teleworking. Mobility umfasst Mobilität unterwegs, Mobilität im Büro und Mobilität zu Hause.

Zugehörige Konzepte

Teilnehmer auf Seite 428

19.1 Integrierte Mobilitätslösungen

Die im Kommunikationssystem integrierten Mobilitätslösungen bieten effiziente Kommunikation überall und mit unterschiedlichsten Endgeräten.



19.2 Mobilität unterwegs

Mobilität unterwegs wird erreicht über die Mobiltelefon-Integration über myPortal to go oder Mobility Entry. Über den One Number Service ist der Teilnehmer weltweit unter einer Rufnummer erreichbar. Über Dual-Mode-Telefonie können zusätzlich Kosten gespart werden, wenn sich der Teilnehmer in Reichweite eines WLAN befindet.

Mobilität unterwegs ist die Kombination von:

- Bürotelefon und Smartphone (myPortal to go)
  - Erreichbarkeit unter einer Rufnummer (One Number Service)
  - Steuerung von Leistungsmerkmalen über Web-Client
  - UC-Funktionen wie z.B. Steuerung des Anwesenheitsstatus

- Bürotelefon und Mobiltelefon (Mobility Entry)
  - Erreichbarkeit unter einer Rufnummer (One Number Service)
  - Steuerung von Leistungsmerkmalen über DTMF-Codes

Neben der Kombination von Mobiltelefon und Bürotelefon ist es auch möglich, ein Mobiltelefon alleine (d.h. ohne paralleles Bürotelefon) für die Erreichbarkeit unter einer Festnetznummer zu konfigurieren.

Der volle Funktionsumfang wird mit Systemtelefonen (HFA) erreicht. SIP-Telefone können mit Einschränkungen verwendet werden.

19.2.1 myPortal to go

myPortal to go ist eine leistungsfähige Unified Communications Anwendung für Smartphones und Tablet-PCs und bietet den Teilnehmern Zugriff auf die Unified Communications Leistungsmerkmale des Kommunikationssystems. Neben komfortablen Wahlhilfen über Verzeichnisse und Favoriten sowie Informationen über den Anwesenheitsstatus von Kollegen wird auch der Zugriff z. B. auf Sprachnachrichten zur Verfügung gestellt.

myPortal to go gibt es in drei Varianten:

- als Mobile UC App für das Betriebssystem Android (Version 5.0 oder höher)
- als Mobile UC App für das Betriebssystem Apple iOS (Version 12.5 oder höher)
- als Web Edition für mobile Web-Browser mit HTML5-Unterstützung, z. B. für die Betriebssysteme Windows Phone (Version 8.0 oder höher) oder Blackberry (Version 10 oder höher):

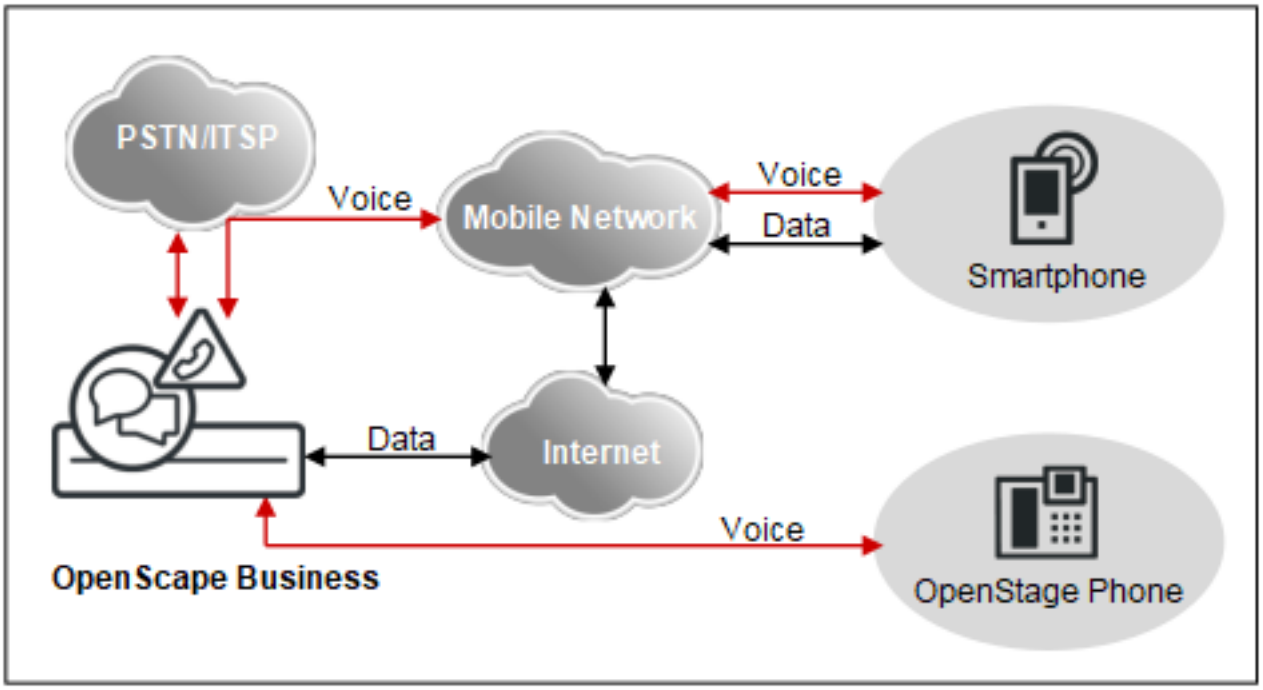
  `http://<IP-Adresse des Kommunikationssystems>:8801`

  `https://<IP-Adresse des Kommunikationssystems>:8802`

  Aus Sicherheitsgründen wird empfohlen ausschließlich https zu verwenden. Dafür muss im Router ein Port Forwarding von extern TCP/443 nach intern TCP/8802 eingerichtet werden.

  Anmerkung: Bitte beachten Sie, dass bei Verwendung von myPortal to go Web Edition im Tischtelefon-Betriebsmodus keine Telefonie über den Client möglich ist. Sie können Anrufe tätigen, aber die Payload wird durch das verbundene Telefon geleitet.

myPortal to go kann sowohl auf reinen GSM-Mobiltelefonen als auch auf Dual-Mode-Telefonen genutzt werden. Für die Nutzung von myPortal to go ist ein Mobilfunkvertrag mit Datenoption (Flatrate empfohlen) erforderlich.



Der Leistungsumfang ist für die Varianten bis auf wenige Ausnahmen (z. B. Zugriff auf Kontaktdaten im Mobiltelefon) identisch.

myPortal to go unterstützt folgende Leistungsmerkmale:

- Anwesenheitsstatus
- Statusbezogene Anrufumleitung
- CallMe-Dienst (nur mit UC Suite)
- Verzeichnisse
- Favoritenliste
- Journal
- Rufnummern- und Namenssuche
- Anruffunktionen
- One Number Service (ONS)
- Voicemail
- Textnachrichten

CTI-Leistungsmerkmale während eines Gesprächs:

- Rückfrage
- Makeln
- Attendant
- Konferenzschaltung
- Trennen

myPortal to go kann mit beiden UC-Lösungen UC Smart und UC Suite verwendet werden. Je nach UC-Lösung und den Ihnen zugeordneten Lizenzen kann das Angebot der Leistungsmerkmale leicht variieren.

myPortal to go unterstützt folgende Betriebsarten:

- Mobiler Benutzer:

  Uneingeschränkter Zugriff auf die Telefonie- und UC-Leistungsmerkmale unabhängig von Standort (inkl. One Number Service).

- Office-Benutzer:

  Nutzung der UC-Leistungsmerkmale und als Komfort-Wahlhilfe für das Bürotelefon (ohne One Number Service).

Weitere Leistungsmerkmale können Sie mit den UC Clients (z. B. myPortal for Desktop) nutzen.

myPortal to go stellt eine verschlüsselte Verbindung (https) zum OpenScape Business UC Server her. Ist die Verbindung unterbrochen (Offline-Modus) können Sie noch zwischengespeicherte Einträge aus dem Journal und der Favoritenliste per GSM wählen sowie eine manuelle GSM-Wahl ausführen.

Anmerkung: Zur Unterstützung der Mobilität muss myPortal to go zunächst als VoIP (HFA) Benutzer registriert werden, damit der für OpenScape Business System relevante Port aktiv wird.

Wahlverfahren von myPortal to go

Für gehende Gespräche kann der Smartphone-Teilnehmer abhängig von der Betriebsart zwischen unterschiedlichen Wahlverfahren wählen:

- Call through (nur in der Betriebsart Mobiler Benutzer)
- Callback bevorzugt (nur in der Betriebsart Mobiler Benutzer)
- Assoziierte Wahl (nur in der Betriebsart Office-Benutzer)

  myPortal to go steuert den Verbindungsaufbau für das Telefon am Arbeitsplatz. Wird über die assoziierte Wahl ein SIP-Telefon oder ein SIP-Softclient gesteuert, stehen einige CTI-Leistungsmerkmale wie Rückfrage und Konferenz nicht zur Verfügung.

19.2.1.1 Voraussetzungen:myPortal to go

Um myPortal to go zu nutzen muss das Smartphone über geeignete Hardware und Software verfügen.

Es gelten folgende Anforderungen:

- myPortal to go als Mobile UC App: Android-Betriebssystem (Version 5.0 oder höher) oder Apple iOS (Version 12.5 oder höher)
- myPortal to go als Web Edition: Für mobile Web-Browser mit HTML5-Unterstützung, z.B. für Betriebssysteme Windows Phone (Version 8.1 oder höher) oder Blackberry (Version 10 oder höher). Webbrowser ohne TLS 1.2-Unterstützung werden nicht mehr unterstützt.

  Für den Zugriff muss im Router ein Port Forwarding von extern TCP/443 nach intern TCP/8802 (https) oder TCP/8801 (http) eingerichtet werden. Aus Sicherheitsgründen wird empfohlen ausschließlich https zu verwenden.
- myPortal to go iOS-Client:
  - Es muss ein geeigneter DNS-Server konfiguriert und Internetzugang gewährt werden, damit öffentliche Domänennamen aufgelöst werden können und Push-Benachrichtigungen über die APNS-Server von Apple an das iOS-Gerät gesendet werden können.
  - Wenn die Firewall des Unternehmens den ausgehenden Internetzugang einschränkt, stellen Sie sicher, dass die Firewall für APNS auf Port TCP/443 offen ist.

  - Für iOS-Push-Benachrichtigungen ist es zwingend erforderlich, die Systemsoftware auf dem neuesten Stand zu halten, da die obligatorischen Zertifikate für die Kommunikation mit dem APNS-Dienst von Apple häufig mit größeren/kleineren Systemversionen und Korrekturversionen aktualisiert werden.
  - Die neuesten Versionen von myPortal to go (iOS) unterstützen die CallKit API von Apple. CallKit ist ein Framework, das darauf abzielt, das VoIP-Erlebnis zu verbessern, indem es myPortal to go (iOS) ermöglicht, sich in die nativen Anruffunktionen des Geräts zu integrieren. Die erforderliche Mindestversion der Systemsoftware ist V3R2.

    Aktuelle myPortal to go (iOS) Clients können sich nicht bei älteren OpenScape Business Versionen anmelden.
  - Für die Verbindung zum Kommunikationsserver gelten die iOS-Sicherheitsanforderungen. Das aktuelle, von Openscape Business automatisch generierte, selbstsignierte Zertifikat ist nicht ausreichend, wenn die Anwendung eine Verbindung zum Kommunikationsserver über einen Domänennamen statt über eine Server-IP-Adresse herstellt. Apple hat seine Sicherheitsanforderungen für TLS-Serverzertifikate überarbeitet https://support.apple.com/de/HT210176.

    Um Probleme zu vermeiden, wenn myPortal to go (iOS) keine Verbindung zum Kommunikationsserver herstellen kann, empfehlen wir, sich entweder über die IP-Adresse mit dem Kommunikationsserver zu verbinden oder ein vertrauenswürdiges SSL-Zertifikat auf der Serverseite zu installieren.
- Touchscreen (empfohlen für komfortable Bedienung)
- Display-Auflösung für Smartphones: mindestens 240 Pixel * 320 Pixel (empfohlen: 320 Pixel * 480 Pixel oder höher)
- Display-Auflösung für Tablet-PCs: mindestens 800 Pixel * 480 Pixel (empfohlen: 1024 Pixel * 600 Pixel oder höher)
- Internet-Zugang
- Unterstützung der gleichzeitigen Übertragung von Sprache und Daten durch Mobiltelefon und Mobilnetz
- Eine stabile 3G/4G/5G-Datenverbindung. Bitte beachten Sie, dass langsame Verbindungen – insbesondere 2G/EDGE/GPRS zu einer schlechten Benutzererfahrung und Funktionseinschränkungen (VoIP) führen können.

  Alternativ: reine WLAN-Verbindung mit einem SIP-Client für Telefonie.
- Eine Datenflatrate wird dringend empfohlen.

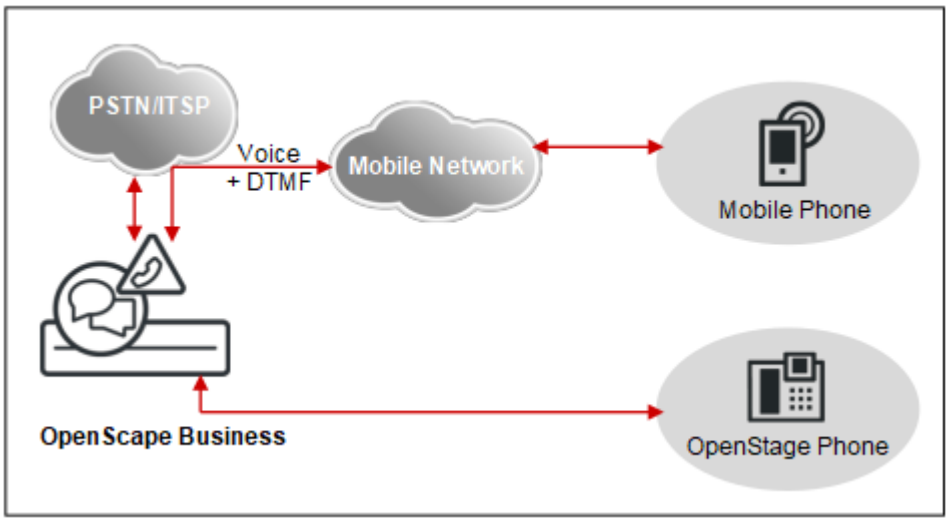
Die Mobile UC App kann kostenfrei im Google Play Store oder im Apple App Store heruntergeladen werden.

Abhängig vom verwendeten Gerät und Betriebssystem können Bedienkomfort oder Funktion beeinflusst werden. Support wird nur geleistet, wenn ein Problem mit einem Referenzgerät nachweisbar ist. Informationen zu den Referenzgeräten, Browsern und Betriebssystemen finden Sie in der Freigabemitteilung und im Experten-Wiki unter `https://wiki.unify.com/wiki/myPortal_to_go`.

19.2.2 Mobility Entry

Durch Mobility Entry können Mobiltelefone integriert werden. Dadurch hat der Teilnehmer über das Mobiltelefon Zugriff auf bestimmte System-Leistungsmerkmale.

Mobility Entry ermöglicht nach Einwahl die Steuerung von Sprachverbindungen über DTMF.



Wahlverfahren von Mobility Entry

Für gehende Gespräche kann der Mobiltelefon-Teilnehmer zwischen unterschiedlichen Wahlverfahren wählen.

Mobility Entry bietet folgende Wahlverfahren:

- Rückruf
- Call Through

Ruft bei Callback der Mobiltelefon-Teilnehmer am Kommunikationssystem eine spezielle Durchwahlnummer an, dann wird der Anruf noch vor dem Aufbau der Verbindung automatisch getrennt und es wird sofort ein Rückruf (Callback) durchgeführt. Nach dem Rückruf ist keine weitere Autorisierung notwendig. Der Mobiltelefon-Teilnehmer kann über das Kommunikationssystem interne und externe Anrufe durchführen sowie alle Mobility-Leistungsmerkmale nutzen.

Voraussetzungen für Callback sind:

- Die externe Rufnummer des anrufenden Telefons ist am Kommunikationssystem registriert und konfiguriert. Wenn nicht, wird der Anruf getrennt und kein Rückruf durchgeführt
- Die DISA-Durchwahlnummer ist konfiguriert.
- Die externe Rufnummer des Mobiltelefon-Teilnehmers wird zum Kommunikationssystem übertragen (CLIP-Information).

Leistungsmerkmale im Ruhezustand

- Rufnummer wählen
- Anrufumleitung programmieren oder löschen
- Anrufschutz aktivieren oder deaktivieren
- Info senden
- Alle Dienste zurücksetzen
- Rufnummernunterdrückung (CLIR) ein- oder ausschalten

Leistungsmerkmale im Gesprächszustand

- Rückfrage

- Makeln
- Konferenz
- Trennen und zurück zum Wartenden
- Rückruf aktivieren
- MFV-Nachwahl ermöglichen

Zur Signalisierung der Leistungsmerkmale werden System-Kennzahlen verwendet (z.B. *1 für Anrufumleitung programmieren).

Anmerkung: Für Mobility Entry-Teilnehmer muss das Teilnehmer-Flag **DISA Berechtigung** aktiviert sein.

Bei OpenScape Business X stehen maximal 16 DTMF-Code Receiver-Ressourcen zur Verfügung, d.h. es können maximal 16 Teilnehmer (analoge, Mobility, etc.) gleichzeitig DTMF-Code-Receiver reservieren. Teilnehmer, bei denen das Flag **DTMF-basierte Leistungsmerkmalaktivierung** gesetzt ist, reservieren sich für die Dauer des Gespräches jeweils einen Code-Receiver.

Bei OpenScape Business S wird die Steuerung der Funktionen über DTMF-Codes unterstützt, wenn die DTMF-Ziffern nach RFC 2833 übertragen werden. Wird im Netzwerk ein externer Session Border Controller (SBC) genutzt, ist keine DTMF-Erkennung möglich.

Anmerkung: Mobility Entry darf nur an Knoten mit direktem Amtszugang konfiguriert werden.

Zugehörige Konzepte

One Number Service auf Seite 964
Vergleich Mobile Clients und Mobility Entry auf Seite 961
Abhängigkeiten für Mobile Clients und Mobility Entry auf Seite 963

19.2.3 Vergleich Mobile Clients und Mobility Entry

Die Mobile Clients myPortal for Mobile und myPortal to go und Mobility Entry unterstützen unterschiedliche Leistungsmerkmale.

Leistungsmerkmal	**myPortal to go**	Mobility Entry
Allgemeine Funktionen		
Mobilfunkvertrag mit Datenoption	Ja (Flatrate empfohlen)	Nein
Parallele Rufsignalisierung an Systemtelefon und Mobiltelefon (Twinning)	Ja	Ja
Übertragung der Anrufer-Rufnummer zum Mobiltelefon (wenn das Netz externe Rufnummern als CLIP überträgt, CLIP no Screening)	Ja	Ja
One Number Service (wenn das Netz externe Rufnummern als CLIP überträgt, CLIP no Screening)	Ja	Ja

Leistungsmerkmal	**myPortal to go**	Mobility Entry
Anrufschutz/abschaltbare Anrufweiterleitung	Nein	Ja
Rufnummernunterdrückung ein-/ausschaltbar	Nein	Ja
Automatische Identifizierung registrierter Teilnehmer	Ja	Ja
Betrieb ohne Bürotelefon (als virtueller Teilnehmer)	Ja	Ja
Nutzbar mit OpenScape Business S	Ja	Ja
Anwesenheitsstatus, Journal, Sprachbox		
Eigenen Anwesenheitsstatus ändern	Ja	Nein
Anwesenheitsstatus anderer Teilnehmer sehen	Ja	Nein
Journal	Neue, Alle, Entgangen, Angenommen, Ankommend, Sprachnachrichten	Nein
Gemeinsame Sprachbox, Abfrage auch von unterwegs möglich	Ja	Ja
Anzeige eingegangener Sprachnachrichten	Anzeige neuer, abgehörter und gespeicherter Sprachnachrichten	Nein
Wählen		
Zugriff auf Kontakte im Mobiltelefon	Ja	Ja
Zugriff auf Kontakte im Kommunikationssystem	Externes Vezeichnis (UC Suite), internes Verzeichnis, persönliche Kontakte und Systemtelefonbuch	Nein
Favoriten	Ja	Nein
Manuelle Wahl	Ja	Ja
Wahlwiederholung	Ja	Nein
Wahlverfahren	Callback, Call Through, Assoziierte Wahl	Callback, Call Through
Während des Gesprächs		
Rückfrage	Ja (nicht mit SIP-Telefon)	Ja
Makeln	Ja (nicht mit SIP-Telefon)	Ja
Vermitteln	Ja (nicht mit SIP-Telefon)	Ja

Leistungsmerkmal	myPortal to go	Mobility Entry
Konferenz	Ja (nicht mit SIP-Telefon)	Ja
Rückruf bei Frei und Besetzt	Nein	Ja
Anrufübernahme vom Mobiltelefon auf das Systemtelefon	Ja	Ja
Besetztanzeige auch bei Gesprächen am Mobiltelefon (bei One Number Service)	Ja	Ja

Zugehörige Konzepte

Mobility Entry auf Seite 959

19.2.4 Abhängigkeiten für Mobile Clients und Mobility Entry

myPortal to go und Mobility Entry besitzen Abhängigkeiten zu anderen Leistungsmerkmalen (z.B. zu DISA).

Abhängigkeit	myPortal to go	Mobility Entry
Mobility-Callback-DuWa	Beim Wahlmodus Mobile Callback muss die Mobility-Callback-Durchwahlnummer konfiguriert sein.	
Externe Zielrufnummer	Die Anwahl von externen Zielrufnummern durch den mobilen Teilnehmer wird aufgrund der LCR-Konfiguration im System gesteuert. Sie kann damit über das ISDN-Festnetz, analoge Festnetz oder über ITSP erfolgen.	
CLIP no Screening aktivieren	Um beim mobilen Teilnehmer die Nummer eines Anrufers anzeigen zu können, muss sie vom Netzanbieter ungeprüft durchgereicht werden.	
CLIP des mobilen Teilnehmers	Die CLIP des mobilen Teilnehmers muss zum Kommunikationssystem übertragen werden. Der Netzanbieter muss diese zur Verfügung stellen.	
LCR-Administration	Da manche Netzanbieter (Festnetz oder ITSP) Zielrufnummern mit eigenem internationalen Präfix nicht akzeptieren, muss vom System die Zielrufnummer um diesen Präfix gekürzt werden. Dies kann bei der Leitweglenkung (LCR) administriert werden.	
B-Kanäle/Externverbindungen	Die Anzahl der B-Kanäle ist abhängig von der Verbindungsdauer bzw. der Anzahl mobiler Teilnehmer. Jede von Extern kommende Verbindung zu einem mobilen Teilnehmer erfordert im System 2 Sprachkanäle. Falls zu wenig Sprachkanäle zur Verfügung stehen, ist die Erreichbarkeit des mobilen Teilnehmers nicht gewährleistet und der mobile Teilnehmer kann selbst keine Anrufe mit One Number Service tätigen.	
Notrufnummern	Wenn ein mobiler Teilnehmer eine Notrufnummer über das Kommunikationssystem wählt, kann der Standort seines Mobiltelefons nicht ermittelt werden. Es ist empfehlenswert, eine Notrufnummer direkt zu wählen.	
Anwahl interner Rufnummern	Bei Anwahl interner Rufnummern durch den mobilen Teilnehmer im internationalen Format (z.B. 0004989100) muss die Standortnummer des Kommunikationssystems konfiguriert sein. Ansonsten werden interne Ziele über Amt angewählt und damit entstehen Kosten.	

Abhängigkeit	myPortal to go	Mobility Entry
Pflege von Verzeichnissen	Um in allen Wahlmodi die Erreichbarkeit von Gesprächspartnern bei der Wahl aus Verzeichnissen sicherzustellen, sollten alle externen Rufnummern im kanonischen Format (z.B. +49 89 100) eingetragen sein.	-
Firewall	Es wird ein Datenkanal zum integrierten Web-Server des Kommunikationssystems aufgebaut. Deshalb muss in der Firewall eine Portweiterleitung auf Port 8801 (http) bzw. Port 8802 (https) eingerichtet sein. Es wird jedoch empfohlen keine Portweiterleitung für Port 8803 (https) für den Zugriff auf UC Smart Assistant zu konfigurieren.	-
Datenverbindung	Es wird empfohlen einen Mobilfunkvertrag mit Datenflatrate abzuschließen. Nutzer von Volumentarifen sollten in den Einstellungen von myPortal to go die Option "Automatisches Refresh" ausschalten.	-
Parallele Verbindungen	Für einige Leistungsmerkmale ist eine gleichzeitige Spach- und Datenverbindung erforderlich. Dies muss sowohl vom Mobilfunknetzbetreiber, als auch vom mobilen Endgerät unterstützt werden.	-
Verbindungsaufbau vom Kommunikationssystem zum mobilen Teilnehmer über	Alle Leitungstypen	Alle Leitungstypen, die DTMF-Übertragung unterstützen.

Zugehörige Konzepte

Mobility Entry auf Seite 959

19.2.5 One Number Service

Über den One Number Service (ONS) wird das Mobiltelefon zur Festnetz-Nebenstelle. Der Teilnehmer ist unter einer Rufnummer weltweit erreichbar und identifiziert sich nur noch mit seiner Festnetzrufnummer.

Durch Einrichtung einer Teamschaltung ist One Number Service mit einer gemeinsamen Rufnummer für Büroarbeitsplatz (Systemtelefon) und Mobiltelefon möglich. Der Anrufer wählt die Rufnummer des Systemtelefons (Festnetz). Gehende Anrufe vom Mobiltelefon werden dem Angerufenen mit der

Festnetzrufnummer signalisiert. Ein weiterer Vorteil des One Number Services ist die Besetztanzeige für den mobilen Teilnehmer.

Zugehörige Konzepte

Mobility Entry auf Seite 959

19.2.6 Dual-Mode-Telefonie

Dual-Mode-Mobiltelefone unterstützen sowohl GSM/UMTS-Netze als auch WLAN-Netze. SIP-Teilnehmer oder System-Clients (d.h. HFA-Teilnehmer) können sich über WLAN am Kommunikationssystem registrieren.

Befindet sich das Dual-Mode-Mobiltelefon in WLAN-Reichweite, wird es automatisch als SIP-Teilnehmer oder System-Client (HFA-Teilnehmer) gerufen. Außerhalb der WLAN-Reichweite wird das Dual-Mode-Mobiltelefon über GSM/UMTS gerufen (Mobiltelefon-Integration-Leistungsumfang möglich).

Anmerkung: Der Dualmodus für HFA wird nur bei Verwendung des myPortal to Go-Clients und nicht bei anderen Geräten oder Clients unterstützt.

Das automatische Weiterleiten an die GSM-Rufnummer funktioniert nur dann, wenn der zugehörige HFA- oder SIP-Teilnehmer im System als Mobiltelefon-Teilnehmer eingetragen ist (Mobiltelefon Integration). Das bedeutet, wenn der HFA- oder SIP-Teilnehmer registriert ist, wird er als HFA- oder SIP-Teilnehmer gerufen, wenn nicht, dann wird er über die in der Mobiltelefon-Integration-Konfiguration zugeordnete GSM-Rufnummer gerufen. CTI-Anruffunktionen sind für SIP-Clients nicht in myPortal to go verfügbar. Stattdessen erfolgt die Steuerung gegebenenfalls innerhalb des HFA- oder SIP-Clients (siehe auch Freigabemitteilung und `http://wiki.unify.com`).

Die Gespräche laufen auf dem Firmengelände über WLAN. Solange über WLAN telefoniert wird, fallen auf dem Mobiltelefon keine Gesprächsgebühren an. Handover und Roaming werden innerhalb der WLAN-Reichweite unterstützt (wenn die WLAN-Infrastruktur dafür ausgelegt ist), nicht jedoch von WLAN nach GSM und umgekehrt.

19.2.7 Konfiguration von myPortal to go und Mobility Entry

myPortal to go (Web Edition) und Mobility Entry werden mit dem Wizard **Mobiltelefon Integration** konfiguriert.

Mit dem Wizard **Mobiltelefon Integration** kann der Administrator:

- One Number Service einrichten
- myPortal to go (Web Edition) einrichten
- Mobility Entry einrichten
- Dual-Mode-Telefone einrichten

Die Mobiltelefon-Integration von GSM-Telefonen erfolgt über virtuelle Teilnehmer. Damit werden Leistungsmerkmale auf den mobilen Teilnehmer übertragen. Jedem Teilnehmer mit einer entsprechenden Lizenz (Mobility User) kann maximal ein mobiler Teilnehmer zugeordnet werden

Betriebsmode von Mobiltelefonen

Es sind folgende Betriebsmodi für Mobiltelefone realisiert:

- **GSM Mode**

  Ein Anruf der internen mobilen Rufnummer wird am GSM-Mobiltelefon signalisiert.
- **WLAN Mode**

  Ist das WLAN-Mobiltelefon über WLAN erreichbar, wir der Anruf über WLAN geführt. Ist das WLAN nicht erreichbar, wird der Anruf über GSM geführt.

Twinning

Ein Anruf wird parallel am Mobiltelefon und am Systemtelefon signalisiert (Twinning). Um Twinning zu realisieren, muss nach Konfiguration der **Mobiltelefon Integration** eine Teamschaltung konfiguriert werden. Verwenden Sie dazu den Wizard **Teamschaltung** und wählen als erstes Telefon die Rufnummer aus, unter der die Parallelsignalisierung erfolgen soll (z.B. das Systemtelefon). Für die Nutzung von myPortal to go (Web Edition) wird als letzter Schritt im Wizard **Mobiltelefon Integration** der Benutzername auf die Team-Gruppe umkonfiguriert. Auf dem Systemtelefon kann für die unterbrechungsfreie Übernahme von Mobiltelefongesprächen eine Direktruftaste zu dem Mobility-Teilnehmer programmiert werden. Der volle Funktionsumfang wird mit Systemtelefonen (HFA) erreicht. SIP- Telefone können mit Einschränkungen verwendet werden, sie unterstützen z.B. keine MULAP-Taste.

Zugehörige Konzepte

Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Wizards auf Seite 720

Voraussetzungen für Application Launcher auf Seite 1203

19.2.7.1 Wie Sie ein GSM-Mobiltelefon integrieren

Mit dem Wizard **Mobiltelefon Integration** integrieren Sie Mobiltelefone in das Kommunikationssystem.

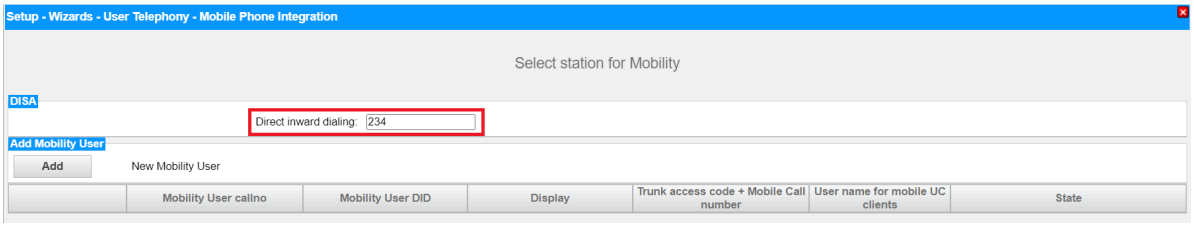
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Mobiltelefon Integration** zu starten. Das Fenster **Teilnehmer für Mobility auswählen** wird angezeigt.

4) Wählen Sie bei **DISA Zugang** die **Durchwahl**-Nummer aus (oder geben Sie sie ein), unter der sich mobile Teilnehmer in das Kommunikationssystem einwählen können.



Anmerkung: DISA ist erforderlich für Mobilty Entry (Steuerung des Systems über DTMF) und für myPortal for Mobile (nur bei Verwendung von Call-Through).

5) Klicken Sie auf **Hinzufügen** bzw. **Bearbeiten** des entsprechenden Teilnehmers, dessen GSM-Mobiltelefon Sie ins Kommunikationssystem integrieren wollen. Das Fenster **Mobility Teilnehmer zuweisen** wird angezeigt.

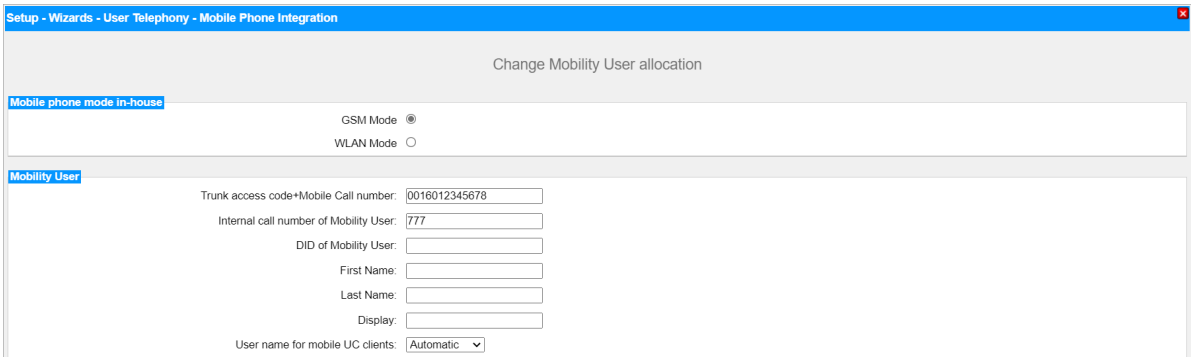
6) Wählen Sie **GSM Mode** als Handybetriebsmode aus.

7) Geben Sie unter **Kennzahl zur Amtsholung+Mobile Rufnummer** die Rufnummer des Mobiltelefons ein (z.B. 0016012345678) ein.

8) Geben Sie die **Interne Rufnummer des Mobility-Teilnehmers** (z.B. 777), einen beliebigen **internen Namen** und die **Durchwahlnummer** ein. Beachten Sie, dass die interne Rufnummer noch nicht vergeben sein darf.

: Wenn Sie DID 879, 890 oder 891 verwenden wollen, müssen Sie die Einstellung über ManagerE und nicht über WBM vornehmen.

9) Wählen Sie in der Aufklappliste **Benutzername für myPortal to go (Web Edition)** den Eintrag **Automatisch** aus (bei Auswahl von Automatisch wird als Benutzername die interne Rufnummer des Teilnehmers vergeben).



10) Nur mit UC Smart: Ordnen Sie bei Bedarf dem Teilnehmer eine Mailbox zu:

a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

d) Wenn das Passwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

Anmerkung: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox deaktiviert werden. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

11) Klicken Sie auf **OK & Weiter**.

12) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

19.2.7.2 Wie Sie ein Dual-Mode-Telefon (GSM/WLAN) mit HFA- oder SIP-Client integrieren

Mit dem Wizard **Mobiltelefon Integration** konfigurieren Sie ein Mobiltelefon als Dual-Mode-Telefon mit System-Client (HFA-Client) oder SIP-Client (WLAN Mode).

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Das HFA-Gerät bzw. der SIP-Teilnehmer muss über WBM eingerichtet sein.

Dem Teilnehmer wurde eine Mobility User Lizenz zugewiesen.

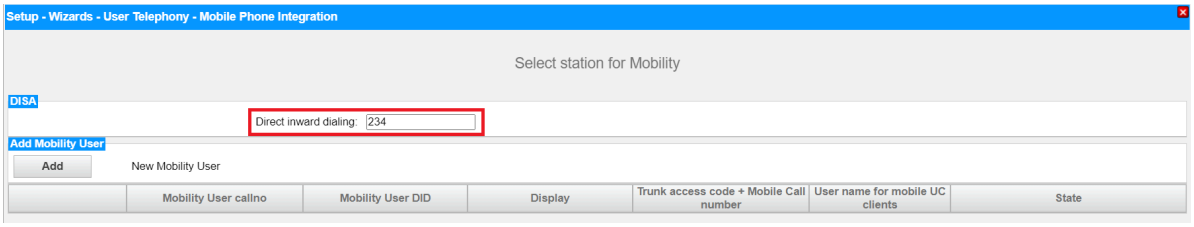
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Mobiltelefon Integration** zu starten. Das Fenster **Teilnehmer für Mobility auswählen** wird angezeigt.

4) Wählen Sie bei **DISA Zugang** die **Durchwahl**-Nummer aus (oder geben Sie sie ein), unter der sich mobile Teilnehmer in das Kommunikationssystem einwählen können.



Anmerkung: DISA ist erforderlich für Mobilty Entry (Steuerung des Systems über DTMF) und für myPortal for Mobile (nur bei Verwendung von Call-Through).

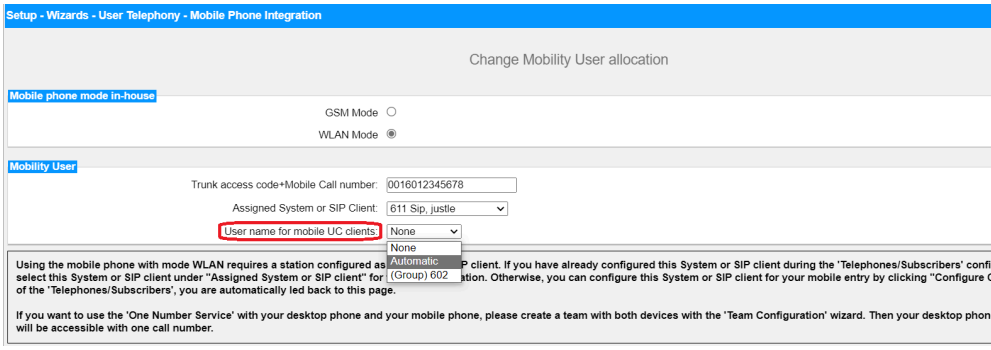
5) Klicken Sie auf **Hinzufügen** bzw. **Bearbeiten** des entsprechenden Teilnehmers, dessen GSM-Mobiltelefon Sie ins Kommunikationssystem integrieren wollen. Das Fenster **Mobility Teilnehmer zuweisen** wird angezeigt.

6) Wählen Sie **WLAN Mode** als Handybetriebsmode aus.

7) Geben Sie unter **Kennzahl zur Amtsholung+Mobile Rufnummer** die Rufnummer des Mobiltelefons ein (z.B. 0016012345678) ein.

8) Wählen Sie aus der Aufklappliste den **Zugeordneten System- oder SIP-Client** aus.

   Wenn das zugewiesene System (HFA-Client) bzw. der SIP-Client noch nicht konfiguriert ist, klicken Sie auf **Client konfigurieren** und richten Sie ein System bzw. einen SIP-Client ein. Nach der System- oder SIP-Teilnehmer-Konfiguration werden Sie automatisch auf diese Seite zurück geführt.



9) Wählen Sie in der Aufklappliste **Benutzername für myPortal to go (Web Edition)** das gewünschte SIP- oder HFA-Gerät aus. Wenn Sie die Option **Automatisch** auswählen, wird als Benutzername die interne Rufnummer des Teilnehmers vergeben.

10) Klicken Sie auf **OK & Weiter**.

11) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

19.2.7.3 Wie Sie die Web-Schnittstelle für Mobiltelefone und Web-Clients aktivieren

Voraussetzungen

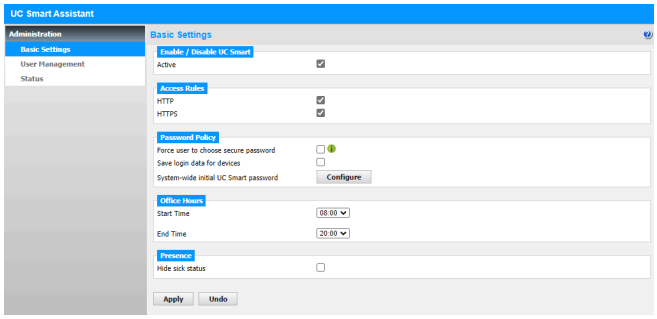
Sie sind am WBM mit dem Profil **Expert** angemeldet.

Aktivieren Sie Web Services als Voraussetzung für folgende Leistungsmerkmale:

- Mobiltelefon Integration
- Application Launcher

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Wenn Sie UC Smart verwenden, klicken Sie im Navigationsbaum auf **Applikationen** > **UC Smart** > **Grundeinstellungen**.
3) Prüfen Sie, ob UC Smart **Aktiv** ist.
4) Wenn Sie Web Services für Mobiltelefone aktivieren möchten, wählen Sie mindestens eine der folgenden Möglichkeiten:
   - Wenn Sie verschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTPS**.
   - Wenn Sie unverschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTP**.



Anmerkung: Aus Sicherheitsgründen wird dringend empfohlen, bei Nutzung von myPortal to go (Web Edition) über Internet nur eine verschlüsselte Verbindung (HTTPS) zu nutzen.

---

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.2.7.4 Wie Sie die Mobiltelefon-Integration löschen

Mit dem Wizard **Mobiltelefon Integration** löschen Sie die Integration des Mobiltelefons.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **User-Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Mobiltelefon Integration** zu starten. Das Fenster **Teilnehmer für Mobility auswählen** wird angezeigt.
4) Klicken Sie auf **Bearbeiten** des entsprechenden Teilnehmers, den Sie löschen wollen. Das Fenster **Mobility Teilnehmer zuweisen** wird angezeigt.
5) Klicken Sie im Fenster unten auf **Daten löschen**.
6) Klicken Sie auf **OK & Weiter**.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

19.3 Mobilität im Büro

Mobilität im Büro wird erreicht über DeskSharing, Cordless-Telefone und WLAN-Telefone. Für DeskSharing werden mit IP-Mobility (Mobiles Logon und Flex Call) Leistungsmerkmale für mobile Teilnehmer angeboten, die das Telefon an einem fremden Arbeitsplatz wie ihr eigenes nutzen möchten.

19.3.1 Desk Sharing

Mit Desk Sharing können sich mehrere Teilnehmer ein Systemtelefon und damit ein IP-Telefon (HFA) teilen.

Mit Desk Sharing haben Abonnenten keinen festen Arbeitsplatz und kein festes Bürotelefon. Desk Sharing ermöglicht es mehreren mobilen Abonnenten des Kommunikationssystems, einen Büroarbeitsplatz und/oder das Telefon zu teilen. Der Abonnent meldet sich einfach am Arbeitsplatz-Telefon, an dem er gerade arbeitet, an.

Nach der Anmeldung wird die Rufnummer des angemeldeten Abonnenten an das verwendete Systemtelefon übertragen. Das verwendete Systemtelefon ist unter seiner ursprünglichen Stationsnummer nicht mehr erreichbar. Meldet sich der Teilnehmer an einem anderen Systemtelefon an, wird seine oder ihre Stationsnummer auf dieses neue Systemtelefon übertragen. Wenn sich der Benutzer abmeldet (Anmelden), meldet sich das Systemtelefon automatisch mit seiner eigenen Nicht-Mobilnummer wieder an.

Um das Merkmal zu aktivieren, muss einer der folgenden Schritte am Systemtelefon durchgeführt werden:

- Geben Sie Code für "mobile Anmeldung" und Nummer der Mobilstation und optionales Passwort/PIN ein

Bei der Verwendung von Telefonen mit einer unterschiedlichen Anzahl von Funktionstasten kann die Übertragung von Tastenlayouts Einschränkungen unterliegen.

Soll Desk Sharing für IP-Telefone (HFA) in vernetzten Knoten implementiert werden, muss ein externer DLS (Deployment Service) installiert werden. Das erforderliche Fachwissen für diesen Zweck wird vorausgesetzt.

Die folgenden Merkmale können für die Desk Sharing verwendet werden:

- Lautsprecherruf (Paging)
- Konferenzen
- Aufschalten

- Umschalten/Verbinden
- Parken
- Konsultation
- Übergeben
- Rufannahme
- Nicht stören
- Anrufumleitung
- Nachricht senden (Nachricht wartet)
- Rückruf
- Unterdrückung der Stationsnummer
- Klingelgruppe ein

Anmerkung: Für jede Mobiltelefonnummer ist eine zusätzliche Deskshare-Lizenz erforderlich. Diese Deskshare-Lizenz muss für den Abonnenten aktiviert und der Abonnent muss als **mobil** konfiguriert sein. Darüber hinaus muss das Relocate-Merkmal aktiviert sein.

Ein Systemtelefon, das für Desk Sharing verwendet wird, erfordert nicht unbedingt eine Lizenz. Wenn jedoch keine Lizenz aktiviert ist und kein Desk Sharing-Abonnent angemeldet ist, sind von diesem Telefon nicht einmal Notrufe möglich. Das Systemtelefon/Abonnent muss als **Nicht-mobil** konfiguriert sein.

Wenn ein Systemtelefon nicht für Desk Sharing verwendet werden soll, muss es als **Nicht-Mobil konfiguriert und blockiert sein**.

Anmerkung: Das Desk Sharing-Merkmal darf nicht mit den ersten beiden aktiven Systemstationen verwendet werden.

19.3.2 Integrierte Cordless-Lösung

OpenScape Business Cordless ist die integrierte Cordless-Lösung zum Betrieb von Cordless-Telefonen (DECT-Telefonen) über das Kommunikationssystem. Mit den angeschlossenen DECT-Telefonen können die HFA-Leistungsmerkmale von OpenScape Business genutzt werden.

Bei der integrierten Cordless-Lösung sind die DECT-Telefone interne, systemspezifische Teilnehmer, im Gegensatz zu separaten DECT-Anlagen, die über Standardschnittstellen angeschaltet werden.

Die Anschaltung der OpenScape Business-Basisstationen für den Betrieb der DECT-Telefone kann realisiert werden über:

- Für OpenScape Business X1/X3/X5: Anschaltung direkt an die $U_{P0/E}$-Schnittstellen des Mainboards des Kommunikationssystems (DECT Light)
- Für OpenScape Business X3/X5: Anschaltung an die $U_{P0/E}$-Schnittstellen einer SLU8N/SLU8NR-Baugruppe (DECT Light)
- Für OpenScape Business X8: Anschaltung an die $U_{P0/E}$-Schnittstellen einer SLMUC- (SLMU und CMAe)

Die Cordless-Funktechnologie entspricht dem DECT-Standard (Digital Enhanced Cordless Telecommunications). Der gesamte, vom System verwaltete Funkbereich besteht aus Basisstationen, die entweder zusammen ein lückenloses Netz sich überschneidender Funkzellen oder einzelne Funkinseln bilden. Die Größe einer Funkzelle ist abhängig von den örtlichen/ baulichen Gegebenheiten.

ECO Mode

Im ECO Mode (Economic Mode) wird die Sendeleistung der DECT-Telefone entweder um einen fest eingestellten Wert (statisch) gesenkt oder jedes DECT-Telefon passt seine Sendeleistung selbstständig an die empfangene Signalstärke an (adaptiv). Der ECO Mode kann am Kommunikationssystem für alle DECT-Telefone systemweit aktiviert werden (**Experten Modus** > **Telefonie** > **Cordless** > **Systemweit**). Eine Konfiguration an den DECT-Telefonen ist nicht notwendig. Ein manueller Restart des Systems ist erforderlich, um das Leistungsmerkmal bei OpenScape Business X1, X3, X5 zu aktivieren

- Statische Sendeleistungsanpassung

  Die DECT-Telefone und die Basisstation senken die Sendeleistung auf einen fest eingestellten Wert ab.
- Adaptive Sendeleistungsanpassung

  Die DECT-Telefone senden abhängig von der jeweiligen Empfangsfeldstärke mit normaler oder mit reduzierter Sendeleistung. Bei Handover wird zuerst auf die hohe Sendeleistung geschaltet und anschließend abhängig vom Empfang die Sendeleistung reduziert.

DECT-Telefone

Die integrierte Cordless-Lösung unterstützt die Anschaltung GAP-fähiger Mobiltelefone fremder Hersteller. Der volle HFA-Leistungsumfang kann aber nur mit den freigegebenen DECT-Telefonen genutzt werden.

Konfiguration

Für die Beschreibung der Konfiguration siehe Konfiguration der integrierten Cordless-Lösung.

Baugruppen und Basisstationen

Die Beschreibung der Baugruppen und Basisstationen finden Sie unter *OpenScape Business Servicedokumentation iin den Kapiteln Baugruppen und Basisstationen*.

19.3.2.1 Systemübersicht

Die Anschaltung der OpenScape Business Basisstationen erfolgt bei OpenScape Business X3/X5 entweder direkt an den $U_{P0/E}$-Schnittstellen des Mainboards oder an den UP0/E-Schnittstellen einer installierten SLU8N/ SLU8NR-Baugruppe (DECT Light). Bei OpenScape Business X8 können die Basisstationen an den Cordless-Baugruppen SLMUC angeschlossen werden.

Direktanschaltung (DECT Light)

Die Basisstationen können direkt an den $U_{P0/E}$-Schnittstellen von OCCM, OCCMB, OCCMA und OCCMR, OCCMBR, OCCMAR der

Kommunikationssysteme OpenScape Business X3R/X3W und OpenScape Business X5R/X5W angeschlossen werden oder an den UP0/E-Schnittstellen einer SLU8N/SLU8NR-Baugruppe.

Durch Einsatz des Submoduls CMAe auf den Mainboards werden die Funktionen ADPCM-Wandlung und Echokompensation zur Verfügung gestellt (48 Kanäle für CMAe). Es können bis zu vier Gespräche pro Basisstation geführt werden. Bis zu sieben Basisstationen können an die $U_{P0/E}$-Schnittstellen der Mainboards OCCM, OCCMB, OCCMA und OCCMR, OCCMBR, OCCMAR angeschlossen werden.

Falls kein CMAe installiert ist, können maximal zwei Gespräche pro Basisstation geführt werden. In diesem Fall wird die ADPCM-Wandlung direkt von der DECT-Basisstation durchgeführt.

Anmerkung: Wenn kein CMAe installiert ist, stehen keine Echo Handling-Funktionen zur Verfügung.

Für die Anschaltung von Basisstationen an eine SLU8N/SLU8NR-Baugruppe gelten folgende Anschaltbedingungen:

- Insgesamt können maximal 15 Basisstationen (7 am Mainboard und weitere 8 an einer SLU8N/SLU8NR-Baugruppe) betrieben werden. Die max. Anzahl der anschließbaren DECT-Telefone ist 64 bei einem CMAe.
- Es kann nur eine SLU8N/SLU8NR-Baugruppe für die Anschaltung von Basisstationen verwendet werden.
- Für den Anschluss der Basisstation an eine $U_{P0/E}$-Schnittstelle der SLU8N/SLU8NR-Baugruppe kann nur der erste Port der Basisstation verwendet werden. Die Ports 2 und 3 der Basisstation werden nicht für den Anschluss an eine weitere $U_{P0/E}$-Schnittstelle unterstützt.
- Die $U_{P0/E}$-Schnittstellen der SLU8N/SLU8NR-Baugruppe können gemischt mit Basisstationen oder Telefonen beschaltet werden.

Cordless-Baugruppenanschaltung

Die Basisstation BS5 kann an die $U_{P0/E}$-Schnittstellen der folgenden Cordless-Baugruppen angeschlossen werden:

- SLMUC (SLMU + CMAe bei OpenScape Business X8 (siehe Kapitel zu *SLMUC-Servicedokumentation*)

  Der Anschluss der Basisstationen kann über eine, zwei oder drei $U_{P0/E}$-Schnittstellen erfolgen. Die letzten 8 Schnittstellen können nur als zweite oder dritte UP0-Schnittstellen der Basisstation verwendet werden. Der zusätzliche Anschluss von $U_{P0/E}$-Schnittstellen erhöht Verkehrswert der angeschlossenen Basisstation und damit die Anzahl der gleichzeitig verfügbare Gesprächskanäle.

19.3.2.2 Cordless-Baugruppenanschaltung

Bei der Baugruppenanschaltung werden die Basisstationen an die $U_{P0/E}$-Schnittstellen der Cordless-Baugruppen (SLC-Baugruppen) angeschlossen.

Basisstationen können an die $U_{P0/E}$-Schnittstellen folgender Cordless-Baugruppen angeschlossen werden:

- SLC16N bei OpenScape Business X5W (nur Wandsystem)
- SLCN bei OpenScape Business X8

Bis zu vier Cordless-Baugruppen (SLCN) können in OpenScape Business X8 eingesetzt werden. Über alle vier Cordless-Baugruppen steht die volle Cordless-Funktionalität (Roaming und Seamless Connection Handover) zur Verfügung, da die Funkfelder der Cordless-Baugruppen innerhalb des Kommunikationssystems über SLC-Vernetzungsleitungen synchronisiert werden (Multi-SLC). Netzweites Handover wird derzeit nicht unterstützt.

Wenn keine SLCN- oder SLC16N-Baugruppen vorhanden sind und die BS über $U_{P0/E}$ verbunden ist, wird auf der Steuerungsbaugruppe ein CMA- oder CMAe-Modul benötigt, wenn im OpenScape Business-Netzwerk CMI-Roaming vorgesehen ist.

19.3.2.3 Systemausbau

In Abhängigkeit vom Kommunikationssystem können bis zu 64 Basisstationen angeschlossen und bis zu 250 DECT-Telefone genutzt werden.

Die folgende Tabelle zeigt den maximal möglichen Systemausbau der integrierten Cordless-Lösung und informiert, in welchen Fällen analoger Amtszugang des Kommunikationssystems möglich ist.

Anmerkung: Die Basisstationen BS4 (S30807-U5491-X), BS3/1 (S30807-H5482-X), BS3/3 (S30807-H5485-X) und BS3/S (X30807-X5482-X100) befinden sich im Produktauslauf und können nicht mehr bestellt werden. Der Anschluss an die Kommunikationssysteme OpenScape Business X ist aber weiterhin möglich.

Im Falle eines Defekts sind die aktuellen Basisstationen einzusetzen.

Tipp: Falls kein CMA/CMAe installiert ist, können maximal zwei Gespräche pro Basisstation geführt werden. In diesem Fall wird die ADPCM-Wandlung direkt von der DECT-Basisstation durchgeführt. Die Echokompensation wird jedoch nicht direkt unterstützt. Falls Echokompensation erforderlich ist, wird ein CMA/CMAe-Submodul benötigt.

Anmerkung: In der folgenden Tabelle wird die Kombination aus SLMU-Karte und CMAe-Modul als SLMUC bezeichnet.

OpenScape Business	Maximale Anzahl Baugruppen				Clock Module	**Max. Anzahl der Basisstation BS bei Anschluss über 1xU_{P0}**	Ports / gleichzeiti Gespräch pro BS	**Max. Anzahl der registrierten Geräte**	Max. Anzahl gleichzeitiger Rufe
	SLC16N	**SLCN**	**SLUN**	**SLMUC**					
X1	–	–	–	–	–	7	1/2	16	14
	–	–	–	–	CMA	7	1/4	16	16
	–	–	–	–	CMAe	7	1/4	16	16
X3	–	–	–	–	–	7	1/2	32	16
Onboard $U_{P0/E}$ (SLUC)	–	–	–	–	CMA	7	1/4	32	16
	–	–	1	–	CMA	15	1/4	32	16
	–	–	–	–	CMAe	7	1/4	64	28
	–	–	1	–	CMAe	15	1/4	64	48
X5	–	–	–	–	–	7	1/2	32	16
Onboard $U_{P0/E}$ (SLUC)	–	–	–	–	CMA	7	1/4	32	16
	–	–	1	–	CMA	15	1/4	32	16
	–	–	–	–	CMAe	7	1/4	64	28
	–	–	1	–	CMAe	15	1/4	64	48
X5W	1	–	–	–	–	16	3/12	64	32*
X8	–	4	–	–	–	64	3/12	250 (128 pro SLCN)	128**
	–	–	–	4	CMAe	64	3/12	250 (128 pro SLCN)	192***

* Maximalwert je SLCN16 ist 32. Beim Roaming erfolgt die ADPCM-Wandlung immer auf der SLC16N-Baugruppe, an der sich gerade das Mobilteil befindet. Daher könnte die Anzahl gleichzeitiger Anrufe pro System höher als 32 sein, wenn sich das Mobilteil an der Gast-SLC16N befindet

** Der Maximalwert je SLCN ist 32. Je nach Standort der Mobilteile beim Roaming könnten theoretisch alle registrierten Geräte (250) aktiv sein, wenn 4 SLCN-Karten verfügbar sind.

*** SLCN und SLMUC können in einem System kombiniert werden. Der Maximalwert ist 32 je SLCN und 48 je SLMUC. Je nach Standort der Mobilteile beim Roaming könnten theoretisch alle registrierten Geräte (250) aktiv sein, wenn insgesamt 4 SLCN/SLMUC verfügbar sind.

19.3.2.4 Cordless/DECT-Telefone

Mit Stecken der SLC-Baugruppe und Eingabe der DECT-Systemkennung werden 16 Mobilteile eingerichtet. Die Mobilteil-Codes (PIN) werden vergeben und die Mobilteile können angemeldet werden. Weitere zu nutzende Mobilteile müssen erst freigeschaltet werden.

Wird im Servicefall ein Mobilteil ausgetaucht, muss vor Anmeldung des Austauschgerätes die PIN geändert werden. Beim Austausch ist grundsätzlich im Kommunikationssystem für den betreffenden Teilnehmer eine neue PIN zu vergeben. Dadurch wir das Mobilteil automatisch abgemeldet. Und zur Sicherheit ist es nicht mehr möglich, in Kenntnis der alten PIN, ein Mobilteil missbräuchlich anzumelden.

19.3.2.5 Bedeutung der Ergebnisse beim Test des Funkbereichs

Wichtig:

Ergebnisse, die von einem Mobiltelefon erhoben wurden, sind nicht sehr genau und dienen nur einer groben Einschätzung. Von jedem Mobiltelefon werden zudem, unter sonst gleichen Bedingungen, unterschiedliche Werte gemessen. Wenn Sie genauere Ergebnisse brauchen, empfehlen wir die Verwendung des Hicom Cordless Service Tool (HCS-DECT).

Die folgende Abbildung zeigt eine Beispielanzeige der Messergebnisse bei einem Gigaset Mobiltelefon während eines Anrufs:

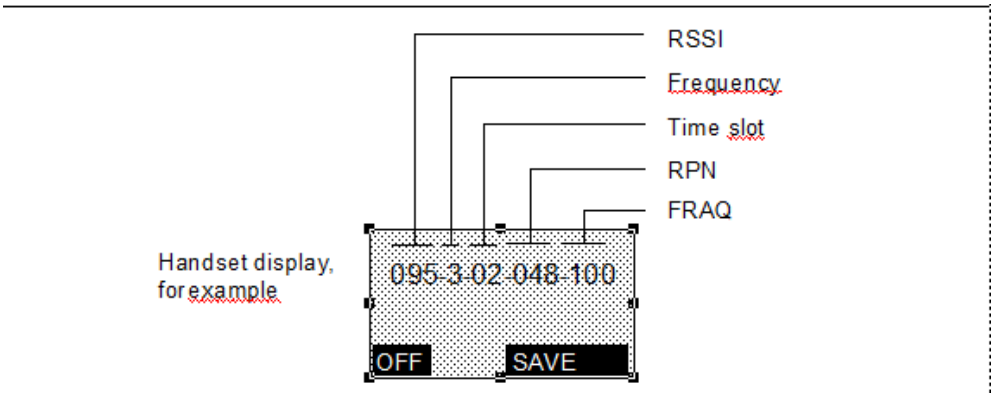


Abbildung 8: Messergebnis

Kapitel	Beschreibung
RSSI (Funksignal)	Feldstärke, der von der Basisstation empfangenen Funksignale, normiert auf maximal 100. Bei einem Wert <50 ist die Funkverbindung zur Basisstation nicht mehr sichergestellt. Eine akzeptable Feldstärke liegt bei >50 (> –60 dBm).
Frequenz	Frequenz (0 – 9)
Zeitschlitz (Slot)	Zeitschlitz (0 – 11) des Empfangskanals, auf dem die Messung durchgeführt wurde.

Kapitel	Beschreibung
RPN (Portnummer)	**OpenScape Business X1/X3/X5/X8** ID der Basisstation, zum Beispiel, 048, Portnummer in den SLC-Baugruppen. Wenn das Mobilteil in eine überschneidende Funkzelle/Basisstation wechselt, wird die aktuelle Portnummer (wo der D-Kanal der Basisstation konfiguriert ist) auf dem Display angezeigt. Formel: A x 16 + B A = Nummer der SLC-Baugruppe (1 - 127); 16 = Faktor B = Port der zugewiesenen SLC-Baugruppe (wo der D-Kanal der Basisstation konfiguriert ist) Beispiele: RPN = 1 x 16 + Port 0 = 016 RPN = 2 x 16 + Port 8 = 040. Die Portnummer (PRN) wird für die Geräte Gigaset S3 Professional und Gigaset SL3 Professional in hexadezimaler Form mit angehängtem H angezeigt. Der hexadezimale Wert wird ohne angehängtes H angezeigt, z.B. "-028-" bei den Geräten Gigaset S4 Professional und OpenStage SL4 Professional. Beispiel: Wenn zuvor der Wert 040 angezeigt wurde, wird jetzt für das Gigaset S3/SL3 Professional der Wert 028H angezeigt. Die hexadezimale Darstellung unterscheidet sich nur durch angehängtes oder nicht angehängtes „H“. Dies gilt auch für OpenScape DECT Phone S5/SL5/S6/SL6/R6 Geräte (kein vorangestelltes H vorhanden).
FRAQ (Frame Quality)	Übertragungsqualität in %. 95 % bis 100 % zufriedenstellend (für kurze Zeiträume 90 % bis 94 % nicht kritisch), < 95 % fehlerhaft.

Weitere Informationen zum Menü der Messung, siehe: *OpenScape Cordless Enterprise, Servicedokumentation, Kapitel: Testen des Funkbereichs* und *OpenScape Business X3/X5/X8, Servicedokumentation, Kapitel: Funkabdeckung prüfen.*

19.3.3 Konfiguration der integrierten Cordless-Lösung

Die Konfiguration der integrierten Cordless-Lösung umfasst die Einrichtung der Basisstationen und die Anmeldung der DECT-Telefone/Mobilteile am Kommunikationssystem.

Die Konfiguration erfolgt über den Experten-Modus.

Die Voraussetzungen wie Projektierung, Ausleuchtung, Montage und Verkabelung, Aufstellen des Systems und Stecken der SLC- oder CMAe-Baugruppen sind abgeschlossen (siehe auch Servicedokumentation). Die DECT-Telefone sind aufgeladen. Die DECT-Systemkennung ist bekannt. Informationen über Teilnehmer, Rufnummern, Namen und ggf. deren Zuordnung zur SLC-Baugruppe liegen vor.

Genereller Ablauf zur Konfiguration der integrierten Cordless-Lösung

1) DECT-Systemkennung eingeben und ggf. weitere Cordless-Parameter konfigurieren
2) Cordless-Basisstationen konfigurieren
3) DECT-Telefone an Cordless anmelden
4) Bei Bedarf weitere DECT-Telefone hinzufügen

Nach der Inbetriebnahme der DECT-Telefone können Rufnummer und Name und weitere Einstellungen der DECT-Teilnehmer über das WBM über den Wizard **Endgeräte/Teilnehmer** geändert werden.

DECT-Systemkennung

Die DECT-Systemkennung dient zur Unterscheidung der einzelnen DECT-Systeme und somit zur Kennzeichnung der Funksignale. Erst dadurch wird die Synchronisation der angemeldeten Mobilteile auf das System ermöglicht.

Die DECT-Systemkennung ist eine 8-stellige, hexadezimale Ziffernfolge und wird beim Erwerb des DECT-Systems mitgeliefert. Sie ist systemweit gültig (auch im Servicefall).

Die DECT-Systemkennung setzt sich zusammen aus:

Ziffer	Bedeutung
1. Ziffer	E/ARC (Access Right Code)
2. - 5. Ziffer	EIC (Equipment Installers Code)
6. - 7. Ziffer	FPN (Fixed Part Number)
8. Ziffer	FPS (Fixed Part Subscriber)

19.3.3.1 Wie Sie die DECT-Systemkennung eingeben und weitere Cordless-Parameter (systemweite Daten) konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** oder mit dem Hipath 3000 Manager angemeldet. Die folgenden Schritte beziehen sich nur auf das WBM, aber ähnliche Aktionen können auch mit dem Hipath 3000 Manager durchgeführt werden.

Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Die bei der Bestellung des DECT-Systems mit ausgelieferte 8-stellige DECT-Systemkennung ist vorhanden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Cordless**.
3) Klicken Sie im Menübaum auf **Cordless** > **Systemweit**.
4) Geben Sie unter **Systemkennung** die 8-stellige DECT-Systemkennung ein.
5) Ändern Sie die systemweiten Einstellungen unter **Echo Handling** und **Economic Mode** nur bei Bedarf. Eine Erklärung zu den Einstellungen finden Sie unter Cordless>Systemweit.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.3.3.2 Wie Sie Cordless-Basisstationen konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** oder mit dem Hipath 3000 Manager angemeldet. Die folgenden Schritte beziehen sich nur auf das WBM, aber ähnliche Aktionen können auch mit dem Hipath 3000 Manager durchgeführt werden.

Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Cordless**.
3) Klicken Sie im Menübaum auf **Cordless** > **Basisstationen**. Es werden alle angeschlossenen Basisstationen angezeigt.
4) Falls eine oder mehrere Basisstationen direkt (ohne SLC-Baugruppe) am System angeschlossen sind (SLUC), können Sie die Basisstationen über die Auswahlliste **Typ** aktivieren oder deaktivieren:
   a) **Basisstation**: Die Basisstation wird aktiviert und es werden automatisch 16 DECT-Telefone und eine SLC-Vernetzungsleitung vorkonfiguriert.
   b) **Kein Port**Die Basisstation wird deaktiviert mit allen zugehörigen DECT-Telefonen und der SLC-Vernetzungsleitung.
5) Ändern Sie bei Bedarf unter **Name** den vorkonfigurierten Namen der Basisstation (z. B. `Basis 1`).
6) Legen Sie unter **Pegel** den Pegel für die Basisstation fest (50 % oder 100 %).
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.3.3.3 Wie Sie DECT-Telefone erstmalig konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet oder Sie verwenden den Hipath 3000 Manager.

Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Die folgenden Konfigurationsschritte sollten durchgeführt werden, bevor DECT-Geräte im System registriert werden.

Schritt für Schritt

1) Führen Sie die folgenden Schritte aus, wenn Sie das WBM verwenden:

a) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
b) Klicken Sie im Navigationsbaum auf **Telephonie** > **Cordless**.
c) Klicken Sie im Menübaum auf **Cordless** > **SLC**. Es werden alle bereits konfigurierten DECT-Telefone angezeigt. Beim Anschluss einer Basisstation werden automatisch 16 DECT-Telefone vorkonfiguriert.
d) Ändern Sie bei Bedarf unter **Rufnr.** die vorkonfigurierte interne Rufnummer des DECT-Telefons.
e) Ändern Sie bei Bedarf unter **DuWa** die vorkonfigurierte Durchwahlnummer des DECT-Telefons.
f) Ändern Sie bei Bedarf unter **Name** den vorkonfigurierten Namen des DECT-Telefons.
g) Ändern Sie bei Bedarf unter **Mobilcode** den vorkonfigurierten Mobilcode (PIN) des DECT-Telefons. Dieser Code muss am DECT-Telefon eingegeben werden bei der erstmaligen Anmeldung an der Basisstation.
h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

2) Führen Sie die folgenden Schritte aus, wenn Sie den Hipath 3000 Manager verwenden:

a) Laden Sie die KDS-Datenbank hoch, indem Sie **Datenbank lesen/ schreiben** und **System > PC**prüfen.
b) Gehen Sie im Menübaum auf **Einstellungen > Cordless** im Navigationsbaum.
c) Klicken Sie im Menübaum auf **Cordless > SLC** und dann auf den Parameter **Portable Parts**, um alle zu prüfen. Es werden alle bereits konfigurierten DECT-Telefone angezeigt. Beim Anschluss einer Basisstation werden automatisch 16 DECT-Telefone vorkonfiguriert.
d) Ändern Sie bei Bedarf unter **Rufnr.** die vorkonfigurierte interne Rufnummer des DECT-Telefons.
e) Ändern Sie bei Bedarf unter **Name** den vorkonfigurierten Namen des DECT-Telefons.
f) Ändern Sie bei Bedarf unter **Mobilcode** den vorkonfigurierten Mobilcode (PIN) des DECT-Telefons. Dieser Code muss am DECT-Telefon eingegeben werden bei der erstmaligen Anmeldung an der Basisstation.
g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
h) Übertragen Sie das KDS in das System, falls Änderungen vorgenommen wurden.

Zugehörige Tasks

Wie Sie DECT-Teilnehmer konfigurieren auf Seite 466

19.3.3.4 Wie Sie ein DECT-Telefon (OpenStage/Gigaset-Mobilteil) an Cordless anmelden

Vor Registrierung eines DECT-Telefons müssen Sie das Anmeldefenster durch ein Systemtelefon mittels DECT-Registrierungscode öffnen. Anschließend können Sie die Rufnummern der zu registrierenden DECT-Telefone eingeben. Im gleichen Registrierungsfenster können maximal 10 Rufnummern gleichzeitig registriert werden. Ein Registrierungsfenster ist bis zu 10 Minuten lang geöffnet.

Wenn kein Systemtelefon verfügbar ist, können Sie die Funktion Hipath 3000 Manager **Online** nutzen und die Aktionen von dort aus durchführen, anstatt ein physisches Telefon zu verwenden. Die folgenden Schritte beziehen sich auf das physische Telefon.

Die folgenden Schritte beziehen sich auf das physische Telefon.

Schritt für Schritt

1) Öffnen Sie das Registrierungsfenster am Kommunikationssystem:
   a) Geben Sie auf dem physischen Telefon den Code *94 2 und dann 19970707 ein.
   b) Geben Sie die Rufnummern der registrierenden DECT-Telefone ein.

2) Registrieren Sie das DECT-Telefon:
   a) Drücken Sie auf dem Bildschirm des DECT-Telefons von der Startseite aus die **Menütaste**.
   b) Navigieren Sie zu **Einstellungen > Registrierung > Handapparat registrieren** und wählen Sie **Basis**.
   c) Sie werden zur Eingabe des System-PINs der Rufnummer aufgefordert. Geben Sie die den achtstellige Mobiltelefoncode ein und bestätigen Sie Ihre Eingabe.

      Sie müssen ein oder zwei Silent Calls (d. h. kurze automatische Anrufe) abwarten (bei manchen Geräten klingelt es zweimal).

      Wenn Sie eine inaktive Rufnummer registrieren (die vorher nicht benutzt wurde, sie sieht im WBM schwarz und im KDS grau aus), wird die Registrierung mit einem Silent Call abgeschlossen. Beim Registrieren einer aktiven Rufnummer, die bereits verwendet wurde (im WBM und KDS grün), wird die Registrierung mit zwei Silent Calls abgeschlossen.

      Bitte führen Sie keine weiteren Aktionen (z. B. DECT-Telefongespräche) durch, bis dieser Vorgang abgeschlossen ist!

Nach erfolgreicher Registrierung wird die Rufnummer auf dem Startbildschirm angezeigt, und Sie können das Gerät verwenden.

Beispiel: Registrieren des Mobiltelefons (Rufnummer 125) mit dem Mobiltelefoncode (PIN) 11112345 am DECT-Telefonsystem (als Mobilcode über Manager E bzw. WBM konfiguriert, siehe Kapitel: Wie Sie DECT-Telefone erstmalig konfigurieren auf Seite 981.)

1) Aktivieren Sie das Registrierungsfenster von einem mit dem System verbundenen physischen Telefon durch Eingabe von *942.
2) Im Display des Telefons sehen Sie: **Kennzahl**
3) Geben Sie 19970707 ein; dies wird auf dem Display des Telefons angezeigt: **Tel.-Nr:** Geben Sie 125 ein

4) Schalten Sie bei Bedarf das Mobiltelefon ein, indem Sie die Auflegen-Taste länger als 1 s drücken. Anschließend ertönt der Quittungston.
5) Führen Sie die folgenden Eingaben innerhalb von zehn Minuten durch. Drücken Sie die Menütaste.
6) Navigieren Sie im Telefonmenü zu **Einstellungen** und bestätigen Sie.
7) Navigieren Sie zu **Registrierung** und bestätigen Sie die erste Auswahl: **Handapparat registrieren** (wählen Sie nicht die zweite Option: Basis auswählen).
8) Wählen Sie eine Basis (in diesem Beispiel **Basis 2**) aus und bestätigen Sie diese. In der Mitte des Displays sehen Sie **Registrierung** und **Bitte System-PIN eingeben**.
9) Geben Sie die achtstellige PIN = Mobiltelefoncode (hier **11112345**) ein und bestätigen Sie diese. Bei erfolgreicher Registrierung müssen Sie einen Silent Call (d. h. kurzen automatischen Anruf) abwarten (bei manchen Geräten klingelt es zweimal). Wenn Sie eine inaktive Rufnummer registrieren (die vorher nicht benutzt wurde, sie sieht im WBM schwarz und im KDS grau aus), wird die Registrierung mit einem Silent Call abgeschlossen. Beim Registrieren einer aktiven Rufnummer, die bereits verwendet wurde (im WBM und KDS grün), wird die Registrierung mit zwei Silent Calls abgeschlossen. Bitte führen Sie keine weiteren Aktionen (z. B. DECT-Telefongespräche) durch, bis dieser Vorgang abgeschlossen ist! Auf der linken Seite des Bildschirms sehen Sie dann „Basis 2“ (in diesem Fall). Danach sehen Sie die Rufnummer (125) auf Ihrem Startbildschirm.
10) Sie können die Bezeichnung „Basis 2“ bei Bedarf ändern. Navigieren Sie dazu zu den Einstellungen und bestätigen Sie, gehen Sie zur Registrierung und bestätigen Sie. Wählen Sie dann die zweite Option „Basis auswählen“. Wählen Sie den Basisnamen aus, der umbenannt werden soll, drücken Sie auf **Name**und benennen Sie den Basisnamen um (z. B. in 125).

19.3.3.5 Wie Sie weitere DECT-Telefone hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** oder mit dem Hipath 3000 Manager angemeldet. Die folgenden Schritte beziehen sich nur auf das WBM, aber ähnliche Aktionen können auch mit dem Hipath 3000 Manager durchgeführt werden.

Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Cordless**.
3) Klicken Sie im Menübaum auf **Cordless** > **SLC**.
4) Klicken Sie im Menübaum auf die gewünschte Baugruppe.
5) Klicken Sie auf die Registerkarte **DECT-Teilnehmer hinzufügen**.
6) Geben Sie unter **Anzahl DECT-Telefone** die Anzahl der neu hinzuzufügenden DECT-Telefone ein. Die neu hinzugefügten DECT-Telefone werden unter der Registerkarte **DECT Teilnehmer ändern** angezeigt.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.3.3.6 Wie Sie DECT-Telefone löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** oder mit dem Hipath 3000 Manager angemeldet. Die folgenden Schritte beziehen sich nur auf das WBM, aber ähnliche Aktionen können auch mit dem Hipath 3000 Manager durchgeführt werden.

Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

DECT-Telefone sind konfiguriert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Cordless**.
3) Klicken Sie im Menübaum auf **Cordless** > **SLC**. Es werden alle bereits konfigurierten DECT-Telefone angezeigt.
4) Markieren Sie in der Spalte **Löschen** die zu löschenden DECT-Telefone.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.3.3.7 Wie Sie die Multi-SLC-Parameter konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** oder mit dem Hipath 3000 Manager angemeldet. Die folgenden Schritte beziehen sich nur auf das WBM, aber ähnliche Aktionen können auch mit dem Hipath 3000 Manager durchgeführt werden.

Es sind mehrere SLMUC-Baugruppen in der OpenScape Business X8 gesteckt.

Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Cordless**.
3) Klicken Sie im Menübaum auf **Cordless** > **Multi-SLC**.

4) Parameter der SLMUC-Baugruppe ändern:
   a) Ändern Sie bei Bedarf unter **SLC-Nr.** die vorkonfigurierte systemweit eindeutige ID-Nummer der SLMUC-Baugruppe.

      Wertebereich: 1-15,17-31,33-47,...,127. Vielfache von 16 sind nicht erlaubt.
   b) Ändern Sie bei Bedarf unter **SLC-Rufnummer** die vorkonfigurierte systemweit eindeutige Rufnummer der SLC-Vernetzungsleitung der SLMUC-Baugruppe.

      Anmerkung: Für jede SLC-Vernetzungsleitung wird ein interner S_0-Teilnehmer eingerichtet. Die SLC-Rufnummer entspricht der Rufnummer des internen S_0-Teilnehmers.

      ---
   c) Kontrollieren Sie, dass bei dem internen S_0-Teilnehmer das Teilnehmer-Flag **Anklopfschutz ein** deaktiviert ist.
5) Wiederholen Sie bei Bedarf den Schritt 4 für die anderen SLMUC-Baugruppen.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.3.3.8 Wie Sie die Daten zu den Basisstationen abfragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** oder mit dem Hipath 3000 Manager angemeldet. Die folgenden Schritte beziehen sich nur auf das WBM, aber ähnliche Aktionen können auch mit dem Hipath 3000 Manager durchgeführt werden.

Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Cordless**.
3) Klicken Sie im Menübaum auf **Cordless** > **Basisstationen**.
4) Klicken Sie im Menübaum auf die gewünschte Basisstation. Die Daten zur Basisstation werden angezeigt. Eine Erklärung zu den Daten finden Sie unter Cordless>Basisstationen.
5) Sie können bis zu 10 verschiedene Frequenzkanäle gleichzeitig für eine Basisstation auswählen. Eine Erklärung zu den Frequenzkanälen finden Sie in der Tabelle unter Cordless>Basisstationen.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.3.3.9 Wie Sie den Hinweiston der Message Waiting Indication (MWI) für DECT-Telefone aktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** oder mit dem Hipath 3000 Manager angemeldet. Die folgenden Schritte beziehen sich nur auf das WBM, aber

ähnliche Aktionen können auch mit dem Hipath 3000 Manager durchgeführt werden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Systemflags**.
4) Aktivieren Sie im Bereich **Systemflags** das Kontrollkästchen **CMI MWI Hinweiston**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.3.3.10 Wie Sie den Anmeldestatus der DECT-Telefone abfragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** oder mit dem Hipath 3000 Manager angemeldet. Die folgenden Schritte beziehen sich nur auf das WBM, aber ähnliche Aktionen können auch mit dem Hipath 3000 Manager durchgeführt werden.

Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephonie** > **Cordless**.
3) Klicken Sie im Menübaum auf **Cordless** > **SLC**. Es werden alle bereits konfigurierten DECT-Telefone angezeigt.
4) In der Spalte **Aktiv** wird Ihnen zu jedem DECT-Telefon der Anmeldestatus angezeigt:
   - Grün: Mobiltelefon ist aktiv.
   - Rot: Baugruppen-Sperrschalter bei angemeldetem Mobiltelefon gesetzt.
   - Gelb: Mobiltelefon wurde durch Änderung der PIN automatisch wieder abgemeldet.
   - Grau: An diesem Port wurde noch nie ein Mobiltelefon angemeldet.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.3.4 Cordless IP

Cordless IP (DECT IP) ist die optionale Cordless-Lösung als Alternative zur integrierten Cordless-Lösung oder zum Einsatz mit OpenScape Business S.

Die DECT-Telefone an Cordless IP kommunizieren über die BSIP-Basistation mit dem Kommunikationssystem wie SIP-Telefone. Mit Cordless IP können deshalb nur SIP-Leistungsmerkmale genutzt werden. Weitere Informationen zu Cordless IP siehe Dokumentation zu HiPath Cordless IP.

Für alle SIP-Teilnehmer, die an einer Cordless-IP angemeldet sind, muss der Teilnehmer-Parameter **Autom. Rufannahme, CSTA** deaktiviert sein. Ansonsten

kann es dazu führen, dass Anrufe zwischen SIP-Teilnehmern über DECT IP nicht zustande kommen.

19.3.5 WLAN-Telefone und Access Points

WLAN-Telefone und Dual-Mode-Telefone ermöglichen mobile Kommunikation. Diese Telefone können in bereits vorhandene WLAN-Infrastrukturen integriert werden. Mit WLAN Access Points können Sie drahtlose Netze aufbauen und über die gleiche Infrastruktur Sprach- und Datendienste nutzen. Es wird empfohlen nur high-performance WLAN Access Points (z.B. von Enterasys) zu verwenden.

19.3.5.1 Anforderungen an das WLAN

Beim Einsatz von WLAN muss geprüft werden, ob die grundlegenden Anforderungen für Voice-over-WLAN-Einsatz erfüllt sind. Zur Umsetzung des Wireless-Anteils des Netzwerks muss ggf. eine Funkausleuchtung (Site Survey) durchgeführt werden.

Entscheidungshilfen:

- Kleine Installationen bis zu 3 AP können bei einem Standortbesuch oder durch die Bewertung eines Gebäudeplans wirkungsvoll eingestuft werden. Hier ist eine Funkausleuchtung in der Regel nicht erforderlich.
- Bei Installationen ab 4 AP ist in jedem Fall eine Funkausleuchtung durchzuführen. Dies gilt speziell bei Installationen, die sich über mehrere Gebäude oder Stockwerke innerhalb von Gebäuden erstrecken.
- Eine Funkausleuchtung ist unabhängig von der Anzahl der AP auch erforderlich, wenn es sich um eine funk-intensive (RF = radio frequency) Umgebung handelt, oder wenn die Lösung neben anderen, bereits bestehenden WLAN-Systemen existieren soll.

19.4 Heim-Mobilität

Heim-Mobilität wird durch Telearbeit erreicht. Dies geschieht durch die Integration von nicht lokalen Telefonen (wie z. B. einem Festnetz- oder Mobiltelefon) in das OpenScape Business Kommunikationsnetzwerk.

Die folgenden Arten von Telearbeitsplätzen stehen zur Verfügung:

- VPN-Arbeitsplätze

  OpenScape Business verfügt über eine integrierte VPN-Funktionalität. Insgesamt können 10 Telearbeiter gleichzeitig über VPN aktiv sein. Dies kann über einen Heim-PC oder ein Mobiltelefon mit Android- oder iOS-Betriebssystem erfolgen. Die VPN-Verbindung wird zwischen dem nativen VPN-Client des PCs oder Mobiltelefons und dem OpenVPN-Server von OpenScape Business hergestellt.

  Benutzer der UC Suite können ihre private Telefonnummer von zu Hause aus über ihren UC-Client angeben und dann ihr privates Telefon als Bürotelefon verwenden (CallMe).

- Device@Home: SIP@Home Stationen oder System Device@Home Stationen

  STUN-fähige SIP-Telefone (z. B. Yealink T19) (SIP Device@Home-Stationen) oder HFA-Telefone (System Device@Home-Stationen) können sich über das Internet mithilfe der internen SBC-Funktion von OpenScape Business beim Kommunikationssystem registrieren. Dazu muss die Funktion in den Stationsdaten für jedes SIP-Telefon oder HFA-Telefon über das WBM aktiviert werden.

  Ein STUN-Server muss zusätzlich im WBM angegeben werden, nur wenn kein ITSP verwendet wird oder wenn der verwendete ITSP keinen STUN-Server anbietet.

  SIP Device@Home unterstützt keine Übertragung von Videosignalen.

  Anmerkung: Bei der Verwendung mehrerer SIP/HFA @Home Geräte hinter demselben Router können NAT-Einschränkungen aufgrund von Konflikten bei der Wiederverwendung von Ports zu Problemen mit der Anruf-Nutzlast führen. Um dies zu vermeiden, konfigurieren Sie bitte jedes Gerät mit einem eindeutigen Quellport (RTP).

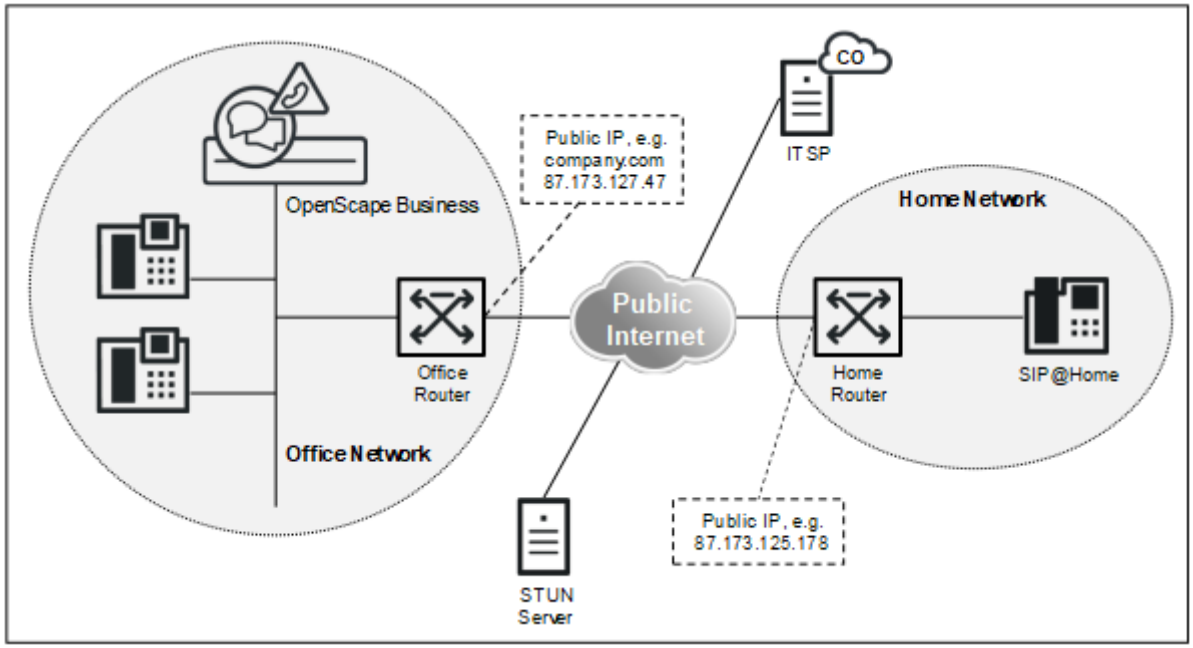


Abbildung 9: Device@Home-Komponenten (SIP Device@Home oder System Device@Home)

19.4.1 Konfiguration für VPN

Um Teilnehmer über die integrierte VPN-Funktionalität an das Kommunikationssystem anzuschließen, sind Konfigurationen an OpenScape Business und den VPN-Teilnehmern durchzuführen.

Konfiguration OpenScape Business

Für die VPN-Konfiguration des Kommunikationssystems siehe Wie Sie die Anbindung von Teleworkern über VPN konfigurieren .

Konfiguration VPN-Teilnehmer (VPN-Client)

Für die Konfiguration der VPN-Clients siehe VPN-Clients .

19.4.2 Konfiguration für SIP-Gerät@Home

Um Verbindungen über das Internet von einem STUN-fähigen SIP-Telefon zu OpenScape Business über das Internet herzustellen, sind bestimmte Konfigurationen durchzuführen.

Konfiguration von OpenScape Business

Damit sich ein SIP-Teilnehmer über das Internet am Kommunikationssystem registrieren kann, muss für den SIP-Teilnehmer die integrierte SBC-Funktion aktiviert werden (siehe Wie Sie Gerät@Home aktivieren).

Die integrierte SBC-Funktion erkennt mit Hilfe des STUN-Protokolls die öffentliche IP-Adresse des Kommunikationssystems und den verwendeten Port. Ist das Kommunikationssystem mit einem ITSP verbunden, der einen STUN-Server anbietet, muss keine weitere Konfiguration am Kommunikationssystem vorgenommen werden. Wird aber entweder kein ITSP verwendet oder bietet der genutzte ITSP keinen STUN-Server an, muss ein STUN-Server im System konfiguriert werden (siehe Wie Sie einen STUN-Server für Gerät@Home angeben).

Konfiguration des Office-Internet-Routers

Damit das SIP-Telefon das Kommunikationssystem über das Internet erreichen kann, muss im Office-Internet-Router eine Portweiterleitung für den externen SIP-Port eingerichtet werden. Um SIP-Attacken aus dem Internet zu vermeiden, muss als externer SIP-Port ein vom Standard abweichender SIP-Port verwendet werden.

Das Transport-Protokoll ist am SIP-Telefon einzustellen.

Tabelle 9: Portweiterleitung im Office-Router konfigurieren

Transportpr	Interner SIP-Port	Externer SIP-Port	Kommentar
UDP	5070	Eingabe von z. B. 5090.	Für die Portweiterleitung müssen externer und interner SIP-Port nicht gleich sein. Als externer SIP-Port kann somit ein vom internen Standard-SIP-Port 5070 abweichender Wert eingegeben werden. Daher wird UDP empfohlen.

Transportpr	Interner SIP-Port	Externer SIP-Port	Kommentar
TCP	5070 Ändern in z. B. 5080.	Eingabe von z. B. 5080 (= interner SIP-Port)	Für die Portweiterleitung müssen externer und interner SIP-Port gleich sein. Um einen vom Standard-SIP-Port 5070 abweichenden externen SIP-Port zu verwenden, muss der interne SIP-Port geändert werden. Das erfordert eine Umkonfiguration aller IP-Komponenten, die SIP verwenden. Daher wird TCP **nicht** empfohlen.
TLS	5071	Eingabe von 5071 (= interner SIP-TLS-Port)	Für die Portweiterleitung müssen externer und interner SIP-TLS-Port gleich sein. Da bereits der interne SIP-TLS-Port vom Standard-SIP-TLS-Port abweicht, kann als externer SIP-TLS-Port auch 5071 eingegeben werden. Daher wird TLS empfohlen.

Anmerkung: In einem aktualisierten System wird eine Änderung der SIP-Ports nicht automatisch durchgeführt. Nach der Aktualisierung sind die Ports:

SIP_EXT = 5060

SIP_TLS_SUB_EXT = 5062

Diese Werte müssen vom Administrator manuell vorgenommen werden, wenn Gerät@Home im migrierten System genutzt wird.

Für TLS müssen im Kommunikationssystem gültige Zertifikate aktiviert sein. TLS Verbindungen für SIP-Teilnehmer werden an der LAN-Schnittstelle des Kommunikationssystems unterstützt, nicht aber an der WAN-Schnittstelle. SRTP-Payload mit SDES-Signalisierung wird nicht unterstützt.

Ist der Office-Internet-Router ohne feste IP-Adresse mit dem Internet verbunden, muss im Office-Internet-Router DynDNS konfiguriert sein, damit der SIP-Teilnehmer das Kommunikationssystem über das Internet erreichen kann. Über den DynDNS-Account wird die aktuelle IP-Adresse in regelmäßigen Abständen registriert. Bei kostenlosen DynDNS-Accounts, die in regelmäßigen Abständen ablaufen, kann das zeitweise zu Störungen führen.

Konfiguration SIP-Telefon

Als Konfigurationsbeispiel finden Sie eine Liste aller getesteten SIP-Telefone, die STUN unterstützen, im Internet im Unify Experts Wiki. Sie finden dort die Werte, die am SIP-Telefon eingegeben werden müssen.

Konfiguration des Home-Internet-Routers

Am Home-Internet-Router ist keine spezielle Konfiguration erforderlich.

Folgende Anforderungen muss der Home-Internet-Router erfüllen:

- Der Router muss VoIP-Funktionalität mit eingeschalteter NAT zur Verfügung stellen (keine symmetrische NAT).
- Die ALG-Funktion muss im Router deaktiviert sein.

Die Internetverbindung muss genügend Bandbreite für die Gesprächsübertragung zur Verfügung stellen. Besonders bei asymmetrischen DSL-Verbindungen ist auf genügend Upload-Bandbreite zu achten.

myPortal @work konfigurieren

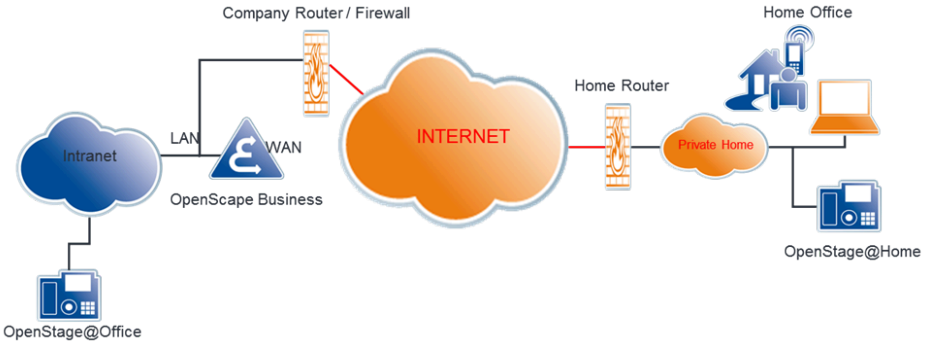
Damit myPortal @work über das Internet auf das Kommunikationssystem zugreifen kann, müssen Sie Folgendes durchführen:

- STUN-Server für System/Client konfigurieren
- Port 8802 öffnen und weiterleiten (andere Weiterleitungen sind ungültig)
- Das SBC-Flag wird nicht benötigt. Es ist keine Authentifizierung erforderlich.

19.4.3 Konfiguration für Systemgerät@Home

Um Verbindungen über das Internet von einem Systemgerät-Telefon zur OpenScape Business herzustellen, sind bestimmte Konfigurationen an OpenScape Business, dem Office-Internet-Router und dem Systemgerät-Telefon durchzuführen.

- **Abbildung 10: Beispiel für einen Systemgerät@Home-Anwendungsfall**



Konfiguration von OpenScape Business

Damit sich ein Systemgerät@Home-Teilnehmer über das Internet am Kommunikationssystem registrieren kann, muss für den Systemgerät@Home-Teilnehmer die integrierte SBC-Funktion aktiviert werden (siehe Wie Sie Gerät@Home aktivieren auf Seite 993).

Die integrierte SBC-Funktion erkennt mit Hilfe des STUN-Protokolls die öffentliche IP-Adresse des Kommunikationssystems und den verwendeten Port. Ist das Kommunikationssystem mit einem ITSP verbunden, der einen STUN-Server anbietet, muss keine weitere Konfiguration am Kommunikationssystem vorgenommen werden. Wird aber entweder kein ITSP verwendet oder bietet der genutzte ITSP keinen STUN-Server an, muss dem Kommunikationssystem ein STUN-Server bekanntgegeben werden (siehe STUN-Server für Systemgerät@Home angeben).

Konfiguration des Office-Internet-Routers

Damit Systemgerät@Home-Teilnehmer das Kommunikationssystem über das Internet erreichen können, muss im Office-Internet-Router eine Portweiterleitung für den Systemgerät-Port eingerichtet werden. Um sich aus dem Internet registrieren zu können, muss im Office-Router bzw. in der Firewall eine Regel für Portweiterleitung eingerichtet werden:

- externer Port TCP/4060 zu interner Port TCP/4062 (HFA), für nicht-TLS

  externer Port TCP/4061 zu interner Port TCP/4063 (HFA), für TLS

  Anmerkung: Während der Migration von V2R1 auf eine höhere Version sollte der Office-Internet-Router entsprechend dieser Regel umkonfiguriert werden.

  Die oben genannten Ports werden nur für Systemgeräte (HFA-Telefon) benötigt.

- RTP-Port-Bereich für OpenScape Business X: 30274-30529. RTP-Port-Bereich für OpenScape Business S: 30528-30887 (Standardwerte)

  VoIP-fähige UC-Clients wie myPortal to go, myPortal @work benötigen diese Ports ebenfalls.

- TCP/8802 (HTTPS) (erforderlich für den Unified Communications-Client (z. B. myPortal to go, my Portal to go Web, my Portal @work oder VoIP für myPortal to go, wenn als Systemgerät@Home konfiguriert)

  Anmerkung: Die interne Firewall-Zone muss geschlossen werden.

Das Transport-Protokoll ist am Systemgerät@Home-Teilnehmer einzustellen.

Ist der Office-Internet-Router ohne feste IP-Adresse mit dem Internet verbunden, muss im Office-Internet-Router DynDNS konfiguriert sein, damit der Systemgerät@Home-Teilnehmer das Kommunikationssystem über das Internet erreichen kann. Über den DynDNS-Account wird die aktuelle IP-Adresse in regelmäßigen Abständen registriert. Bei kostenlosen DynDNS-Accounts, die in regelmäßigen Abständen ablaufen, kann das zeitweise zu Störungen führen.

Konfiguration des Home-Internet-Routers

Am Home-Internet-Router ist keine spezielle Konfiguration erforderlich.

Folgende Anforderungen muss der Home-Internet-Router erfüllen:

- Der Router muss VoIP-Funktionalität mit eingeschalteter NAT zur Verfügung stellen (keine symmetrische NAT).
- Die ALG-Funktion muss im Router deaktiviert sein.

Die Internetverbindung muss genügend Bandbreite für die Gesprächsübertragung zur Verfügung stellen. Besonders bei asymmetrischen DSL-Verbindungen ist auf genügend Upload-Bandbreite zu achten.

Konfiguration des HFA-Telefons

Das Gateway muss mit dem DNS-Namen (z.B. meinefirma.net) so konfiguriert werden, dass das Telefon das System über das Internet erreichen kann. Die IP von DLI muss auch konfiguriert werden. Für den Teilnehmer muss eine interne Rufnummer hinzugefügt werden. Außerdem muss das Gerätepasswort festgelegt werden.

Einschränkungen

- Die Konfiguration von XML-Anwendungen an OpenStage ist nicht möglich.

19.4.4 Wie Sie Gerät@Home aktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer** > **IP-Clients** > **SIP-Clients** oder **System-Clients**
4) Klicken Sie im Menübaum auf den gewünschten SIP- oder HFA-Teilnehmer.
5) Klicken Sie auf die Registerkarte **Workpoint-Clientdaten ändern**.
6) Achten Sie darauf, dass ein Passwort eingegeben wurde. Die hier angegebenen Werte müssen auch am SIP-Telefon oder Systemgerät eingetragen sein.

Anmerkung:

Bei einer Verbindung über das Internet sollte unbedingt ein sicheres Kennwort verwendet werden (mindestens 8 Zeichen inkl. Großbuchstaben, Ziffer und Sonderzeichen).

Anmerkung: Das Passwort von als @Home deklarierten of Deskshare-Clients darf nur numerische Zeichen enthalten. Dieses Passwort ist eigentlich der PIN-Code für die Aktivierung der Mobility-Funktion (Servicecode der Funktion: *9419). Die Geräte unterstützen nur numerische Zeichen als PIN.

Nach dem Festlegen des Passworts kann die Option **Internet-Registrierung mit internem SBC** aktiviert werden.

Anmerkung: Nach einem Speed-Upgrade oder dem Neustart des Systems wird das Kontrollkästchen **Authentifizierung aktiv** für alle SIP-Endpunkte aktiviert und ausgegraut, damit der Benutzer sie nicht deaktivieren kann, wenn mindestens ein SIP-Teilnehmer das Flag **Internet-Registrierung mit internem SBC** aktiviert hat.

19.4.5 Software-Update für Systemgerät (HFA) @Home

Der normale SW-Update-Vorgang des DLI für ein intern angeschlossenes Gerät kann nicht für Systemgerät (HFA) @Home verwendet werden, da hierfür

ein direkter Zugriff auf die IP-Adresse des Geräts für die Dateiübertragung erforderlich ist. Das DLI kann die IP-Adresse des Systemgeräts@ Home aus folgenden Gründen nicht ermitteln:

- Das Gerät@Home befindet sich in einem Heimnetzwerk und nutzt private IP-Adressen. Der Internetzugang erfolgt über einen Home Router mit NAT (Network Address Translation).
- Das DLI innerhalb von OpenScape Business befindet sich in einem Unternehmens-/Büronetzwerk und nutzt private IP-Adressen. Das Unternehmensnetzwerk ist über den Firmen- /Büro-Router mit dem Internet verbunden.

Daher verwendet das DLI SW-Update-Verfahren eine zusätzliche HTTPS-Verbindung über Port 8804 (Standardeinstellung) in Kombination mit dem DLI-Port 18443 (Standardeinstellung), um die SW-Version des Gerät@Home zu ermitteln und das SW-Update vorzunehmen.

Die SW-Versionsprüfung für ein Gerät@Home wird nur durchgeführt, wenn eine der folgenden Bedingungen zutrifft:

- Geräte-Neustart
- Konfigurationsänderung lokal oder remote
- Inventory-Änderungen des Geräts
- An- oder Abmelden eines mobilen Benutzers auf einem Gerät

In diesen Fällen prüft das DLI die Softwareversion des Geräts und führt ein SW-Update durch, wenn in OpenScape Business eine neuere SW-Version verfügbar ist.

Das automatische Software-Update eines Gerät@ Home durch das DLI muss in OpenScape Business konfiguriert werden. Es ist standardmäßig deaktiviert und muss explizit aktiviert werden.

Die folgenden Schritte sind erforderlich.

Schritt für Schritt

1) Sie sind am WBM mit dem Profil Expert angemeldet.

2) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

3) Klicken Sie im Navigationsbaum auf **Telefonie-Server> Grundeinstellungen**.

4) Klicken Sie im Navigationsbaum auf **Grundeinstellungen > Telefonparameter-Bereitstellung**.

- Durch Klicken auf **SW an @Home-Geräte verteilen** werden Berechtigungen für das Software-Update über das DLI für Systemgeräte (HFA) @Home erteilt. Der Standardwert ist ’deaktiviert’.
- Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

5) Firewall-Einstellungen

In OpenScape Business sind keine manuellen Firewall-Einstellungen erforderlich. Der Port 8804 wird während des Systemstarts geöffnet, und eingehende Anforderungen werden nur dann vom System beantwortet, wenn das Flag **SW an@Home-Geräte verteilen** gesetzt ist.

6) Öffnen Sie die verwendeten Ports 18443 und 8804 für das DLI mit der richtigen Konfiguration (Portweiterleitung) im Unternehmens-/Büro-Router.

Einschränkungen

Das HFA@Home-Gerät befindet sich hinter einer Firewall (Home-Router). Der Router oder die Firewall veranlasst eine Netzwerkadressübersetzung (Network Address Translation, NAT), sodass die IP-Adresse von außen nicht sichtbar ist. Daher können IP-Telefone nicht per Fernzugriff angezeigt und vom DLI verwaltet werden.

Aufgrund dieser Einschränkung können DLI-gesteuerte Ereignisse nicht ausgeführt werden, da diese Ereignisse an die lokale (nicht zugängliche) IP-Adresse des Geräts gesendet werden.

Dies hat zur Folge, dass kein On-Demand-Software-Update möglich ist. Andererseits ist ein Software-Update möglich, wenn das Gerät einen Nachrichtenaustausch initiiert, indem es eine HTTPS-Sitzung zum DLI öffnet. Sitzungen werden aufgrund bestimmter gerätegesteuerter Ereignisse geöffnet, etwa:

- Neustart des Geräts
- Konfigurationsänderung am Gerät (über lokales oder webbasiertes Management)
- Inventory-Änderungen des Geräts
- An- oder Abmeldung eines mobilen Benutzers auf einem Gerät

In all diesen Fällen überprüft das DLI die Software des Geräts und bei Bedarf wird das Gerät auf die offizielle Software aktualisiert, die von OSBiz unterstützt wird.

Anmerkung: Die Softwareverteilung erfolgt bei Inbetriebnahme des Telefons (entweder bei der Registrierung bei OSBiz oder bei Inbetriebnahme des OSBiz-Systems).

19.4.6 Wie Sie einen STUN-Server für Gerät@Home angeben

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Es wird kein ITSP verwendet oder der genutzte ITSP bietet kein STUN-Server an.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sprachgateway**.

3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.

4) Klicken Sie auf die Registerkarte **STUN-Konfiguration ändern**.

5) Geben Sie im Bereich **Default STUN Server** unter **IP-Adresse / Hostname** die IP-Adresse oder den Hostnamen des STUN-Servers ein (z.B. `stun.serviceprovider.com`).

6) Geben Sie im Bereich **Default STUN Server** unter **Port** den Port des STUN-Servers ein (z.B. `3478`).

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20 Sicherheit

Security umfasst den Schutz des Kommunikationssystems und der gespeicherten und übertragenen Daten vor unbefugtem Zugriff. Dieser kann unter anderem durch Zugriffsschutz für das IP-Netz (Firewall) und verschlüsselte Übertragung (SSL, VPN) erfolgen.

Security Checklist

Das Kommunikationssystem berücksichtigt in den Voreinstellungen die Sicherheit der Kommunikation. Bei der Inbetriebnahme sind Funktionen an die individuelle Situation des Kunden anzupassen und weitere Vorkehrungen im Kundenumfeld zu treffen. Um das Bewusstsein für Sicherheitsrisiken zu schärfen und geeignete Maßnahmen zu implementieren, wird mit der Produktdokumentation eine Security Checklist bereitgestellt. Es wird dringend empfohlen, diese bei der Inbetriebnahme mit dem Kunden zu besprechen und die Maßnahmen zu dokumentieren.

20.1 Firewall

Eine Firewall ist ein System aus Software- und Hardwarekomponenten, das den Zugriff zwischen verschiedenen Netzwerken beschränkt, um ein Sicherheitskonzept umzusetzen.

Firewalls sitzen an den Schnittstellen zwischen einzelnen Netzen und kontrollieren den Datenverkehr zwischen den Teilbereichen, um ungewünschten Datenverkehr zu verhindern und nur den gewünschten Verkehr passieren zu lassen. Der häufigste Einsatz einer Firewall besteht darin, den Verkehr zwischen einem lokalen Netz (LAN) und dem Internet zu kontrollieren.

In jedem Firmennetz entkoppelt eine Firewall das interne LAN vom Internet.

Das Kommunikationssystem bietet integrierte Sicherheitsfunktionen; dabei unterscheiden sich OpenScape Business X und OpenScape Business S in der Funktionalität.

OpenScape Business X bietet folgende Leistungsmerkmale:

- Port Firewall / NAT (Firewall zwischen WAN-Port und LAN)
- Application Firewall (Firewall für den Zugang zum Kommunikationssystem)

OpenScape Business S nutzt die Linux-Firewall.

20.1.1 Porthandling

Das Porthandling dient zur Portfreischaltung (Port Mapping, Portweiterleitung) in der Firewall des integrierten Routers der OpenScape Business X.

Portnummern

Anmerkung: Öffnen Sie nur dann Ports, wenn es für eine bestimmte Anwendung zwingend erforderlich ist!

Ports (Services oder Dienste) sind für die Kommunikation über die Protokolle TCP und UDP erforderlich, da sie es mehreren Anwendungen ermöglichen über eine einzige Verbindung gleichzeitig Daten auszutauschen.

Unter dem Begriff Firewall versteht man im Allgemeinen eine Port-Firewall (also das Sperren einzelner Dienste/Services oder auch Ports genannt). Die Port-Firewall wirkt nur auf den WAN-Anschluss von OpenScape Business.

Bei OpenScape Business S kann man auf dem LAN-Anschluss unter Linux eine Port-Firewall aktivieren. Bei OpenScape Business X ist die Firewall auf dem WAN-Anschluss aktiv um das interne Netz (am LAN-Anschluss) vor Angriffen aus dem Internet zu schützen. Sollen trotzdem bestimmte Ports/Dienste aus dem Internet erreichbar sein müssen diese freigegeben werden (siehe Portfreigabe). Alle Ports/Dienste für die Funktionalität von OpenScape Business X sind auf dem LAN-Anschluss (zum internen Kundennetz hin) automatisch freigegeben.

OpenScape Business S besitzt nur einen LAN-Anschluss (ins interne Kunden-Netz) und wird gegenüber dem Internet durch andere Komponenten/Router im Kundennetz geschützt. Zusätzlich ist die Server-interne Linux-Firewall aktiviert. Für die OpenScape Business Funktionalität müssen bestimmte Ports/Dienste freigegeben werden (damit z.B. die Telefone mit OpenScape Business S kommunizieren können). Dies geschieht automatisch, der Administrator kann jedoch einzelne Dienste sperren.

Portnummern können Werte zwischen 0 und 65535 annehmen und werden so den verschiedenen Anwendungen zugeordnet. Zwischen 0 und 1023 liegen die sogenannten 'Well Known Ports', welche von der IANA (Internet Assigned Numbers Authority) fest zugeordnet worden und allgemein bekannt sind. Eine Liste dieser Ports können Sie unter http://www.iana.org/assignments/port-numbers einsehen.

20.1.1.1 Portfreigabe

Stellt das System den Internetzugang (über den WAN-Port) her, so ist standardmäßig nur die Kommunikation erlaubt, die von innen (aus dem Firmennetz oder vom Kommunikationssystem selbst) ins Internet führt und die dazugehörigen Antwortpakete. Anfragen, die initial aus dem Internet kommen, werden geblockt. Diese Sicherheitseinstellung kann durch die gezielte Portfreigabe umgangen werden, um z.B. einen Webserver im Netz zu betreiben.

Anmerkung: Wenn das Kommunikationssystem als Internet Router genutzt wird, muss Port 5060 geschlossen sein (Standardeinstellung). Bei Internettelefonie über ITSP öffnet das Kommunikationssystem die relevanten Ports und hält diese offen.

Auch wenn ein externer Router bzw. Firewall genutzt wird, muss Port 5060 geschlossen sein. Es liegt in der Verantwortung des Kommunikationssystems diesen Port (falls benötigt) zu öffnen.

20.1.1.2 Wie Sie die Portfreigabe konfigurieren

Mit dem Wizard **Firewall** können Sie Portfreigaben aktivieren, so dass das Kommunikationssystem oder der PC am LAN über den WAN-Port erreichbar sind. Portfreigaben bergen das Risiko des Zugriffs durch Unbefugte. Daher sollten nur die Ports freigegeben werden, die dringend erforderlich sind.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Sicherheit**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Firewall** zu starten. Es öffnet sich das Fenster **Portfreigabe**.
4) Aktivieren Sie in der Zeile der gewünschten Anwendung bzw. des gewünschten Dienstes das Kontrollkästchen **NAT-Regel aktiv**, für die Sie Ports freigeben möchten.
5) Geben Sie in den Feldern **Globaler Port**, **Lokale IP-Adresse** und **Lokaler Port** jeweils die Daten zur Freigabe ein.
6) Klicken sie für die Portfreigabe eines nicht eingetragenen Dienstes auf **Hinzufügen** und füllen Sie die Felder **Beschreibung**, **NAT-Regel aktiv**, **Globaler Port**, **Lokale IP-Adresse** und **Lokaler Port** aus.
7) Klicken Sie auf **OK & Weiter**.
8) Klicken Sie auf **Beenden**.

20.1.1.3 Port-Verwaltung

Die Port-Verwaltung ermöglicht es, einige der Ports, die das Kommunikationssystem selbst verwendet, zu verändern. Dadurch kann z.B. in einem Netzwerk die Kommunikation auf das Kundennetz abgestimmt werden, auch wenn die Ports bereits anderweitig verwendet werden.

Wenn an der Portverwaltung Änderungen vorgenommen werden, muss dies in der Regel an allen Komponenten (Telefone, Anlagen etc.) gleichzeitig geändert werden, damit die Funktionalität gewährleistet bleibt.

20.1.1.4 Wie Sie globale Port-Manager-Einstellungen ändern

Hier geben Sie die Portnummern für die einzelnen Funktionen ein.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Port-Verwaltung**. Es öffnet sich die Registerkarte **Globale Port-Manager-Einstellungen ändern**.
4) Geben Sie unter **Port-Nummer** den Port für die jeweilige Funktion ein, bzw. lassen die Voreinstellung bestehen.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.1.2 NAT

NAT (Network Address Translation) ist ein Adressenumsetzungsverfahren, um eine IP-Adresse in einem Datenpaket durch eine andere zu ersetzen. In einem internen Netz nutzen die Clients private IP-Adressen. Da private IP-Adressen in einem öffentlichen Netz nicht weitergeleitet werden, ist es mit NAT möglich, die privaten IP-Adressen auf eine öffentliche IP-Adresse abzubilden. Somit haben die internen Clients Zugang zum öffentlichen Netz und die Struktur des internen Netzes mit den privaten IP-Adressen ist gegenüber dem öffentlichen Netz (z.B. Internet) unsichtbar (maskiert). NAT bzw. NAT-Regeln werden für die Portfreigabe benötigt.

Die Adressenumsetzung wird an dem Übergang zwischen einem internen und einem öffentlichen Netz durchgeführt. NAT kann auf einem Internet-Router, einem Server oder einem anderen spezialisierten Gerät laufen. So kann z.B. ein Internet-Router mit Hilfe von NAT das interne Netz mit dem Internet verbinden.

Das interne Netz tritt gegenüber dem Internet mit nur einer einzigen öffentlichen IP-Adresse auf, die dem Internet-Router vom Internet-Service-Provider (ISP) zugewiesen wird. Alle Zugriffe aus dem internen Netz heraus in das Internet werden über diese offizielle IP-Adresse mit verschiedenen Port-Nummern abgewickelt. Der Internet-Router ersetzt die privaten IP-Adressen durch die vom ISP zugewiesene offizielle IP-Adresse. Bei ankommenden Datenpaketen wird die offizielle IP-Adresse wieder durch die privaten IP-Adressen ersetzt. Für die Zuordnung sind die jeweiligen Portnummern entscheidend. Nur extra freigeschaltete private IP-Adressen sind direkt aus dem Internet zu erreichen.

NAT-Regeln

Mit Hilfe von NAT-Regeln kann festgelegt werden, ob private (lokale) IP-Adressen direkt aus dem Internet erreichbar sein sollen. Dazu können eigene NAT-Regeln definiert oder die bereits vorgeleisteten Standard-NAT-Regeln für die Dienste FTP-Server, HTTP-Server usw. verwendet werden. Insgesamt sind 20 NAT-Regeln definierbar. Um eine NAT-Regel zu nutzen, müssen die lokalen Adressendaten des Client-PCs eingegeben werden, der diese Dienste für das Internet zur Verfügung stellen will und die NAT-Regel muss aktiviert werden. Mehrere NAT-Regeln können zusammen mit Hilfe eines Tabelleneditors konfiguriert werden. Nicht mehr benötigte NAT-Regeln können gelöscht werden.

Ports

Startende Server fordern beim Betriebssystem bestimmte Ports an, um Verbindungen annehmen zu können. Ein HTTP-Server den Port 80, ein FTP-Server der Port 21 usw. Clients fordern beim Betriebssystem normalerweise einen zufälligen Port an, um Verbindungen aufbauen zu können.

20.1.2.1 Wie Sie eine NAT-Regel konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Routing**.
3) Konfigurieren Sie die NAT-Regel:
   - Wenn Sie eine neue NAT-Regel definieren wollen, klicken Sie im Menübaum auf **NAT** und anschließend auf die Registerkarte **NAT hinzufügen**.
   - Wenn Sie eine vorhandene NAT-Regel ändern wollen, navigieren Sie im Menübaum **NAT** zur gewünschten NAT-Regel.
4) Geben Sie im Feld **Beschreibung** einen Namen für die NAT-Regel an. Bei einer Standard-NAT-Regel kann dieser Name nicht geändert werden.
5) Geben Sie im Feld **Lokale IP-Adresse** die IP-Adresse des Clients im internen Netz ein, der freigeschaltet werden soll.
6) Geben Sie im Feld **Lokaler Port** die Port-Nummer ein, die die Anwendung des internen Clients verwendet.
7) Geben Sie im Feld **Globaler Port** die Port-Nummer ein, die die Anwendung des externen Kommunikationspartners verwendet.
8) Wählen Sie in der Aufklappliste **Protokoll** das von der Anwendung verwendende Transportprotokoll (**TCP** oder **UDP**) aus. Bei einer Standard-NAT-Regel kann das Protokoll nicht geändert werden.
9) Wenn Sie die NAT-Regel anwenden möchten, aktivieren Sie das Optionsfeld **NAT-Regel aktiv**.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**. Die aktivierte NAT-Regel wird unter dem Menüpunkt **NAT** mit einem grünen Symbol gekennzeichnet.

20.1.2.2 Wie Sie mehrere NAT-Regeln mit dem NAT-Tabelleneditor konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie in der Navigationsleiste auf **Telefonie** > **Routing**.
3) Klicken Sie im Menübaum auf **Routing**.
4) Klicken Sie im Menübaum auf **NAT** und anschließend auf die Registerkarte **NAT Tabelleneditor**.

5) Konfigurieren Sie die NAT-Regel:
   - Wenn Sie eine neue NAT-Regel definieren wollen, füllen Sie die Felder der ersten Zeile wie unten beschrieben aus.
   - Wenn Sie eine vorhandene NAT-Regel ändern wollen, klicken Sie in die gewünschten Felder der NAT-Regel und füllen Sie diese wie unten beschrieben aus.
6) Geben Sie in der Spalte **Lokale IP-Adresse** die IP-Adresse des Clients im internen Netz ein, der freigeschaltet werden soll.
7) Geben Sie in der Spalte **Lokaler Port** die Port-Nummer ein, die die Anwendung des internen Clients verwendet.
8) Geben Sie in der Spalte **Globaler Port** die Port-Nummer ein, die die Anwendung des externen Kommunikationspartners verwendet.
9) Wählen Sie in der Aufklappliste **Protokoll** das von der Anwendung verwendende Transportprotokoll (**TCP** oder **UDP**) aus. Bei einer Standard-NAT-Regel kann das Protokoll nicht geändert werden.
10) Um die NAT-Regel anzuwenden, setzen Sie in der Spalte **Aktiv** das Häkchen.
11) Geben Sie in der Spalte **Beschreibung** einen Namen für die NAT-Regel an. Bei einer Standard-NAT-Regel kann dieser Name nicht geändert werden.
12) Speichern Sie die NAT-Regel:
   - Wenn Sie eine neue NAT-Regel konfiguriert haben, klicken Sie auf **Hinzufügen** und anschließend auf **OK**. Die neue NAT-Regel wird am Ende der Tabelle eingefügt.
   - Wenn Sie eine vorhandene NAT-Regel geändert haben, gehen Sie zu Schritt 5.
13) Klicken Sie auf **Übernehmen**. Eine aktivierte NAT-Regel wird unter dem Menüpunkt **NAT** mit einem grünen Symbol gekennzeichnet.

20.1.2.3 Wie Sie eine NAT-Regel löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Telefonie** > **Routing**.
2) Klicken Sie im Navigationsbaum auf **Routing**.
3) Klicken Sie im Menübaum auf **NAT**.
4) Klicken Sie im Menübaum auf die zu löschende NAT-Regel und klicken Sie auf die Registerkarte **NAT löschen**. Vordefinierte Standard-NAT-Regeln können nicht gelöscht werden.
5) Bestätigen Sie den Warnhinweis mit **Löschen** und klicken Sie anschließend auf **OK**. Die NAT-Regel wird unter dem Menüpunkt **NAT** aus der Liste der NAT-Regeln gelöscht.

20.1.3 Application Firewall

Die Anwendungsfirewall wird verwendet, um den Zugriff auf bestimmte Dienste wie FTP oder LDAP einzuschränken. Es ist standardmäßig deaktiviert und kann durch Definieren geeigneter Regeln aktiviert werden.

Die folgenden Dienste können von der Anwendungsfirewall in OpenScape Business X entweder blockiert oder auf bestimmte IP-Adressen oder IP-Adressbereiche beschränkt werden:

Dienst	Ports
FTP	21, 40000 - 40040
ssh (standardmäßig gesperrt)	22
LDAP	389
HTTPS	443
Postgres	5432
Manager E	7000
CSTA	7001 (FP), 7004 (FP), 8800 (CSP)
OBSERVER	Dieser Dienst ermöglichte den Zugriff von einer OpenScape Observer-Anwendung, die nicht mehr unterstützt wird.

Nur die aufgeführten Dienste können über ein Auswahlmenü im Expertenmodus gesperrt werden.

Telefonmerkmale wie SIP, HFA usw. können über die Anwendungsfirewall nicht blockiert werden.

Ein Dienst kann mehrfach ausgewählt werden; Jedes Mal können unterschiedliche IP-Beschränkungen angegeben werden.

Anmerkung: Die Aktivierung/Deaktivierung oder Änderung von Firewall-Parametern kann die Funktionalität der Platine stark einschränken (z.B. eine LAN-basierte Administration ist nicht mehr möglich).

Anmerkung: Wenn die Anwendungsfirewall aktiviert ist, werden Dienste standardmäßig erst blockiert, wenn eine Regel für diesen Dienst hinzugefügt wird. Zu diesem Zeitpunkt können nur IP-Adressen, die in der Regel enthalten sind, auf diesen bestimmten Dienst zugreifen.

Die Anwendungsfirewall kann den Zugriff auf Merkmale zwischen Knoten einschränken, wenn das System mit anderen OpenScape Business-Systemen vernetzt ist. Wenn in diesem Fall eine Regel für den POSTGRES-Dienst hinzugefügt wird, fügen Sie der POSTGRES-Regel manuell die IP-Adressen der anderen OpenScape Business-Netzwerkknoten hinzu, um den korrekten Betrieb der Überlebensfähigkeit sicherzustellen.

20.1.3.1 Wie Sie die Konfiguration der Application Firewall anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **Application Firewall**.
4) Klicken Sie auf die Registerkarte **Services anzeigen** um die gesperrten Dienste anzuzeigen.
5) Im Feld **Regelname** wird Ihnen der Name der Regel angezeigt.
6) Unter **Regel aktiviert** sehen Sie am Häckchen ob eine Regel aktiviert ist oder nicht.
7) Im Feld **Untergrenze des Quell-IP-Adressbereichs** sehen Sie die untere Grenze der gesperrten IP-Adressen.
8) Im Feld **Obergrenze des Quell-IP-Adressbereichs** sehen Sie die obere Grenze der gesperrten IP-Adresse.

20.1.3.2 Wie Sie Dienste über die Application Firewall einschränken

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **Application Firewall**.
4) Klicken Sie auf die Registerkarte **Service hinzufügen**, um einen IP-Adressbereich bzw. Dienst zu sperren.
5) Vergeben Sie unter **Regelname** einen Namen für diesen Dienst (diese Regel).
6) Unter **Adressbereich** legen Sie die **Untergrenze** und die **Obergrenze** der zulässigen Quell-IP-Adressen fest.

   Es ist möglich den Zugriff komplett zu sperren durch die Eingabe von 127.0.0.1.

   Tipp: Aktivieren sie eine Regel erst nachdem sie sich überzeugt haben, dass die berechtigten IP-Adressen korrekt konfiguriert wurden!

   ---

7) Klicken Sie auf **Speichern**.

20.1.3.3 Wie Sie die Konfiguration der Application Firewall löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **Application Firewall**.
4) Klicken Sie auf die Registerkarte **Delete all Services** um alle Dienste zu löschen.

20.1.4 Diensteverwaltung (OpenScape Business S)

Die Linux-interne Firewall ist standardmäßig aktiviert, wodurch der Zugriff auf OpenScape Business S unterbunden ist. Das Kommunikationssystem stellt allerdings Dienste zur Verfügung (z.B. den Dienst Telefonie), für den offene Ports (Dienste oder Services) erforderlich sind. Nach der Installation von OpenScape Business S sind diese erforderlichen Ports/Dienste in der Firewall geöffnet. Falls Dienste wie z.B. SNMP nicht genutzt werden sollen, können sie in der Linux-Firewall gesperrt werden.

Anmerkung: Beachten Sie, dass das Sperren von Diensten, die von OpenScape Business S verwendet werden, zu Beeinträchtigungen und/oder zum Ausfall der Funktionalität des Kommunikationssystems führen können.

20.1.4.1 Wie Sie Dienste hinzufügen oder sperren

Schritt für Schritt

1) Klicken Sie in der Taskleiste auf **Computer**.
2) Klicken Sie im Menübaum auf **System** > **YaST**.
3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**.
4) Klicken Sie im Menübaum auf **Security and Users**.
5) Klicken Sie im Bereich **Security and Users** auf **Firewall**.
6) Klicken Sie im Menübaum des Fensters **Firewall Configuration: Start-UP** auf **Allowed Services**.
7) Wählen Sie im Feld **Allowed Services for Selectet Zone** den Bereich aus, für den Sie Dienste ändern wollen (**External Zone**, **Demilitarized Zone**, **Internal Zone**).
8) Wählen Sie im Feld **Service to allow** die Dienste aus, die Sie gezielt freigeben (hinzufügen) möchten und klicken Sie auf **Add**. Im Pull-Down-Menü werden alle derzeit erlaubten Dienste aufgelistet.
9) Wählen Sie im Feld **Allowed Service** die Dienste aus, die Sie sperren möchten und klicken Sie auf **Delete**.

10) Aktivieren Sie ggf. das Kontrollkästchen **Protect Firewall from Internal Zone**.

11) Klicken Sie auf **Advanced** um ggf. Ports oder numerische Protokolle zur Firewall hinzuzufügen (**TCP Ports**, **UDP Ports**, **RPC Ports** und **IP Protocols**). Klicken Sie anschließend auf OK.

12) Klicken Sie auf **Next**. Die gemachten Einstellungen für die Firewall werden Ihnen angezeigt. Bei Bedarf können Sie über **Show Details** weitere Informationen einsehen.

13) Klicken Sie auf **Beenden**.

20.2 Signaling- und Payload-Encryption (SPE)

SPE dient der Sicherheit bei der Übertragung von Signalisierungs- und Nutzdaten zwischen IP-Systemtelefonen und dem Kommunikationssystem. Dem Leistungsmerkmal liegt ein asymmetrisches Verschlüsselungsverfahren zugrunde, bei dem öffentliche und private Schlüssel verwendet werden.

Verschlüsselung der Signalisierungs- und Nutzdaten:

- Signaling encryption: Die Signalübertragung zwischen Gateway und Clients wird mit einem 128-Bit-Schlüssel verschlüsselt. Für die Übertragung wird das TLS Protokoll mit AES-Verschlüsselung genutzt.
- Payload Encryption: Die Nutzdaten, auch Sprachdaten oder Payload genannt, werden mittels Secure Real-time Transport Protocol (SRTP) übertragen. Sie werden mit einem 128-Bit-Schlüssel (AES) verschlüsselt. SRTP wird ebenfalls für die IP-Vernetzung verwendet. Das Verfahren zum Austauschen der Schlüssel für SRTP heißt Multimedia Internet KEYing oder kurz, MIKEY.

Für SPE muss gewährleistet werden, dass sich die einzelnen Systemtelefone und die beteiligten Kommunikationssysteme eindeutig identifizieren. Dies wird durch Zertifikate erreicht, die auch die öffentlichen Schlüssen bereitstellen.

Die Schlüssel bzw. Zertifikate werden durch den DLS-Server verteilt (können aber auch manuell verteilt werden).

Tipp: Die SPE-Funktion wird nicht für SIP- und WL2-Teilnehmer angeboten.

Eine verschlüsselte Verbindung besteht nur in einer direkten Verbindung zweier Systemtelefone oder für Konferenzen.

SRTCP Verschlüsselung

SRTCP (Secure Real-Time Transport Control Protocol) ist eine Erweiterung des SRTP-Protokolls und realisiert die Sicherheit von Steuerungsdaten. Die Erweiterung besteht aus drei zusätzlichen Feldern: Einem SRTCP-Index, einem Encryption-Flag und einem Authentifizierungs-Tag.

SPE Konformität

Family	Protocol / Interface	Signalling Encryption								Payload Encryption				
		HFA Subscriber	SIP Subscriber	TDM Subscriber	Analog Subscriber	SIP-Q Trunking	ISDN CO	FAX (T38, G711)		HFA Subscriber2	SIP Subscriber2	TDM Subscriber2	Analog Subscriber2	IP-Q Trunking (GW)
OpenScape Office MX/LX														
	HFA	s	nv	t	t	s	t	t		y	n	y	y	y
	SIP-UA	t*	t*	nv	nv	t*	nv	nv		n	n	n	n	n
	SIP-Trunking/ITSP	t*	nv	nv	nv	t*	nv	nv		n	n	n	n	n
	SIP-Q Homogenous	s	t*	t	t	s	t	t*		y	n	y	y	y
	Media Server / Conference	t	nv	nv	nv	t	nv	nv		n	n	n	n	n
Openscape Business X3/X5/X8														
	HFA	s	nv	t	t	s	t	t		y	n	y	y	y
	SIP-UA	t*	t*	nv	nv	t*	nv	nv		n	n	n	n	n
	SIP-Trunking/ITSP	t*	nv	nv	nv	t*	nv	nv		n	n	n	n	n
	SIP-Q Homogenous	s	t*	t	t	s	t	t*		y	n	y	y	y
	SIP-Q Heterogenous - H4k	s	t*	t	t	s	t	t*		y	n	y	y	y
	SIP-Q Heterogenous - OSV	s	t*	t	t	s	t	t*		y	n	y	y	y
	Media Server / Conference	t	nv	nv	nv	t	nv	nv		n	n	n	n	n
	MEB / VSL	t	nv	nv	nv	t	nv	nv		n	n	n	n	n

Legende:

Signaling Encryption	
nv	Keine VoIP Sicherheit
t	Standard: TLS auf der VoIP Seite; keine End-to-end Secure Payload
s	Signaling- und Payload-Encryption (SPE)
*	Keine End-to-end Signaling Encryption (TLS)
Payload Encryption	
y	Secure Payload (SRTP)
n	Non-Secure Payload (RTP)

20.2.1 Wie Sie SPE Unterstützung aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie Signaling and Payload Encryption einschalten möchten, aktivieren Sie das Kontrollkästchen **SPE Unterstützung**.
   - Wenn Sie Signaling and Payload Encryption ausschalten möchten, deaktivieren Sie das Kontrollkästchen **SPE Unterstützung**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.2.2 Wie Sie SPE-Sicherheitseinstellungen ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Sicherheit** > **Signaling and Payload Encryption (SPE)**.
3) Wählen Sie in der Registerkarte **SPE Sicherheitseinstellungen ändern** unter **Minimale Länge des RSA Schlüssels** die minimale Schlüssellänge des Sicherheitsprotokolls aus (512, 1024 oder 2048).
4) Markieren Sie den Eintrag **Zertifikatsüberprüfung mit CRL-Überwachung**, wenn Sie einen Abgleich mit den CRL-Listen (Zertifikatswiderruflisten) wünschen.
5) Geben Sie unter **Maximales Interval für Schlüssel-Neuverhandlung (Stunden)** die Zeit (in Stunden) ein, nach der die Schlüsselpaare neu vergeben werden.
6) Klicken Sie auf **Übernehmen**.

20.2.3 Wie Sie ein SPE-Zertifikat und den privaten Schlüssel importieren (PKCS#12)

Wenn kein kundenspezifisches Zertifikat zur Verfügung steht, kann über SSL > Zertifikatsgenerierung ein selbst signiertes CA-Zertifikat generiert werden und damit ein CA-signiertes Server Zertifikat (PKCS#12) erzeugt und abgespeichert werden. Dieses wird dann für SPE importiert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Sicherheit** > **Signaling and Payload Encryption (SPE)**.
3) Navigieren Sie im Menübaum zu **SPE-Zertifikat**.
4) Geben Sie unter **SPE Zertifikat und privaten Schlüssel importieren (PKCS#12)** im Feld **Entschlüsselungskennwort** das beim Generieren der Datei entstandene Kennwort zur Entschlüsselung ein.
5) Geben Sie unter **Datei mit Zertifikat und privatem Schlüssel (PEM- oder PKCS#12-Format)** die Zertifikatsdatei ein bzw. wählen Sie diese durch **Durchsuchen** der Verzeichnisse.

   Tipp: Wenn Sie bei aktiviertem SPE das erste Mal ein Zertifikat installieren wird anschließend automatisch ein Reset durchgeführt!
6) Klicken Sie auf **Fingerabdruck des Zertifikats anzeigen**, wenn Sie die Integrität überprüfen wollen.

20.2.4 Wie Sie das SPE CA-Zertifikat importieren

Dieser Schritt ist nicht erforderlich bei Verwendung von Zertifikaten die unter **SSL Zertifikatsgenerierung** selbst erzeugt worden sind.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Sicherheit** > **Signaling and Payload Encryption (SPE)**.
3) Navigieren Sie im Menübaum zu **SPE CA-Zertifikate**.
4) Geben Sie im Fenster **Verrtrauenswürdiges CA-Zertifikat (X.509 Datei) für SPE importieren** unter **Datei mit Zertifikat (PEM oder Binär-Format)** den Dateinamen der Zertifikatsdatei ein bzw. wählen Sie unter **Durchsuchen** die Datei aus.
5) Markieren Sie unter **CRL Distribution Point (CDP) Protokoll** das Protokoll für die CRL-Listen (Zertifikatswiderrufslisten) ein (**LDAP** oder **HTTP**).
6) Geben Sie unter **CDP (ohne z.B. ldap://)** den gewünschten Server ein.
7) Klicken Sie auf **Fingerabdruck des Zertifikats** anzeigen.

20.2.5 Wie Sie SPE für einen Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Navigieren Sie im Menübaum unter **Teilnehmer** > **Teilnehmer** > **IP-Clients** zum gewünschten Teilnehmer (System-Client)
3) Navigieren Sie im Fenster **Teilnehmer** unter der Registerkarte **Teilnehmer-Parameter ändern** zum Eintrag **Payload Security**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, wählen Sie unter **Payload Security** den Eintrag **Ein**.
   - Wenn Sie die Funktion deaktivieren möchten, wählen sie unter **Payload Security** den Eintrag **Aus**.
5) Klicken Sie auf **Übernehmen**.

20.3 Virtual Private Network VPN

Ein VPN (Virtual Private Network) ist ein PC-Netz, das zum Transport privater Daten ein öffentliches Netz (z.B. das Internet) nutzt. Es ermöglicht somit eine sichere Übertragung über ein unsicheres Netzwerk. Die Übertragung von Daten geschieht dabei verschlüsselt.

Übersicht VPN

VPN bietet Ihnen:

- Sichere Verbindung über ein ungeschütztes Medium (Internet)
- Schutz vertraulicher Daten vor Manipulation
- Sichere Integration von externen Partnern ins Firmennetz
- Zugriff auf Unternehmensinformationen für den Außendienst

Um eine sichere Kommunikation zu gewährleisten, funktioniert VPN folgendermaßen: Es wird ein Tunnel zwischen den Kommunikationspartnern aufgebaut. Bei diesem Tunnelaufbau findet eine Authenifizierung und Autorisierung statt. Nach dem Tunnelaufbau werden die eigentlichen Daten verschlüsselt übertragen.

Ein VPN kann zwischen (mindestens) zwei Rechnern bzw. Netzen (Tunnelendpunkten) aufgebaut werden.

Es gibt 2 Vernetzungsarten:

- Site-to-Site-VPN

  Hierbei findet die Verschlüsselung zwischen zwei VPN-Gateways statt; innerhalb des LANs werden die Daten unverschlüsselt übertragen.

- End-to-Site-VPN

  Remote Access VPN (Fernzugriff von mobilen Mitarbeitern)

Systemspezifische Informationen

Die Administration für die VPN-Parameter erfolgt prinzipiell über den Wizard VPN.

Beachten Sie, dass die Verbindung zum Kommunikationssystem über eine gesicherte Verbindung mit SSL verlaufen muss. Diese wird über OpenSwan und OpenSSL realisiert.

Abhängigkeiten

Themenbereich	Abhängigkeit
DynDNS	Die VPN-Endpunkte müssen über einen Domain Namen oder eine feste IP-Adresse erreichbar sein. Ist dies nicht der Fall, kann DynDNS genutzt werden.
DynDNS	Wenn sich eine IP-Adresse bei VPN ändert, aktualisiert das Kommunikationssystem die auf den Hostnamen bezogenen Daten (IP-Adresse) im DynDNS.
DNS	Jeder VPN-Partner kann den Hostnamen/die IP-Adresse über das Standard-DNS-Protokoll auflösen. Sämtliche DNS-Namen (z.B. Hostname) müssen vollqualifizierte Domänennamen (FQDN) sein. Während der Aktualisierung der IP-Adresse über DNS sind keine Verbindungen über IPSec-Tunnels möglich.

20.3.1 Anforderungen für VPN

Um die Qualität der Sprach- und Datenübertragung sicherzustellen, müssen die verwendeten Netze bestimmte Anforderungen erfüllen. Besonders im Hinblick auf eine Verschlüsselung ist mehr Bandbreite als bei einer anderen Vernetzung einzuplanen.

Für die folgenden Beispiele in den Tabellen wurde als Verschlüsselungsmodus "ESP Tunnel Modus mit Authentication" zugrunde gelegt. Dieser Modus bietet die höchste Sicherheit bei Site-to-Site VPNs.

Struktur eines verschlüsselten Sprachpaketes:

Länge des ESP-Headers

Padding

Bandbreiten-Kalkulation für den Verschlüsselungs-Algorithmus AES:

Bandbreiten-Kalkulation für den Verschlüsselungs-Algorithmus DES / 3DES:

Bandbreite für Fax T.38

Protokoll	Bytes	
ESP Trailer	12	
ESP Padding	variiert (y)	Verschlüsselt
ESP Padding Header	2	Verschlüsselt
Sprach-Payload	variiert (x)	Verschlüsselt
RTP	12	Verschlüsselt
UDP	8	Verschlüsselt

Protokoll	Bytes	
IP (original)	20	Verschlüsselt
ESP-Header	8 + iv	
IP (Tunnel)	20	
802.1Q VLAN Tagging	4	
MAC (incl. Preamble, FCS)	26	
Summe	**112 + iv + x + y**	

Die Länge der ESP-Headers hängt vom verwendeten Verschlüsselungs-Algorithmus ab.

Erforderlich bei Cipher Block Chaining (Blockchiffre-Verkettung). Der ESP-Header enthält einen Initialisierungsvektor (IV). Die Länge des IV ist identisch mit der Länge des Chiffreblocks.

Padding ist erforderlich, da die Verschlüsselungs-Algorithmen auf Blockchiffrierung beruhen. Dies bedeutet, dass der gesamte verschlüsselte Teil des Pakets (Original IP-/UDP-/RTP-Header + Sprach-Nutzlast + ESP-Header-Padding) einem ganzzahligen Vielfachen der Chiffreblocklänge entsprechen muss.

Blocklänge des Verschlüsselungs-Algorithmus:

Verschlüsselungs-Algorithmus	Blocklänge	Länge iv des Initialisierungs-Vektors
AES	16 Byte (128 Bit)	16 Byte (128 Bit)
3DES	8 Byte (64 Bit)	8 Byte (64 Bit)

Kalkulation der benötigten Padding-Bytes für Sprachpakete:

(42 + x + y) (Bytes) = N x (0 oder 16 (Bytes)) (N integer)

Codec	Paketierungs Parameter	Rahmengröß (ms)	Payload (Bytes)	Padding (Bytes)	Ethernet Paketlänge (Bytes)	Payload/ Packet overhead ration	Ethernet Load (inkl. Header) (kBit/s)
G.711	20	20	160	6	294	75%	117,6
G.711	30	30	240	6	372	50%	99,2
G.711	40	40	320	6	454	38%	90,8
G.711	60	60	480	6	614	25%	81,9
G.729A	1	20	20	2	150	600%	60,0
G.729A	2	40	40	6	182	300%	36,4
G.729A	3	60	60	2	198	200%	26,4

Codec	Paketierungs Parameter	Rahmengröß (ms)	Payload (Bytes)	Padding (Bytes)	Ethernet Paketlänge (Bytes)	Payload/ Packet overhead ration	EthernetLoad (inkl.) Header) (kBit/s)
G.711	20	20	160	6	286	75%	114,4

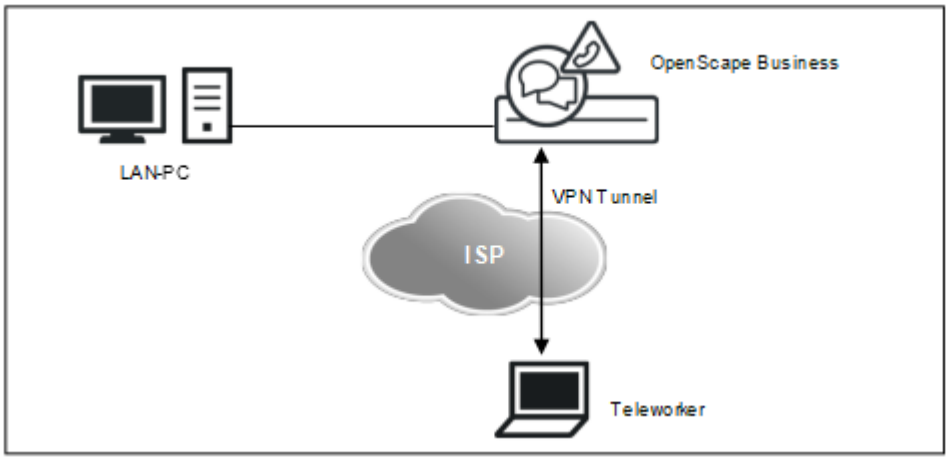
Codec	Paketierungs Parameter	Rahmengröß (ms)	Payload (Bytes)	Padding (Bytes)	Ethernet Paketlänge (Bytes)	Payload/ Packet overhead ration	EthernetLoad (inkl.) Header) (kBit/s)
G.711	30	30	240	6	366	50%	97,6
G.711	40	40	320	6	446	38%	89,2
G.711	60	60	480	6	606	25%	80,8
G.729A	1	20	20	2	142	600%	56,8
G.729A	2	40	40	14	166	300%	33,2
G.729A	3	60	60	10	182	200%	24,3

Verschlüsselu Algorithmus	Rahmengröße (ms)	Payload y (Bytes)	Padding x (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	EthernetLoad (inkl.) Header) (kBit/s)
DES / 3DES	30	169	1	278	64%	74,1
AES	30	169	9	294	74%	78.3

20.3.2 Anbindung von Teleworkern über VPN

Durch eine gesicherte Verbindung über VPN können Teleworker an das Kommunikationssystem angeschlossen werden.

Stand-alone-System mit Anbindung von Teleworkern über VPN



Das Kommunikationssystem verfügt über eine intergrierte VPN-Funktionalität (Konfiguration über Wizard). Bis zu 10 Teleworker können über VPN pro Kommunikationssystem gleichzeitig aktiv sein.

Folgende VPN-Clients sind für OpenScape Business freigegeben:

- NCP VPN Client
- Shrew Soft VPN Client
- Android VPN Client
- iOS VPN Client

- Mac OS-X VPN Client

Export der Teleworker-Daten

Die Teleworker-Daten können als ZIP-Datei (unverschlüsselt) exportiert werden. In der Zip-Datei befindet sich für jeden unterstützten VPN Client eine eigene Text-Datei mit den Teleworker-Daten. Für den NCP VPN Client in Form einer `.ini`-Datei, für den Shrew Soft VPN Client in Form einer `.vpn`-Datei und für den OS-X VPN Client in Form einer `.networkConnect`-Datei. Diese Text-Dateien können am VPN-Client importiert werden.

Tipp: Evtl. vorkommende Umlaute oder Akzente werden in den Text-Dateien mit den Teleworker-Daten nicht behandelt. Leerzeichen werden durch Unterstriche ersetzt.

Statusanzeige der VPN-Verbindungen

Eine Statusanzeige aller VPN-Verbindungen finden Sie im Wizard **VPN**. Eine detailliertere Übersicht aller VPN-Verbindungen finden Sie im **Service-Center** unter **Diagnose** > **Status** > **VPN Status**.

VPN bei OpenScape Business S

Bei OpenScape Business S wird VPN über einen externen Router terminiert. Die Beschreibung von externen Applikationen ist nicht Bestandteil dieser Anleitung.

20.3.2.1 Wie Sie die Anbindung von Teleworkern über VPN konfigurieren

Mit dem Wizard **VPN** können Sie über VPN (Virtual Private Network) Teleworkern (VPN-Partnern) den Zugriff auf das interne LAN ermöglichen und Kommunikationssysteme per VPN verbinden. Hat das Kommunikationssystem keine feste externe IP-Adresse (öffentliche IP-Adresse, globale IP-Adresse), muss ein DynDNS-Service z.B. auf www.dyndns.org eingerichtet werden.

Voraussetzungen

Der Internet-Zugang über die WAN-Schnittstelle ist konfiguriert.

Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, muss DynDNS konfiguriert sein. Für einen erfolgreichen DynDNS-Test wird eine Verbindung zum Internet benötigt.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.
4) Klicken Sie auf **VPN konfigurieren**.
5) Wenn Sie eine konfigurierte VPN-Verbindung bearbeiten wollen, klicken Sie bei der gewünschten VPN-Verbindung auf **Bearbeiten**.
6) Wenn Sie eine neue VPN-Verbindung erstellen wollen, klicken Sie auf **Hinzufügen**.

7) Vergeben Sie im Feld **System Name** einen Namen für die VPN-Verbindung (z.B. `node2mch.dyndns.org`).
8) Geben Sie ggf. einen **Kommentar** in das dafür vorgesehe Feld ein.
9) Aktivieren Sie das Kontrollkästchen **aktiviert** (standardmäßig vorbelegt).
10) Markieren Sie das Kontrollkästchen **Daten des eigenen Systems verwenden**.
11) Wählen Sie bei Bedarf den **Adresstyp** aus:
    - Hat die WAN-Schnittstelle eine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **IP-Adresse** aus und geben Sie unter **globale IP-Adresse / DNS Name (WAN)** die feste (öffentliche) IP-Adresse ein.
    - Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **DNS-Name** aus. Unter **globale IP-Adresse / DNS Name (WAN)** wird der für DynDNS bereits konfigurierte DNS-Namen des Kommunikationssystems angezeigt.
12) Ändern Sie nur bei Bedarf die **lokale IP-Adresse (LAN)**.
13) Ändern Sie nur bei Bedarf die **lokale Subnetzmaske (LAN)**.
14) Wenn Sie einen bereits eingerichteten Teleworker bearbeiten wollen, klicken Sie im Bereich **Teleworker** beim gewünschten Teleworker auf **Bearbeiten**.
15) Wenn Sie einen neuen Teleworker einrichten wollen, klicken Sie im Bereich **Teleworker** auf **Hinzufügen**.
16) Vergeben Sie im Feld **Name** einen Namen für die Konfiguration dieses Teleworkers.
17) Konfigurieren Sie den Typ des verwendeten VPN-Clients:
    - Für reine IPSec-VPN Teleworker (NCP und Shrew Soft VPN Clients):

      Deaktivieren Sie das Kontrollkästchen **L2TP/IPSec**, wählen Sie als **Adresstyp** den Eintrag **IP-Adresse** aus und geben Sie im Feld **virtuelle IP-Adresse / DynDNS-Name** eine virtuelle IP-Adresse für den Teleworker ein, wenn der eingesetzte VPN-Client virtuelle IP-Adressen unterstützt (unabhängig davon, ob der Teleworker per DSL-Router oder DSL-Modem Verbindung ins Internet hat).
    - Für L2TP/IPSec-VPN Teleworker (iOS, Android und MAC OS-X VPN Clients):

      Aktivieren Sie das Kontrollkästchen **L2TP/IPSec** und vergeben Sie **Benutzername** und **Passwort** für den Teleworker.
18) Aktivieren Sie das Kontrollkästchen **aktiviert** (standardmäßig vorbelegt).
19) Klicken Sie auf **OK**. Das Fenster mit der Übersicht über die Teleworker wird wieder angezeigt. Sie können weitere Teleworker eingeben.
20) Wenn Sie alle Teleworker eingerichtet haben, klicken Sie auf **OK & Weiter**. Das Fenster **System auswählen** wird angezeigt.
21) Klicken Sie auf **OK & Weiter**. Es öffnet sich das Fenster **Sicherheitseinstellungen für Verbindungen**.
22) Vergeben Sie für die gerade konfigurierte VPN-Verbindung einen Schlüssel für die sichere VPN-Verbindung unter **PreShared Secret** und wiederholen Sie diesen Schlüssel unter **Wiederholen des PreShared Secret**. Der Schlüssel muss mindestens 20 Zeichen lang sein.
23) Geben Sie ggf. noch einen **Kommentar** ein.
24) Klicken Sie auf **OK**. Es erscheint das Fenster **VPN Statusinformationen**.

25) Klicken Sie auf **VPN einschalten**.
26) Nur wenn als Adresstyp DNS-Name ausgewählt wurde: Kontrollieren Sie die bereits konfigurierten Daten des DynDNS-Accounts und klicken Sie auf **Verbindung testen**. Die DNS-Zugangsdaten werden zum Service-Provider übermittelt. Dieser Vorgang dauert ca. 10 Sekunden. Ist der Test nicht erfolgreich, überprüfen Sie bitte Ihre Zugangsdaten. Klicken Sie nach erfolgreichem Test auf **OK**.
27) Klicken Sie auf **OK & Weiter**. Die Teleworker greifen nun auf die WAN-Schnittstelle des Kommunikationssystems zu.
28) Klicken Sie auf **Beenden**.

20.3.2.2 Wie Sie die Teleworker-Daten exportieren

Mit dem Wizard **VPN** können Sie die Teleworker-Daten exportieren.

Voraussetzungen

Eine VPN-Verbindung ist konfiguriert.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.
4) Klicken Sie auf **Export/Import**.
5) Klicken Sie im Bereich **Exportieren der Teleworker-Daten vom System** auf **Export**. Speichern Sie die ZIP-Datei an einem Ort Ihrer Wahl.

   Tipp: In der ZIP-Datei befindet sich für jeden unterstützten VPN-Client eine eigene Datei mit den Teleworker-Daten. Die Teleworker-Daten werden nicht verschlüsselt! Bitte gehen Sie mit den Daten verantwortungsbewusst um.

6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

20.3.3 Vernetzung von Kommunikationssystemen über VPN

Mehrere OpenScape Business Kommunikationssysteme können über eine Site-to-Site-VPN-Vernetzung sicher miteinander vernetzt werden.

Vernetzung über VPN

Sie haben die Möglichkeit in einem Kommunikationssystem alle Daten für eine Vernetzung mehrerer Systeme zu konfigurieren, diese Topologie-Daten verschlüsselt zu exportieren und in alle anderen Systeme im Netzverbund zu importieren. Dadurch wird an allen Systemen im Netzverbund eine schnelle und konsistente Konfiguration möglich.

Die Unterscheidung zwischen dem eigenen und den fremden Systemen findet über die Erkennung des eigenen DynDNS-Namens oder (bei Verwendung von festen IP-Adressen) über die eigene Internet-Adresse statt.

- Exportieren der Topologie-Daten vom System
  - Alle Daten über den Aufbau des VPN-Netzwerks werden in einer verschlüsselten XML-Datei zusammengefasst und als ZIP-Datei zum Export in ein anderes System bereitgestellt.
- Import der Topologie-Daten ins System
  - Alle Daten über den Aufbau des VPN-Netzwerks können als ZIP-Datei (beinhaltet die verschlüsselte XML-Datei) importiert und für dieses System übernommen werden.

Der Schlüssel (Passwort) für den Export ist frei wählbar und muss einem anderen Administrator, der diese Einstellungen importieren möchte, mitgeteilt werden.

Statusanzeige der VPN-Verbindungen

Eine Statusanzeige aller VPN-Verbindungen finden Sie im Wizard **VPN**. Eine detailliertere Übersicht aller VPN-Verbindungen finden Sie im **Service-Center** unter **Diagnose** > **Status** > **VPN Status**.

20.3.3.1 Wie Sie die Vernetzung über VPN konfigurieren

Mit dem Wizard **VPN** können Sie an einem System alle Kommunikationssysteme der VPN-Vernetzung konfigurieren. Diese Topologie-Daten können Sie exportieren und an allen Systemen im VPN-Netzverbund importieren.

Voraussetzungen

Der Internet-Zugang über die WAN-Schnittstelle ist konfiguriert.

Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, muss DynDNS konfiguriert sein. Für einen erfolgreichen DynDNS-Test wird eine Verbindung zum Internet benötigt.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.
4) Klicken Sie auf **VPN konfigurieren**.
5) Klicken Sie auf **Hinzufügen**.
6) Vergeben Sie im Feld **System Name** einen Namen für das erste System des VPN-Netzverbunds (z.B. `node1mch.dyndns.org`).
7) Geben Sie ggf. einen **Kommentar** in das dafür vorgesehe Feld ein.
8) Aktivieren Sie das Kontrollkästchen **aktiviert** (standardmäßig vorbelegt).
9) Markieren Sie das Kontrollkästchen **Daten des eigenen Systems verwenden**. Die nachstehenden Felder werden mit den Daten des Systems vorbelegt.

10) Wählen Sie nur bei Bedarf den vorbelegten **Adresstyp** aus:
    - Hat die WAN-Schnittstelle eine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **IP-Adresse** aus und geben Sie unter **globale IP-Adresse / DNS Name (WAN)** die feste (öffentliche) IP-Adresse ein.
    - Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **DNS-Name** aus. Unter **globale IP-Adresse / DNS Name (WAN)** wird der für DynDNS bereits konfigurierte DNS-Namen des Kommunikationssystems angezeigt.
11) Ändern Sie nur bei Bedarf die vorbelegte **lokale IP-Adresse (LAN)**.
12) Ändern Sie nur bei Bedarf die vorbelegte **lokale Subnetzmaske (LAN)**.
13) Klicken Sie auf **OK & Weiter**. Das Fenster **System auswählen** wird angezeigt.
14) Klicken Sie erneut auf **Hinzufügen**.
15) Vergeben Sie im Feld **System Name** einen Namen für das zweite System des VPN-Netzverbunds (z.B. `node2mch.dyndns.org`).
16) Geben Sie ggf. einen **Kommentar** in das dafür vorgesehe Feld ein.
17) Aktivieren Sie das Kontrollkästchen **aktiviert** (standardmäßig vorbelegt).
18) Wählen Sie den **Adresstyp** des zweiten Systems aus:
    - Hat die WAN-Schnittstelle eine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **IP-Adresse** aus und geben Sie unter **globale IP-Adresse / DNS Name (WAN)** die feste (öffentliche) IP-Adresse ein.
    - Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **DNS-Name** aus. Unter **globale IP-Adresse / DNS Name (WAN)** wird der für DynDNS bereits konfigurierte DNS-Namen des Kommunikationssystems angezeigt.
19) Geben Sie die **lokale IP-Adresse (LAN)** des zweiten Systems ein.
20) Geben Sie die **lokale Subnetzmaske (LAN)** des zweiten Systems ein.
21) Klicken Sie auf **OK & Weiter**. Das Fenster **System auswählen** wird angezeigt.
22) Wiederholen Sie die Schritte 14 bis 21 für weitere Systeme im VPN-Netzverbund.
23) Klicken Sie anschließend auf **OK & Weiter**. Es öffnet sich das Fenster **Sicherheitseinstellungen für Verbindungen**.
24) Vergeben Sie für jede VPN-Verbindung von einem System zum anderen einen eigenen Schlüssel unter **PreShared Secret** und wiederholen Sie diesen Schlüssel unter **Wiederholen des PreShared Secret**. Der Schlüssel muss mindestens 20 Zeichen lang sein.
25) Geben Sie ggf. noch einen **Kommentar** für jede VPN-Verbindung ein.
26) Klicken Sie auf **OK**. Es erscheint das Fenster **VPN Statusinformationen**.
27) Klicken Sie auf **Export/Import** um die Topologie-Daten zu exportieren. Es erscheint das Fenster **Exportieren und Importieren von VPN Konfigurationsdaten**.
28) Vergeben Sie im Bereich **Exportieren der Topologie-Daten vom System** unter **Schlüssel** und **Schlüssel wiederholen** einen Schlüssel (mind. 7-stellig) für die Sicherung der Daten und klicken Sie auf **Export**. Speichern Sie die Datei an einem Ort Ihrer Wahl.
29) Klicken Sie auf **OK & Weiter**.

30) Klicken Sie auf **VPN einschalten**.
31) Nur wenn als Adresstyp **DNS-Name** ausgewählt wurde: Kontrollieren Sie die bereits konfigurierten Daten des DynDNS-Accounts und klicken Sie auf **Verbindung testen**. Die DNS-Zugangsdaten werden zum Service-Provider übermittelt. Dieser Vorgang dauert ca. 10 Sekunden. Ist der Test nicht erfolgreich, überprüfen Sie bitte Ihre Zugangsdaten. Klicken Sie nach erfolgreichem Test auf **OK**.
32) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.
33) Klicken Sie im WBM des zweiten Systems in der Navigationsleiste auf **Einrichtung** und im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
34) Klicken Sie auf **Bearbeiten**, um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.
35) Klicken Sie auf **Export/Import** um die Topologie-Daten zu importieren. Es erscheint das Fenster **Exportieren und Importieren von VPN Konfigurationsdaten**.
36) Klicken Sie auf **Importieren der Topologie-Daten ins System** um die Topologiedaten zu importieren.
37) Geben Sie den **Schlüssel** (Passwort) ein, den Sie beim Export der Daten am ersten System eingegeben haben.
38) Navigieren Sie zum Ablageort der ZIP-Datei. Klicken Sie anschließend auf **Import**.
39) Klicken Sie auf **OK & Weiter**. Sie sehen die konfigurierten Systeme.
40) Klicken Sie auf **VPN einschalten**.
41) Nur wenn als Adresstyp **DNS-Name** ausgewählt wurde: Kontrollieren Sie die bereits konfigurierten Daten des DynDNS-Accounts und klicken Sie auf **Verbindung testen**. Die DNS-Zugangsdaten werden zum Service-Provider übermittelt. Dieser Vorgang dauert ca. 10 Sekunden. Ist der Test nicht erfolgreich, überprüfen Sie bitte Ihre Zugangsdaten. Klicken Sie nach erfolgreichem Test auf **OK**.
42) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.
43) Wiederholen Sie die Schritte 33 bis 42 für die restlichen Systeme im VPN-Netzverbund.

20.3.3.2 Wie Sie Topologie-Daten einer VPN-Vernetzung exportieren und importieren

Mit dem Wizard **VPN** können Sie die Topologie-Daten der Vernetzung über VPN exportieren und importieren.

Voraussetzungen

Eine VPN-Verbindung ist konfiguriert.

Für einen Import der Topologie-Daten müssen Sie den beim Export vergebenen Schlüssel wissen.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.

4) Klicken Sie auf **Export/Import**.
5) Wenn Sie die Topologie-Daten exportieren wollen, vergeben Sie im Bereich **Exportieren der Topologie-Daten vom System** unter **Schlüssel** und **Schlüssel wiederholen** einen Schlüssel (mind. 7-stellig) für die Sicherung der Daten und klicken Sie auf **Export**. Speichern Sie die Datei an einem Ort Ihrer Wahl.
6) Wenn Sie die Topologie-Daten importieren wollen, geben Sie im Bereich **Importieren der Topologie-Daten zum System** unter **Schlüssel** den Schlüssel für die Entschlüsselung der Daten ein und navigieren Sie zum Ablageort der ZIP-Datei. Klicken Sie anschließend auf **Import**.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

20.3.4 VPN - Sicherheitsmechanismen

Die Verschlüsselung der Daten geschieht bei VPN über verschiedene Sicherheitsmechanismen wie IPSec-Tunnel, Security Associations und Authentifizierungsmethoden (Peer-to-Peer, Digitale Signaturen).

IPSec-Tunnel

IPSec dient zur Verschlüsselung von Daten und kann generell mit und ohne Tunnel eingesetzt werden. IPSec ist eine Möglichkeit VPN zu realisieren. Es ist dabei möglich, das gesamte IP-Paket inklusive IP-Header zu verschlüsseln: Dies geschieht im Tunnelmodus.

Tunnel müssen immer bei beiden VPN-Partnern eingerichtet werden.

Bei IPSec kann die automatische Schlüsselverwaltung Internet Key Exchange (IKE) eingesetzt werden. Dabei handelt es sich um einen Standard, der in IPSec integriert ist.

Security Associations SA

IKE-SA

Payload-SA

Authentifizierung

Eine Security Association SA ist eine Vereinbarung zwischen zwei kommunizierenden Einheiten in Rechnernetzen. Sie beschreibt, wie die beiden Parteien Sicherheitsdienste anwenden, um sicher miteinander kommunizieren zu können.

VPN-Verbindungen erfordern immer drei Security Associations SA, die in zwei Phasen ausgehandelt werden:

- Phase 1 - Herstellen der IKE-SA

  eine für die anfängliche gegenseitige Authentifizierung und für den Austausch der Session-Keys (IKE-SA)

- Phase 2 - Aushandeln der Payload-SAs

  jeweils eine pro Richtung der aufgebauten Verbindung für den Payload-Verkehr (Payload-SAs)

Das IKE-Protokoll hat im Wesentlichen zwei verschiedene Aufgaben. Zunächst ist eine ausschließlich vom IKE-Protokoll genutzte SA herzustellen (IKE-SA). Anschließend wird die vorhandene IKE-SA zur sicheren Aushandlung aller weiteren für die Übertragung von Payload-Daten benötigten SAs (Payload-SA) genutzt. IKE operiert daher in zwei aufeinanderfolgenden Phasen:

Beim Verbindungsaufbau zwischen den VPN-Partnern müssen diverse Parameter ausgehandelt werden (z.B. wie oft ein Schlüssel neu generiert wird oder welches Verschlüsselungsverfahren verwendet wird). Diese Parameter werden in IKE-SAs abgelegt und verwaltet.

Die IKE-Phase 2 dient dem Aushandeln aller Sicherheitsparameter für die Payload-SAs zwischen den VPN-Partnern.

Es müssen immer zwei SAs hergestellt werden, für Übertragung und Empfang.

Im Wesentlichen werden folgende Schritte ausgeführt:

- Aushandeln der Algorithmen für Verschlüsselung und Authentifizierung
- Aushandeln der angewendeten Sicherheitsprotokolle (ESP und AH)
- Aushandeln des Betriebsmodus der Sicherheitsprotokolle
- Aushandeln der SA-Lebensdauer
- Festlegen des Schlüsselmaterials

Bei VPN findet eine Peer-to-peer-Kommunikation statt. Die Authentifizierung von VPN-Partnern ist auf zwei Arten möglich:

- Pre-shared Keys

  Meist werden bei VPN auch vorher verteilte Schlüssel (Preshared Keys) verwendet. Dazu wird bei beiden VPN-Partnern je ein Schlüsselpaar konfiguriert. Von diesen Schlüsseln wird zur Authentifizierung ein sogenannter Hash-Wert gebildet, den der jeweilige Partner überprüft.
- Digitale Signaturen

  Jedem VPN-Partner ist ein Zertifikat zugeordnet. Für eine erfolgreiche Authentifizierung müssen die VPN-Partner an beiden Tunnelendpunkten die digitale Signatur des jeweils gegenüberliegenden Partners gegen eine vertrauenswürdige CA prüfen.

Systemspezifische Informationen

Die Administration für die VPN-Parameter erfolgt prinzipiell über den Wizard.

Beachten Sie, dass die Administratorverbindung über eine gesicherte Verbindung mit SSL verlaufen muss.

- Security Associations SA

  Das Kommunikationssystem unterstützt die Oakley-Gruppen 1, 2 und 5
- IPSec

  Das Kommunikationssystem verwendet den IPSec-Tunnelmodus mit ESP (Encapsulating Security Payload). Bei ESP handelt es sich um ein IPSec-Protokoll, durch das die Paketverschlüsselung, Paketintegrität sowie die Paketauthentizität sichergestellt wird

- Payload-SA

  Das Kommunikationssystem unterstützt als Verschlüsselungsalgorithmen DES, 3DES und AES

  Von den bekannten Gruppen von MAC-Algorithmen (MAC=Message Authentication Code) zur Authentifizierung von Datenherkunft und Datenintegrität werden HMAC-SHA1, HMAC-SHA2 und HMAC-MD5.
- Empfohlene Betriebsmodi
  - IKE im "Main Mode" mit Perfect Forward Secrecy
  - Hash-Funktion mit SHA-2
  - Authentifizierung mit Zertifikaten (RSA)
  - Verschlüsselung mit AES (bis zu 256 Bit)
  - Unterstützung dynamischer öffentlicher IP-Adressen über virtuelle IP-Adressen oder mittels DynDNS-Aktualisierungsmechanismen für Teleworker-PC

20.3.5 VPN - Zertifikate

Ein Zertifikat bindet einen bestimmten öffentlichen Schlüssel an einen bestimmten VPN-Client; bei dem Client kann es sich sowohl um einen Client des Kommunikationssystems als auch um einen Teleworker handeln. Die eindeutige Kombination aus öffentlichem Schlüssel und VPN-Client ist die Grundlage des Authentifizierungsvorgangs.

Zertifikate und Zertifizierungsstelle

Lightweight CA

CRL Certificate Revocation Lists - Zertifikatswiderrufslisten

Zertifikate werden digital signiert und von einer so genannten Zertifizierungsstelle (CA Certification Authority) ausgestellt. IPSec akzeptiert ein Zertifikat, wenn es von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt ist.

In einer einfachen VPN-Umgebung ist die Festlegung einer einzelnen Zertifizierungsstelle unter Umständen schon ausreichend; diese CA fungiert als vertrauenswürdige Stamm-Zertifizierungsstelle für das gesamte VPN und identifiziert sich gegenüber allen VPN-Clients anhand ihres selbst signierten CA-Zertifikats.

Jeder VPN-Client benötigt ein von dieser CA ausgestelltes Zertifikat.

Zertifikate nach dem X.509-Standard (dem heute gängigsten Standard) enthalten folgende Hauptelemente:

- Informationen über die Identität des Zertifikatseigentümers
- den öffentlichen Schlüssel des Zertifikatseigentümers
- Informationen bezüglich der CA, die das Zertifikat signiert hat (eine Seriennummer, die Gültigkeitsdauer, Informationen über die Identität der CA sowie die digitale Signatur der CA)

Für Umgebungen, in denen der Kunde nicht bereits eine PKI nutzt, hilft eine Lightweight-CA-Funktionalität bei der Zertifizierung. Eine Lightweight-CA bietet folgende Möglichkeiten:

- Erstellen öffentlicher/privater Schlüsselpaare
- Signieren und Ausstellen entsprechender Zertifikate
- Speichern von Schlüsselpaaren mit zugehörigen Zertifikaten in Dateien

Als PKI (Public-Key-Infrastruktur) bezeichnet man in der Kryptografie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen.

Eine kritische Situation entsteht, wenn ein Zertifikat bekannt geworden ist (oder der Verdacht darauf besteht) und dieses Zertifikat für die Peer-Authentifizierung nicht mehr vertrauenswürdig ist. In diesem Fall muss die Zertifizierungsstelle das Zertifikat widerrufen und sämtliche Peers müssen baldmöglichst über den Widerruf informiert werden. Der Versuch eines Remote-Peers, seine Identität anhand eines widerrufenen Zertifikats zu authentifizieren, wird abgewiesen.

Grundsätzlich ist eine CRL eine Aufstellung sämtlicher widerrufener Zertifikate. CRLs müssen immer von der CA erzeugt werden, von der die Zertifikate stammen.

Eine CRL enthält folgende Hauptelemente:

- Aufstellung der widerrufenen Zertifikate; die Identifizierung der Zertifikate erfolgt durch die Seriennummern
- Zeitpunkt der Veröffentlichung der nächsten aktualisierten CRL (Angabe der Gültigkeitsdauer der CRL)
- Informationen bezüglich der CA, die das Zertifikat erzeugt hat (Informationen über die Identität der CA sowie die digitale Signatur der CA)

Eine regelmäßige Aktualisierung und Verteilung der CRLs muss manuell durch den Administrator erfolgen.

Systemspezifische Informationen

Die Authentifizierung erfolgt aufgrund von Algorithmen zur Kryptografie mit öffentlichen Schlüsseln. Das Kommunikationssystem unterstützt RSA als Algorithmus zur Kryptografie mit öffentlichen Schlüsseln. Das Kommunikationssystem unterstützt nur Zertifikate, die dem X.509-Standard entsprechen.

Das Kommunikationssystem agiert bei der Authentifizierung immer als VPN-Client.

- Lightweight CA

  Das Kommunikationssystem bietet eine eingeschränkte CA-Funktionalität (Lightweight CA). Der Administrator stellt für ein System das Schlüsselmaterial bereit, indem er manuell über die SSL-gesicherte Administrationsverbindung private/öffentliche Schlüsselpaare und Zertifikate in alle beteiligten Kommunikationspartner importiert

- CRL

  Es werden CRLs (Certificate Revocation Lists - Zertifikatswiderrufslisten) zum Widerruf von Zertifikaten verwendet. Der Import der CRL zum Kommunikationssystem geschieht durch den Administrator über eine SSL-gesicherte Verbindung.

20.3.5.1 VPN - Wie Sie Lightweight-CA-Zertifikate generieren

Lightweight CA ist eine lizenzpflichtige Funktion zum Generieren und Verwalten von CA- und Peer-Zertifikaten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Lightweight CA**. Im Fenster **Zertifikat generieren** können Sie ein eigenes CA-Zertifikat generieren.
4) Vergeben Sie unter **Name des Zertifikats** einen Namen für das angeforderte Zertifikat.
5) Vergeben Sie unter **Seriennummer des Zertifikats** eine Seriennummer für das Zertifikat.

   Tipp: Eine vergebene Seriennummer darf nicht noch einmal für ein anderes Zertifikat verwendet werden, da die Seriennummer aller jemals erzeugten Zertifikate eindeutig sein muss.

6) Geben Sie unter **Signatur-Algorithmus-Typ** den gewünschten Algorithmus für das Zertifikat ein (sha256RSA oder sha512RSA).
7) Geben Sie unter **Länge des öffentlichen Schlüssels** die Länge des öffentlichen Schlüssels ein (z.B. 2048).
8) Geben Sie unter **Beginn der Zertifikatsgültigkeit (GMT)** Datum und Uhrzeit für den Beginn der Gültigkeit ein. Das Datum wird als Greenwich Mean Time (GMT) interpretiert.
9) Geben Sie das Datum und die Zeit für das Ende der Gültigkeitsperiode unter **Ende der Zertifikatsgültigkeit (GMT)** ein.
10) Geben Sie unter **Antragsteller** das **Land (C)**, die **Organisation (O)**, die **Organisationseinheit (OU)** und **Allgemeiner Name (CN)** ein.
11) Optional können Sie unter **Alternativer Antragsteller** einen anderen Antragsteller eingeben. Wenn Sie dies getan haben, müssen Sie auch ein Format (z.B. IP-Adresse oder DNS-Name) eingeben. Das Eingabefenster ist von der Auswahl des Formats abhängig.
12) Geben Sie im Feld **CRL-Verteilungspunkt** den Verteilungspunkt für die CRL-Listen ein (werden in einer Pull-Down-Menü angezeigt).
13) Klicken Sie auf **Zertifikat erzeugen**.

20.3.5.2 VPN - Zertifikatsverwaltung - Wie Sie ein Zertifikat anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Zertifikatsverwaltung**. Es öffnet sich das Fenster **Zertifikat aus Datei anzeigen**.
4) Aktivieren Sie ggf. das Kontrollkästchen **PKCS#12-Format**.
5) Geben Sie das **Entschlüsselungskennwort** ein.
6) Geben Sie unter **Datei mit dem Zertifikat** die Zertifikatsdatei an oder wählen Sie sie über das Feld **Durchsuchen** aus.
7) Klicken Sie auf **Laden**.

20.3.5.3 VPN - Wie Sie ein Trusted CA-Zertifikat importieren (X.509)

X.509 ist ein Standard für Zertifikate. Dabei werden im Zertifikat auch der Name und die digitale Signatur des Zertifikatsausstellers gespeichert. X.509 ist Bestandteil des Verzeichnisdienstes X.500 für weltweite, verteilte und offene Systeme.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Zertifikatsverwaltung** > **Trusted CA-Zertifikate** > **Konfigurierte Zertifikate**.
4) Vergeben Sie unter **Name des Zertifikats** einen Namen für das angeforderte Zertifikat.
5) Geben Sie unter **Datei mit dem Zertifikat** die Zertifikatsdatei an oder wählen Sie diese über das Feld **Durchsuchen** aus.
6) Bestätigen Sie und klicken Sie auf **Aktivieren der konfigurierten VPN Tabellen.**

20.3.5.4 VPN - Peer Zertifikate - Wie Sie eine Zertifikatsanforderung (CSR) generieren

Sie können ein CA-signiertes Peer-Zertifikat, das auf einem CA-Zertifikat basiert, erzeugen. Voraussetzung ist, dass mindestens ein CA-Zertifikat generiert wurde. Das erzeugte Zertifikat wird in einer PKCS#12-Datei gespeichert. PKCS#12- Dateien (PKCS#12 Personal Information Exchange Syntax Standard) speichern Zertifikate mit dem privaten Schlüssel. Eine PKCS#12-Datei enthält also die entscheidenden Daten für persönliche Ver- und Entschlüsselung.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Peer-Zertifikate**.

4) Geben Sie in der Registerkarte **Zertifikatsanforderung (CSR) generieren** die erforderlichen Daten ein.
5) Geben Sie den **Name der Zertifikatsanforderung** ein.
6) Geben Sie unter **Signatur-Algorithmus-Typ** den gewünschten Algorithmus ein (sha256RSA oder sha512RSA).
7) Geben Sie unter **Länge des Schlüssels** die Schlüssellänge (2048) ein.
8) Geben Sie unter **Antragsteller** alle Daten für **Land (C)**, **Organisation (O)**, **Organisationseinheit (OU)** und **Allgemeiner Name (CN)** ein.
9) Geben Sie unter **Alternativer Antragsteller** das **Format des DN-Namens**, ein ggf. **Anderes Format** oder einen **Alternativen Antragsteller** ein.
10) Speichern Sie die *.csr Datei, die von einem CA signiert werden soll..

20.3.5.5 VPN - Peer Zertifikate - Wie Sie ein Zertifikat (PKCS#12) generieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Lightweight CA**.
4) Klicken Sie auf das CA-Zertifikat, anschließend auf **CA-signiertes Peer Zertifikat (PKCS#12) generieren**.
5) Geben Sie das **Entschlüsselungskennwort** ein.
6) Geben Sie eine Seriennummer Ihrer Wahl unter **Seriennummer des Zertifikats** ein.
7) Geben Sie unter **Länge des Schlüssels** die Schlüssellänge ein (1024, 1536 oder 2048).
8) Geben Sie unter **Beginn der Zertifikatsgültigkeit (GMT)** Datum und Uhrzeit für den Beginn der Gültigkeit ein. Das spezifizierte Datum ist Greenwich Mean Time.

Anmerkung: Die Gültigkeitsdauer des Peer Zertifikats sollte sorgfältig auf die im Unternehmen geltende Sicherheitsrichtlinie angepasst werden. Kurz vor Ablauf der Gültigkeitsperiode muß das Zertifikat verlängert oder ggf. ein neues Zertifikat ausgestellt werden.

---

9) Geben Sie das Datum und die Zeit für das Ende der Gültigkeitsperiode unter **Ende der Zertifikatsgültigkeit (GMT)** ein.
10) Geben Sie unter **Antragsteller** alle Daten für **Land (C)**, **Organisation (O)**, **Organisationseinheit (OU)** und **Allgemeiner Name (CN)** ein.
11) Optional können Sie unter **Alternativer Antragsteller** einen anderen Antragsteller eingeben. Wenn Sie dies getan haben, müssen Sie auch ein Format (z.B. IP-Adresse oder DNS-Name) eingeben. Das Eingabefenster ist von der Auswahl des Formats abhängig.
12) Geben Sie den **CRL Verteilungspunkt** ein (optional).
13) Klicken Sie auf **Zertifikat erzeugen**.

20.3.5.6 VPN - Wie Sie ein Peer Zertifikat importieren (PKCS#12)

PKCS#12- Dateien (PKCS#12 Personal Information Exchange Syntax Standard) speichern Zertifikate mit dem privaten Schlüssel. Eine PKCS#12-Datei enthält somit die entscheidenden Daten für die persönliche Ver- und Entschlüsselung.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Peer-Zertifikate**.
4) Klicken Sie auf die Registerkarte **Peer-Zertifikat importieren (PKCS#12)**.
5) Vergeben Sie unter **Name des Zertifikats** einen Namen für das angeforderte Zertifikat.
6) Geben Sie unter **Entschlüsselungskennwort** Ihr persönliches Kennwort zur Entschlüsselung dieses Zertifikats ein.
7) Geben Sie unter **Datei mit dem Zertifikat** den Dateinamen ein bzw. suchen Sie die Datei über die Schaltfläche **Durchsuchen**.
8) Klicken Sie auf **Fingerabdruck des Zertifikats** anzeigen.
9) Klicken Sie auf **Zertifikat aus Datei importieren**.

20.3.6 VPN-Clients

Ein Teleworker kann mit Hilfe eines VPN-Tunnels über das Internet eine sichere VPN-Verbindung zum Firmennetz herstellen. Dazu benötigt er auf seinem Gerät (PC, Tablet-PC, Smartphone) einen VPN-Client. Alle zwischen dem VPN-Client, der Firmen-Firewall und dem VPN-Server des Kommunikationssystems übertragenen Daten sind verschlüsselt.

Folgende VPN-Clients werden unterstützt:

- **NCP VPN Client**

  NCP-Clients können in beliebigen VPN-Umgebungen mit IPSec eingesetzt werden. Das ist von Bedeutung, wenn von einem Remote-PC auf VPN-Gateways verschiedener Hersteller zugegriffen werden soll oder bereits ein zentrales VPN-Gateway von einem Dritthersteller im Firmennetz installiert ist. Im Falle einer Filialvernetzung kann das NCP Secure Enterprise Gateway mit anderen VPN Gateways auf der Basis von IPSec-Verbindungen kommunizieren.

  Der NCP-Client ist kostenpflichtig, bietet aber eine grafische Benutzeroberfläche und eine Statusanzeige der Verbindung.

- **Shrew Soft VPN Client**

  Der Shrew Soft VPN Client ist ein kostenloser VPN-Client mit grafischer Oberfläche, der ab Version 2.1.5 auch die Hybrid-Authentifizierung unterstützt.

  Der Shrew Soft VPN Client beinhaltet unter anderem ISAKMP, Xauth- und RSA-Unterstützung, AES, Blowfish, 3DES-Verschlüsselungsprotokolle und zahlreiche weitere Features, die sonst nur in professionellen Lösungen zu finden sind.
- **iOS und Android VPN Client**

  Das Betriebssystem iOS oder Android hat den L2TP/IPSec VPN-Client integriert.

  Die L2TP/IPSec VPN-Clients benutzen den IP-Adress-Bereich `10.254.253.x`. Werden IP-Adressen aus diesem Bereich im Kundennetz bereits verwendet, muss der IP-Adress-Bereich im WBM geändert werden über **Experten-Modus** > **Wartung** > **Applikat.-Diagnose** > **IPSec Test: IPSec Test Routines** > **Set IP Address for L2TP** (z.B. von `10.254.253.1` auf `10.254.252.1`).
- **Mac OS-X VPN Client**

  Das Betriebssystem MAC OS-X hat den Mac OS-X-VPN-Client integriert.

Systemspezifische Informationen

- Die Teleworker-Daten eines VPN Clients können als ZIP-Datei (unverschlüsselt) exportiert werden. In der Zip-Datei befindet sich für jeden unterstützten VPN Client eine eigene Text-Datei mit den Teleworker-Daten. Für den NCP VPN Client in Form einer `.ini`-Datei, für den Shrew Soft VPN Client in Form einer `.vpn`-Datei und für den OS-X VPN Client in Form einer `.networkConnect`-Datei. Diese Text-Dateien können am VPN-Client importiert werden.
- LAN-Infrastruktur mit mehreren Subnetzen

  Wenn bei einer LAN-Infrastruktur mit mehreren Subnetzen VPN genutzt werden soll, ist es notwendig Regeln für diese Subnetze zu erstellen. Die Regeln können nicht über den Wizard, sondern müssen über den Experten-Modus konfiguriert werden.
- Tunnel-im-Tunnel

  Es ist nicht möglich einen zweiten VPN-Tunnel durch einen bereits existierenden VPN-Tunnel zu führen.

20.3.6.1 NCP VPN Client Einstellungen

Für eine VPN-Anbindung über den NCP VPN Client sind die nachfolgend genannten Einstellungen zu beachten, wenn die Konfiguration manuell erfolgen soll. Über das Kommunikationssystem ist es möglich, eine Text-Datei `ncp_vpn.ini` mit den konfigurierten VPN-Client-Daten zu exportieren und am VPN-Client zu importieren. Somit sind diese Einstellungen bereits vorbelegt.

Grundeinstellungen

- Profil-Name

  frei wählbar, aussagekräftiger Name zu empfehlen

- Verbindungstyp

  VPN zu IPSec-Gegenstelle
- Verbindungsmedium

  Gemäß der benutzten Internetverbindung

  z.B. LAN (over IP) oder xDSL (PPPoE)

Netzeinwahl

Keine Konfiguration notwendig.

HTTP-Anmeldung

Keine Konfiguration notwendig.

Modem

Keine Konfiguration notwendig.

Line Management

- Verbindungsaufbau

  automatisch oder manuell

  Timeout = 0

  Anmerkung: Damit wird die Verbindung nicht mehr bei Leerlauf getrennt!
- Voice over IP (VoIP) priorisieren

  Haken setzen
- EAP-Authentisierung

  Keine Konfiguration notwendig
- HTTP-Authentisierung

  Keine Konfiguration notwendig

IPSec-Einstellungen

- Gateway = IP-Adresse oder DNS-Name des Kommunikationssystems

  Unter dieser IP-Adresse oder DNS-Name ist das Kommunikationssystem über das Internet zu erreichen

  Bezeichnung im VPN-Wizard: **IP-Adresse/DynDNS-Name**
- IKE-Richtlinie = Automatischer Modus
- IPSec-Richtlinie = Automatischer Modus
- Exchange Mode = Main Mode
- PFS-Gruppe = DH-Group 2 (1024 Bit)
- Gültigkeit / Dauer
  - IKE-Richtlinie: 000:00:07:00 (7 Minuten)
  - IPSec-Richtlinie: 000:00:08:00 (8 Minuten)
- Editor

  Keine Konfiguration notwendig

Erweiterte IPSec-Optionen

Keine Konfiguration notwendig

Identität

- Typ = IP Address

  ID = IP-Adresse des Teleworker PCs (siehe auch IP-Adressen-Zuweisung)

  Pre-shared Key verwenden

  Haken setzen

  Shared Secret = Dies ist das Passwort für die VPN-Verbindung

  Bezeichnung im VPN-Wizard: **PreShared Secret**
- Extended Authentication (XAUTH)

  Nicht verwendet, keine Konfiguration notwendig

IP-Adressen-Zuweisung

- IP-Adresse manuell vergeben

  IP-Adresse = IP-Adresse des Teleworker PCs

  Bezeichnung im VPN-Wizard: **IP-Adresse/DynDNS-Name**
- DNS / WINS

  Haken setzen
- DNS-Server = IP-Adresse des Kommunikationssystems

  Bezeichnung im VPN-Wizard: **lokale IP-Subnetzadresse (LAN)**

VPN-IP-Netze

Keine Konfiguration notwendig.

Zertifikats-Überprüfung

Keine Konfiguration notwendig

Link Firewall

- Stateful Inspection aktivieren:

  bei bestehender Verbindung
- Ausschließlich Kommunikation im Tunnel zulassen:

  Haken setzen

20.3.6.2 Wie Sie einen NCP VPN Client konfigurieren

Für die sichere VPN-Verbindung zum Kommunikationssystem muss am Teleworker-Gerät ein NCP VPN Client installiert und konfiguriert werden.

Voraussetzungen

Der Administrator Ihres Kommunikationssystems hat Sie im WBM von OpenScape Business als Teleworker eingerichtet und Ihnen die Export-ZIP-Datei mit den Teleworker-Daten zur Verfügung gestellt.

Der Administrator Ihres Kommunikationssystems hat Ihnen den PreShared Secret Schlüssel für die VPN-Verbindung mitgeteilt.

Auf dem Teleworker-Gerät ist der NCP VPN Client (LANCOM Advanced VPN-Client) installiert. Die dazu notwendigen Informationen finden Sie in der Dokumentation des NCP VPN Clients.

Das Teleworker-Gerät hat eine bestehende, aktive Verbindung ins Internet.

Schritt für Schritt

1) Extrahieren Sie die Dateien `ncp_readme.txt` und `ncp_vpn.ini` und legen Sie diese in einem lokalen Verzeichnis ab. Die Einträge in der Datei `ncp_vpn.ini` beziehen sich auf das Profil `HOOME`.
2) Importieren Sie das Profil `HOOME` in den NCP VPN Client.
3) Erweitern Sie das Profil `HOOME` um einen DNS-Server. Die Adresse des DNS-Servers ist die private IP-Adresse (LAN) Ihres Kommunikationssytems.
4) Starten Sie den NCP VPN Client
5) Markieren Sie das Profil `HOOME` und klicken Sie auf **Connect**.

20.3.6.3 Wie Sie einen Shrew Soft VPN Client konfigurieren

Für die sichere VPN-Verbindung zum Kommunikationssystem muss am Teleworker-Gerät ein Shrew Soft VPN Client installiert und konfiguriert werden.

Voraussetzungen

Der Administrator Ihres Kommunikationssystems hat Sie im WBM von OpenScape Business als Teleworker eingerichtet und Ihnen die Export-ZIP-Datei mit den Teleworker-Daten zur Verfügung gestellt.

Der Administrator Ihres Kommunikationssystems hat Ihnen den PreShared Secret Schlüssel für die VPN-Verbindung mitgeteilt.

Auf dem Teleworker-Gerät ist der Shrew Soft VPN Client installiert.
Ein Download des Shrew Soft VPN Clients finden Sie unter `http://www.shrew.net`.

Das Teleworker-Gerät hat eine bestehende, aktive Internet-Verbindung.

Schritt für Schritt

1) Extrahieren Sie die Dateien `shrewsoft_readme.txt` und `shrewsoft_openswan.vpn` und legen Sie diese in einem lokalen Verzeichnis ab.
2) Starten Sie den **Shrew Soft VPN Client Access Manager** und konfigurieren Sie diesen. Sichern Sie die Eingaben.
3) Importieren Sie die Datei `shrewsoft_openswan.vpn` in den Shrew Soft Client.
4) Anschließend sehen Sie im **Shrew Soft Client VPN Access Manager** unter **Connect** die Verbindung.

20.3.6.4 Wie Sie einen iOS oder Android VPN Client konfigurieren

Für die sichere VPN-Verbindung zum Kommunikationssystem muss am Teleworker-Gerät eine L2TP-VPN-Verbindung konfiguriert werden.

Voraussetzungen

Der Administrator Ihres Kommunikationssystems hat Sie im WBM von OpenScape Business als Teleworker eingerichtet und Ihnen Benutzername, Kennwort und PreShared Secret Schlüssel für die VPN-Verbindung mitgeteilt.

Das Teleworker-Gerät hat eine bestehende, aktive Verbindung ins Internet.

Schritt für Schritt

1) Öffnen Sie am iOS- oder Android-Teleworker-Gerät das Menü **Einstellungen** > **Allgemein** > **VPN**.
2) Fügen Sie mit **VPN hinzufügen** eine neue VPN-Verbindung hinzu.
3) Klicken Sie auf die Registerkarte **L2TP**.
4) Vergeben Sie im Feld **Beschreibung** einen Namen für diese VPN-Verbindung.
5) Geben Sie im Feld **Server** die öffentliche IP-Adresse oder den DNS-Namen des Kommunikationssystems ein.
6) Geben Sie im Feld **Account** den Teleworker-Benutzernamen ein.
7) Geben Sie im Feld **Kennwort** das Teleworker-Kennwort ein.
8) Geben Sie im Feld **Shared Secret** den Schlüssel (Preshared Secret) des VPN-Tunnels ein.
9) Aktivieren Sie den Schalter **Für alle Daten**.
10) Aktivieren Sie im Menü **Einstellungen** den Schalter **VPN**.

20.3.6.5 Wie Sie einen Mac OS-X VPN Client konfigurieren

Für die sichere VPN-Verbindung zum Kommunikationssystem muss am Teleworker-Gerät eine L2TP-VPN-Verbindung konfiguriert werden.

Voraussetzungen

Der Administrator Ihres Kommunikationssystems hat Sie im WBM von OpenScape Business als Teleworker eingerichtet und Ihnen die Export-ZIP-Datei mit den Teleworker-Daten zur Verfügung gestellt.

Der Administrator Ihres Kommunikationssystems hat Ihnen Benutzername, Kennwort und PreShared Secret Schlüssel für die VPN-Verbindung mitgeteilt.

Das Teleworker-Gerät hat eine bestehende, aktive Verbindung ins Internet.

Schritt für Schritt

1) Extrahieren Sie die Datei `.networkConnect` und legen Sie diese in einem lokalen Verzeichnis ab.
2) Klicken Sie auf die Datei `.networkConnect` doppelt.
3) Klicken Sie auf **VPN (L2TP)**.
4) Wählen Sie im Feld **Konfiguration** die VPN-Verbindung aus.

5) Geben Sie im Feld **Serveradresse** die öffentliche IP-Adresse oder den DNS-Namen des Kommunikationssystems ein.
6) Geben Sie im Feld **Benutzername** den Teleworker-Benutzernamen ein.
7) Setzen Sie die Sicherheitseinstellungen:
   a) Klicken Sie auf **Authentifizierungseinstellungen**.
   b) Geben Sie im Feld **Kennwort** das Teleworker-Kennwort ein.
   c) Geben Sie im Feld **Schlüssel ("Shared Secret")** den Schlüssel (Preshared Secret) des VPN-Tunnels ein.
   d) Klicken Sie auf **OK**.
8) Klicken Sie auf **Weitere Optionen** und aktivieren Sie das Kontrollkästchen **Gesamten Verkehr über die VPN-Vebindung senden**. Klicken Sie abschließend auf **OK**.
9) Klicken Sie auf **Anwenden** und anschließend auf **Verbinden**. Bei erfolgreicher Verbindung zur OpenScape Business wird als Status **Verbunden** angezeigt.

20.3.7 VPN - Dienste

Über die Funktion Konfigurierte Dienste können Sie Dienste verwalten. Konfigurierte Dienste werden erst durch Aktivieren zu aktiven Diensten.

20.3.7.1 VPN - Aktive Dienste - Wie Sie alle IPsec-Dienste anzeigen

Sie können eine Liste aller aktiven IPsec-Dienste mit Detaildaten in Tabellenform ansehen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Dienste** > **Aktive Dienste**.
4) Unter der Registerkarte **IPsec-Dienste anzeigen** können Sie die Detaildaten für die aktiven IPsec-Dienste ansehen.

20.3.7.2 VPN - Aktive Dienste - Wie Sie einen speziellen IPsec-Dienst anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Dienste** > **Aktive Dienste**.

4) Klicken Sie im Menübaum den speziellen Dienst an, zu dem Sie alle Informationen einsehen möchten (**Name des Dienstes**, **Quell-Port**, **Ziel-Port**, **IP-Protokoll**, **Zugehörige 'pass'-Regel**, **Zugehörige 'deny'-Regel**).

20.3.7.3 VPN - Konfigurierte Dienste - Wie Sie alle IPsec-Dienste anzeigen

Sie können eine Liste aller konfigurierten IPsec-Dienste mit Detaildaten in Tabellenform ansehen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Dienste** > **Konfigurierte Dienste**.
4) Unter der Registerkarte **IPsec-Dienste anzeigen** können Sie die Detaildaten für die konfigurierten IPsec-Dienste ansehen.

20.3.7.4 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Anmerkung: Vor dem Ändern bzw. Einschalten des IPsec-Dienstes sollte ein Backup durchgeführt werden. IPsec-Regeln verhalten sich wie Firewall-Einträge und können den Zugriff auf das System einschränken. Sollte es doch vorkommen, dass Sie IPsec aktivieren und keinen Zugriff mehr auf das System haben, können Sie das Kommunikationssystem mit **Reload** zurücksetzen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Dienste** > **Konfigurierte Dienste**.
4) Klicken Sie im Menübaum den speziellen Dienst an, den Sie ändern möchten.
5) Ändern Sie den Namen des Dienstes unter **Name des Dienstes**.
6) Ändern Sie den Quell-Port unter **Quell-Port**.
7) Ändern Sie den Ziel-Port unter **Ziel-Port**.
8) Ändern Sie unter **IP-Protokoll** den Dienst (z.B. UDP).
9) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

20.3.7.5 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst umbenennen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Dienste** > **Konfigurierte Dienste**.
4) Klicken Sie im Menübaum den speziellen Dienst an, den Sie umbenennen möchten.
5) Ändern Sie den Namen des Dienstes unter **Name des Dienstes**.
6) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

20.3.7.6 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Dienste** > **Konfigurierte Dienste**.
4) Klicken Sie im Menübaum den speziellen Dienst an, den Sie löschen möchten.
5) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

20.3.8 VPN-Tunnel

Ein Tunnel bezeichnet einen Transport von verschlüsselten Datenpaketen zu einem fest definierten Endpunkt. Aktive Tunnel sind konfigurierte Tunnel nach einer Aktivierung der Konfiguration. Insgesamt lassen sich bis zu 256 Tunnel pro Gateway einrichten.

20.3.8.1 VPN - Aktive Tunnel - Wie Sie allgemeine Tunneldaten anzeigen

Sie können alle aktiven Tunneldaten in Tabellenform mit Detailinformationen ansehen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Tunnel** > **Aktive Tunnel**.
4) Unter der Registerkarte **Allgemeine Tunneldaten anzeigen** sehen Sie die Detailinformationen zu den jeweils aktiven Tunneln. Dies beinhaltet Folgendes:
   - **Name des Tunnels**
   - **Status im IP-Stack**
   - **Endpunktyp des lokalen Tunnels**
   - **Endpunktadresse des lokalen Tunnel**
   - **Endpunkttyp des Remote Tunnel**
   - **Endpunktadresse des Remote Tunnel**
   - **Vorgeschlagene Lebensdauer der Session-Keys**
   - **Vorgeschlagene Lebensdauer der Schlüsseltausch-Session**
   - **Zugehörige Regeln Zugehörige Senderegel**
   - **Zugehörige Regeln Zugehörige Empfangsregel**

20.3.8.2 VPN - Aktive Tunnel - Wie Sie Regeln für alle Tunnel anzeigen

Sie können sich in einem Fenster die Regeln für alle aktiven Tunnel anzeigen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Tunnel** > **Aktive Tunnel**.
4) Unter der Registerkarte **Regeln für alle Tunnel anzeigen** sehen Sie die Detailinformationen zu den jeweils aktiven Tunneln, wie
   - **Tunneldaten**
   - **Regeldaten**
   - **Quelladresse**
   - **Zieladresse**
   - **Dienstdaten**

20.3.8.3 VPN - Konfigurierte Tunnel - Wie Sie allgemeine Tunneldaten anzeigen

Sie können alle Daten für konfigurierte Tunnel in Tabellenform mit Detailinformationen ansehen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Tunnel** > **Konfigurierte Tunnel**.

4) Unter der Registerkarte **Allgemeine Tunneldaten anzeigen** sehen Sie die Detailinformationen zu den jeweils konfigurierten Tunneln. Dies beinhaltet Folgendes:

   - **Name des Tunnels**
   - **Endpunktyp des lokalen Tunnels**
   - **Endpunktadresse des lokalen Tunnel**
   - **Endpunkttyp des Remote Tunnel**
   - **Endpunktadresse des Remote Tunnel**
   - **Vorgeschlagene Lebensdauer der Session-Keys**
   - **Vorgeschlagene Lebensdauer der Schlüsseltausch-Session**
   - **Zugehörige Regeln Zugehörige Senderegel**
   - **Zugehörige Regeln Zugehörige Empfangsregel**

20.3.8.4 VPN - Konfigurierte Tunnel - Wie Sie Regeln für alle Tunnel anzeigen

Sie können sich in einem Fenster die Regeln für alle konfigurierten Tunnel anzeigen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Tunnel** > **Konfigurierte Tunnel**.
4) Unter der Registerkarte **Regeln für alle Tunnel anzeigen** sehen Sie die Detailinformationen zu den jeweils konfigurierten Tunneln, wie

   - **Tunneldaten**
   - **Regeldaten**
   - **Quelldaten**
   - **Zieldaten**
   - **Dienstdaten**

20.3.8.5 VPN - Wie Sie einen konfigurierten Tunnel hinzufügen

Sie können einen neuen IPsec-Tunnel einrichten. Insgesamt lassen sich bis zu 256 Tunnel pro Gateway einrichten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Tunnel** > **Konfigurierte Tunnel**.
4) Unter der Registerkarte **Tunnel hinzufügen** erhalten Sie das Eingabefenster für den neuen Tunnel.

5) Markieren Sie **Tunneldaten**.

6) Geben Sie unter **Name des Tunnels** den gewünschten Namen für den neuen Tunnel ein.

7) Wählen Sie in der Aufklappliste **Endpunkttyp des lokalen Tunnel** den Typ der Endpunktadresse auf der Tunnel-Sendeseite aus (möglich ist die Angabe eines Host- oder DNS-Namens).

8) Geben Sie unter **Endpunktadresse des lokalen Tunnel** die Senderadresse in dem zum Endpunkttyp passenden Format ein.

9) Wählen Sie in der Aufklappliste **Endpunkttyp des Remote Tunnel** den Typ der Endpunktadresse auf der Tunnel-Empfängerseite aus (es wird die Angabe der IP-Adresse unterstützt).

10) Geben Sie unter **Endpunktadresse des Remote Tunnel** die Empfängeradresse in dem zum Endpunkttyp passenden Format ein. Wird die Adresse 0.0.0.0 eingestellt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z.B. Teleworker).

11) Geben Sie unter **Session-Key-Handhabung** das Verfahren für den Schlüsselaustausch ein (möglich ist: Automatisch, mit dem IKE-Protokoll).

12) Wählen Sie unter **Vorgeschlagene Verschlüsselungsalgorithmen** aus, welche Algorithmen verwendet werden dürfen (AES oder 3DES).

13) Wählen Sie unter **Vorgeschlagene Hash-Algorithmen** aus, welche Prüfalgorithmen verwendet werden dürfen (MD5, SHA1 oder SHA2). Die ausgewählten Algorithmen werden vom Initiator der IKE-Aushandlung angeboten.

14) Geben Sie unter **Vorgeschlagene Lebensdauer der Session-Keys** eine Gültigkeitsdauer für die Session Keys (Sitzungsschlüssel) ein, die verwendet werden. Nach Ablauf dieser Zeit werden keine Daten mehr innerhalb dieser Sitzung ausgetauscht. Als Ersatz für ungültig gewordene Session Keys werden automatisch neue Session Keys ausgehandelt.

15) Geben Sie unter **Vorgeschlagene Lebensdauer der Schlüsseltausch-Session** eine Gültigkeitsdauer ein. Nach Ablauf der Schlüsseltausch-Session werden automatisch neue Schlüssel durch IKE ausgehandelt.

16) Geben Sie unter **Vorgeschlagene Datenvolumen der Session-Keys** das maximale Datenvolumen für die Session Keys ein. Nach Überschreiten des Datenvolumens wird automatisch ein neuer Session-Key mittels IKE ausgehandelt. Bei der Auswahl von **unbegrenzt** wird die Gültigkeit der Session Keys nicht durch die Datenmenge begrenzt.

17) Aktivieren Sie im oberen Teil des Fensters das Kontrollkästchen **Schlüsseltauschdaten**.

18) Geben Sie alle Schlüsseltauschdaten ein (**'Perfect Forward Secrecy' aktivieren und wählen Sie das Authentifizierungsverfahren für die VPN-Peers (Pre-Shared-Key** oder **Digitale Signaturen**) aus.

Tipp: Wenn Sie als Authentifizierungsverfahren **Pre-Shared Keys** gewählt haben, so müssen Sie einen 20stelligen Pre-Shared Key eingeben (und diesen wiederholen).

Tipp: Wenn Sie als Authentifizierungsverfahren **Digitale Signaturen** (von einem Lightweight CA) in einem VPN-

Netzwerk mit mehreren Knoten nutzen, müssen Sie zusätzliche Schritte konfigurieren.

a) Erstellen Sie ein LWCA-Zertifikat an einem Knoten.
b) Exportieren Sie das Zertifikat (.crt) in eine Datei.
c) Erstellen und exportieren Sie eine Certificate Revocation List (.crl) in eine Datei.
d) Erstellen und exportieren Sie ein Peer-Zertifikat (.p12), das vom CA-Zertifikat signiert ist, für jeden Knoten.
e) Das CA-Zertifikat (.crt), die Certificate Revocation List (.crl) und die entsprechenden Peer-Zertifikate müssen in jeden Knoten importiert werden.

19) Geben Sie die **Vorgeschlagene Diffie-Hellmann-Gruppen** (DH-Gruppe 2, 5 oder 14) ein.

20) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

20.3.9 VPN-Regeln

Regeln legen fest, was mit einem IP-Paket geschehen soll. Die Regelaktion *Pass* bedeutet, dass das IP-Paket weitertransportiert (durchgelassen) wird. Die Regelaktion *Deny* bedeutet, dass das IP-Paket nicht weitertransportiert (ignoriert) wird. Es kann jeweils ausgewählt werden, ob das IP-Paket einen (verschlüsselten) VPN-Tunnel benutzt oder nicht.

Das Kommunikationssystem kann 640 Regeln verwalten, davon sind 6 Regeln vorbelegt (Default-Regeln) und 634 frei zur Vergabe.

20.3.9.1 VPN - Aktive Regeln - Wie Sie Regeln anzeigen

Sie können sich alle aktiven Regeln anzeigen lassen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN** > **Regeln** > **Aktive Regeln**.

4) Klicken Sie auf die Registerkarte **Regeln anzeigen**, dann sehen Sie die Detailinformationen zu der aktiven Regeln, wie

- **Priorität**
- **Dienst**
- **Aktion für die Regel**
- **Verschlüsselung erforderlich**
- **Regel-Status**
- **Status im IP-Stack**
- **Quelladresse**
- **Zieladresse**
- **Tunnel für die Verschlüsselung**

20.3.9.2 VPN - Aktive Regeln - Wie Sie spezielle Regel anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Regeln** > **Aktive Regeln**.
4) Klicken auf die gewünschte Regel im Menübaum. Das Fenster **Regel anzeigen** mit allen Detaildaten erscheint für diese Regel (**Priorität**, **Dienst**, **Aktion für die Regel**, **Verschlüsselung erforderlich**, **Regel-Status**, **Quelladresse**, **Zieladresse**)

20.3.9.3 VPN - Konfigurierte Regeln - Wie Sie alle Regeln anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Regeln** > **Konfigurierte Regeln**.
4) Klicken Sie auf die Registerkarte **Regeln anzeigen**, dann sehen Sie die Detailinformationen zu der aktiven Regeln, wie

- **Priorität**
- **Dienst**
- **Aktion für die Regel**
- **Verschlüsselung erforderlich**
- **Regel aktivieren**
- **Quelladresse (Typ und IP-Adresse)**
- **Zieladresse (Typ und IP-Adresse)**

20.3.9.4 VPN - Konfigurierte Regeln - Wie Sie eine Regel hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Regeln** > **Konfigurierte Regeln** > **Regel hinzufügen**.
4) Nehmen Sie die Einstellungen für folgende Parameter vor:
   - **Priorität**
   - **Dienst**
   - **Aktion für die Regel (PASS, PASS_INCOMING, PASS_OUTGOING, DENY)**
   - **Verschlüsselung erforderlich**
   - **Regelstatus**
   - **Quelladresse - Typ**
   - **Quelladresse - Adresse (unterste des Bereichs)**
   - **Quelladresse - Subnetzmaske (oberste Adr. des Bereichs)**
   - **Zieladresse - Typ**
   - **Zieladresse - Adresse (unterste des Bereichs)**
   - **Zieladresse - Subnetzmaske (oberste Adr. des Bereichs)**
   - **Tunnel auf der Empfangsseite**
   - **Tunnel auf der Sendeseite**
5) Klicken Sie auf **Übernehmen**.

20.3.9.5 VPN - Wie Sie eine Regel ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Regeln** > **Konfigurierte Regeln**.
4) Markieren Sie die Regel im Menübaum, die Sie ändern möchten.
5) Geben Sie unter **Priorität** die Priorität ein.
6) Geben Sie unter **Dienst** den Dienst (z.B. DNS) ein.
7) Geben Sie unter **Aktion für die Regel** die Regel (**PASS**, **PASS_INCOMING**, **PASS_OUTGOING**, **DENY**) ein.
8) Aktivieren Sie ggf. das Kontrollkästchen **Verschlüsselung erforderlich**.
9) Aktivieren Sie das Kontrollkästchen **Regel aktivieren**.
10) Geben Sie unter **Quelladresse** den **Typ** und die **IP-Adresse** für die geänderte Regel ein.

11) Geben Sie unter **Zieladresse** den **Typ** und die **IP-Adresse** für die geänderte Regel ein.
12) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

20.3.9.6 VPN - Wie Sie eine Regel für die Gegenrichtung hinzufügen

Wenn eine IPsec-Regel für eine Übertragungsrichtung angelegt ist, sollte gleich danach die Regel für die Gegenrichtung hinzufügt werden. Mit der Funktion „Regel für die Gegenrichtung hinzufügen“ werden die Einträge der ausgewählten Regel übernommen, wobei Quell- und Zieladresse gegeneinander getauscht und die Tunnelzuordnung entsprechend gewechselt wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Regeln** > **Konfigurierte Regeln**.
4) Markieren Sie die Regel im Menübaum, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Regel für Gegenrichtung hinzufügen**.
6) Klicken Sie auf **Übernehmen**.
7) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

20.3.9.7 VPN - Wie Sie eine Regel löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Regeln** > **Konfigurierte Regeln**.
4) Markieren Sie im Menübaum die Regel, die Sie löschen möchten.
5) Klicken Sie auf die Registerkarte **Regel löschen**. Die ausgewählte Regel mit allen Daten wird angezeigt.
6) Klicken Sie auf **Löschen**. Es erscheint eine Warnung, dass Sie im Begriff sind diese Regel zu löschen.
7) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

20.3.10 PKI-Server

Der PKI-Server bezeichnet einen Server, der digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI (Public Key Infrastruktur) ausgestellten Zertifikate werden zur Absicherung der Kommunikation verwendet.

Über die vom PKI-Server konfigurierte PKI-URL wird bei Verwendung von Zertifikaten (digitalen Signaturen) versucht, die CRL herunterzuladen.

20.3.10.1 VPN - Wie Sie den PKI-Server anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Public Key Infrastructure (PKI)**.
4) Klicken Sie auf die Registerkarte **PKI-Server anzeigen**. Es werden Ihnen der **Name des PKI-Servers**, der **PKI-Servertyp** und die **URL des PKI-Servers** angezeigt.

20.3.10.2 VPN - Wie Sie einen PKI-Server hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN** > **Public Key Infrastructure (PKI)**.
4) Klicken Sie auf die Registerkarte **PKI-Server hinzufügen**.
5) Geben Sie den **Namen des PKI-Servers** an.
6) Geben Sie den **PKI-Servertyp** (z. B. LDAP) an.
7) Geben Sie die **URL des PKI-Servers** ein.
8) Bestätigen Sie und klicken auf **Übernehmen**.

20.4 Zertifikatshandling

Das Zertifikatshandling (für Secure Sockets Layer SSL) ermöglicht die gesicherte Administration des Kommunikationssystems. Die Daten können nicht von unberechtigten Stellen gelesen bzw. manipuliert werden. Die Autorisierung erfolgt über Zertifikate. Zertifikate können Sie generieren und verwalten.

Der Administrationszugriff erfolgt verschlüsselt über HTTPS unter Verwendung des TLS 1.2-Protokolls. Zertifikate dienen zur Authentifizierung des Kommunikationssystems. Standardmäßig wird ein selbstsigniertes Zertifikat

verwendet. Zur Erhöhung der Sicherheit kann ein Kundenspezifisches Zertifikat verwendet werden.

SSL stellt folgende Sicherungsdienste zur Verfügung:

- Authentizität (der Kommunikationspartner ist der, der er zu sein vorgibt)
- Vertraulichkeit (die Daten können von einem Dritten nicht gelesen werden)
- Integrität (die Daten wurden so empfangen, wie sie gesendet wurden)

Diese Sicherungsdienste erfordern eine vorherige Verständigung auf einen Sicherheitsmechanismus und den Austausch von kryptographischen Schlüsseln. Diese beiden Aufgaben werden beim Verbindungsaufbau erledigt.

SSL verwendet Zertifikate und Schlüssel, um eine gesicherte Datenübertragung zu ermöglichen.

CRL (Certificate Revocation Lists)

Certificate Revocation Lists CRL sind Dateien, welche eine Liste gesperrter Zertifikate, ihrer Seriennummer und ihrer Sperr-Daten enthält. Außerdem enthält eine CRL-Liste den Namen des Ausstellers der Zertifikationsperrliste und des nächsten Aktualisierungszeitpunkts.

CDP (CRL Distribution Point)

CRL Distribution Point (CDP) ist das Verzeichnis (der Ort, in welchem die aktuelle Version der CRLs liegt (z.B. http://sectestcal.microsoft.com/ErtEnvoll/SecTestCAL.crl).

Systemspezifische Informationen

Bei SSL-basierter Administration findet eine Client-Server-Kommunikation statt.

Der Server authentifiziert sich gegenüber dem Client mit Hilfe der im WBM generierten oder importierten Zertifikate. Im Browser kann ein solches Zertifikat als vertrauliches Zertifikat importiert werden, um Warnmeldungen des Browsers beim Verbinden zum SSL-Server zu vermeiden.

Tipp: Die SSL-Zertifikatsgenerierung kann auch für SPE verwendet werden.

20.4.1 Einführung

Was sind SSL-Zertifikate?

TLS/SSL-Zertifikate dienen dazu, Daten bei der Kommunikation zwischen Servern wie OpenScape Business und webbasierten Clients durch Verschlüsselung zu schützen und die Identität des zur Website gehörenden Unternehmens zu überprüfen, damit der Benutzer sicher sein kann, dass er wirklich mit dem richtigen Server kommuniziert.

OpenScape Business stellt sich bei der Erstinstallation des Systems oder bei Änderung der LAN-IP-Adresse ein temporäres ("selbstsigniertes") SSL-Zertifikat aus, das aber außer der eigenen LAN-IP-Adresse keine ausreichenden Daten zur Identitätsprüfung enthält.

Ein solches Zertifikat entspricht nicht den aktuellen Sicherheitsstandards und muss so bald wie möglich nach der Erstinstallation von OpenScape Business durch ein vertrauenswürdiges, individuelles SSL-Zertifikat ersetzt werden, das von einer offiziellen Zertifizierungsstelle (CA) ausgestellt wurde. Nur so können die Mindestanforderungen der aktuellen Client-Betriebssysteme und Webbrowser für eine sichere Internetkommunikation erfüllt werden.

CAs bieten in der Regel SSL-Zertifikate mit verschiedenen Vertrauensstufen an: Bereichsvalidierung (DV), Organisationsvalidierung (OV) und erweiterte Validierung (EV). Für OpenScape Business sind domänenvalidierte Zertifikate ausreichend. Dies ist in der Regel die billigste Option, bei einigen Zertifizierungsstellen ist sie sogar kostenlos.

Für welche Webdienste verwendet OpenScape Business das SSL-Zertifikat?

Das aktive SSL-Zertifikat wird für den Administrator-Zugang über das Admin-Portal sowie für verschiedene andere webbasierte Anwendungen (z. B. Schlüsselprogrammierung) und WSI-basierte UC-Clients wie myPortal @work, myPortal to go, Application Launcher, myContacts und myPortal for Teams verwendet.

Wo erhalte ich ein vertrauenswürdiges SSL-Zertifikat?

Um ein SSL-Zertifikat zu erhalten, müssen Sie sich an eine Zertifizierungsstelle (CA) wenden. Dabei müssen Sie den Domänennamen verifizieren, mit dem Sie OpenScape Business erreichen, um eine Zertifikatsanforderung (Certificate Signing Request, CSR) zu erstellen, die dann zur Validierung an die CA gesendet wird.

Es ist zu beachten, dass von einer Zertifizierungsstelle ausgestellte, vertrauenswürdige SSL-Zertifikate nur eine begrenzte Gültigkeitsdauer von einigen Monaten bis zu einigen Jahren haben, um sicherzustellen, dass sie den aktuellen Sicherheitsstandards entsprechen. Es ist wichtig, das Ablaufdatum im Auge zu behalten und SSL-Zertifikate zu erneuern, bevor das Ablaufdatum erreicht ist.

Werden die SSL-Zertifikate nicht erneuert, kann dies dazu führen, dass die Client-Umgebung die Website als "unsicher" einstuft und die Kommunikation mit dem Server verhindert.

Bitte beachten Sie, dass einige Client-Umgebungen besondere Anforderungen an SSL-Zertifikate stellen, die möglicherweise nicht von jeder CA erfüllt werden. Solche besonderen Anforderungen sind weiter unten im Abschnitt "Client-seitige Überlegungen" aufgeführt. Bei der Auswahl Ihrer CA befolgen Sie bitte die entsprechenden Anweisungen.

Warum ist die Frage der Zertifikate so wichtig geworden?

Die Verwendung von vertrauenswürdigen, kunden- oder serverspezifischen SSL-Zertifikaten ist äußerst wichtig und wird von den großen Betriebssystem- und Browserherstellern zunehmend durchgesetzt. Sicherheit, Professionalität, Integrität und Vertraulichkeit im Umgang mit personenbezogenen Daten sind die wichtigsten Argumente dafür.

Aufgrund der zunehmenden Nutzung von webbasierten Diensten und Clients, auch über das Internet, kommt die dauerhafte Verwendung des temporären, selbstsignierten (und damit unsicheren) Standard-SSL-Zertifikats von OpenScape Business nicht in Frage.

Außerdem hat das temporäre, selbstsignierte Zertifikat von OSBiz eine mehrjährige Gültigkeit, während einige Client-Umgebungen damit begonnen

haben, die Gültigkeit des Zertifikats einzuschränken – manchmal auf nicht mehr als ein Jahr.

Außerdem läuft bei vielen Kundeninstallationen, die ursprünglich mit älteren Softwareversionen vor V3R2.1 eingerichtet wurden, die Gültigkeit dieser temporären, selbstsignierten Zertifikate am 1. Januar 2024 ab.

Das Admin-Portal von OpenScape Business bietet eine Reihe von Instrumenten zur Erzeugung und Verwaltung von SSL-Zertifikaten und unterstützt den Systemadministrator auch bei der Erstellung von Zertifikatsanforderungen. Die wichtigsten Funktionen in diesem Zusammenhang werden im Folgenden erläutert.

20.4.2 CA-Zertifikat generieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsgenerierung**.
4) Klicken Sie auf die Registerkarte **CA-Zertifikat generieren**.
5) Geben Sie unter **Name des Zertifikats** den Namen an.
6) Geben Sie zudem eine laufende Nummer im Feld **Seriennummer des Zertifikats** ein.
7) Wählen Sie unter **Signatur-Algorithmus-Typ** (**sha256RSA**, **sha512RSA** den Algorithmus aus.
8) Wählen Sie unter **Länge des öffentl. Schlüssels** den öffentlichen Schlüssel aus.
9) Geben Sie in den entsprechenden Feldern den Beginn und das Ende der Zertifikatsgültigkeit ein.
10) Füllen Sie anschließend die Felder **Antragsteller** bzw. **Alternativer Antragstellername** aus.
11) Tragen Sie den **CRL-Verteilerpunkt** ein.
12) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.4.3 Wie Sie ein selbstsigniertes Zertifikat generieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsgenerierung**.
4) Klicken Sie auf die Registerkarte **Selbstsigniertes Zertifikat generieren** im Fenster **Zertifikatsgenerierung**.

5) Vergeben Sie im Feld **Name des Zertifikats** einen Namen für das generierte Zertifikat.
6) Vergeben Sie ebenfalls eine laufende Nummer im Feld **Seriennummer des Zertifikats**.
7) Wählen Sie unter **Signatur-Algorithmus-Typ** den Algorithmus aus.
8) Wählen Sie unter **Länge des öffentl. Schlüssels** den öffentlichen Schlüssel aus.
9) Geben Sie in den entsprechenden Feldern den Beginn und das Ende der Zertifikatsgültigkeit ein.
10) Füllen Sie anschließend die Felder zum **Antragsteller** bzw. **Alternativer Antragstellername** aus.
11) Tragen Sie den **CRL-Verteilungspunkt** ein.
12) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.4.4 Zertifikatsanforderungen (CSR) generieren

Abhängig von der Zertifizierungsstelle Ihrer Wahl gibt es verschiedene Möglichkeiten, Zertifikatsanforderungen online (z. B. über das Webportal einer CA) oder offline zu erstellen. Das OpenScape Business Admin Portal bietet die Möglichkeit, eine CSR zum Download und zur Übertragung an die CA zu erstellen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Auf der Seite zur Generierung einer Zertifikatsanforderung (CSR) müssen die folgenden Felder ausgefüllt werden, um den Schlüssel und die CSR-Dateien zu generieren.

Allgemein:

Name der Zertifikatsanforderung: Ein Name für die CSR, der im Namen der heruntergeladenen Datei verwendet werden soll.

Signatur-Algorithmus-Typ: Wählen Sie zwischen sha256RSA und sha512RSA

Länge des öffentl. Schlüssels: Die einzige Option ist 2048

Land (C): Verwenden Sie einen zweistelligen Ländercode, z. B. DE

Organisation (O): bezeichnet den formalen Namen der übergeordneten Einrichtung oder des Unternehmens, dem das Zertifikat zugeordnet ist.

Organisationseinheit (OE): bezeichnet eine bestimmte Untereinheit oder Abteilung innerhalb einer Organisation und bietet eine zusätzliche Granularität zur Identifizierung der Organisationsstruktur.

Common Name (CN): ein wichtiger Identifikator, der in der Regel den Domänennamen darstellt, für den das Zertifikat ausgestellt wird, und der ein Schlüsselelement für die Überprüfung der Identität des Zertifikatsinhabers darstellt.

Alternativer Antragstellername (optional):

Die Erweiterung um einen alternativen Antragstellernamen (SAN) ist ein Merkmal von X.509-Zertifikaten, das im Bereich der Kryptographie verwendet wird. X.509 ist ein Standard, der das Format von Zertifikaten mit öffentlichem Schlüssel definiert. Mit der SAN-Erweiterung können zusätzliche Identitäten wie Hostnamen, IP-Adressen oder E-Mail-Adressen mit einem einzigen X.509-Zertifikat verknüpft werden. Dies ist besonders nützlich in Szenarien, in denen unter verschiedenen Namen oder Adressen auf einen Server zugegriffen werden kann.

Format des DN-Namens: Neben Informationen zum Antragsteller müssen auch unter anderem Angaben zu Land (C), Organisation (O), Organisationseinheit (OE) und Common Name (CN) ausgefüllt werden.

Anderes Format:

Erweiterung alternativer Antragstellername: Optionen sind DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform Resource Indicator, Andere

Alternativer Antragstellername: Die SAN-Erweiterung hilft in Fällen, in denen ein einziger gemeinsamer Name nicht ausreicht oder wenn mehrere Identitäten in einem einzigen Zertifikat enthalten sein müssen. Dies ist wichtig für moderne Webdienste, bei denen ein Server über mehrere Domänennamen oder IP-Adressen erreichbar sein kann.

Hier ist ein Beispiel dafür, wie die SAN-Erweiterung in einem Zertifikat aussehen könnte:

Alternativer Antragstellername:

DNS:www.beispiel.com

DNS:mail.beispiel.com

IP-Adresse:192.168.1.1

E-Mail:admin@beispiel.com

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.
4) Auf der Registerkarte **Zertifikatsanforderung (CSR) generieren**:
5) Geben Sie im Feld **Name der Zertifikatsanforderung** den Namen des Zertifikats ein.
6) Klicken Sie entweder auf **sha256RSA** oder **sha512RSA**, um den **Signatur-Algorithmus-Typ** aus der Aufklappliste auszuwählen.
7) Die **Länge des öffentl. Schlüssels** ist auf **2048** Zeichen festgelegt.
8) Geben Sie das Land **Land C** ein.
9) Geben Sie die Organisation **Organisation O** ein.
10) Geben Sie die **Organisationseinheit (OE)** ein.
11) Geben Sie den **Common Name (CN)** ein.
12) Klicken Sie entweder auf **Format des DN-Namens** oder **Anderes Format**, um das Zertifikatsformat auszuwählen.
13) Wählen Sie optional einen der Werte für **Erweiterung alternativer Antragstellername**.

14) Klicken Sie optional auf die Schaltfläche **Hinzufügen**, um unter **Alternativer Antragstellername** einen entsprechenden Namen im CSR hinzuzufügen.
15) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.4.5 Server-Zertifikat importieren (PKCS#12)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.
4) Klicken Sie auf die Registerkarte **Server-Zertifikat importieren (PKCS#12)** im Fenster **Server-Zertifikate**.

Anmerkung: Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.

---

5) Geben Sie unter **Name des Zertifikats** den entsprechenden Namen ein.
6) Geben Sie das **Entschlüsselungskennwort** ein.
7) Geben Sie unter **Datei mit dem Zertifikat** die gewünschte Zertifikatsdatei ein, indem Sie auf die Schaltfläche **Datei auswählen** klicken.
8) Klicken Sie auf **Zertifikat aus Datei importieren** und anschließend auf **OK**.

20.4.6 Server-Zertifikat importieren (PEM)

Als Alternative werden Zertifikate im PEM-Format unterstützt. Importieren Sie dafür das Zertifikat und die Schlüsseldatei als zwei separate Dateien.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.
4) Klicken Sie auf die Registerkarte **Server-Zertifikat importieren (PKCS#12)** im Fenster **Server-Zertifikate**.

Anmerkung: Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.

---

5) Unter dem Abschnitt **Zertifikat- und Schlüsseldateien importieren**:

6) Geben Sie unter **Name des Zertifikats** den entsprechenden Namen ein. (Sie können einen Namen Ihrer Wahl eingeben.)
7) Geben Sie das **Entschlüsselungskennwort** ein. (Sie können ein Kennwort Ihrer Wahl eingeben.)
8) Wählen Sie unter **Zertifikatsdatei** die Zertifikatsdatei über die Schaltfläche **Datei auswählen** aus.
9) Wählen Sie unter **Schlüsseldatei** die Schlüsseldatei über die Schaltfläche **Datei auswählen** aus.
10) Klicken Sie auf **Zertifikat und Schlüssel importieren** und anschließend auf **OK**.

20.4.7 Wie Sie Zertifikate anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.
4) Klicken Sie auf das gewünschte Zertifikat. Das Fenster **Server-Zertifikate** erscheint.
5) Klicken Sie auf die Registerkarte **Zertifikat anzeigen** und Sie können das aktuelle Zertifikat ansehen.

20.4.8 Wie Sie ein Zertifikat löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.
4) Klicken Sie auf das gewünschte Zertifikat. Das Fenster **Server-Zertifikate** erscheint.
5) Klicken Sie auf die Registerkarte **Zertifikat löschen**. Der Name des aktuell gültigen Zertifikats wird angezeigt mit der Warnung, dass Sie im Begriff sind dieses zu löschen.
6) Wenn Sie das Zertifikat wirklich löschen wollen, klicken Sie auf **Löschen**.

20.4.9 Wie Sie ein Zertifikat exportieren (X.509)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.
4) Klicken Sie auf das gewünschte Zertifikat. Das Fenster **Server-Zertifikate** erscheint.
5) Klicken Sie auf die Registerkarte **Zertifikat exportieren (X.509)**. Sie können das Zertifikat öffnen oder speichern.

20.4.10 Wie Sie ein verlängertes Zertifikat importieren (X.509)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.
4) Klicken Sie auf das gewünschte Zertifikat. Das Fenster **Server-Zertifikate** erscheint.
5) Klicken Sie auf die Registerkarte **Verlängertes Zertifikat importieren (X.509)**. Der Name des aktuell gültigen Zertifikats wird angezeigt.
6) Im Feld **Datei mit dem Zertifikat** geben Sie das gewünschte Zertifikat ein oder wählen es über das Feld **Durchsuchen** aus.
7) Beenden Sie Ihre Eingabe mit **Fingerabdruck des**.

20.4.11 Wie Sie ein Zertifikat aktivieren

Mit dieser Funktion legen sie das zu verwendende Zertifikat für die web-basierte Administration fest.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.

4) Klicken Sie auf das gewünschte Zertifikat.
5) Klicken Sie auf die Registerkarte **Zertifikat aktivieren**. Es erscheint eine Warnung, dass diese Aktion alle bestehenden HTTP-Verbindungen unterbricht.
6) Wählen Sie aus der Aufklappliste **System** das gewünschte System aus (OpenScape Business, UC Booster Server, UC Booster Card), für das Sie das Zertifikat aktivieren wollen.

Anmerkung: Für eine korrekte Funktion muss in jedem Zertifikat im Feld **Allgemeiner Name** die IP-Adresse des Systems eingetragen sein. Achten Sie darauf, dass Sie das richtige Zertifikat für das ausgewählte System aktivieren.

---

7) Klicken Sie auf **Sofort aktivieren**.

Anmerkung: Das importierte Serverzertifikat muss direkt von einer Stammzertifizierungsstelle (Root CA) ausgestellt werden. Zwischenzertifizierungsstellen dürfen nicht verwendet werden.

20.4.12 Zertifikatshandling für Booster Server

Bei der Erstinstallation eines Booster Servers wird ein Zertifikat mit der IP-Adresse des Booster Servers als Common Name erstellt. Das Zertifikat hat eine Gültigkeitsdauer von 10 Jahren und ist für die Organisation „Unify Software and Solutions GmbH & Co. KG“ ausgestellt, wobei als Organisationseinheit „Unify“ angegeben ist.

Es ist möglich, das Standardzertifikat auf dem Booster Server zu ersetzen, indem ein anderes Zertifikat über die Web-Based Management (WBM) Schnittstelle des Systems übertragen wird. Sobald das neue Zertifikat übertragen wurde, kann es aktiviert werden und bietet eine alternative Sicherheitskonfiguration für den Booster Server.

Anmerkung: Wenn Ihr System stattdessen UC Booster Card (OCAB) verwendet, können Sie **UC Booster Card** aus dem Dropdown-Menü in **Schritt 6** auswählen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **SSL** > **Zertifikatsverwaltung** > **Server-Zertifikate**.
4) Wählen Sie eines der importierten Zertifikate aus.
5) Navigieren Sie zur Registerkarte **Zertifikat aktivieren**.
6) Wählen Sie im Dropdown-Menü des Systems die Option **OpenScape Business UC Booster Server**.
7) Klicken Sie auf die Schaltfläche **Jetzt aktivieren**, um das ausgewählte Zertifikat auf den Booster Server anzuwenden.

20.5 Web Sicherheit

Unter Web-Sicherheit finden Sie den Web-Zugriffs-Filter, mit dem Sie Berechtigungen für Clients steuern, und das Admin-Protokoll über das Sie Recherchen über Zugriffe und Änderungen am Kommunikationssystem nachverfolgen können.

20.5.1 Verbindungen zum Web-Server

Die Verbindungen der Clients (z.B. myPortal to go) zum internen Web-Server des Kommunikationssystems können entweder verschlüsselt (HTTPS) oder unverschlüsselt (HTTP) erfolgen.

Anmerkung: Unverschlüsselte Verbindungen zum Web-Server können Unbefugten den Zugriff auf sensible Daten ermöglichen! Aus Sicherheitsgründen wird dringend empfohlen, bei Nutzung von myPortal to go (Web Edition) über Internet nur eine verschlüsselte Verbindung (HTTPS) zu nutzen.

Für myPortal to go (App Edition) steht nur eine verschlüsselte Verbindung zum Web-Server zur Verfügung.

20.5.1.1 Wie Sie die Verbindungen zum Web-Server konfigurieren (UC Suite)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Sicherheit**.
3) Navigieren Sie im Menübaum zu **Web-Zugriff**.
4) Konfigurieren Sie die Verbindungen zum Web-Server:
   - Wenn Sie verschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTPS**.
   - Wenn Sie unverschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTP**.
5) Aktivieren Sie ggf. das Feld **Anmeldedaten im Endgerät speichern**, wenn Sie diese Funktion zulassen wollen. Hiermit werden über sogenannte Cookies die Anmeldedaten im Web-Browser des Mobiltelefons gespeichert.
6) Klicken Sie auf **Speichern**.

20.5.1.2 Wie Sie die Verbindungen zum Web-Server konfigurieren (UC Smart)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **UC Smart** > **Grundeinstellungen**.
3) Prüfen Sie, ob UC Smart **Aktiv** ist.
4) Konfigurieren Sie die Verbindungen zum Web-Server:
   - Wenn Sie verschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTPS**.
   - Wenn Sie unverschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTP**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.5.2 Admin-Protokoll

Das Admin-Protokoll bietet die Möglichkeit zu erfahren, wann welche Änderungen am Kommunikationssystem durchgeführt worden sind und von wem diese gemacht wurden.

20.5.2.1 Wie Sie das Admin.-Protokoll laden

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung**.
3) Navigieren Sie im Menübaum zu **Admin.-Protokoll** > **Admin.-Protokoll-Daten**.
4) Im Fenster **Admin.-Protokoll-Daten** erscheint die Meldung "Das Admin-Log wird vom System geladen. Bitte bestätigen".
5) Klicken Sie auf **Laden**.

20.5.2.2 Wie Sie die Admin.-Protokoll-Sprache ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Wartung**.
3) Navigieren Sie im Menübaum zu **Admin.-Protokoll** > **Konfiguration**.
4) Stellen Sie im Fenster **Konfiguration ändern** unter **Admin.-Protokoll-Sprache** die gewünschte Sprache ein.
5) Klicken Sie auf **Übernehmen**.

20.6 SQL-Sicherheit

OpenScape Business speichert Systemkonfigurationsdaten, Anrufdatensätze, Anmeldeinformationen für Benutzerkonten, UC-Daten etc. in einer internen SQL-Datenbank. Der Zugriff auf die Datenbank wird über Login-Daten geschützt.

Bis SW-Version V2R2 waren die verwendeten Anmeldedaten durch ein Passwort geschützt, das vom OpenScape Business-Administrator nicht geändert werden konnte. Ab V2R2 ist das Passwort änderbar. Das Passwort wird maschinell generiert und ist für den Administrator nicht einsehbar. Um in Mehrfachknoten-Szenarien die Kompatibilität zu alten SW-Versionen zu gewährleisten, kann ein geändertes Passwort wieder auf den "alten" Wert zurückgesetzt werden. Die Konfiguration des SQL-Zugangskennworts erfolgt unter SQL-Sicherheit. Die Konfiguration des SQL-Zugangskennworts ist möglich in Netzwerkumgebungen und Einzelknoten-Umgebungen. Die Vorgehensweise für bestimmte Einzel- bzw. Mehrfachknoten-Szenarien wird in den nachfolgenden Kapiteln beschrieben.

20.6.1 Einzelknoten

SW-Upgrade von V2R1 oder älter

Nach einem SW-Upgrade von V2R1 ist das alte SQL-Datenbankkennwort aktiv. Das SQL-Kennwort muss in der neuen Software-Version vom Systemadministrator über das Administrationsportal (WBM) geändert werden.

Einrichtung des neuen Systems

Bei der Ersteinrichtung des Datums im System wird ein neues SQL-Kennwort generiert. Nur beim ersten Einstellen von Datum und Uhrzeit wird das SQL-Kennwort automatisch geändert.

Einrichtung eines neu geladenen "Einzelknotensystems"

Nach jedem Neuladen des Systems ist das alte SQL-Datenbankkennwort im System aktiv. Das SQL-Kennwort muss in der neuen Software-Version vom Systemadministrator über das Administrationsportal (WBM) geändert werden.

20.6.2 Mehrfachknoten

Das Einzelknotensystem wird mit der bereits bekannten Methode konfiguriert und in das Netzwerk integriert. Nach der Einrichtung des Systems synchronisiert der neue Slave-Knoten sein SQL-Kennwort mit dem Master-Knoten. Eine Anpassung des SQL-Kennworts innerhalb des Slave-Knotens ist nicht erforderlich.

Neuladen eines V2R2 oder höher Knotens in einem V2R2 oder höher Netzwerk

Nach dem Neuladen eines Netzwerkknotens in einem Netzwerk muss der Knoten neu konfiguriert und wieder in das Netzwerk integriert werden.

Neuladen des Master-Knotens

Bei einem Master-Knoten muss das SQL-Kennwort vom Systemadministrator über das Administrationsportal (WBM) geändert werden. Alle Slave-Knoten synchronisieren ihr SQL-Kennwort mit dem neuen Kennwort innerhalb des Master-Knotens. Eine Anpassung des SQL-Kennworts innerhalb der Slave-Knotens ist nicht erforderlich.

Neuladen des Slave-Knotens

Bei einem Slave-Knoten sind keine weiteren Maßnahmen erforderlich, da der Slave-Knoten sein SQL-Kennwort mit dem Master-Knoten synchronisiert.

Neuer V2R2 oder höher Slave-Knoten in einem V2R1-Netzwerk (Szenario wird nicht empfohlen)

Das Einzelknotensystem wird mit der bereits bekannten Methode konfiguriert und in das Netzwerk integriert. Nach der Einrichtung des Systems erkennt der neue Slave-Knoten, dass der Master-Knoten das alte SQL-Kennwort verwendet und verwendet dieses ebenfalls. Eine zusätzliche Anpassung des SQL-Kennworts innerhalb des Slave-Knotens ist nicht erforderlich.

Anmerkung: Es wird dringend empfohlen, das gesamte Netzwerk auf die letzte Softwareversion zu aktualisieren.

Neuer V2R2 oder höher Master-Knoten in einem V2R1-Netzwerk (Szenario wird nicht empfohlen)

Das Masterknotensystem wird mit der bereits bekannten Methode konfiguriert und in das Netzwerk integriert. Nach der Einrichtung des Systems verwendet der neue Master-Knoten das alte SQL-Kennwort. Der Systemadministrator darf das alte Kennwort nicht ändern, da die V2R1-Slaves keine Synchronisierung mit einem neuen SQL-Kennwort auf dem Master-Knoten durchführen können. In diesem Fall würde die Zusammenarbeit zwischen den Knoten innerhalb des Netzwerkes nicht funktionieren. Wenn der Systemadministrator das SQL-Kennwort versehentlich geändert hat, muss er dieses wieder auf das "Standardkennwort" der Masterknotenkonfiguration zurücksetzen.

Anmerkung: Es wird dringend empfohlen, das gesamte Netzwerk auf die letzte Softwareversion zu aktualisieren.

20.6.3 Wie Sie die SQL-Datenbankkennwörter konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephony Server** > **Sicherheit**.

3) Navigieren Sie im Menübaum zu **SQL-Sicherheit**.

4) Konfigurieren Sie die SQL-Datenbankkennwörter:

- Wenn Sie ein neues, dem Benutzer nicht bekanntes Kennwort generieren möchten, aktivieren Sie das Kontrollkästchen **Neu generieren**.
- Wenn Sie das Standardkennwort aktivieren möchten, aktivieren Sie das Kontrollkästchen **Default aktivieren**.

Anmerkung: Im Benachrichtigungsbereich der Landung Page erscheint bei Verwendung des Standard-SQL-Kennworts (oder eines mit dem alten Algorithmus generierten Kennworts) die folgende Meldung:

'`Default SQL password is in use. Please consider changing it via Expert mode`' (Zurzeit wird das Standard-SQL-Kennwort verwendet. Bitte ändern Sie das Kennwort im Expertenmodus)

Bei dieser Meldung handelt es sich um einen URL-Link, der direkt zur SQL-Sicherheitsseite führt, wo das Kennwort geändert werden kann.

20.7 Schutz vor SIP-Attacken (SIP Attack Protection)

Sogenannte SIP-Attacken stellen eine neue Form der Angriffe auf Kommunikationsanlagen über die IP-Telefonie dar. Angriffe können entweder aus dem LAN als auch über das Internet (via falsch konfigurierte Router) erfolgen. Schutz vor SIP-Attacken bietet ein passwortgeschützter SIP-Zugang.

Für einen SIP-Teilnehmerzugang sollten folgende Regeln gelten:

- Aktive Authentifikation
- Ein qualifiziertes Passwort, das
- – zwischen 8 und 20 Zeichen lang ist,
  – einen oder mehrere Großbuchstaben enthält (A bis Z),
  – einen oder mehrere Kleinbuchstaben enthält (a bis z),
  – eine oder mehrere Ziffern enthält (0 bis 9),
  – ein oder mehrere Sonderzeichen enthält (z.B.: %),
  – nicht mehr als 3 Zeichen wiederholt.
- Definition einer SIP-Teilnehmer-ID die sich von der Rufnummer unterscheidet.

Wenn ein neuer SIP-Teilnehmer eingerichtet wird, ist standardmäßig die Authentifikation aktiviert und ein zufälliges Passwort wird generiert. Da dieses zufällige Passwort nicht bekannt ist, muss es vom Administrator geändert werden.

Im Kommunikationssystem werden die entsprechenden Einstellungen über den Wizard "Zentrale Telefonie" gemacht bzw. über den Manager E.

Während des Systemstarts wird die Passwortliste geprüft und ein EventLog-Eintrag (Ereignisanzeige) gemacht, falls ein SIP-Teilnehmer ohne Passwort konfiguriert wurde.

Tipp: Wenn das Kommunikationssystem als Internet Router genutzt wird, muss Port 5060 geschlossen sein (Standardeinstellung). Bei Internettelefonie über ITSP öffnet

das Kommunikationssystem die relevanten Ports und hält diese offen.

Auch wenn ein externer Router bzw. Firewall genutzt wird, muss Port 5060 geschlossen sein. Es liegt in der Verantwortung des Kommunikationssystems diesen Port (falls benötigt) zu öffnen.

21 Vernetzung von OpenScape Business

OpenScape Business Kommunikationssysteme können untereinander vernetzt werden und zusätzlich auch mit den Kommunikationssystemen OpenScape 4000 (HiPath 4000) und OpenScape Voice. Bei einer homogenen OpenScape Business Vernetzung können Teilnehmer Leistungsmerkmale wie Anwesenheitsstatus, Voicemail, Konferenzen und vieles mehr so nutzen, wie dies bislang nur in einem einzelnen OpenScape Business Kommunikationssystem der Fall war.

Mögliche Vernetzungen:

- Reine Sprachvernetzung von OpenScape Business X
- OpenScape Business X und OpenScape Business S Vernetzung (optional mit UC Suite oder UC Smart).
- OpenScape Business X mit OpenScape 4000 (UC-Funktionalität bei OpenScape Business nur unter bestimmten Voraussetzungen)
- OpenScape Business X mit OpenScape Voice (ohne UC-Funktionalität bei OpenScape Business)
- Anbindung von externen Anschaltungen an OpenScape Business über SIP-Interconnection.
- Vernetzung über ISDN
- OpenScape Business-Netzverbund mit zentralem ITSP-Amtsanschluss

Die Kommunikationssysteme werden mit dem Wizard **Vernetzungs-Konfiguration** für die Vernetzung vorbereitet. In diesem Wizard wird angegeben, ob es sich um einen Master- oder Slave-Knoten handelt. Zusätzlich werden der Richtung 16 (Networking) automatisch 16 Leitungen zugeordnet.

Alle Vernetzungen, die Unified Communications Leistungsmerkmale nutzen (wie z.B. UC Smart oder UC Suite), müssen auf einem geschlossenen Rufnummernplan aufsetzen. Vernetzungen ohne Unified Communications Leistungsmerkmale können auf einem offenen oder geschlossenen Rufnummernplan basieren. Um flexibel auf Erweiterungswünsche von Kunden reagieren zu können, wird empfohlen, bei einem neu angelegten Netzverbund immer die geschlossene Nummerierung zu nutzen.

Tipp: Die Einrichtung einer IP-Vernetzung ist ein komplexes Thema und sollte nur von erfahrenen Servicetechnikern durchgeführt werden.

Ein reiner OpenScape Business X1 Netzverbund ist nicht möglich, da ein X1-System kein Master-System sein kann und es im Netzverbund immer ein Master-System geben muss.

Eine Vernetzung von OpenScape Business mit folgenden Systemen wird nicht unterstützt:

- HiPath 3000 SIP-Q, lediglich TDM-Vernetzung auf Basis S_0/S_{2M} mit CorNet NQ wird unterstützt, siehe Vernetzung über ISDN.
- HiPath 5000 RSM
- OpenScape Office MX
- OpenScape Office LX

Die Migration einer HiPath 3000 (inklusive HiPath 5000 RSM) nach OpenScape Business ist im Kapitel Migration beschrieben.

Anmerkung: Informationen zur Lizenzierung und zum Upgrade oder zur Migration von Systemen in einem Netzwerk finden Sie im Abschnitt **Netzwerk - Lizenzierung** im Kapitel Updates.

21.1 Vernetzungsplan

Bevor ein Netzverbund eingerichtet wird, sollte in Absprache mit dem Kunden ein Vernetzungsplan erstellt werden.

Der Vernetzungsplan sollte folgende Daten enthalten:

- Knoten-ID (Node-ID) und zugehörige IP-Adressen
- Rufnummernplan

21.1.1 Homogene und inhomogene Netze

Generell wird bei der Vernetzung zwischen homogenen (alle Komponenten gehören zu einer einzigen Systemfamilie) und inhomogenen Netzen (unterschiedliche Systeme) unterschieden.

Homogenes Netz (Natives Netzwerk)

Inhomogenes Netz (Hybrides Netzwerk)

Ein homogenes (natives) Netz besteht aus Komponenten der OpenScape Business Systemfamilie.

Ein inhomogenes (hybrides) Netz besteht aus Komponenten der Systemfamilie OpenScape Business und z.B. einer OpenScape 4000 oder einer OpenScape Voice.

Übersicht aller OpenScape Business Knoten im Netzverbund

Über den Eintrag **Netzwerk** in der Navigationsleiste des WBM können alle OpenScape Business Knoten eines Netzverbundes angezeigt werden. Zusätzlich können auch alle OpenScape Business Teilnehmer des Netzverbundes nach Knoten sortiert angezeigt werden.

Folgende Informationen können angezeigt werden:

- **Knoten-ID**: Knoten ID
- **M** / **S**: Kennzeichnung, ob der Knoten Master oder Slave ist
- **Netzwerkname**: Name des Knotens
- **Typ**: Typ des Knotens (**OSBiz X**: Hardware-Modell, **OSBiz S**: Softswitch)
- **OSBiz X / OSBiz S**: IP-Adresse des Knotens, klickbar (öffnet das WBM des Knotens)
- **Applikationsserver**: IP-Adresse des UC Servers (UC Booster Card oder UC Booster Server)
- **Registrierungsstatus**: Status der Registrierung
- **Aktiv**: Anzeige, ob der Knoten aktiv ist oder nicht

21.1.1.1 Wie Sie die Übersicht aller OpenScape Business Knoten anzeigen

Voraussetzungen

Mehrere OpenScape Business Kommunikationssysteme sind miteinander vernetzt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Vernetzung**.
2) Klicken Sie im Navigationsbaum auf **Knoten-Sicht**. Es sind alle OpenScape Business Knoten im Netzverbund aufgelistet.

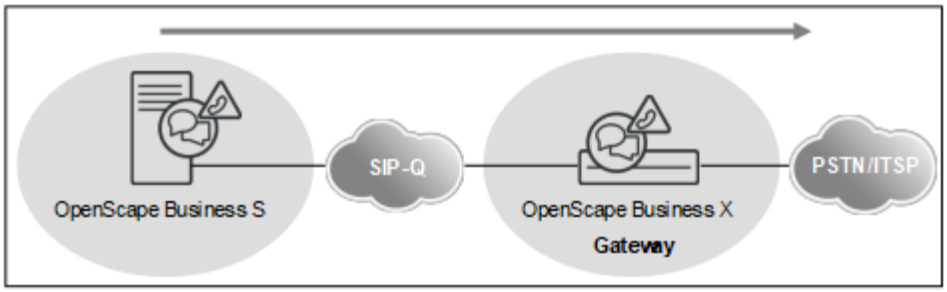
21.1.2 Single- und Multi-Gateway

Bei einer homogenen Vernetzung von OpenScape Business wird zwischen Single- und Multi-Gateway unterschieden, wobei Single-Gateway die Vernetzung mit einem einzigen Gateway und Multi-Gateway die Vernetzung mit mehreren Gateways beschreibt.

Single-Gateway

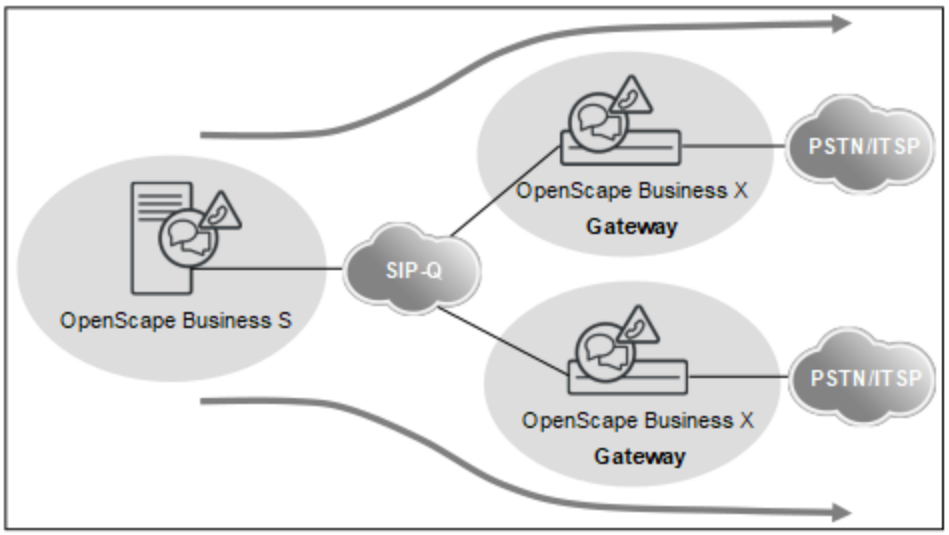
Multi-Gateway

Bei einer Single-Gateway-Vernetzung werden die Anrufe vom und zum Server über ein einziges Gateway geroutet. Alle IP-Teilnehmer, die am Server registriert sind, nutzen dieses eine Gateway.



- Wird unterstützt, wenn sich ein oder mehrere OpenScape Business S im Netzwerk befinden.
- Die IP-Teilnehmer sind an den unterschiedlichen Kommunikationssystemen angeschlossen.
- OpenScape Business X wird als Gateway genutzt.

Bei einer Multi-Gateway-Vernetzung werden die Anrufe über mehrere, verschiedene OpenScape Business Gateways geroutet.



- Nur 1 PSTN-Provider bzw. eine Amtsrufnummer pro Gateway
- Die Teilnehmer unterschiedlicher Standorte sind an einem zentralen System (OpenScape Business S) registriert.
- Jedem Teilnehmer der OpenScape Business S wird ein bestimmtes Gateway (OpenScape Business X) zugeordnet.
- Es darf nur eine einzige OpenScape Business S im Netzwerk befinden.
- OpenScape Business und OpenScape Business S befinden sich in derselben Zeitzone und im gleichen Land (gleicher Country-Code).
- Es gibt nur eine Amtskennzahl netzweit.
- An den Gateways können z.B. ISDN- und analoge Teilnehmer lokal eingerichtet sein.

21.2 Netzweite Leistungsmerkmale

Netzweite Voice-Leistungsmerkmale werden im wesentlichen bestimmt durch das SIP-Q-Vernetzungsprotokoll. Netzweite UC-Leistungsmerkmale werden bestimmt durch die Vernetzung der UC-Lösung (UC Suite oder UC Smart) und deren UC Clients.

21.2.1 Netzweite Leistungsmerkmale der UC-Lösungen

Die folgende Tabelle bietet Ihnen einen Überblick über die netzweiten Leistungsmerkmale der beiden UC-Lösungen UC Smart und UC Suite.

Das UC-Interworking zur OpenScape 4000 und OpenScape Voice ist nicht möglich. In einem OpenScape Business Netzverbund sollte entweder UC Smart oder UC Suite verwendet werden. Gemischte UC-Lösungen werden nicht unterstützt.

Netzweite UC-Funktionen	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Netzweite Sichtbarkeit des Anwesenheitsstatus (Präsenz-Management)	x	x	x	x	x
Änderung des eigenen Anwesenheitsstatus über Client	x	x	x	x	x
Änderung des eigenen Anwesenheitsstatus über TUI	x	x	x	x	x
Statusbezogene Anrufumleitung	x	x	x	Über andere UC Suite Clients definierte Ziele	über myPortal definierte Ziele
Netzweite Statusanzeige in Favoriten	x	x	x	x	x
Netzweite Statusanzeige in Verzeichnissen	x	x	x	x	x
Netzweite Statusanzeige im Journal	-	-	x	-	-
CallMe aktivieren	-	-	x	x	x
Kalender-Integration (Outlook)	-	-	x	-	-
Kalenderintegration (iCal) (nur mit myPortal for Desktop)	-	-	x	-	-
Netzweite Anzeige des Anrufstatus (Frei, Besetzt, Rufzustand)	x	x	x	x	x
Anlegen von Gruppen netzweit	x	x	x	-	-
Kompakte Anzeige der Favoriten	-	-	x	-	-
Gespräche	x	-	-	x	-
Persönliches Verzeichnis	Lokal	Lokal	Lokal	Lokal	Lokal
Internes Verzeichnis	Lokal	Lokal	Lokal	Lokal	Lokal
Externes Verzeichnis	-	-	x	x	x
Suche in Verzeichnissen netzweit	x	x	x	x	x

Netzweite UC-Funktionen	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Zugriff auf im System definierte Kurzwahlziele (KWZ)	Lokal	Lokal	-	Lokal	Lokal
Import/Verwalten persönlicher Kontakte (CSV/XML)	x	-	x	-	-
Zugriff auf Outlook-Kontakte	x	-	x	-	-
Import von persönlichen Kontakten (Mac OS) (myPortal for Desktop)	-	-	x	-	-
Integration externer Verzeichnisserver über LDAP	-	-	x	-	-
Alle Anrufe	x	x	x	x	x
Offene Anrufe	-	x	x	-	-
Entgangene Anrufe	x	x	x	x	x
Angenommene Anrufe	x	x	x	x	x
Geplante Anrufe	-	-	x	-	-
VoIP Anrufe	x	-	x	x	-
Fax-Journal	-	-	x	-	-
Manuelle Wahl	x	x	x	x	x
Desktop-Wahl (Click to Call)	-	-	x	-	-
Umleiten	x	x	x	x	x
Anruf halten	x	x	x	x	x
Aufzeichnen von Anrufen (Voice Recording)	-	-	x	-	-
E-Mail senden	x	x	x	x	x
SMS senden	-	x	-	-	x
Popups	x	-	x	x	-
AdHoc-Konferenz	x	x	x	x	x
Geplante Konferenzen	-	-	x	-	-
Permanente und offene Konferenzen (Drag&Drop-Konferenz)	x	-	x	-	-

Netzweite UC-Funktionen	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Web Collaboration-Einbindung	x	-	x	x	-
Sprachbox (Visuelle Voicemail)	x	x	x	x	x
Sprachnachricht abhören über Telefon	x	x	x	x	x
Sprachnachricht abhören über PC-Soundkarte	-	-	x	-	-
Senden einer Sprachnachricht als E-Mail	x	x	x	-	-
Fax (für Windows Betriebssysteme)	-	-	x	-	-
Instant Messaging (Chat) netzweit	x	-	x	-	-

21.2.2 Netzweite Voice-Leistungsmerkmale

Bei einer Vernetzung über das SIP-Q-Protokoll werden folgende Sprachleistungsmerkmale für OpenScape Business und andere Kommunikationssysteme unterstützt.

Leistungsmerkmal	SIP-Q (IP-Netzwerk)
Basic Call	Ja
Rückruf bei Besetzt	Ja
Rückruf im Freifall	Ja
Aufschalten	Ja
Anklopfen	Ja
Zweitanruf	Ja
Calling Line Identification Presentation (CLIP)	Ja
Calling Line Identification Restriction (CLIR)	Ja
Connected Line Identification Presentation COLP	Ja
Connected Line Identification Restriction COLR	Ja
Calling / Connected Name Identification Presentation CNIP	Ja
Calling / Connected Name Identification Restriction CNIR	Ja
Anrufschutz	Ja
Anrufumleitung	Ja

Leistungsmerkmal	SIP-Q (IP-Netzwerk)
Rufweiterschaltung im Besetztfall	Ja
Rufweiterschaltung im Freifall	Ja
Call Deflection	Ja
Advice of Charge at Call Setup	Nein
Advice of Charge during Call	Ja
Advice of Charge at the end of the call	Ja
Wegeoptimierung	Nein
Rerouting	Nein
Message Waiting Indication / Info	Ja
Fangen	Ja
Halten	Ja
Makeln	Ja
Übergabe	Ja
Konferenz	Ja
Wiederanruf	Ja
Notruf	Ja
Abwurf	Ja
Private Numbering Plan PNP	Nein
Anrufübernahme	Nein
Sammelanschluss	Ja
SPE (außer bei Konferenz und Applikationen)	Ja

21.3 Lizenzierung eines Netzverbundes

Für ein vernetztes Kommunikationssystem kann eine zentrale Lizenzierung ausgewählt werden.

Alle Lizenzen der Einzelsysteme werden zu einer netzweiten Lizenz am Lizenzserver zusammengefasst. Im Netzverbund können die Lizenzen über das WBM den einzelnen Knoten beliebig zugeordnet werden.

Weitere Informationen siehe Lizenzierung mehrerer Kommunikationssysteme (Netzverbund).

21.4 Anforderungen an die Vernetzung

Um die Qualität der Sprachübertragung sicherzustellen, müssen die verwendeten IP-Netze und das Kommunikationssystem bestimmte

Anforderungen erfüllen. Die Sprachqualität und die Zuverlässigkeit der Sprachkommunikation hängen hierbei von der eingesetzten Netzwerktechnik ab.

Netzwerkparameter, Anforderung für LAN und WAN

Parameter	Mindestanfo	Hinweise
Delay (one way)	50 ms	Höhere Werte verschlechtern die Sprachqualität.
Round Trip Delay	100 ms	Höhere Werte verschlechtern die Sprachqualität.
Jitter	20 ms	Höhere Werte verschlechtern die Sprachqualität.
Packet Loss	3%	Bei Fax- oder Modem-Übertragungen über G.711 sollte der Paketverlust 0,05% nicht übersteigen (für den Fall, dass kein T.38 möglich ist).
Consecutive Packet Loss	3 bei G.711	Höhere Werte verschlechtern die Sprachqualität.

Empfehlung zur Bandbreitenkalkulation

- Im Netzverbund ist eine Bandbreite von mindestens 256 kBit/s (jeweils in Sende- und Empfangsrichtung) erforderlich.
- Die Bandbreitenkalkulation sollte von maximal 50 % für den Sprachanteil bzgl. der Gesamtbandbreite ausgehen, d.h. zum Beispiel bei einem 1 MBit-WAN sollten maximal 500 KBit/s für Sprache kalkuliert werden. Bei G.711-Codec sind das beispielsweise maximal 5 IP-Trunks.
- Unabhängig davon sind die Netzeigenschaften bzgl. QoS, Delay, Packet Loss etc. zu beachten.

21.4.1 Anforderungen an die LAN-Vernetzung

Um die Qualität der Sprach- und Datenübertragung sicherzustellen, müssen die verwendeten IP-Netze und das Kommunikationssystem bestimmte Anforderungen an das LAN erfüllen.

LAN-Anforderungen

Das Datennetzwerk muss vom Typ Ethernet sein:

- Empfohlen werden mindestens Cat.5-Kabel (geschirmte/ungeschirmte mehradrige Kabel bis 100 MHz für den Horizontal- und Steigbereich gemäß EN 50288).
- Unterstützung für QoS: IEEE 802.1p, DiffServ (RFC 2474).
- Alle aktiven LAN-Ports müssen 100 / 1000 MBit/s und Vollduplex-Kommunikation unterstützen.

Jedes Kommunikationssystem muss über einen Switch oder einen dedizierten Port eines Routers angeschlossen sein. Hubs oder Repeater werden nicht unterstützt.

Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer LAN-Umgebung

Die erforderliche Bandbreite für Sprachübertragung in einem IP-Netzwerk lässt sich mit Hilfe der folgenden Tabelle berechnen:

Codec-Typ	Paketierungs-Parameter	Sample Rate (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	Ethernet Load (inkl. Header) (kBit/s)
G.711	20	20	160	230	44%	92
G.711	30	30	240	310	29%	82,7
G.711	40	40	320	390	22%	78
G.711	60	60	480	550	15%	73,3
G.729A	1	20	20	90	350%	36
G.729A	2	40	40	110	175%	22
G.729A	3	60	60	130	117%	17,3
RTCP		5000		280		0,4

Der Load im LAN ist jeweils für Sende- und Empfangsrichtung gültig.

Die Berechnung schließt VLAN-Tagging entsprechend IEEE 802 1q ein. Ohne VLAN-Tagging ist die Länge eines Pakets um 4 Bytes kürzer.

Der Overhead berechnet sich wie folgt:

Protokoll	Bytes
RTP-Header	12
UDP-Header	8
IP-Header	20
802.1Q VLAN Tagging	4
MAC (incl. Preamble, FCS)	26
Summe	70

Payload Transport in T.38 LAN-Umgebung:

	Sample Rate (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	Payload- Paket (Overhead in Prozent)	Ethernet Load (inkl. Header) (kBit/s)
T.38	30	169	227	34%	60,5

Payload-Verbindungen mit SRTP (Secure Realtime Transport Protocol) in einer LAN-Umgebung:

Codec-Typ	Sample Rate (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	SRTP-Ethernet Paketlänge (kBit/s)	RTP-Ethernet Paketlänge (kBit/s	Zusätzliche Bandbreite bei SRTP (%)
G.711	20	160	244	97,6	92	6,1

Codec-Typ	Sample Rate (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	SRTP-Ethernet Paketlänge (kBit/s)	RTP-Ethernet Paketlänge (kBit/s	Zusätzliche Bandbreite bei SRTP (%)
G.711	30	240	324	86,4	82,4	4,5
G.711	40	320	404	80,8	78	3,6
G.711	60	480	564	75,2	73,3	2,5
G.729A	20	20	104	41,6	36	15,6
G.729A	40	40	124	24,8	22	12,7
G.729A	60	60	144	19,2	17,3	10,8

21.4.2 Rufnummernplan im Netz

Der Rufnummernplan ist eine wichtige Voraussetzung für die Vernetzung. Abhängig vom Rufnummernplan gestaltet sich die Konfiguration des Netzverbundes mehr oder weniger aufwändig. Open Scape Business unterstützt im Netzverbund generell die offene und geschlossene Nummerierung, wobei der volle Umfang der UC-Leistungsmerkmale nur bei geschlossener Nummerierung genutzt werden kann.

Geschlossene Nummerierung

Bei der verdeckten (geschlossenen) Nummerierung wird ein Teilnehmer im Netzverbund eindeutig durch die Teilnehmerrufnummer identifiziert. Jeder Teilnehmer im Netzverbund kann einen anderen Teilnehmer durch direktes Wählen von dessen Rufnummer erreichen.

Die verdeckte Nummerierung hat den Vorteil, dass keine Knotenrufnummer gewählt werden muss, um einen anderen Teilnehmer in einem anderen vernetzten Kommunikationssystem zu erreichen.

Tabelle 10: Beispiel für verdeckte Nummerierung

	Knoten 1	Knoten 2	Knoten 3	Knoten 4
Rufnummern	100	200	300	400
	101	201	301	401
	102	202	302	402
	103	203	303	403
	104	204	304	404

Offene Nummerierung

Bei der offenen Nummerierung wird ein Teilnehmer eindeutig durch die Knotenrufnummer und die Teilnehmerrufnummer identifiziert. Teilnehmer unterschiedlicher Kommunikationssysteme (Knoten) im Netzverbund können somit die gleiche Teilnehmerrufnummer haben.

Bei der offenen Nummerierung muss zusätzlich zur Rufnummer des Teilnehmers immer die Knotenrufnummer mitgewählt werden. Dafür können

die Rufnummernbänder mehrfach verwendet werden, und es sind mehr Rufnummern nutzbar.

Folgende UC-Leistungsmerkmale werden bei einer offenen Nummerierung nicht unterstützt:

- UC Smart
- UC Suite
- netzweiter CSP (CSTA Service Provider)
- DSS-Server
- CMD (CSTA Message Dispatcher)

Tabelle 11: Beispiele für offene Nummerierung

	Knoten 1	Knoten 2	Knoten 3	Knoten 4
Knotenrufnummer (Anlagenrufnummer)	95	96	97	98
Rufnummern	100	100	100	100
	101	101	101	101
	102	102	102	102
	103	103	103	103
	104	104	104	104

21.4.2.1 Wahl von öffentlichen Rufnummern im Netz

Unabhängig von geschlossener oder offener Nummerierung ist es sinnvoll, sowohl knoteninterne Ziele als auch netzinterne Ziele über öffentliche Rufnummern anzuwählen. (z.B. als UC Client, der Kontakte im voll qualifizierten Format aus Verzeichnissen wählt).

21.5 Wegeoptimierung (Path Replacement)

Mit Hilfe der Wegeoptimierung (Path Replacement) wird bei vernetzten Kommunikationssystemen eine Doppelbelegung von IP-Leitungen vermieden.

Wenn mehrere OpenScape Business-Systeme vernetzt sind, kann z. B. folgendes Problem auftreten: Nehmen wir zunächst an, Teilnehmer A ruft Teilnehmer B an, der seinerseits alle Anrufe an Teilnehmer C umgeleitet hat. Die Teilnehmer A und C befinden sich im gleichen Netzknoten, aber Teilnehmer B befindet sich in einem anderen Netzknoten. Daher belegt der Anruf mit Rufumleitung zunächst zwei Leitungen zwischen den beiden Netzknoten. Um diese Doppelbelegung zu vermeiden sollte die Wegeoptimierung aktiviert sein.

Tipp: Das System-Flag für die Wegeoptimierung muss bei allen vernetzten OpenScape Business Systemen aktiviert werden!

: Es wird dringen empfohlen, die Funktion Wegeoptimierung nicht in Netzwerken zu verwenden, in denen analoge Faxstationen verwendet werden. Diese Einschränkung wird mit einer kommenden Softwareversion behoben.

Die Wegeoptimierung wird ausgeführt:

- Innerhalb des OpenScape Business Netzanteils
- Nach dem Verbindungsaufbau (nicht in der Rufphase!)
- Nach Transferszenarien
- Nach Rufweiterschaltung bzw. Anrufumleitung

Die Wegeoptimierung wird nicht ausgeführt:

- Einer Rufzuschaltung bzw. Gruppenruf
- Bei Konferenzen
- Wenn während der Ausführung der Wegeoptimierung ein anderes Leistungsmerkmal aktiviert wird, wird die Wegeoptimierung abgebrochen.
- Bei inhomogener Vernetzung werden die Fremdsysteme über SIP-Interconnection konfiguriert. In diesem Fall ist, unabhängig von der Konfiguration des Flags, kein Path Replacement möglich (z.B. OpenScape 4000, OpenScape Voice, Externe SIP-Server).

21.5.1 Wie Sie die Wegeoptimierung (Path Replacement) aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System** > **System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Anrufübernahme von Wiederanrufen möglich sein soll, aktivieren Sie das Kontrollkästchen **Wegeoptimierung**.
   - Wenn die Anrufübernahme von Wiederanrufen nicht möglich sein soll, deaktivieren Sie das Kontrollkästchen **Wegeoptimierung**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6 Vernetzungsszenarien

Es gibt mehrere Szenarien, wie OpenScape Business Systeme untereinander und mit anderen Kommunikationssystemen vernetzt werden können.

- Vernetzung von mehreren OpenScape Business X
- Vernetzung von OpenScape Business X und OpenScape Business S (Single Gateway)
- Vernetzung von OpenScape Business X und OpenScape Business S (Multi Gateway)

- Vernetzung von OpenScape Business S in einer Hosting-Umgebung
- Vernetzung von OpenScape Business X und OpenScape 4000
- Vernetzung von OpenScape Business X und OpenScape Voice
- Anbindung von externen Anschaltungen an OpenScape Business über SIP-Interconnection
- Offene Nummerierung in OpenScape Business X Netzwerken
- Vernetzung über ISDN
- OpenScape Business Netzverbund mit zentralem ITSP-Amtsanschluss

Gesprächsdaten können nur per Netzknoten, nicht knotenübergreifend abgerufen werden.

21.6.1 Abhängigkeiten und Einschränkungen

Für die möglichen Vernetzungsszenarien gilt es einige Abhängigkeiten und Einschränkungen zu beachten.

Abhängigkeiten und Einschränkungen

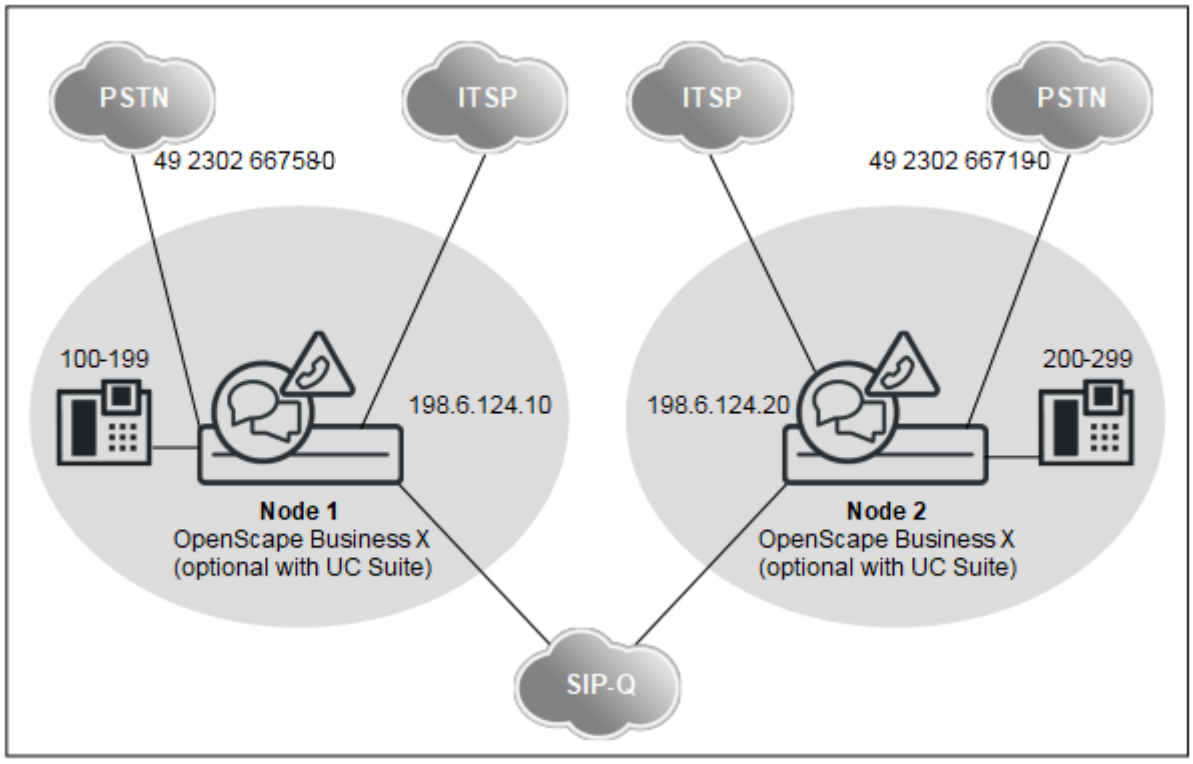
- Jedes System im Netzverbund ist einer eigenen Zeitzone zugeordnet. Alle Teilnehmer eines Systems haben daher dieselbe Zeitzone.
- OpenScape Business S Multi-Gateway-Vernetzungen sind nur innerhalb eines Landes (gleiche Zeitzone, gleiche Amtskennzahl) freigegeben.
- Generell wird jeder Netzverbund der OpenScape Business über Wizards konfiguriert. OpenScape Voice und OpenScape 4000 werden in der Vernetzung je Knoten über den Expertenmodus konfiguriert.
- Der Presence Manager (DSS Server Funktionalität = netzweite Anzeige von Besetztzuständen an DSS-Tasten + Anrufübernahme) steht in OpenScape Business Netzwerken zur Verfügung.
- SIP-Q Leitungen mit Richtung 16 (letzte Richtung) werden genutzt um homogene OpenScape Business Kommunikationssysteme über den Wizard **Vernetzung-Konfiguration** zu konfigurieren. Externe SIP-Leitungen (SIP-Interconnection) werden für die Vernetzung von OpenScape 4000, OpenScape Voice oder andere Kommunikationssysteme genutzt; die Konfiguration erfolgt über den Experten-Modus.
- Wird das System über den Wizard **Vernetzung-Konfiguration** als Slave oder Master konfiguriert, wird geprüft, ob der Richtung "Networking" Leitungen zugeordnet sind. Wenn nicht, werden der Richtung "Networking" automatisch 16 Leitungen zugeordnet. Wird das System aus dem Netzverbund genommen, bleiben diese Zuordnungen bestehen.
- In jedem Knoten kann nur EIN Voicemail-System zum Einsatz kommen. Generell sind in einem OpenScape Business Netzverbund verschiedenen Voicemail-Systeme erlaubt:
  - Kommt die UC Suite zum Einsatz, müssen andere im Netzverbund vorhandene Voicemail-Systeme vom Administrator deaktiviert werden.
  - Ein HiPath 3000 Netzverbund mit verschiedenen Voicemailsystemen kann 1:1 nach OpenScape Business migriert werden.
- Aus technischen Gründen können OpenScape Business X1-Systeme nicht als Master eingerichtet werden. Da in jedem OpenScape Business-Netzwerk ein Master-System erforderlich ist, muss mindestens ein System größer als X1 sein.

Tipp: Das vertriebliche Limit kann von diesen Angaben (und den nachfolgenden Angaben in den einzelnen Szenarien) abweichen. Bitte beachten Sie die Hinweise in der Vertriebsinformation.

21.6.2 Vernetzung von mehreren OpenScape Business X

Bis zu 32 Kommunikationssysteme OpenScape Business X können miteinander vernetzt werden.

Netzwerkdaten



- Mit UC-Lösung (UC Smart oder UC Suite): nur geschlossene Nummerierung möglich
- Ohne UC-Lösung: geschlossene oder offene Nummerierung möglich
- Konfiguration über WBM (Wizards) bei geschlossener Nummerierung
- UC Suite Funktionalität basiert auf UC Booster Server oder UC Booster Card
- Bis zu 32 vernetzte Systeme und 1500 User ohne UC-Lösung
- Bis zu 8 vernetzte Systeme und 1500 User mit UC-Lösung

Netzweite Leistungsmerkmale

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 mit UC-Lösung und 32 ohne UC-Lösung	
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl von Teilnehmern im Netz	1500	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
UC Booster Card	UC Smart: 51 - 150 Teilnehmer (0 - 50 Teilnehmer ohne UC Booster Card) UC Suite: 0 - 150 Teilnehmer	Wird nicht unterstützt
UC Booster Server	UC Smart: ab 150 Teilnehmer UC Suite: ab 150 Teilnehmer	Wird nicht unterstützt

Administration	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Netzweite Administration Expertenmodus
Manager E	Netzweite Administration für spezielle Aufgaben	Netzweite Administration für spezielle Aufgaben
UC-Suite-Administration (für UC Booster Server und UC Booster Card)	Netzweite Administration über Wizards	Wird nicht unterstützt
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	

Lizenzierung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	

Konfiguration

Diese Konfiguration (mit geschlossener Nummerierung und UC Suite) zeigt an einem Beispiel, welche Schritte für die Einrichtung einer Vernetzung durchzuführen sind.

Voraussetzungen:

- Es liegt ein Vernetzungsplan vor. Über den Vernetzungsplan ist sichergestellt, dass jede interne Rufnummer im Netzverbund bei verdeckter (geschlossener) Nummerierung nur einmal vergeben ist. Unterschiedliche Rufnummerlängen sind zulässig. Nur Duwa-Rufnummern dürfen mehrfach vorkommen (z.B. Amtsrufnummer 49 2302 66758 100 und 49 2302 66719 100 haben dieselbe Duwa-Nr. 100).

Tipp: Die Rufnummern müssen ggf. angepasst werden. Eine offene Nummerierung ist nicht implementiert!

- Das IP-Netzwerk ist eingerichtet und alle Knoten können untereinander über Ping erreicht werden
- Alle Knoten sind auf die gleiche Softwareversion hochgerüstet

Knotenübergreifende Rufumleitungen: Bei kommenden Rufen über IP-Trunks, die bereits umgeleitet sind, werden weitere Umleitungen zur Sprachbox nicht ausgeführt. Hintergrund ist, dass ansonsten keine eindeutige Zuordnung zur Sprachbox erfolgen kann

Falls knotenübergreifende Stellvertreterregelungen gewünscht werden, sind diese über Profile der OpenScape Business Teilnehmer oder Rufzuschaltungen einzurichten. Entsprechende knotenübergreifende Anrufe werden in diesem Fall nicht als umgeleitet signalisiert, sondern als Direktruf. Daher werden Rufumleitungen des Stellvertreters zur Sprachbox umgeleitet.

Tabelle 12: Einrichtung der Standortdaten für Knoten 1

Knoten 1		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66758
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 1 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 13: Übersicht der Einträge im LCR für Knoten 1

Rufnummernplan		**Wegetabelle**			**Wahlregel**		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 2 Internat	0C0049230266719-Z	Vernetzung	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-Z						
Knoten 2 Teiln.	0C66719-Z						

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Tabelle 14: Einrichtung der Standortdaten für Knoten 2

Knoten 2		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 2 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 15: Übersicht der Einträge im LCR für Knoten 2

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266758-Z	Vernetzung	Erzwungen	1	D49230266758E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Vorgehensweise bei der Einrichtung der Vernetzung:

1) Basisinstallation für Knoten 1 (Master) konfigurieren

2) Vernetzung konfigurieren für Knoten 1
3) Basisinstallation für Knoten 2 (Slave) konfigurieren
4) Vernetzung konfigurieren für Knoten 2
5) Vernetzungsfunktion kontrollieren für Master
6) Richtungen und Richtungsparameter überprüfen (Master)
7) Richtungen und Richtungsparameter (Rtg. 16) überprüfen (Master)
8) LCR für die Vernetzung konfigurieren (Master)
9) Richtungen und Richtungsparameter überprüfen (Slave)
10) LCR für die Vernetzung konfigurieren (Slave)

21.6.2.1 Wie Sie die Basisinstallation für Knoten 1 (Master) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.
4) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
5) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.
6) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
7) Vergeben Sie im Feld **Knoten-ID** für eine OpenScape Business eine im Netzverbund eindeutige Knoten-ID (eine "**1**" für das Einrichtebeispiel).
8) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
9) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.
10) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

Anmerkung: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

---

11) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
12) Konfigurieren Sie jetzt die IP-Clients.

13) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
14) Konfigurieren Sie jetzt den E-Mail-Versand.
15) Klicken Sie auf **Beenden**.

21.6.2.2 Wie Sie die Vernetzung für Knoten 1 (Master) konfigurieren

Im nächsten Schritt wird der Wizard für die Vernetzung konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) Definieren Sie den Knotentyp (**Master**).
6) Geben Sie unter **Node-ID** die entsprechenden Knotennummern der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die des Slaves mit der Node-ID 2).
7) Geben Sie unter **IP-Adresse** die IP-Adressen der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die des Slaves mit der Node-ID 2).
8) Geben Sie unter **Name** den entsprechenden Typ der Unteranlage ein.
9) Aktivieren Sie ggf. das Kontrollkästchen **Verschlüsselung erforderlich**.

Tipp: Die Verschlüsselung basiert auf SPE und gilt nicht für die Applikationen!

Anmerkung: Durch die Aktivierung des Kontrollkästchens ist noch keine Verschlüsselung konfiguriert. Siehe Signaling and Payload Encryption (SPE) .

---

10) Klicken Sie auf **Beenden**.

21.6.2.3 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID (eine "**2**" für das Einrichtebeispiel).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.
9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

   Anmerkung: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

   ---

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
11) Konfigurieren Sie jetzt die IP-Clients.
12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
13) Konfigurieren Sie jetzt den E-Mail-Versand.
14) Klicken Sie auf **Beenden**.

21.6.2.4 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren

Im nächsten Schritt wird der Wizard für die Vernetzung konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.

6) Geben Sie unter **IP-Adresse** die IP-Adresse des Masters ein.

Tipp: Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängig gemacht werden!

---

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.
8) Klicken Sie auf **Beenden**.

21.6.2.5 Wie Sie die Vernetzungsfunktion für den Master kontrollieren

Sie können den Status der Vernetzung generell und die einzelnen Rufnummern kontrollieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.
2) In der Statuszeile sehen Sie den **Synchronisationsstatus** für das Netzwerk. Grün bedeutet, dass die Vernetzung keine Probleme hat, Rot bedeutet Probleme im Netzwerk.
3) Markieren Sie im Fenster **Netzwerk** die Registerkarte **Knoten-Sicht** und es werden alle verfügbaren Knoten mit **Knoten ID**, **Name**, **System Typ**, **Server Adresse**, **Registrierungsstatus** und **Verfügbarkeitsstatus** angezeigt.
4) Markieren sie im Fenster **Netzwerk** die Registerkarte **Rufnummern** und es öffnet sich ein Fenster mit allen Angaben zu:
   - **Rufnummer**
   - **DuWa**
   - **Name**
   - **Port Typ**
   - **Knoten**

21.6.2.6 Wie Sie Richtungen und Richtungsparameter konfigurieren (ISDN-Amt für den Master)

Mit folgenden Schritten konfigurieren Sie die Richtungen für die Vernetzung des Masters.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.
5) Geben Sie unter **Richtungskennzahl** die `0` ein.
6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.
7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.
8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66758` ein.
9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.2.7 Wie Sie Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Master)

Für die Richtung 64 (Networking) ist es für Master und Slave zwingend erforderlich, den Eintrag für das 2. AKZ auszufüllen. Richtung 16 ist die Standard-Richtung für die Vernetzung bei OpenScape Business.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf die letzte **Richtung** (**Rtg. 16**).
4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Networking` für die Vernetzungsrichtung ein.
5) Geben Sie unter **Richtungskennzahl** nichts ein.
6) Geben Sie unter **Amtskennziffer (2. AKZ)** die 0 ein.
7) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.2.8 Wie Sie LCR für die Vernetzung konfigurieren (Master)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33 und 34 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zum Knoten 2 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z.B. myPortal for Desktop) verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie im Menübaum auf **Wahlplan**.
4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 37) nach den Standardwerten ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	Amt Internat	0C0049-Z	14
35	Knoten 2 Inter	0C0049230266719-Z	16
36	Knoten 2 NAT	0C0230266719-Z	16
37	Knoten 2 Teiln.	0C66719-Z	16

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
7) Klicken Sie im Menübaum auf **Wegetabelle**.
8) Klicken Sie auf die Wegetabelle 16.
   a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.
   c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
   d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   f) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
   g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.2.9 Wie Sie die Richtung und Richtungsparameter konfigurieren (Slave)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparamter für die Vernetzung des Slaves.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Richtung**.
4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Vernetzungsrichtung ein.
5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.
7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.
8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66719` ein.
9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.
10) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.
11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.2.10 Wie Sie LCR für die Vernetzung konfigurieren (Slave)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zum Knoten 2 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z.B. myPortal for Desktop) verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie im Menübaum auf **Wahlplan**.
4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 37) nach den Standardwerten ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	Amt Internat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266758-Z	16
37	Knoten 1 NAT	0C00230266758-Z	16
38	Knoten 1 Teiln.	0C66758-Z	16

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
6) Klicken Sie im Menübaum auf **Wahlregel** für **Knoten 2**.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

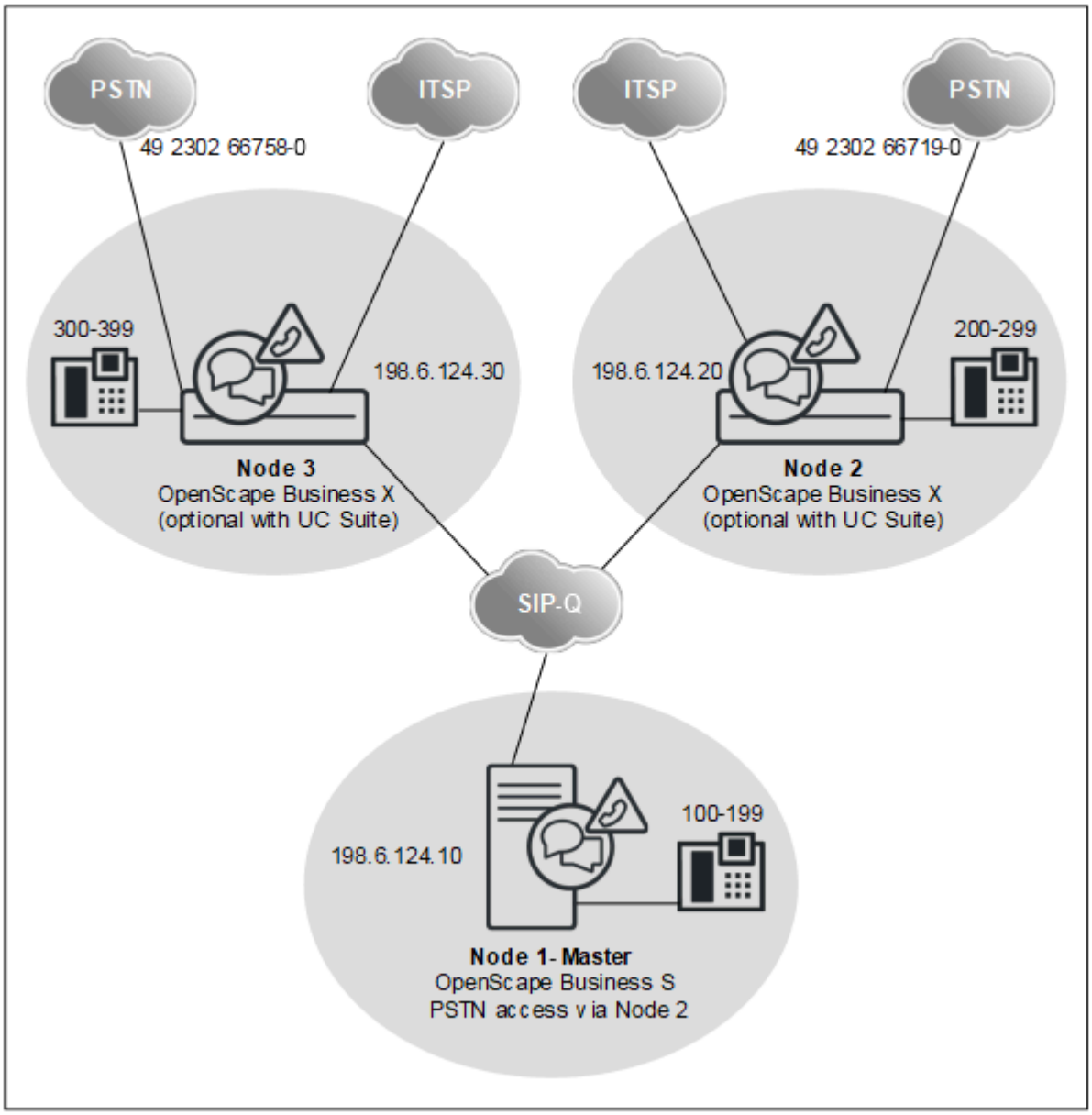
7) Klicken Sie auf die Wegetabelle 16.
   a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
   c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
   d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   f) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
   g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf **Wegetabelle**.

21.6.3 Vernetzung von OpenScape Business X mit OpenScape Business S (Single Gateway)

Bis zu 32 Kommunikationssysteme OpenScape Business X/S können miteinander vernetzt werden. Dabei sind mehrere OpenScape Business S in einem Netzverbund erlaubt. Single Gateway bedeutet, dass alle an OpenScape Business S registrierten IP-Teilnehmer nur EIN Gateway zum PSTN oder ITSP verwenden.

Netzwerkdaten



- Verdeckte (geschlossene) Nummerierung
- Netzweite Sprach- und UC-Funktionalität mit UC Suite Konfiguration über WBM (Wizards)
- Die UC-Funktionalität ist entweder über UC Booster Server oder über UC Booster Card realisiert
- Es sind mehrere OpenScape Business S im Netzverbund erlaubt.
- Bis zu 32 vernetzte Systeme und 1500 User ohne UC-Lösung
- Bis zu 8 vernetzte Systeme und 1500 User mit UC-Lösung

Netzweite Leistungsmerkmale

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 mit UC-Lösung und 32 ohne UC-Lösung	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	
Maximale Anzahl von Teilnehmern im Netz	1500	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
UC Booster Card	UC Smart: 51 - 150 Teilnehmer (0 - 50 Teilnehmer ohne UC Booster Card) UC Suite: 0 - 150 Teilnehmer	Wird nicht unterstützt
UC Booster Server	UC Smart: ab 150 Teilnehmer UC Suite: ab 150 Teilnehmer	Wird nicht unterstützt

Administration	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Wird nicht unterstützt
Manager E	Netzweite Administration für spezielle Aufgaben (nicht für OpenScape Business S)	Wird nicht unterstützt
UC-Suite-Administration (für UC Booster Server und UC Booster Card)	Netzweite Administration über Wizards	Wird nicht unterstützt
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	Wird nicht unterstützt

Lizenzierung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	Wird nicht unterstützt

Konfiguration

Diese Konfiguration (mit geschlossener Nummerierung und UC Suite) zeigt an einem Beispiel, welche Schritte für die Einrichtung einer Vernetzung durchzuführen sind.

Voraussetzungen:

- Es liegt ein Vernetzungsplan vor. Über den Vernetzungsplan ist sichergestellt, dass jede interne Rufnummer im Netzverbund bei verdeckter (geschlossener) Nummerierung nur einmal vergeben ist. Unterschiedliche Rufnummerlängen sind zulässig. Nur Duwa-Rufnummern dürfen mehrfach vorkommen (z.B. Amtsrufnummer 49 2302 66758 100 und 49 2302 66719 100 haben dieselbe Duwa-Nr. 100).

- Das IP-Netzwerk ist eingerichtet und alle Knoten können untereinander über Ping erreicht werden

Knotenübergreifende Rufumleitungen: Bei kommenden Rufen über IP-Trunks, die bereits umgeleitet sind, werden weitere Umleitungen zur Sprachbox nicht ausgeführt. Hintergrund ist, dass ansonsten keine eindeutige Zuordnung zur Sprachbox erfolgen kann

Falls knotenübergreifende Stellvertreterregelungen gewünscht werden, sind diese über Profile der OpenScape Business Teilnehmer oder Rufzuschaltungen einzurichten. Entsprechende knotenübergreifende Anrufe werden in diesem Fall nicht als umgeleitet signalisiert, sondern als Direktruf. Daher werden Rufumleitungen des Stellvertreters zur Sprachbox umgeleitet.

In einem Netzverbund, in dem die Activation Period verwendet wird, muss immer der CLA von OpenScape Business S als zentraler CLA verwendet werden!

Aufgrund unterschiedlichen Mengen-Obergrenzen werden zwei verschiedene Activation-Period-Dateien für OpenScape Business und OpenScape Business S benötigt. Die Activation-Period-Datei für OpenScape Business S enthält für Netzwerkszenarien zusätzlich zur S-Basis auch die Basis für OpenScape Business.

Wenn in diesem Szenario OpenScape Business eine Lizenzanfrage innerhalb der Activation Period an einen CLA der OpenScape Business S richtet, werden die Grenzwerte von OpenScape Business S verwendet.

Würde dagegen der CLA der OpenScape Business verwendet, so würde eine anfragende OpenScape Business S KEINE Activation Period erhalten, da in dieser Datei keine Basis für OpenScape Business S enthalten ist.

Tabelle 16: Einrichtung der Standortdaten für Knoten 1 OpenScape Business S

Knoten 1		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
Rtg. 1	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 1 eingetragen, und zwar die internen Rufnummern

und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 17: Übersicht der Einträge im LCR für Knoten 1

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 2 Internat	0C0049230266719-2Z	Vernetzung	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-2Z						
Knoten 2 Teiln.	0C66719-2Z						
Knoten 3 Internat	0C0049230266758-3Z	Vernetzung	Erzwungen	3	D49230266758E3A	Corp. Network	International
Knoten 3 NAT	0C0230266758-3Z						
Knoten 3 Teiln.	0C66758-3Z						
Amt	0CZ	Vernetzung	Erzwungen	2	E1A	Hauptnetzanbieter	Unbekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Tabelle 18: Einrichtung der Standortdaten für Knoten 2 OpenScape Business

Knoten 2		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 2 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 19: Übersicht der Einträge im LCR für Knoten 2

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266719-1Z	Vernetzung	Erzwungen	1	D49230266719E3A	Corp. Network	International
Knoten 1 NAT	0C0230266719-1Z						
Knoten 1 Teiln.	0C66719-1Z						
Knoten 3 Internat	0C0049230266758-3Z	Vernetzung	Erzwungen	3	D49230266758E3A	Corp. Network	International
Knoten 3 NAT	0C0230266758-3Z						
Knoten 3 Teiln.	0C66758-3Z						
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Tabelle 20: Einrichtung der Standortdaten für Knoten 3 OpenScape Business

Knoten 3		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66758
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 3 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 21: Übersicht der Einträge im LCR für Knoten 3

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266719-1Z	Vernetzung	Erzwungen	1	D49230266719E3A	Corp. Network	International
Knoten 1 NAT	0C0230266719-1Z						
Knoten 1 Teiln.	0C66719-1Z						
Knoten 2 Internat	0C0049230266719-2Z	Vernetzung	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-2Z						
Knoten 2 Teiln.	0C66719-2Z						
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Vorgehensweise bei der Einrichtung der Vernetzung:

1) Basisinstallation für Knoten 1 (Master) konfigurieren
2) Vernetzung konfigurieren für Knoten 1
3) Basisinstallation für Knoten 2 (Slave) konfigurieren
4) Vernetzung konfigurieren für Knoten 2
5) Basisinstallation für Knoten 3 (Slave) konfigurieren
6) Vernetzung konfigurieren für Knoten 3 (Slave)
7) Vernetzungsfunktion kontrollieren für Master
8) LCR für die Vernetzung konfigurieren (Knoten 1, Master)
9) LCR für die Vernetzung konfigurieren (Knoten 2)
10) Richtungen und Richtungsparameter konfigurieren (Knoten 3)
11) Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Knoten 3)
12) LCR für die Vernetzung konfigurieren (Knoten 3)

21.6.3.1 Wie Sie die Basisinstallation für Knoten 1 (Master) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID. Die Knoten-ID muss zwischen "**1**" und "**100**" sein (eine "**1**" für das Einrichtebeispiel wählen).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.
9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

Anmerkung: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

---

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
11) Importieren Sie die IP-Clients.
12) Konfigurieren Sie jetzt die Internet-Telefonie.
13) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
14) Konfigurieren Sie jetzt den E-Mail-Versand.
15) Klicken Sie auf **OK & Weiter**.
16) Klicken Sie auf **Beenden**.

21.6.3.2 Wie Sie die Vernetzung für Knoten 1 (Master) konfigurieren

Im nächsten Schritt wird der Wizard für die Vernetzung von Knoten 1 (Master) konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) Definieren Sie den Knotentyp (**Master**).

6) Geben Sie unter **Node-ID** die entsprechenden Knotennummern der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die des Slaves mit der Node-ID 2).
7) Geben Sie unter **IP-Adresse** die IP-Adressen der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die der Slaves mit der Node-ID 2 und 3).
8) Aktivieren Sie das Kontrollkästchen **Gateway**.
9) Geben Sie unter **Name** die Art der Anlage ein.
10) Geben Sie unter **Typ** den Typ der Unteranlage ein.
11) Aktivieren Sie ggf. das Kontrollkästchen **Verschlüsselung erforderlich**.

Tipp: Die Verschlüsselung basiert auf SPE und gilt nicht für die Applikationen!

Anmerkung: Durch die Aktivierung des Kontrollkästchens ist noch keine Verschlüsselung konfiguriert. Siehe Signaling and Payload Encryption (SPE) .

12) Klicken Sie auf **Beenden**.

21.6.3.3 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für eine OpenScape Business eine im Netzverbund eindeutige Knoten-ID (eine "**2**" und eine "**3**" für das Einrichtebeispiel).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

> **Anmerkung:** Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.
12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
13) Konfigurieren Sie jetzt den E-Mail-Versand.
14) Klicken Sie auf **OK & Weiter**.
15) Klicken Sie auf **Beenden**.

21.6.3.4 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren

Im nächsten Schritt wird über den Wizard die Vernetzung von Knoten 2 konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.
6) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (im Einrichtebeispiel die IP-Adresse von Knoten 1).

> **Tipp:** Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängig gemacht werden!

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.
8) Klicken Sie auf **Beenden**.

21.6.3.5 Wie Sie die Basisinstallation für Knoten 3 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen

netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein. (identisch mit dem zugeordneten Gateway-System).
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für eine OpenScape Business eine im Netzverbund eindeutige Knoten-ID (eine "**3**" für das Einrichtebeispiel).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.
9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

   Anmerkung: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.
12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
13) Konfigurieren Sie jetzt den E-Mail-Versand.
14) Klicken Sie auf **OK & Weiter**.
15) Klicken Sie auf **Beenden**.

21.6.3.6 Wie Sie die Vernetzungsfunktion für den Master kontrollieren

Sie können den Status der Vernetzung generell und die einzelnen Rufnummern kontrollieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.
2) In der Statuszeile sehen Sie den **Synchronisationsstatus** für das Netzwerk. Grün bedeutet, dass die Vernetzung keine Probleme hat, Rot bedeutet Probleme im Netzwerk.
3) Markieren Sie im Fenster **Netzwerk** die Registerkarte **Knoten-Sicht** und es werden alle verfügbaren Knoten mit **Knoten ID**, **Name**, **System Typ**, **Server Adresse**, **Registrierungsstatus** und **Verfügbarkeitsstatus** angezeigt.
4) Markieren sie im Fenster **Netzwerk** die Registerkarte **Rufnummern** und es öffnet sich ein Fenster mit allen Angaben zu:
   - **Rufnummer**
   - **DuWa**
   - **Name**
   - **Port Typ**
   - **Knoten**

21.6.3.7 Vernetzung konfigurieren für Knoten 3 (Slave)

Im nächsten Schritt wird über den Wizard für die Vernetzung von Knoten 3 konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.
6) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (im Einrichtebeispiel die IP-Adresse von Knoten 1).

   Tipp: Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängig gemacht werden!
7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.
8) Klicken Sie auf **Beenden**.

21.6.3.8 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 3, Slave)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 2 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten,

die sich im gleichen Ortsnetz befinden. Die Einträge 36, 37 und 39 für das Interworking mit Knoten 1 (Rufnummer 100 > 199) und die Einträge 39, 40 und 41 für das Interworking mit Knoten 2 (Rufnummer 200 > 299) sind zu ergänzen. Diese Angaben werden für die Wahl aus Applikationen (z.B. myPortal for Desktop) verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 40) nach den Standardwerten ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-371	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	Amt Internat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266719-1Z	16
37	Knoten 1 NAT	0C0230266719-1Z	16
38	Knoten 1 Teiln.	0C66719-1Z	16
39	Knoten 2 Inter	0C0049230266719-2Z	17
40	Knoten 2 NAT	0C0230266719-2Z	17
41	Knoten 2 Teiln.	0C66719-2Z	17

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1 und 2.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 1 + 2** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 1 direkt zuzuordnen.

8) Klicken Sie auf die Wegetabelle 16.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1 + 2** aus.
c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
f) Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 2 direkt zuzuordnen.

10) Klicken Sie auf die Wegetabelle 17.
   a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1 + 2** aus.
   c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
   d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   f) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
   g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.3.9 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 2)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 3 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Die Einträge 36, 37 und 38 für das Interworking mit Knoten 1 (Rufnummer 100 > 199) und die Einträge 39, 40 und 41 für das Interworking mit Knoten 3 (Rufnummer 300 > 399) sind zu ergänzen. Diese Angaben werden für die Wahl aus Applikationen (z.B. myPortal for Desktop) verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie im Menübaum auf **Wahlplan**.
4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 40) nach den Standardwerten ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-271	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	Amt Internat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266719-1Z	16
37	Knoten 1 NAT	0C0230266719-1Z	16
38	Knoten 1 Teiln.	0C66719-1Z	16
39	Knoten 3 Inter	0C0049230266758-3Z	17
40	Knoten 3 NAT	0C0230266758-3Z	17
41	Knoten 3 Teiln.	0C66758-3Z	17

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
6) Klicken Sie im Menübaum auf **Wegetabelle**.

7) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie auf die Wegetabelle 16, um diese für das Networking zum Knoten 1 zu konfigurieren.
   a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
   c) Wählen Sie unter **Min. Ber.** den Eintrag **1** aus.
   d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   f) Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
   g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf **Wegetabelle**.

11) Klicken Sie auf die Wegetabelle 17, um diese für das Networking zum Knoten 3 zu konfigurieren.
   a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3** aus.
   c) Wählen Sie unter **Min. Ber.** den Eintrag **1** aus.
   d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   f) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.
   g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.3.10 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 1, Master)

Im Knoten 1 sind die Einstellungen für die Amtsrichtung bzgl. Standort-Nummer, Richtungskennzahl und Richtungsparameter zu konfigurieren. Hier muss die Anlagenrufnummer zur Definition des Gateway-Standortes eingetragen sein. Diese Angaben werden für die Wahl aus Applikationen wie z.B. MyPortal verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Richtung**.
4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.
5) Geben Sie unter **Richtungskennzahl** die `0` ein.
6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.
7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.
8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66719` ein.
9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.
10) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.
11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.3.11 Wie Sie Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Knoten 1)

Für die Richtung 64 (Networking) ist es für Master und Slave zwingend erforderlich, den Eintrag für das 2. AKZ auszufüllen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf die letzte **Richtung** (**Rtg. 16**).
4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Networking` für die Vernetzungsrichtung ein.
5) Geben Sie unter **Richtungskennzahl** nichts ein.
6) Geben Sie unter **Amtskennziffer (2. AKZ)** die 0 ein.
7) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.3.12 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 1)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 2 und 3 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z.B. myPortal for Desktop) verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 40) nach den Standardwerten ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
16	Standard	0CZ	1
17	Standard	0C1Z	1
18	Standard	0CNZ	1
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	Amt Internat	0C0049-Z	14
36	Knoten 2 Inter	0C0049230266719-2Z	16
37	Knoten 2 NAT	0C0230266719-2Z	16
38	Knoten 2 Teiln.	0C66719-2Z	16
39	Knoten 3 Inter	0C0049230266758-3Z	17
40	Knoten 3 NAT	0C0230266758-3Z	17
41	Knoten 3 Teiln.	0C66758-3Z	17

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**.

8) Klicken Sie auf die Wegetabelle 16, um diese für das Networking zum Knoten 2 zu konfigurieren.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.
c) Wählen Sie unter **Min. Ber.** den Eintrag **1** aus.
d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
f) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E1A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf **Wegetabelle**.

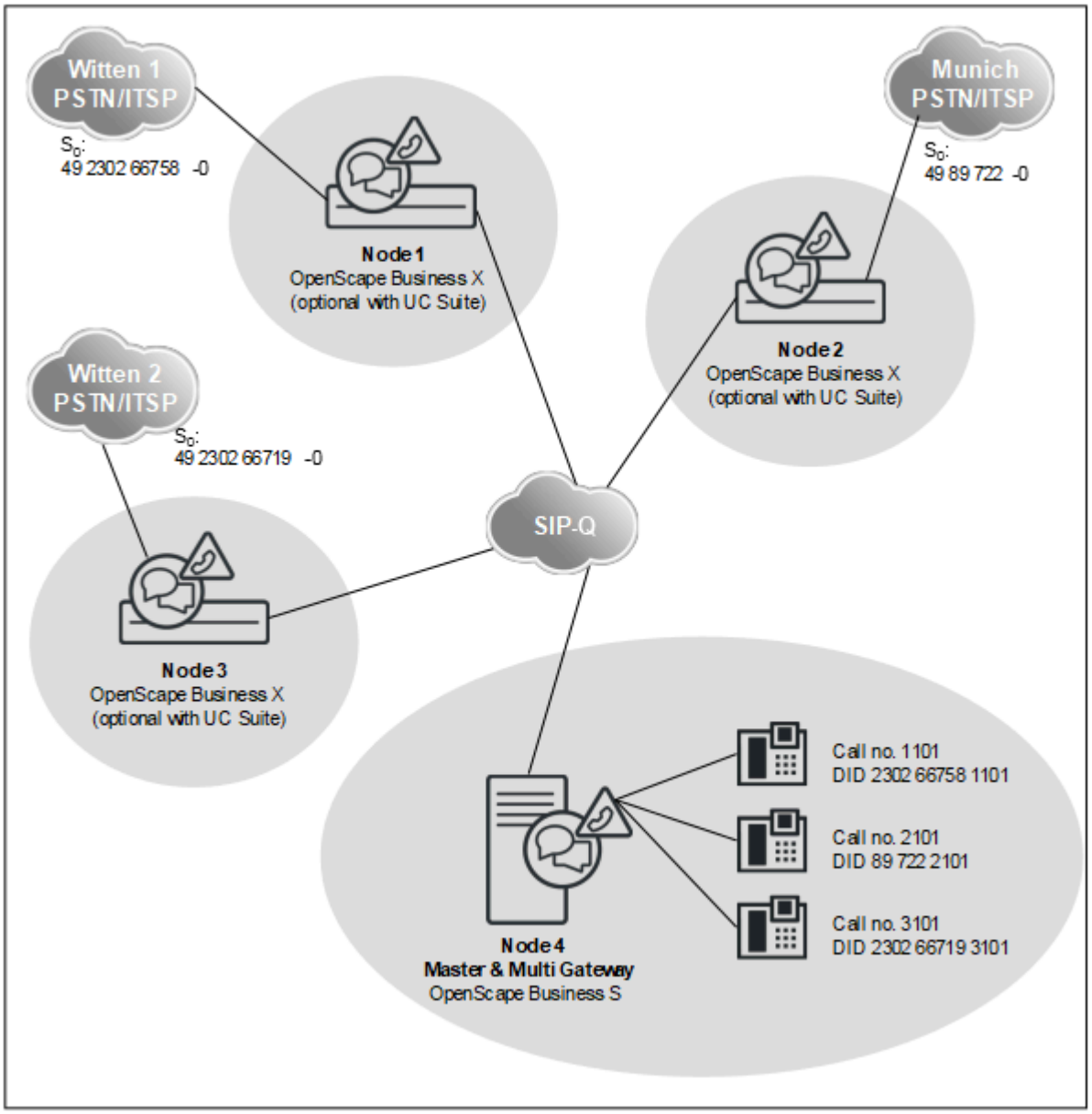
11) Klicken Sie auf die Wegetabelle 17, um diese für das Networking zum Knoten 3 zu konfigurieren.
   a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3** aus.
   c) Wählen Sie unter **Min. Ber.** den Eintrag **1** aus.
   d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   f) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.
   g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12) Klicken Sie im Menübaum auf **Wegetabelle**.

21.6.4 Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway)

Bis zu 32 Kommunikationssysteme OpenScape Business X und OpenScape Business S können miteinander vernetzt werden. Multi Gateway bedeutet, dass jeder an OpenScape Business S registrierte IP-Teilnehmer genau einem bestimmten Gateway zugeordnet sind.

Netzwerkdaten



- Verdeckte (geschlossene) Nummerierung
- Netzweite Sprach- und UC-Funktionalität mit UC Suite Konfiguration über WBM (Wizards)
- Die UC-Funktionalität ist entweder über UC Booster Server oder über UC Booster Card realisiert
- Es ist nur eine einzige OpenScape Business S im Netzverbund erlaubt.
- Alle Systeme müssen den gleichen Länder-Code benutzen
- Alle Systeme müssen sich in der gleichen Zeitzone befinden
- Es darf nur einen einzigen Amtszugangs-Code (z.B. 0) im Netz geben.
- Bis zu 32 vernetzte Systeme und 1500 User ohne UC-Lösung
- Bis zu 8 vernetzte Systeme und 1500 User mit UC-Lösung

Netzweite Leistungsmerkmale

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 mit UC-Lösung und 32 ohne UC-Lösung	
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	
Maximale Anzahl von Teilnehmern im Netz	1500	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
UC Booster Card	UC Smart: 51 - 150 Teilnehmer (0 - 50 Teilnehmer ohne UC Booster Card) UC Suite: 0 - 150 Teilnehmer	Wird nicht unterstützt
UC Booster Server	UC Smart: ab 150 Teilnehmer UC Suite: ab 150 Teilnehmer	Wird nicht unterstützt

Administration	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Wird nicht unterstützt
Manager E	Netzweite Administration für spezielle Aufgaben (nicht für OpenScape Business S)	Wird nicht unterstützt
UC-Suite-Administration (für UC Booster Server und UC Booster Card	Netzweite Administration über Wizards	Wird nicht unterstützt
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	Wird nicht unterstützt

Lizenzierung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	Wird nicht unterstützt

Konfiguration

Diese Konfiguration (mit geschlossener Nummerierung und UC Suite) zeigt an einem Beispiel, welche Schritte für die Einrichtung einer Multi-Gateway Vernetzung durchzuführen sind.

Voraussetzungen:

- Es liegt ein Vernetzungsplan vor. Über den Vernetzungsplan ist sichergestellt, dass jede interne Rufnummer im Netzverbund bei verdeckter (geschlossener) Nummerierung nur einmal vergeben ist. Unterschiedliche

Rufnummerlängen sind zulässig. Nur Duwa-Rufnummern dürfen mehrfach vorkommen.

- Das IP-Netzwerk ist eingerichtet und alle Knoten können untereinander über Ping erreicht werden
- Alle Knoten sind auf die gleiche Softwareversion hochgerüstet

Knotenübergreifende Rufumleitungen: Bei kommenden Rufen über IP-Trunks, die bereits umgeleitet sind, werden weitere Umleitungen zur Sprachbox nicht ausgeführt. Hintergrund ist, dass ansonsten keine eindeutige Zuordnung zur Sprachbox erfolgen kann

Falls knotenübergreifende Stellvertreterregelungen gewünscht werden, sind diese über Profile der OpenScape Business Teilnehmer oder Rufzuschaltungen einzurichten. Entsprechende knotenübergreifende Anrufe werden in diesem Fall nicht als umgeleitet signalisiert, sondern als Direktruf. Daher werden Rufumleitungen des Stellvertreters zur Sprachbox umgeleitet.

Tabelle 22: Einrichtung der Standortdaten für Knoten 1

Knoten 1		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66758
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 1 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 23: Übersicht der Einträge im LCR für Knoten 1

Rufnummernplan		**Wegetabelle**			**Wahlregel**		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 2 Internat	0C004989722-Z	Vernetzung	Erzwungen	2	D4989722E3A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 2 Teiln.	0C722-Z						
Knoten 3 Internat	0C0049230266719-Z	Vernetzung	Erzwungen	3	D49230266719E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Knoten 3 Teiln.	0C66719-Z						
Knoten 4 Internat	0C0049230266758-Z	Vernetzung	NEIN		D230266758E3A	Corp. Network	National
Knoten 4 NAT	0C0230266758-Z						
Knoten 4 Teiln.	0C66758-Z						
Diverse	-Z	Vernetzung	Nein		BA	Corp. Network	Unbekannt
Amt International	0C0049-Z	ISDN	Nein		D0E3A	Hauptnetzanbieter	Unbekannt
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt

Tabelle 24: Einrichtung der Standortdaten für Knoten 2

Knoten 2		
G.-Standort Land		49
G.-Standort Ortsnetz		89
G.-Standort Anlage		722
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 2 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 25: Übersicht der Einträge im LCR für Knoten 2

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266758-Z	Vernetzung	Erzwungen	1	D492302667E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Knoten 3 Internat	0C0049230266719-Z	Vernetzung	Erzwungen	3	D49230266719E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Knoten 3 Teiln.	0C66719-Z						
Knoten 4 Internat	0C004989722-Z	Vernetzung	NO		D89722E3A	Corp. Network	National
Knoten 4 NAT	0C089722-Z						
Knoten 4 Teiln.	0C722-Z						
Diverse	-Z	Vernetzung	Nein		BA	Corp. Network	Unbekannt
Amt International	0C0049-Z	ISDN	Nein		D0E3A	Hauptnetzanbieter	Unbekannt
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt

Tabelle 26: Einrichtung der Standortdaten für Knoten 3

Knoten 3		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa

Knoten 3		
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 3 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 27: Übersicht der Einträge im LCR für Knoten 3

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266758-Z	Vernetzung	Erzwungen	1	D49230266758E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Knoten 2 Internat	0C004989722-Z	Vernetzung	Erzwungen	2	D4989722E3A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						
Knoten 2 Teiln.	0C722-Z						
Knoten 4 Internat	0C004989230266719-Z	Vernetzung	Nein		D230266719E3A	Corp. Network	National
Knoten 4 NAT	0C0230266719-Z						
Knoten 4 Teiln.	0C66719-Z						
Diverse	-Z	Vernetzung	Nein		BA	Corp. Network	Unbekannt
Amt International	0C0049-Z	ISDN	Nein		D0E3A	Hauptnetzanbieter	Unbekannt
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt

Einrichtung der Standortdaten für Knoten 4: Standortdaten an Pseudo-Amtsrichtung (Rtg. 1) inkl. Amtskennzahl = 0 und Typ = Amt binden, da der Knoten 4 keine direkte Anschaltung eines Amts hat.

Tabelle 28: Knoten 4, Pseudo-Amtsrichtung

Knoten 4	
G.-Standort Land	49
G.-Standort Ortsnetz	
G.-Standort Anlage	

Knoten 4		
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 1 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Tabelle 29: Knoten 4, Richtung Networking

Knoten 4		
G.-Standort Land		
G.-Standort Ortsnetz		
G.-Standort Anlage		
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	National	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

Tabelle 30: Übersicht der Einträge im LCR für Knoten 4

Rufnummernplan		**Wegetabelle**			**Wahlregel**		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266758-Z	Vernetzung	Erzwungen	1	D49230266758E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						

Rufnummernplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 2 Internat	0C004989722-Z	Vernetzung	Erzwungen	2	D4989722E3A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						
Knoten 3 Internat	0C004989230266719-Z	Vernetzung	Erzwungen	3	D49230266719E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Diverse	-Z	Vernetzung	NEIN		A	Corp. Network	Unbekannt
Amt	0CZ	Vernetzung	MULTI-GATEWAY	1	E1A	Hauptnetzanbieter	Unbekannt

Vorgehensweise bei der Einrichtung der Vernetzung:

1) Basisinstallation für Knoten 4 (Master) konfigurieren
2) Vernetzung konfigurieren für Knoten 4 (Master)
3) Basisinstallation für Knoten 1 (Slave) konfigurieren
4) Vernetzung konfigurieren für Knoten 1 (Slave)
5) Basisinstallation für Knoten 2 (Slave) konfigurieren
6) Vernetzung für Knoten 2 konfigurieren (Slave)
7) Basisinstallation für Knoten 3 (Slave) konfigurieren
8) Vernetzung konfigurieren für Knoten 3 (Slave)
9) Vernetzungsfunktion kontrollieren für Master
10) Multi-Gateway konfigurieren für Knoten 4 (Master)
11) Richtungen und Richtungsparameter konfigurieren (Knoten 1, Slave)
12) LCR für die Vernetzung konfigurieren (Knoten 1, Slave)
13) Richtungen und Richtungsparameter konfigurieren (Knoten 2, Slave)
14) LCR für die Vernetzung konfigurieren (Knoten 2, Slave)
15) Richtungen und Richtungsparameter konfigurieren (Knoten 3, Slave)
16) LCR für die Vernetzung konfigurieren (Knoten 3, Slave)
17) Richtungen und Richtungsparameter konfigurieren (Knoten 4, Master)
18) LCR für die Vernetzung konfigurieren (Knoten 4, Master)

21.6.4.1 Wie Sie die Basisinstallation für Knoten 4 (OpenScape Business S, Master) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
4) Machen Sie keine Eintragungen für die Felder **Ortskennzahl** und **Anlagenrufnummer**!.
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID. Die Knoten-Id muss zwischen "**1**" und "**100**" sein (eine "**4**" wurde für das Einrichtebeispiel vergeben).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.
9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

   Anmerkung: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

   ---

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
11) Konfigurieren Sie jetzt die IP-Clients.
12) Konfigurieren Sie die IP-Clients.
13) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
14) Konfigurieren Sie jetzt den E-Mail-Versand.
15) Klicken Sie auf **Beenden**.

21.6.4.2 Wie Sie die Vernetzung für Knoten 4 (Master) konfigurieren

Im nächsten Schritt wird über den Wizard für die Vernetzung von Knoten 3 konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) Aktivieren Sie das Kontrollkästchen **Dieses System ist der Master-Knoten**.
6) Geben Sie unter **Node-ID** die entsprechenden Knotennummern der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die der Slaves mit der Node-ID 1, 2 und 3).
7) Geben Sie unter **IP-Adresse** die IP-Adressen der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die der Slaves mit der Node-ID 1, 2 und 3).
8) Aktivieren Sie das Kontrollkästchen **Gateway**.
9) Geben Sie unter **Name** die Art der Anlage (z.B. Slave 1) ein.
10) Geben Sie unter **Typ** den Typ der Unteranlage ein.
11) Aktivieren Sie ggf. das Kontrollkästchen **Verschlüsselung erforderlich**.

Tipp: Die Verschlüsselung basiert auf SPE und gilt nicht für die Applikationen!

Anmerkung: Durch die Aktivierung des Kontrollkästchens ist noch keine Verschlüsselung konfiguriert. Siehe Signaling and Payload Encryption (SPE) .

12) Klicken Sie auf **Beenden**.

21.6.4.3 Wie Sie die Basisinstallation für Knoten 1 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID (eine "**1**" für das Einrichtebeispiel).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
8) Da in einem Netzwerk alle Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

Anmerkung: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

---

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.
12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
13) Konfigurieren Sie jetzt den E-Mail-Versand.
14) Klicken Sie auf **Beenden**.

21.6.4.4 Wie Sie die Vernetzung für Knoten 1 (Slave) konfigurieren

Im nächsten Schritt wird der Wizard für die Vernetzung konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (Eine OpenScape Business wird als Slave-Knoten eingerichtet und die entsprechende IP-Adresse des Master-Knotens, der OpenScape Business S, eingetragen. Master und Multi-Gateway werden immer dem gleichen System, im Einrichtebeispiel der OpenScape Business S zugeordnet).

Tipp: Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängig gemacht werden!

---

6) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.
7) Klicken Sie auf **Beenden**.

21.6.4.5 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen

netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID (eine "**2**" für das Einrichtebeispiel).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.
9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

Anmerkung: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

---

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.
12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
13) Konfigurieren Sie jetzt den E-Mail-Versand.
14) Klicken Sie auf **Beenden**.

21.6.4.6 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren

Im nächsten Schritt wird über den Wizard die Vernetzung von Knoten 2 konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.
6) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (Eine OpenScape Business wird als Slave-Knoten eingerichtet und die entsprechende IP-Adresse des Master-Knotens, der OpenScape Business S, eingetragen. Master und Multi-Gateway werden immer dem gleichen System, im Einrichtebeispiel der OpenScape Business S zugeordnet).

   Tipp: Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängig gemacht werden!

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.
8) Klicken Sie auf **Beenden**.

21.6.4.7 Wie Sie die Basisinstallation für Knoten 3 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z.B. 49 für Deutschland.
4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für eine OpenScape Business eine im Netzverbund eindeutige Knoten-ID (eine "**3**" für das Einrichtebeispiel).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.
8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

> **Anmerkung:** Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.
11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.
12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.
13) Konfigurieren Sie jetzt den E-Mail-Versand.
14) Klicken Sie auf **Beenden**.

21.6.4.8 Wie Sie die Vernetzung für Knoten 3 (Slave) konfigurieren

Im nächsten Schritt wird über den Wizard für die Vernetzung von Knoten 3 konfiguriert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.
6) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (Eine OpenScape Business wird als Slave-Knoten eingerichtet und die entsprechende IP-Adresse des Master-Knotens, der OpenScape Business S, eingetragen. Master und Multi-Location werden immer dem gleichen System, im Einrichtebeispiel der OpenScape Business S zugeordnet).

> **Tipp:** Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängig gemacht werden!

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.
8) Klicken Sie auf **Beenden**.

21.6.4.9 Wie Sie die Vernetzungsfunktion für den Master kontrollieren

Sie können den Status der Vernetzung generell und die einzelnen Rufnummern kontrollieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.
2) In der Statuszeile sehen Sie den **Synchronisationsstatus** für das Netzwerk. Grün bedeutet, dass die Vernetzung keine Probleme hat, Rot bedeutet Probleme im Netzwerk.
3) Markieren Sie im Fenster **Netzwerk** die Registerkarte **Knoten-Sicht** und es werden alle verfügbaren Knoten mit **Knoten ID**, **Name**, **System Typ**, **Server Adresse**, **Registrierungsstatus** und **Verfügbarkeitsstatus** angezeigt.
4) Markieren sie im Fenster **Netzwerk** die Registerkarte **Rufnummern** und es öffnet sich ein Fenster mit allen Angaben zu:
   - **Rufnummer**
   - **DuWa**
   - **Name**
   - **Port Typ**
   - **Knoten**

21.6.4.10 Wie Sie ein Multi-Gateway für Knoten 4 (Master) konfigurieren

Die Einrichtung des Netzwerverbunds als Multi-Gateway-Netzwerk wird am Master-Knoten vorgenommen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Vernetzung-Konfiguration**.
3) Wählen Sie die unter **Netzwerk-Konfiguration** die Einstellung **Multi-Standort-Einrichtung**. Im Fenster **Multi-Standort-Einrichtung** wird die Zuordnung der Teilnehmer zum Standort festgelegt. Die Zuordnung der Rufnummer zur Knoten-ID (Node-ID) wird z.B. für die gehende Amtsbelegung im zugeordneten Standortknoten verwendet.
4) Geben Sie für das Einrichtebeispiel folgende Zuordnungen unter **Multi-Standort-Einrichtung** an (alle Telefone sind an OpenScape Business S registriert):

Rufnummer	Name	Knoten-ID
1101	1101KN1	1-Slave Witten1
1102	1102KN1	1-Slave Witten1
1103	1103KN1	1-Slave Witten1

Rufnummer	Name	Knoten-ID
2101	2101KN2	2-Slave Muenchen
2102	2102KN2	2-Slave Muenchen
2103	2103KN2	2-Slave Muenchen
3101	3101KN3	3-Slave Witten 2
3102	3102KN3	3-Slave Witten 2
3103	3103KN3	3-Slave Witten 2

5) Klicken Sie auf **Beenden**.

21.6.4.11 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 1, Slave)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparamter für die Vernetzung des Slaves.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.

7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.

8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66758` ein.

9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.

10) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.

11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.4.12 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 1, Slave)

Im LCR-Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 2 und 3 sowie zum Multi-Gateway Knoten 4 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 36 bis 43) nach den Standardwerten ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	Amt Internat	0C0049-Z	14
36	Knoten 2 Inter	0C004989722-Z	16
37	Knoten 2 NAT	0C089722-Z	16
38	Knoten 3 Inter	0C0049230266719-Z	17
39	Knoten 3 NAT	0C0230266719-Z	17
40	Knoten 3 Teiln.	0C66719-Z	17
41	Knoten 4 Inter	0C0049230266758-Z	18
42	Knoten 4 NAT	0C0230266758-Z	18
43	Knoten 4 Teiln.	0C66758-Z	18
44			-

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D4989722E3A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 2 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 16.
b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.
d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
g) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 3 direkt zuzuordnen.
   a) Klicken Sie auf die Wegetabelle 17.
   b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3** aus.
   d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
   e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   g) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.
   h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 4.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 4** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D230266758E3A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **National** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 18 für das Networking zu konfigurieren und dem Knoten 4 direkt zuzuordnen.
   a) Klicken Sie auf die Wegetabelle 18.
   b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 4** aus.
   d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
   e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   f) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.4.13 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 2, Slave)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparamter für die Vernetzung des Slaves.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die 49 ein.
7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die 89 ein.
8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die 722 ein.
9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.
10) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.
11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.4.14 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 2, Slave)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 2 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Die Einträge 36, 37 und 38 für das Interworking mit Knoten 1 (Rufnummer 100 > 199) und die Einträge 39, 40 und 41 für das Interworking mit Knoten 3 (Rufnummer 300 > 399) sind zu ergänzen. Diese Angaben werden für die Wahl aus Applikationen (z.B. myPortal for Desktop) verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie im Menübaum auf **Wahlplan**.
4) Geben Sie folgende Werte auf freien Plätzen (hier 36 bis 43) nach den Standardwerten ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	Amt Internat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266758-Z	16
37	Knoten 1 NAT	0C0230266758-Z	16
38	Knoten 3 Inter	0C0049230266719-Z	17
39	Knoten 3 NAT	0C0230266719-Z	17
40	Knoten 3 Teiln.	0C66719-Z	17
41	Knoten 4 Inter	0C004989722-Z	18
42	Knoten 4 NAT	0C089722-Z	18

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
43	Knoten 4 Teiln.	0C722-Z	18
44			-

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 1 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 16.
b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
g) Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 3 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 17.
b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3 direkt** aus.
d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
g) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.
h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 4.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 4** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D89722E3A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ortsnetzkennzahl** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 18 für das Networking zu konfigurieren und dem Knoten 4 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 18.
b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 4** aus.
d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
f) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.4.15 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 3, Slave)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparamter für die Vernetzung des Slaves.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Richtung**.
4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.
5) Geben Sie unter **Richtungskennzahl** die `0` ein.
6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.
7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.
8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66719` ein.
9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.
10) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.
11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.4.16 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 3, Slave)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 2 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z.B. myPortal for Desktop) verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie im Menübaum auf **Wahlplan**.
4) Geben Sie folgende Werte ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	Amt Internat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266758-Z	16
37	Knoten 1 NAT	0C00230266758-Z	16
38	Knoten 1 Teiln.	0C66758-Z	16
39	Knoten 2 Inter	0C004989722-Z	17
40	Knoten 2 NAT	0C0089722-Z	17
41	Knoten 4 Inter	0C0049230266719-Z	18
42	Knoten 4 NAT	0C0230266719-Z	18
43	Knoten 4 Teiln.	0C66719-Z	18
44			-

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 1 direkt zuzuordnen.
   a) Klicken Sie auf die Wegetabelle 16.
   b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
   d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
   e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   g) Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
   h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D4989722E3A** ein.
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 2 direkt zuzuordnen.
   a) Klicken Sie auf die Wegetabelle 17.
   b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.
   d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
   e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
   g) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
   h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 4.
   a) Geben Sie unter **Regelname** den Eintrag **Knoten 4** ein.
   b) Geben Sie unter **Wahlregelformat** den Eintrag **D230266719E3A** ein
   c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
   d) Wählen Sie unter **Type** den Eintrag **Ortsnetzkennzahl** aus
   e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 18 für das Networking zu konfigurieren und dem Knoten 4 direkt zuzuordnen.
   a) Klicken Sie auf die Wegetabelle 18.
   b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
   c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 4** aus.
   d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
   e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
   f) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.4.17 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 4, Master)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparamter für die Vernetzung des Slaves.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.
6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.
7) Machen Sie keine Eintragungen in den Feldern **Ortsnetzkennzahl** und Anlagenrufnummer.
8) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.
9) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.4.18 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 4, Master)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 2 zu ergänzen. "International" und "National" werden immer benötigt. "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z.B. myPortal for Desktop) verwendet.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie im Menübaum auf **Wahlplan**.
4) Geben Sie folgende Werte auf freien Plätzen (hier 36 bis 43) nach den Standardwerten ein:

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
1	Notruf	0C112	19
2	Notruf	0C110	19
3	Teleworking	0C0137Z	19
4	Televoting	0C0138Z	19
5	Premium Dienste	0C0900Z	19
6	Auskunftsdienst	0C118Z	19
7	Sonderrufnummer	0C116116	19
16	Standard	0CZ	19
17	Standard	0C1Z	19
18	Standard	0CNZ	19
31	Appl-Suite	-471	12
32	Standard	88CZ	1
33	IP-Network	-Z	13

Rufnummer	Name	Gewählte Ziffern	Wegetabelle
34	Amt Internat	0C0049-Z	15
36	Knoten 1 Inter	0C0049230266758-Z	16
37	Knoten 1 NAT	0C0230266758-Z	16
38	Knoten 1 Teiln.	0C66758-Z	16
39	Knoten 2 Inter	0C004989722-Z	17
40	Knoten 2 NAT	0C089722-Z	17
41	Knoten 3 Inter	0C0049230266719-Z	18
42	Knoten 3 NAT	0C0230266719-Z	18
43	Knoten 3 Teiln.	0C66719-Z	18
44			-

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 1 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 16.
b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
g) Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D4989722E3A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 2 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 17.
b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.
d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
g) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **D230266719E3A** ein
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 18 für das Networking zu konfigurieren und dem Knoten 3 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 18.
b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3** aus.
d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
g) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.
h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Amtsgespräche. Es handelt sich um die vordefinierte Wahlregel "Gateway Call".

a) Geben Sie unter **Regelname** den Eintrag **Gateway Call** ein.
b) Geben Sie unter **Wahlregelformat** den Eintrag **E1A** ein.
c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
d) Wählen Sie unter **Type** den Eintrag **Unbekannt** aus.
e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 19 für den Amtsausstieg der Slaves zu konfigurieren. Anhand der Eintragung Multi-Gateway wird die Zugehörigkeit des Teilnehmers zum Knoten bestimmt und an diesem Knoten der Amtsausstieg vorgenommen.

14) Klicken Sie auf die Wegetabelle 19.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
b) Wählen Sie unter **Wahlregel** den Eintrag **Gateway Call** aus.
c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Multi-Gateway** aus.
f) Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.6.5 Vernetzung von OpenScape Business in Hosting-Umgebungen

In einer Umgebung mit mehreren Standorten (Hosting-Umgebung) kann jedem Standort eine Richtung und jeder Richtung eine ITSP-Registrierung zugeordnet werden. Es können max. 8 ITSP-Registrierungen verwaltet werden. Dabei ist eine Registrierung pro ITSP möglich oder auch mehrere Registrierungen an einem ITSP. Jeder ITSP-Registrierung kann eine Ortsvorwahl und anschließend mehrere Teilnehmer zugeordnet werden. Der Anschluss der Teilnehmer an den verschiedenen Standorten an das Kommunikationssystem erfolgt über VPN oder MPLS. Befinden sich die Standorte in unterschiedlichen Ländern, ist für jedes Land eine eigene OpenScape Business S zu verwenden (Szenario 1a). Befinden sich alle Standorte innerhalb eines Landes, kann eine OpenScape Business S verwendet werden (Szenario 1b).

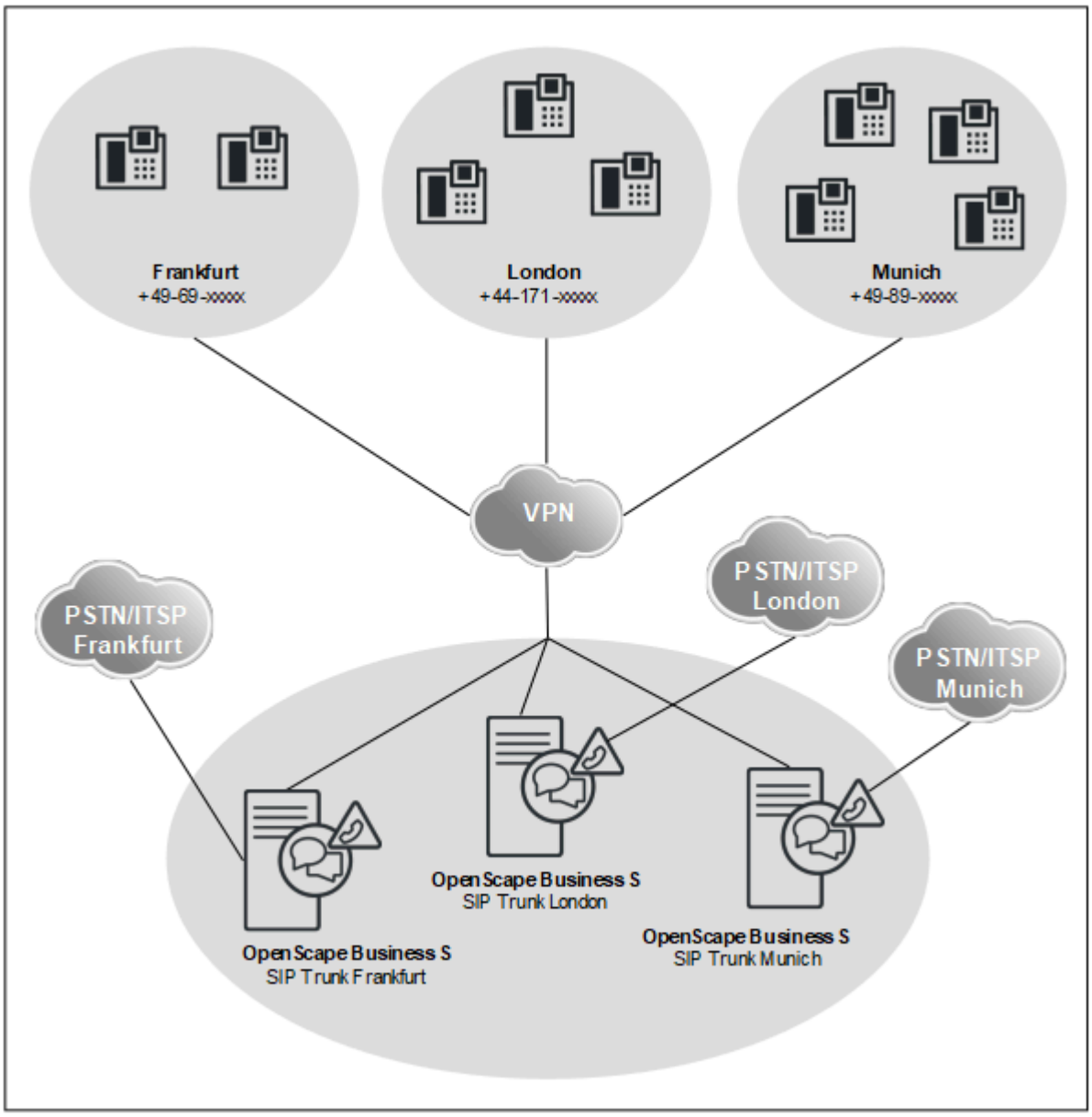
Beide Szenarien sind auch mit den OpenScape Business X Hardwaremodellen realisierbar (z.B. bei kleinen Ausbauten). An einem Standort lassen sich zusätzlich die TDM-Komponenten mit nutzen.

Die nachfolgend genannten Hosting-Szenarien sind allgemein beschrieben. Folgende Ausprägungen sind realisierbar:

- Einsatz von OpenScape Business S und OpenScape Business X im Datacenter des Kunden bzw. beim Hoster
- OpenScape Business S auf dedizierter Server-Hardware oder virtualisiert
- Voraussetzung ist eine VPN-oder MPLS-Infrastruktur, insbesondere bei mehreren Kunden-Standorten (keine standortspezifischen NAT-Router als Internetzugang)
- Bis zu 8 ITSP je System und Land, MSN- oder Durchwahl-Provider
- Bis zu 8 Standort-Vorwahlen (Area Codes) je System und Land, zugeordnet zu bis zu 8 Kunden-Standorten (Multi-Site)
- Multi-Site-Szenarien kombinierbar mit klassischer Vernetzung (Voice und UC)
- Multi-Site >8 Standorte in Vernetzungen realisierbar (n-mal Multi-Site vernetzt)
- Multi-Site länderübergreifend in Vernetzungen realisierbar (n-mal Multi-Site vernetzt)
- Vernetzungsszenarien mit ISDN-Gateways voll integrierbar
- Technische Voraussetzung ist die Möglichkeit, Durchwahlrufnummern für ISDN-Provider wie für SIP-Provider gleichermaßen zu verwenden.

Szenario a: Hosting mit einer OpenScape Business S pro Standort

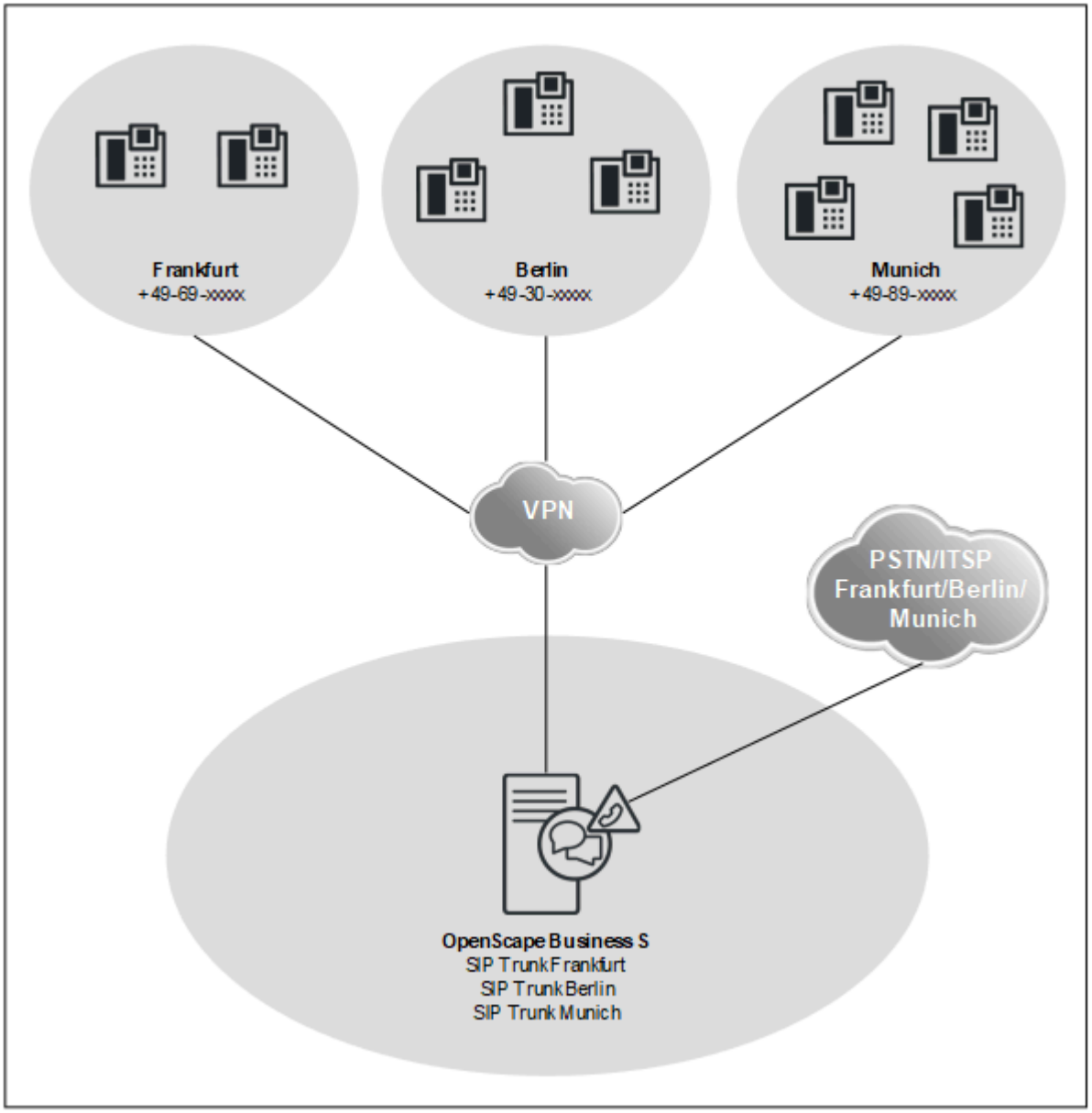
Netzwerkdaten



- Ein Kunde innerhalb eines VPN oder MPLS.
- Eine OpenScape Business S pro Standort.
- Standorte können innerhalb eines Landes oder über mehrere Länder verteilt sein.
- Bis zu 1000 User und 180 SIP-Trunks pro OpenScape Business S.
- OpenScape Business Vernetzung optional, bis zu insg. 1500 User. Größere Ausbauten sind im Rahmen von projektspezifischen Freigaben möglich.

Szenario b: Hosting mit einer OpenScape Business S für mehrere Standorte

Netzwerkdaten



- Ein Kunde innerhalb eines VPN oder MPLS.
- Eine OpenScape Business S für alle Standorte.
- Standorte nur innerhalb eines Landes.
- Bis zu 8 Standorte mit unterschiedlichen Standortvorwahlen.
- Bis zu 8 SIP-Provider pro OpenScape Business S.
- Ein SIP-Provider pro Standort.
- Bis zu 1000 User und 180 SIP-Trunks.
- OpenScape Business Vernetzung mit mehreren OpenScape Business S innerhalb eines VPN optional (OS Biz S 1 in Land 1, OS Biz S 2 in Land 2, usw.), bis zu insg. 1500 User. Größere Ausbauten sind im Rahmen von projektspezifischen Freigaben möglich.

- Konfigurationsbeispiel siehe Unify Experts Wiki im Internet unter *ITSP Configuration Guide*.

21.6.6 Vernetzung von OpenScape Business X und OpenScape 4000

Eine Vernetzung von OpenScape Business X mit OpenScape 4000 kann zwei unterschiedliche Ausprägungen haben. Erstens mit direkter Adressierung zwischen den OpenScape Business Knoten (Szenario 4a) und zweitens mit Routing aller Verbindungen über OpenScape 4000 (Szenario 4b).

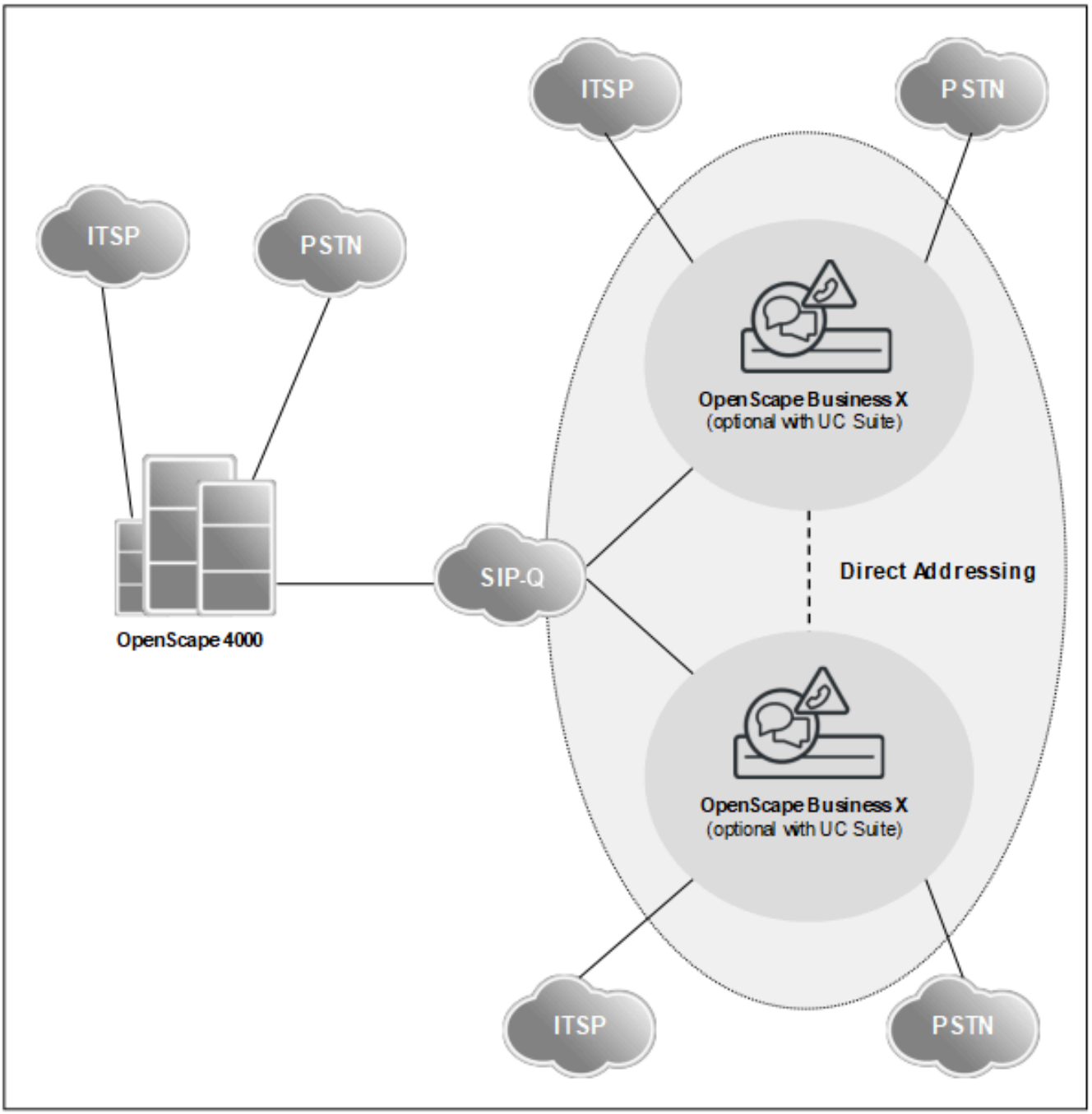
Anmerkung: Ein Einrichtebeispiel zur Vernetzung mit OpenScape Voice finden Sie im Unify Experts Wiki unter `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Szenario a: Netzverbund mit OpenScape 4000 und direkter Adressierung zwischen den OpenScape Business X Knoten

Netzwerkdaten

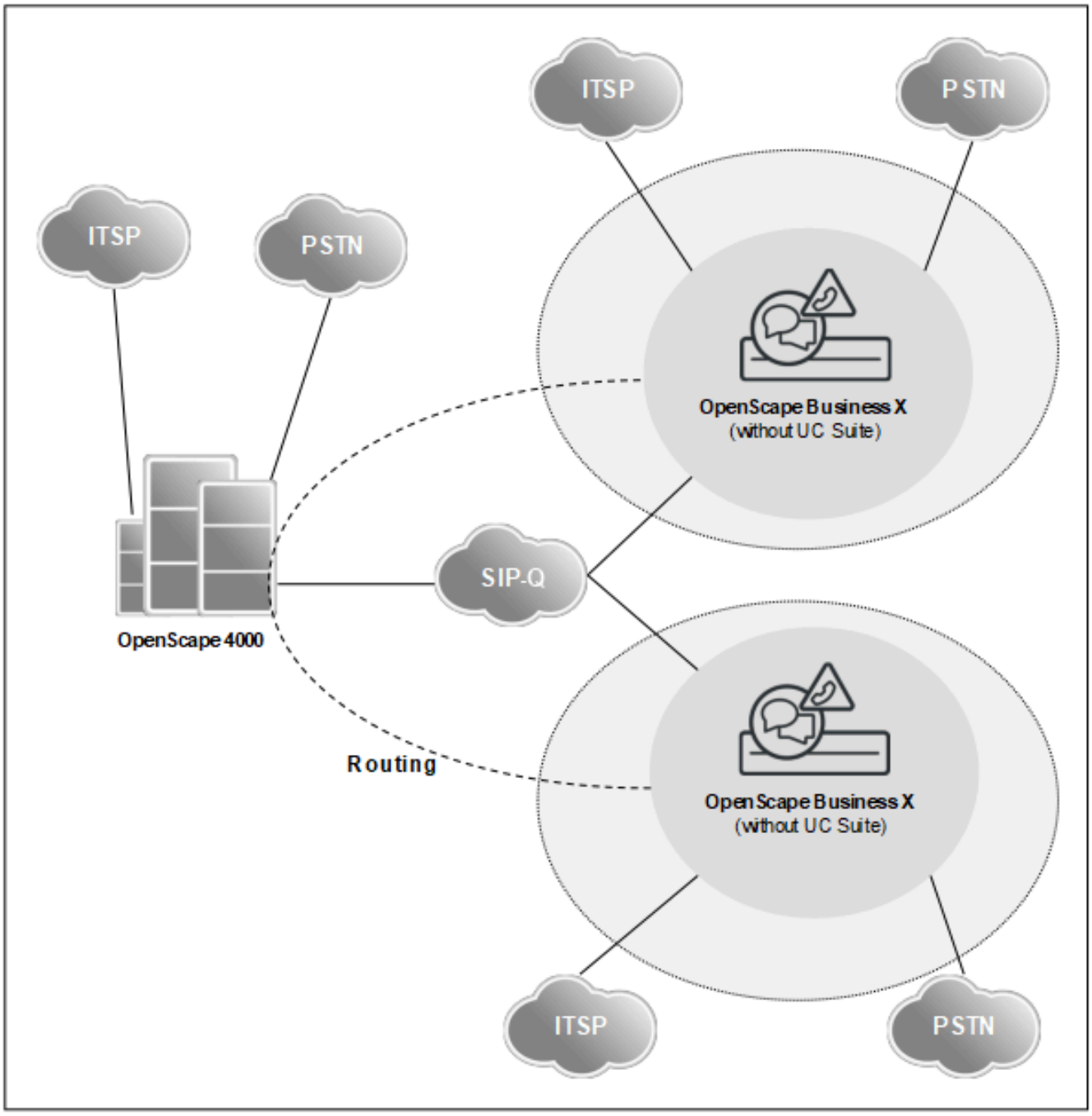
Szenario b: Netzverbund mit OpenScape 4000 und Routing aller Verbindungen über OpenScape 4000

Netzwerkdaten



- Geschlossene Nummerierung innerhalb der OpenScape Business Vernetzung

- Netzweite Sprach- und UC-Funktionalität innerhalb der OpenScape Business Vernetzung
- Konfiguration über den Assistenten "Vernetzung" für die OpenScape Business Vernetzung
- Konfiguration der OpenScape 4000 Netzanteile im Expertenmodus
- Small Remote Site Konzept (SRS) wird nicht unterstützt
- UC-Funktionalität über UC Booster Server oder über UC Booster Card ist optional.
- OpenScape Business S kann im Single oder Multi Gateway Modus integriert werden.



- Offene Nummerierung

- Netzweite Sprach-Funktionalität
- Jedes Gespräch in einen anderen Knoten wird über OpenScape 4000 geroutet
- Keine UC-Lösung bei OpenScape Business wegen offener Nummerierung im Netzverbund
- Small Remote Site Konzept (SRS) wird nicht unterstützt
- Die Konfiguration muss für jeden Knoten im Expertenmodus erfolgen

Netzweite Leistungsmerkmale

Ausbau	Geschlossene Nummerierung innerhalb der OpenScape Business Vernetzung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Maximale Anzahl Knoten	100 (32 freigegeben, abhängig von OpenScape 4000	
Maximale Anzahl von Teilnehmern pro System	Abhängig vom OpenScape Business X Modell	
Maximale Anzahl von Teilnehmern im Netz	1500 für den OpenScape Business Netz-Anteil	Abhängig von OpenScape 4000
Sprachvernetzung	SIP-Q	

UC Vernetzung	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Netzweite Funktionalität innerhalb der OpenScape Business	Nicht unterstützt
UC Booster Card	UC Smart: 51 - 150 Teilnehmer (0 - 50 Teilnehmer ohne UC Booster Card) UC Suite 0 - 150 Teilnehmer	Nicht unterstützt
UC Booster Server	UC Smart: ab 150 Teilnehmer UC Suite: ab 150 Teilnehmer	Nicht unterstützt
OpenScape Business S	Unterstützt	Nicht unterstützt

Administration	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	WBM mit Wizards für OpenScape Business Knoten, OpenScape 4000 wird über Expertenmodus der OpenScape Business administriert	Netzweite Administration Expertenmodus
WBM	WBM mit Wizards	WBM mit Expertenmodus
Manager E	Nicht empfohlen	Nicht empfohlen
UC-Suite-Administration	WBM mit Wizards für OpenScape Business Knoten	Nicht unterstützt

Administration	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	

Lizenzierung	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Lizenzierungsstruktur	Eine Vernetzungslizenz für jede OpenScape Business erforderlich	

myPortal for Desktop / myPortal for Outlook (UC Suite)	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Netzweit mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Nicht unterstützt
Sofortnachricht versenden	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Voicemail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Nicht unterstützt
Anwesenheitsstatus	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Besetztanzeige	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Externes Verzeichnis	Lokal über den Import von CSV-Dateien	Nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Nicht unterstützt

myAttendant	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Nicht unterstützt
Sofortnachricht versenden	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Voicemail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Nicht unterstützt

myAttendant	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Anwesenheitsstatus	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Besetztanzeige	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Externes Verzeichnis	Lokal über den Import von CSV-Dateien	Nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Nicht unterstützt

OpenScape Business Attendant	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Schnittstelle beschränkt auf 8-stellige Rufnummern	Schnittstelle beschränkt auf 8-stellige Rufnummern
Anwesenheitsstatus	Netzweit	
Besetztanzeige	Netzweit	
Externes Verzeichnis	über LDAP	über LDAP
Zentraler Vermittlungsarbeitsplatz	Netzweit, innerhalb der OpenScape Business Vernetzung	

Company AutoAttendant (UC Suite)	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Company AutoAttendant: Nachdem der AutoAttendant einen Anruf beantwortet hat, muss der Anrufer die Rufnummer wählen, mit der er verbunden werden möchte.	ccv-Scripts erlauben es Rufnummern aus dem internen Verzeichnis innerhalb des Netzverbunds zu wählen.	Nicht unterstützt
Persönlicher AutoAttendant: Nachdem der AutoAttendant einen Anruf beantwortet hat, muss der Anrufer eine einstellige Ziffer wählen, um mit seinem Anrufziel verbunden zu werden.	Jede von einem UC Teilnehmer vorkonfigurierte Rufnummer möglich	Nicht unterstützt

Company AutoAttendant (UCSmart)	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Company AutoAttendant (UCSmart)	Lokal	Lokal

myAgent	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S. Alle Agenten sind an EINEM Knoten registriert. Eingehend CC-Anrufe über das lokale PSTN, ITSP und SIP-Q-Amtssätze.	Nicht unterstützt
Sofortnachricht versenden	Netzweit	Nicht unterstützt
VoiceMail (Aufnahme, Message Waiting Indication, Abfrage)	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Nicht unterstützt
Anwesenheitsstatus	Netzweit	Nicht unterstützt
Besetztanzeige	Netzweit	Nicht unterstützt
Agentenstatus	Lokal	Nicht unterstützt
Internes Verzeichnis	Netzweit	Nicht unterstützt
Externes Verzeichnis	Lokal über den Import von CSV-Dateien	Nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Nicht unterstützt
Outlook-Kontakte	Lokal	Nicht unterstützt
Übergabe eines Anrufs	Lokal	Nicht unterstützt
Kundeninformation	Lokal	Nicht unterstützt
Reporting	Lokal	Nicht unterstützt

Fremdapplikationen	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
OpenScape Business TAPI-Applikation	Siehe Application Connectivity	
Externe CSTA-Applikationen		
Application Launcher		
OpenScape Contact Center	Siehe Multimedia Contact Center	

Telefonie	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
SIP-Provider (ITSP)	Lokal	Lokal
PSTN-Provider	Lokal; Netzknoten ohne eigenen PSTN-Provider werden über SIP-Q bzw. das zugehörige Gateway erreicht.	

Telefonie	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Survivability (Ausfallsicherheit im Falle eines Zusammenbruchs des Netzverbundes bzw. der OpenScape Business S)	Wird unterstützt zwischen OpenScape Business X und OpenScape Business S	Nicht unterstützt
Wahl einer öffentlichen Rufnummer im eigenen Knoten	Unterstützt	
Wahl einer öffentlichen Rufnummer in einem vernetzten Knoten	Netzweit, innerhalb der OpenScape Business Vernetzung	

Mobility	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Desk Sharing	Innerhalb eines Knotens; Netzweit, innerhalb der OpenScape Business Vernetzung mit DLS	Nicht unterstützt
Mobility mit DTMF-Steuerung des Systems	Lokal (wird bei OpenScape Business S nicht unterstützt)	Lokal
myPortal to go (Web Edition), UC Suite	Netzweiter Anwesenheitsstatus und Verzeichnisse (jeder Knoten benötigt dafür entweder UC Booster Server, UC Booster Card, oder OpenScape Business S)	Nicht unterstützt
myPortal to go (Web Edition), UC Smart	Lokal, nicht für UC Booster Server, UC Booster Card und OpenScape Business S	Nicht unterstützt

Sonstige Funktionalitäten	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Signaling- und Payload-Encryption (SPE)	Wird in OpenScape 4000 - OpenScape Business Vernetzungen unterstützt. Wird nicht unterstützt bei UC-Verbindungen und Konferenzen	Wird in OpenScape 4000 - OpenScape Business Vernetzungen unterstützt. Wird nicht unterstützt bei Konferenzen
DSS-Server	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Anrufübernahme	Nicht unterstützt	Nicht unterstützt

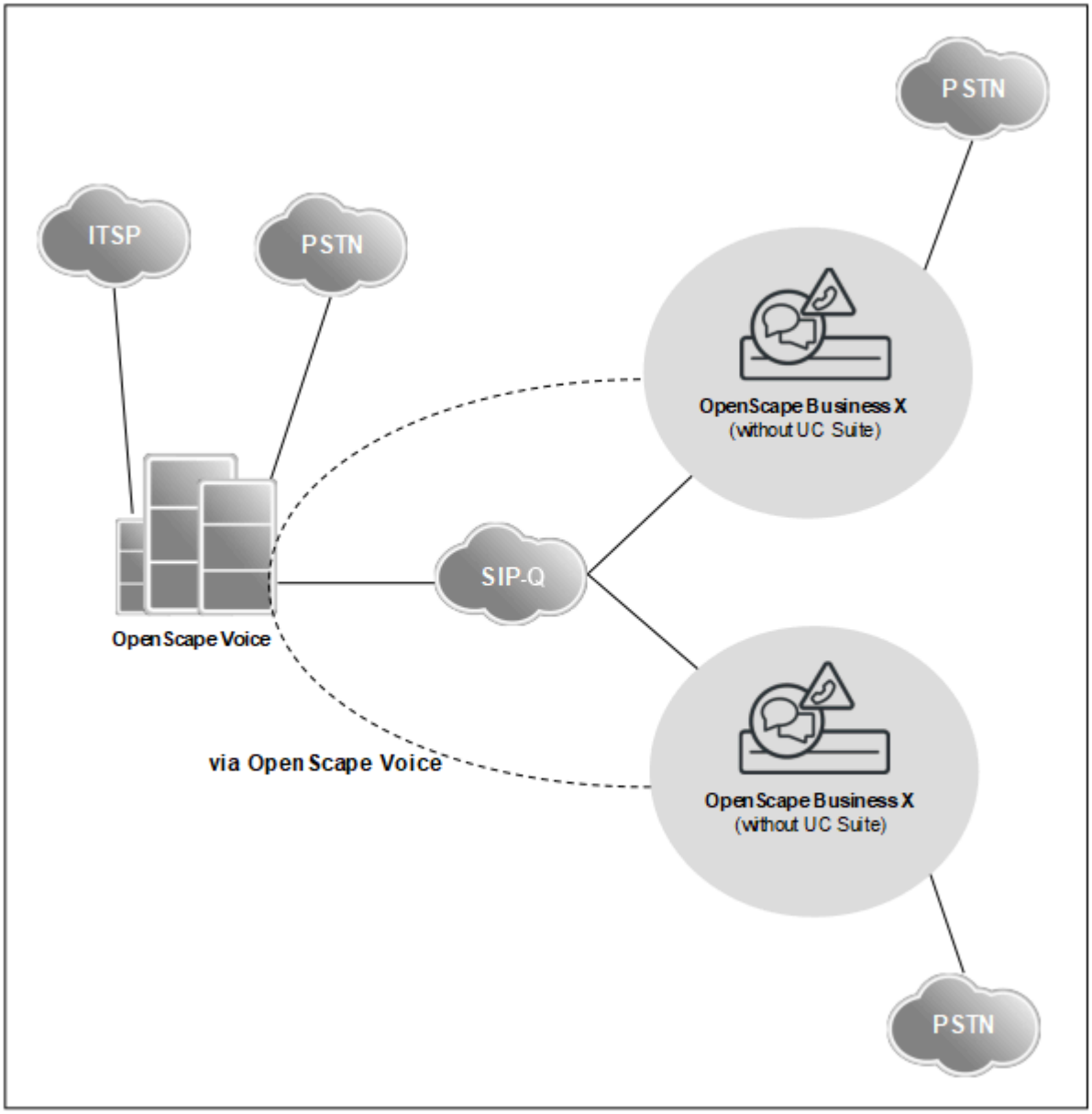
21.6.7 Vernetzung von OpenScape Business X und OpenScape Voice

OpenScape Business X kann mit OpenScape Voice vernetzt werden.

Anmerkung: Ein Einrichtebeispiel zur Vernetzung mit OpenScape Voice finden Sie im Unify Experts

Wiki unter `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Netzwerkdaten



- OpenScape Business X stellt für OpenScape Voice eine netzweite Sprach- und Gateway-Funktionalität zur Verfügung
- Eine oder mehrere OpenScape Business X können als Gateway für digitale Ämter (ISDN, T1, CAS) verwendet werden
- An OpenScape Business X Gateways können folgenden Endgeräte betrieben werden: digital / analog / DECT / IP (HFA)
- UC wird seitens OpenScape Business X in dieser Vernetzung generell nicht unterstützt.
- Jedes Gespräch von einem Knoten auf einen anderen wird über OpenScape Voice geroutet.
- Die Konfiguration jedes Knotens erfolgt über den Expertenmodus.

- Der Rufnummernplan der OpenScape Voice basiert auf E.164, daher gibt es keine offene oder geschlossene Nummerierung.

Netzweite Leistungsmerkmale

Maximalausbau	
Maximale Anzahl Knoten	abhängig von OpenScape Voice
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X
Maximale Anzahl von Teilnehmern im Netz	abhängig von OpenScape Voice

Administration	
WBM	Der Wizard Vernetzung kann nicht genutzt werden. Die OpenScape Voice wird über den Expertenmodus der OpenScape Business knotenweise administriert.
Manager E	Nicht empfohlen
UC-Administration	UC ist nicht relevant in Verbindung mit OpenScape Voice
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten der OpenScape Business im Netzverbund

Lizenzierung	
Lizenzierungsstruktur	Jeder Knoten einzeln, je OpenScape Business Knoten ist eine Netzlizenz erforderlich

Einschränkungen und Hinweise zu den Leistungsmerkmalen

- Die Anschaltung von analogen Amtsleitungen an den OpenScape Business Gateways ist **nur** für Brasilien freigegeben (Aufgrund der Unterstützung von Line Reversal und Rückwärtsauslösen von analogen Amtsleitungen in Brasilianischen Ämtern).
- Eine Vernetzung von OpenScape Business-Gateways untereinander oder mit anderen Systemen als OpenScape Voice wird nicht unterstützt. Die Vernetzung der OpenScape Business-Gateways zur OpenScape Voice muss durch sternförmige Netzstruktur erfolgen.
- Path Replacement (Wegeoptimierung) über SIP-Q wird nicht für die an einem OpenScape Business-Gateway angeschlossenen Endgeräte unterstützt.
- Um schlechte Sprachqualität bei Transit-Leitungsverbindungen zu vermeiden, sollte der Sprach-Codec G.711 verwendet werden. Der Codec G.729 wird nicht empfohlen, da durch Leistungsmerkmale wie Konferenz und Anrufumleitung Transit-Leitungsverbindungen entstehen können, da Path Replacement (Wegeoptimierung) nicht unterstützt wird.
- Keine systemübergreifende Unterstützung von Leistungsmerkmalen, wie zum Beispiel Anrufübernahmegruppen, Gruppenrufe und Sammelanschlüsse zwischen OpenScape Voice und OpenScape Business Gateways. Die Gruppen dürfen entweder nur OpenScape Voice oder nur OpenScape Business Teilnehmer beinhalten.
- Verschlüsselung (SPE) zwischen OpenScape Voice und OpenScape Business Gateways wird unterstützt. Die Verbindung zwischen OpenScape Voice und OpenScape Business muss mittels des

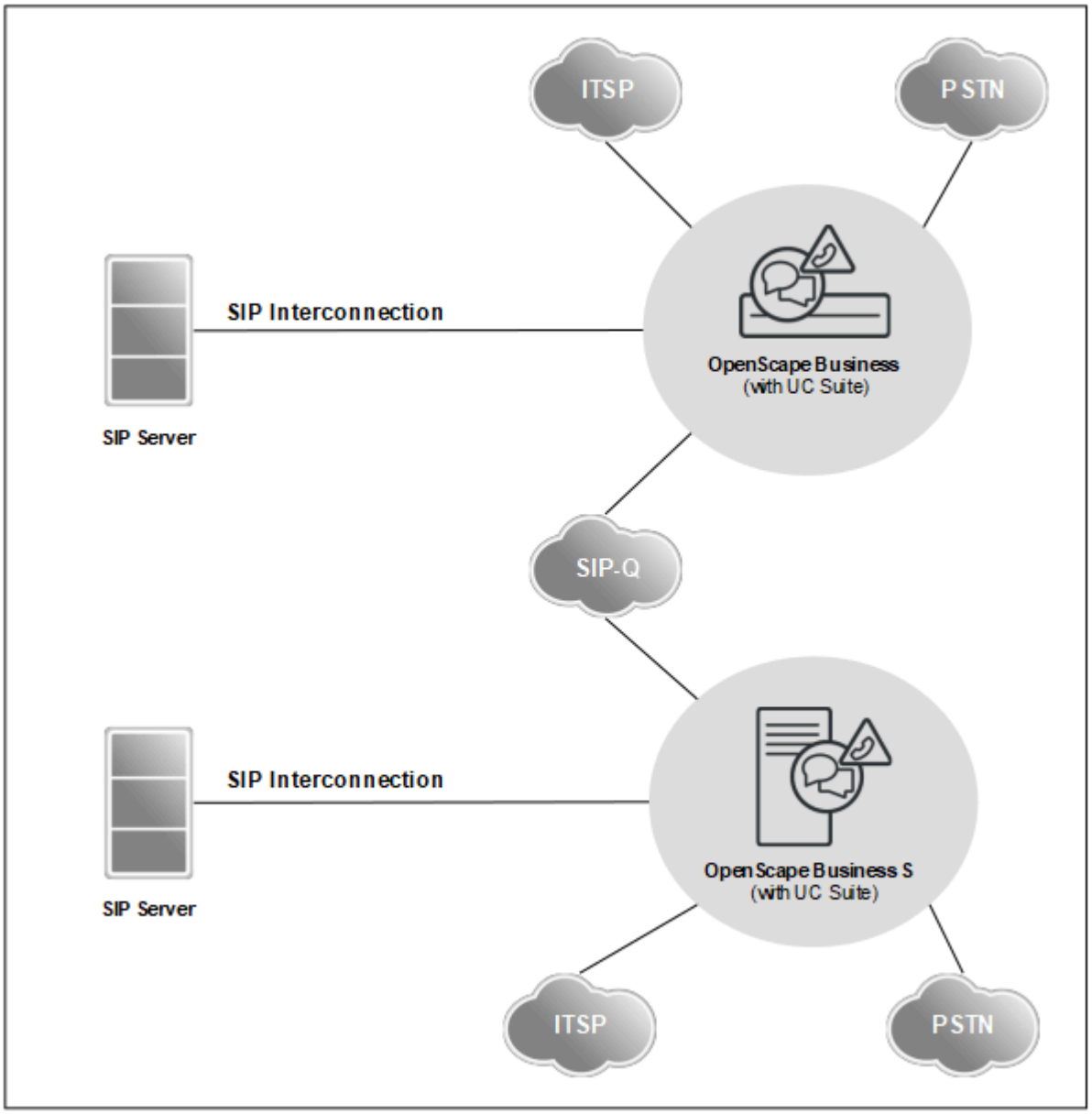
Verschlüsselungsprotokolls TLS erfolgen. SRTP (SDES) wird bei einer Vernetzung mit der OpenScape Voice V7R1 nicht unterstützt.

- Unterstützt wird ausschließlich die Vernetzung mit E.164-Rufnummernplan.
- Für die an OpenScape Business Gateways angeschlossenen IP Endgeräte (HFA) gilt: für jede aktive OpenScape Business/OpenScape Voice-Verbindung werden 2 B-Kanäle pro HFA-Endgerät benötigt (1 B-Kanal pro TDM-Endgerät). Die Notwendigkeit dieser zusätzlichen DSP-Ressourcen sollte überprüft und berücksichtigt werden.

21.6.8 Anbindung von externen Anschaltungen an OpenScape Business über SIP-Interconnection

An OpenScape Business können externe Anschaltungen über SIP-Interconnection angebunden werden, um z.B. Applikation wie OpenScape Alarm Server, OpenScape 4000, OpenScape Voice oder andere zertifizierte SIP-Server nutzen zu können.

Voraussetzungen



- Es dürfen nur zertifizierte Applikationen angeschlossen werden wie z.B. OScAR.
- Ein externer SIP-Server kann über Native SIP- oder SIP-Q-Protokoll angeschlossen sein.
- Es stehen max. zwei SIP-Q-Richtungen zur Verfügung (eine wird für UC-Suite benötigt, falls vorhanden) und max. 10 Native SIP Richtungen (bis zu 8 Native SIP Richtungen können für ITSP verwendet werden).

Weiterführende Information finden Sie im

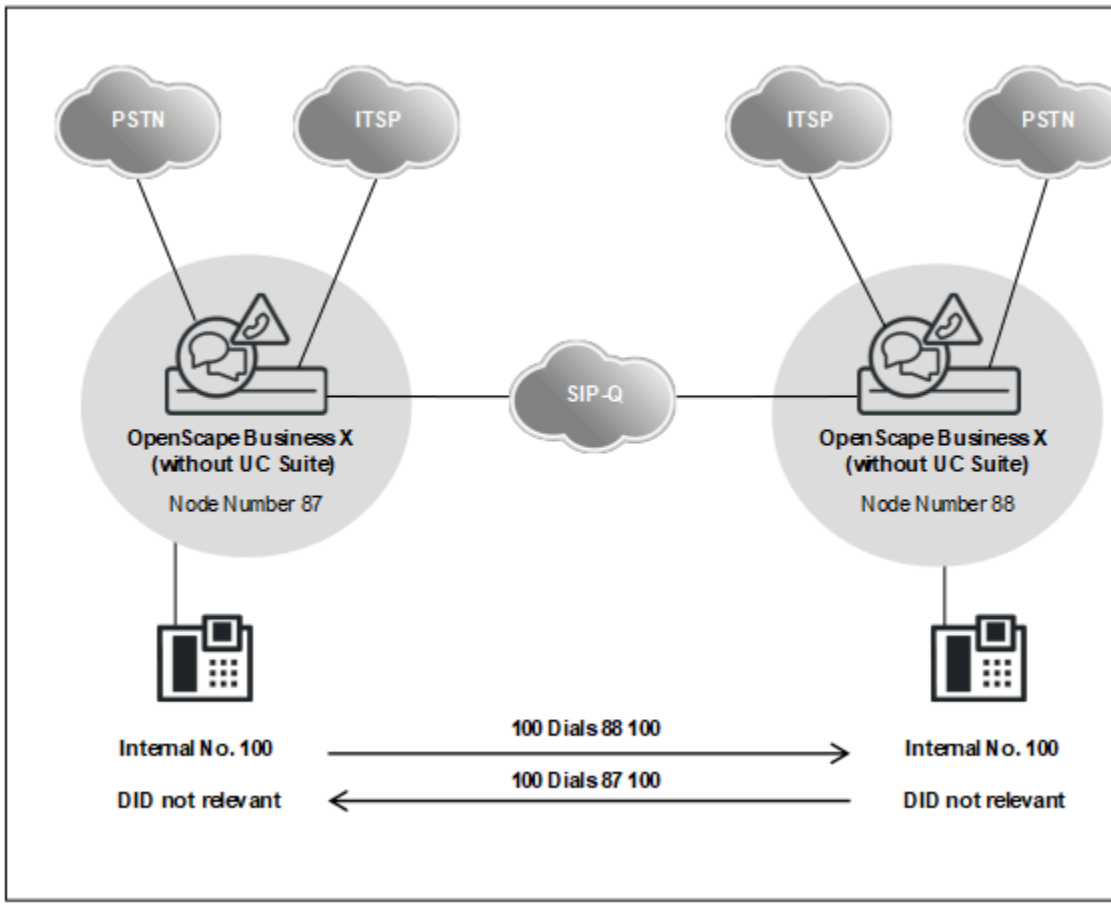
- Experten-Wiki für Telefone, Kommunikationssysteme und UC:

  `http://wiki.unify.com`

21.6.9 Offene Nummerierung in OpenScape Business X Netzwerken

Ein Netzverbund mit offener Nummerierung kann eingerichtet werden, wenn zwei (oder mehrere) Kommunikationssysteme vernetzt werden, bei denen die Nummerierung sich überschneidet (nicht eindeutig ist im Netzverbund).

Netzwerkdaten



- Netzweite Sprachvernetzung über OpenScape Business.
- UC-Leistungsmerkmale werden nicht unterstützt.
- Jeder Anruf innerhalb eines Knotens erfolgt mit interner Rufnummer.
- Jeder Anruf zu einem anderen Knoten erfolgt mit Knotennummer (plus interner Rufnummer).
- Konfiguration jedes Knotens über den Expertenmodus. Der Wizard Vernetzung ist gesperrt, sobald eine Knotennummer für offene Numerierung konfiguriert ist.
- Amtszugang PSTN oder ITSP sind lokal an jedem Knoten möglich.

Anmerkung: Bei erweiterter netzweiter UC-Funktionalität ist eine Umstellung von offener auf verdeckte (geschlossene) Nummerierung erforderlich, um die internen Rufnummern anzupassen. Hierzu muss die offene Nummerierung deaktiviert werden, um anschließend die Knotennummer zu löschen und als Präfix neu hinzuzufügen (beispielsweise als erweiterte Internrufnummer 87100 statt 100 und 88100 statt 100).

Unterschiede:

- Die Auswahl der Teilnehmer auf ihrem eigenen Knoten erfolgt über die erweiterte Internrufnummer.

- Die interne und die DuWa-Rufnummer dürfen voneinander abweichen, die Durchwahlnummern dürfen jedoch nicht geändert werden.

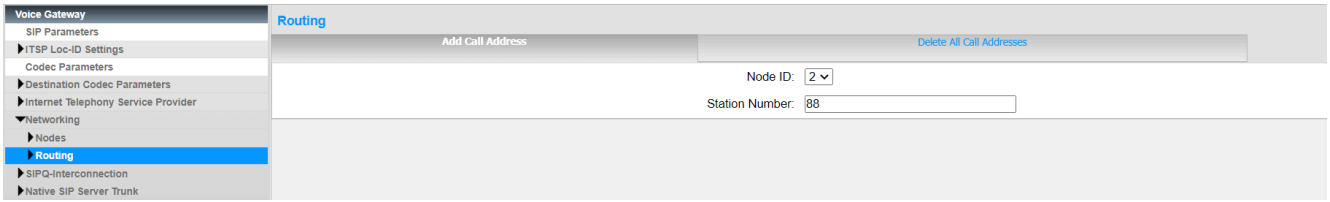
21.6.9.1 Wie Sie die offene Nummerierung konfigurieren

Offene Nummerierung einrichten

1) Offene Nummerierung für das Kommunikationssystem freigeben über das Systemflag **Offene Nummerierung**
2) Eigene Knotennummer eintragen (im Beispiel "87")

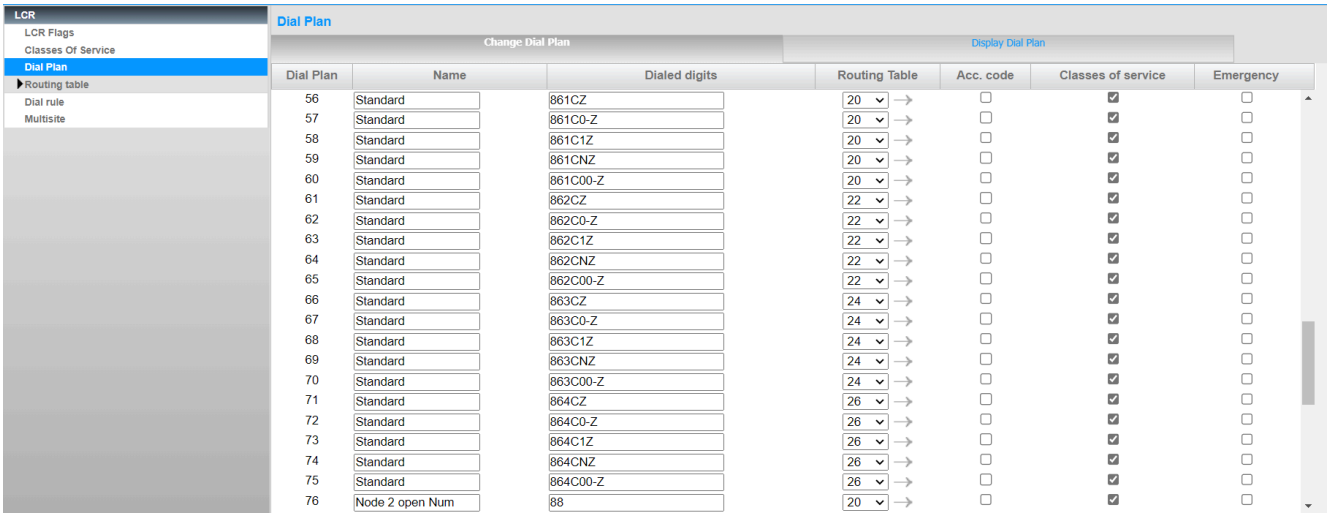
Knoten (Routing) einrichten

1) Die Zielknoten werden über Sprachgateway > Networking > Knoten > Routing addressiert (im Beispiel "88").
2) Bei einer offenen Nummerierung kann der Wizard **Vernetzung** nicht genutzt werden, dies wird durch das Systemflag **Offene Nummerierung** verhindert.

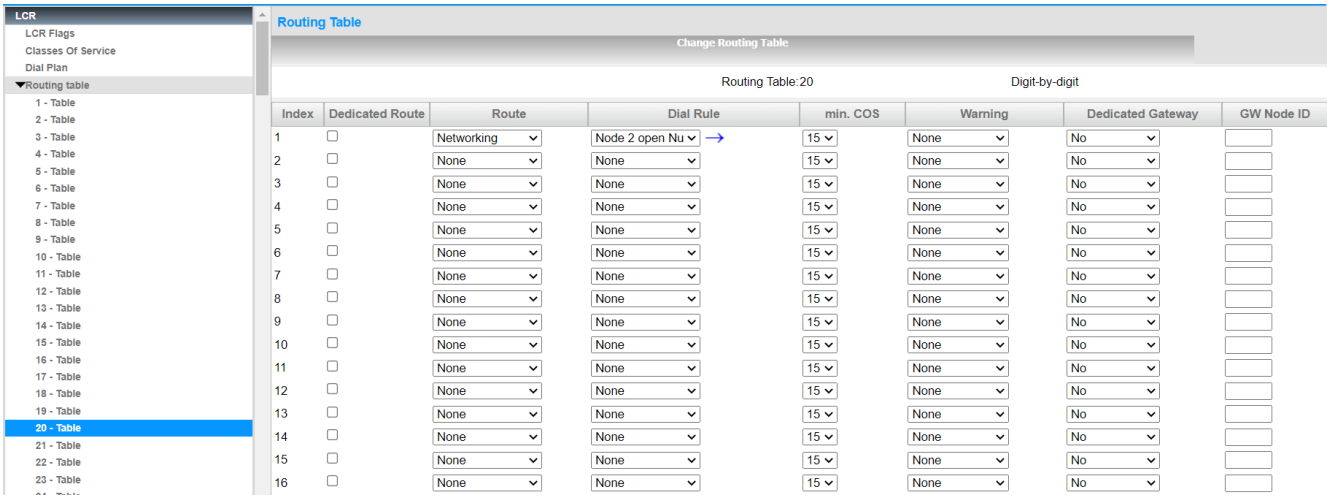


LCR einrichten

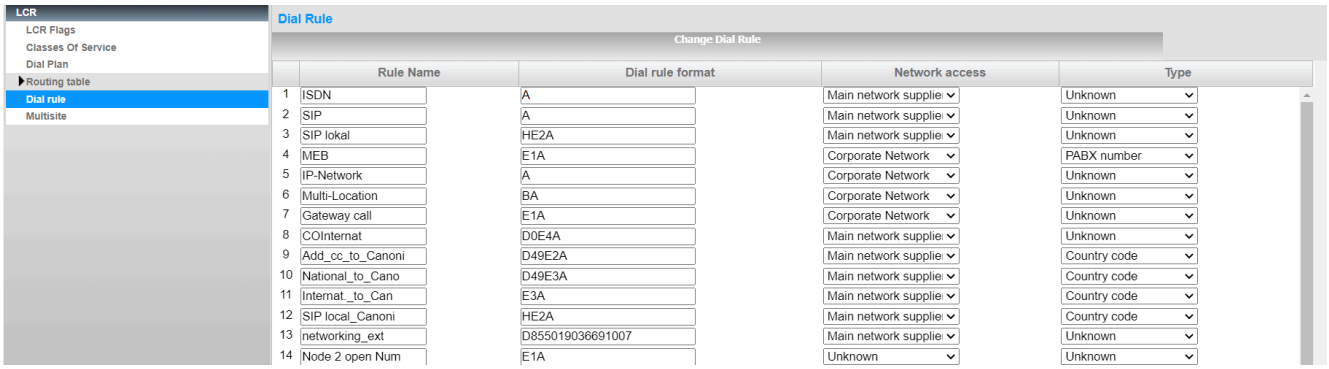
1) Die Wahlregel "Node 2 open Num" für die Knotennummer definieren und die zugehörige Routing Tabelle auswählen.



2) Anzeige der konfigurierten Route



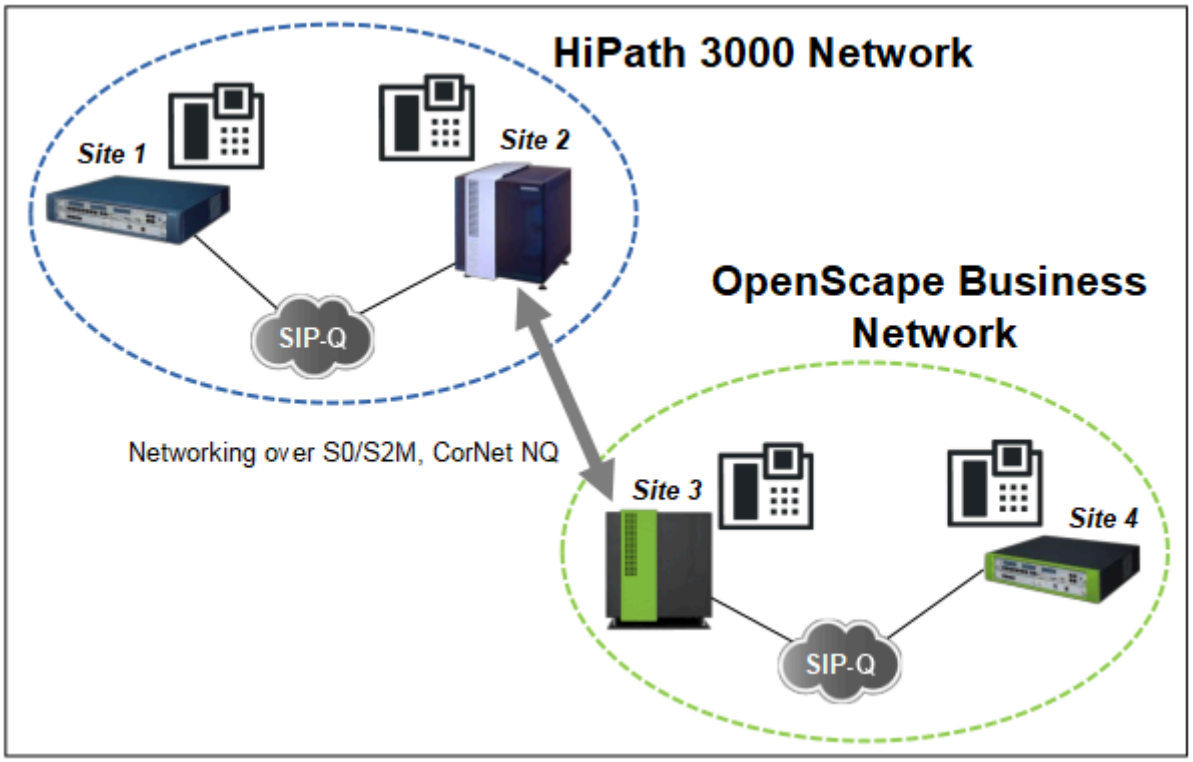
3) Den Namen der Route "Networking" und die dazugehörige Wahlregel "Node 2 open Num" eingeben.



21.6.10 Vernetzung über ISDN

OpenScape Business Systeme können sowohl untereinander als auch mit den Kommunikationssystemen HiPath 3000 und OpenScape 4000 über digitale Verbindungsleitungen vernetzt werden. Die Anschaltung kann sowohl über S_0- als auch über S_{2M}-Leitungen erfolgen.

Vernetzung mit HiPath 3000



Das vorhandene HiPath 3000 Netz bleibt (zunächst) unangetastet. Die Erweiterung des Netzes erfolgt mit OpenScape Business. HiPath 3000-Knoten können bei Bedarf schrittweise in das OpenScape Business Netz migriert werden.

Jeder netzübergreifende Anruf über HiPath 3000/OpenScape Business wird über entsprechende TDM-Gateways geführt (S_0 oder S_{2M} mit CorNet NQ-Protokoll, ggf. QSIG als Hersteller-unabhängiges Protokoll).

Es gelten die folgenden Randbedingungen:

- Separate Lizenzierung HiPath 3000 / OpenScape Business
- Separate Administration HiPath 3000 / OpenScape Business
- Empfehlung: Geschlossene Nummerierung im Gesamtnetz. Bei offener Nummerierung kann es ggf. zu Fehlverhalten bzgl. CLIP und bei Journaleinträgen/Anruferlisten kommen.
- Empfehlung: Ausschließlich Codec G.711 verwenden, um gute Sprachqualität im Gesamtnetz zu gewährleisten.
- Die Anzahl der B-Kanäle ist entsprechend des zu erwartenden Gesprächsaufkommens zu berücksichtigen.
- OpenScape Business benötigt in jedem Fall eine Networking Lizenz.

Anschaltung von Fremdsystemen über QSIG

Bei Anschaltung von Fremdsystemen mit dem QSIG-Protokoll ist folgendes zu beachten:

- Prüfung der QSIG-Varianten der betroffenen Fremdsysteme auf Kompatibilität (QSIG V1 auch QSIG nach ECMA-Standard genannt, bzw. QSIG V2 auch QSIG nach ISO-Standard genannt)

- Gegenüberstellung der Feature-Sets der betroffenen Systeme. Daran kann abgelesen werden, inwieweit der theoretisch zu erwartende Leistungsumfang, d.h. der deckungsgleiche Anteil beider Feature-Sets den Kundenwünschen entspricht.
- Zur weiteren Absicherung der zu erwartenden Funktionalität wird ein Anschaltetest vor Ort empfohlen. Dabei ist insbesondere das Interworking mit anderen Vernetzungsprotokollen bzw. Amtsprotokollen zu beachten.

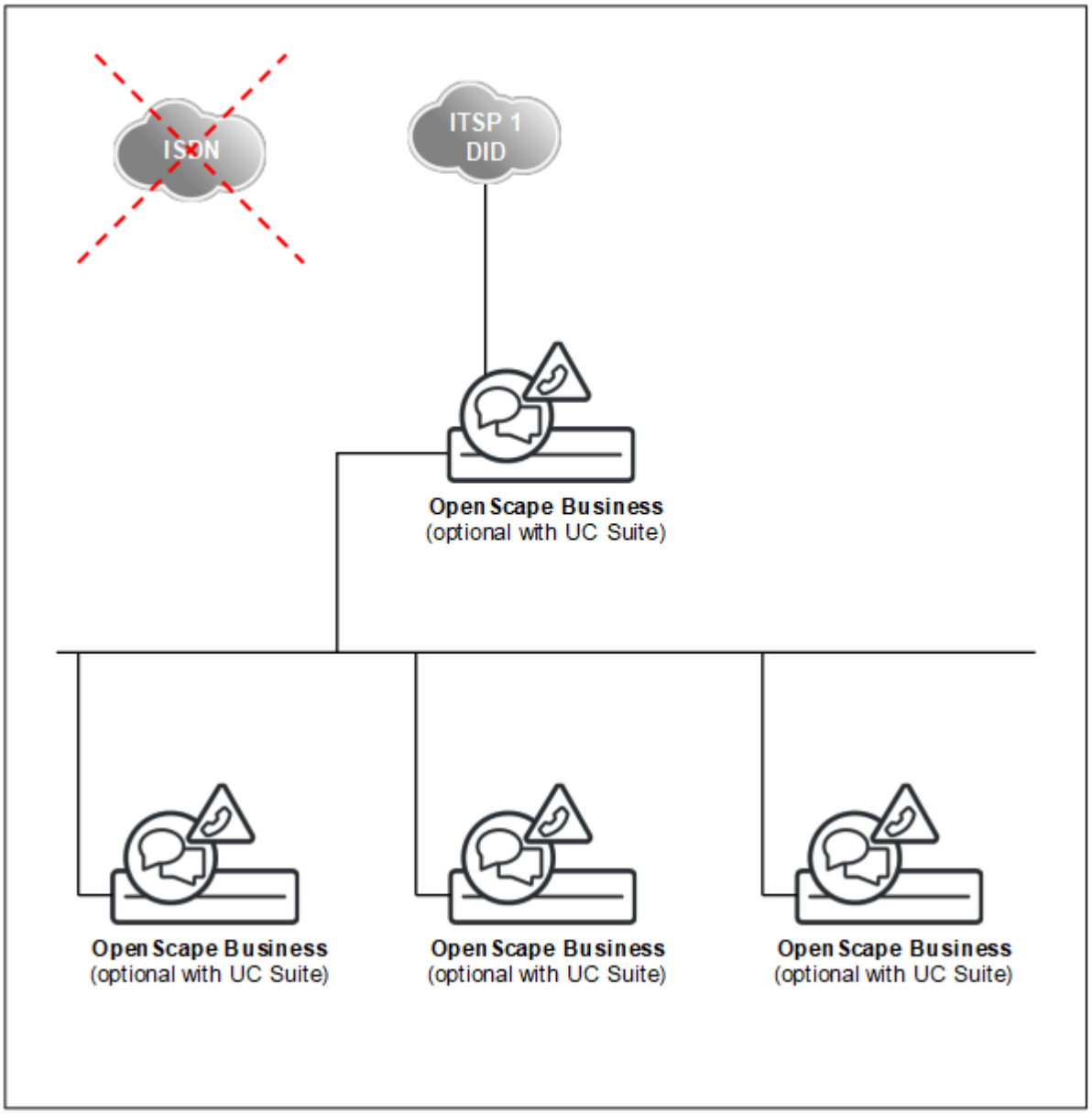
Anmerkung:

Die QSIG-Trunk-Gruppe sollte im OpenScape Business-System als PABX-Routentyp konfiguriert sein. Aus dem QSIG-Netz kommende Anrufe gelten daher als intern und folgen der internen CDL (Rufzielliste).

21.6.11 OpenScape Business Netzverbund mit zentralem ITSP-Amtsanschluss

Ein reiner OpenScape Business Netzverbund kann statt ISDN mit einem zentralen, durchwahlfähigen ITSP-Amtsanschluss realisiert werden.

Vernetzung mit zentralem, durchwahlfähigem ITSP-Amtsanschluss



Folgendes ist bei der Planung von Kundennetzen zu beachten:

- **Ein** zentraler, durchwahlfähiger ITSP-Amtsanschluss für das komplette OpenScape Business Netz.
- Registrierung an genau einem Ortsnetz, d.h. alle Knoten des Netzes nutzen genau eine Amtsrufnummer, z.B. 0049 89 7007-xxxxx.
- Die vernetzten Knoten können für Notfälle, d.h. bei Ausfall des zentralen ITSP-Zugangs, eigene Amtsanschlüsse für ausgehende Verbindungen verwenden. Unter Umständen ist in diesem Fall eine korrekte Anrufer-Identifizierung nach außen nicht möglich. Notrufe können ggf. nicht korrekt zugestellt werden. Die kommende Erreichbarkeit über diesen lokalen Anschluss ist ebenfalls mit Restriktionen verbunden. Aus genannten Gründen werden lokale Anschlüsse nicht empfohlen, werden aber technisch nicht verhindert.
- Aus dem gleichen Grund werden am zentralen Knoten keine zusätzlichen ISDN-Anschlüsse empfohlen, technisch aber nicht verhindert.

- Es gelten alle Regeln für Wahlbewertung und Call-Routing für OpenScape Business-Einzelsysteme und -Netze. Die Rufnummernzuordnung der ITSP-Amtsrufnummern erfolgt in diesem Fall ausschließlich über die Durchwahl-Konfiguration des Teilnehmers (nicht über die Mapping-Tabelle, siehe ITSP-Konfiguration Kapitel 9.2 und siehe im Unify Experts Wiki im Internet).

21.7 Zentraler Abwurfplatz im Netzverbund (nicht für USA)

OpenScape Business ermöglicht, ankommende Rufe, die keinem Teilnehmer zuzuordnen sind oder nicht beantwortet werden, an einen festzulegenden Abwurfplatz im Netzverbund umzuleiten, damit kein Anruf verloren geht.

Wenn der zentrale Abwurfplatz im Netzverbund über ISDN konfiguriert ist, so ist die Funktionsweise identisch mit der Funktionsweise ohne Vernetzung.

In Verbindung mit einem ITSP-Amt ergeben sich für den zentralen Abwurfplatz einige Einschränkungen, da jeder Knoten grundsätzlich seinen eigenen ITSP hat:

- Die ITSP-Abwurfkriterien gelten nur für den jeweiligen Knoten.
- Es funktionieren Abwurf im Freifall, bei Besetzt, bei unvollständiger Wahl, bei Falschwahl und bei unbeantwortetem Wiederanruf.
- Die Abwurfarten "Falschwahl" und "Unvollständig" funktionieren beim ITSP nicht.
- Unvollständige oder falsche Rufnummern werden mit Besetztsignal an den ITSP zurückgegeben.

Wenn ein zentraler Abwurfplatz in einem Netzverbund genutzt werden soll, müssen in jedem Knoten virtuelle Teilnehmer konfiguriert werden. Diese virtuellen Teilnehmer werden über den Netzverbund fest zum myAttendant Benutzer umgeleitet.

Beispiel für ITSP-Amt: ITSP-Anlagenrufnummer ist 0211-23456789 + ITSP-Durchwahlnummer, öffentlich wird die Rufnummer 0211-23456789-0 als zentrale Nummer des Kommunikationssystems bekannt gegeben.

- Teilnehmer 100 ist myAttendant mit eigener ITSP-Durchwahlnummer 100 und einem virtuellem Teilnehmer 199 mit ITSP-Durchwahlnummer "0".
- In der ITSP-Mapping-Liste jedes Knotens wird die ITSP-Durchwahlnummer "0" dem eigenen virtuellen Teilnehmer zugeordnet.
- Unter **Kommende Rufe/Rufweiterschaltung** werden die virtuellen Teilnehmer auf Teilnehmer 100 verwiesen.

  Erstes Ziel: eigener virtueller Teilnehmer

  Zweites Ziel: Teilnehmer 100 im Zielknoten

  Rufzeit 5 Sekunden

Zur besseren Identifikation der Anrufe ist es empfehlenswert, die virtuellen Teilnehmer aller Knoten über die Applikation myAttendant (unter **Einrichtung**/**myAttendant**/**DuWas**) mit ihrer Rufnummer (DID) und einem Namen (z.B. Firma) zu versehen. Damit ist im Fenster **Aktive Anrufe** von myAttendant eine ausführlichere Identifikation des Anrufers möglich.

21.7.1 Wie Sie einen zentralen Abwurfplatz im Multi-Gateway-Netzverbund konfigurieren

Einrichtebeispiel für einen zentralen Abwurfplatz im Multi-Gateway-Netzverbund über die vorgeschalteten OpenScape Business Gateways. Alle Anrufe, die in einem Knoten eingehen und die Abwurfkriterien erfüllen, müssen zu OpenScape Business S werden, wo sich der zentrale AutoAttendant befindet.

Voraussetzungen

OpenScape Business S ist Master (alle HFA- und SIP-Teilnehmer sind hier angemeldet).

Mehrere OpenScape Business X sind als Slave-Knoten (mit PSTN oder ITSP als Amtszugang) eingerichtet. Die Knoten können sich am gleichen Ort oder an unterschiedlichen Standorten befinden (unterschiedliche Vorwahlen).

Schritt für Schritt

1) Einrichten eines virtuellen Teilnehmers an OpenScape Business.
   a) Einrichten eines virtuellen Teilnehmers mit Namen "Abwurf 22 System2"

2) Einrichten eines Zentralen Abwurfplatzes mit Abwurfkriterien an OpenScape Business.
   a) **Experten-Modus**
   b) **Grundeinrichtung** > **System** > **Abwurf/VPL/Hotline**
   c) Virtuellen Teilnehmer 22 unter **Abwurfplatz** bei **Tag und Nacht** auswählen.
   d) Folgende Parameter für den Teilnehmer 22 unter **Abwurfplatz** bei **Abwurf** eingeben:

Name	Abwurf 22 System2
Durchwahl	xxxxxxx22
Gerätetyp	Virtuell

   e) Aktivieren der eingegebenen Parameter unter **Abwurfplatz** bei **Abwurf**.
   f) Einrichten des virtuellen Teilnehmers unter **Abwurfplatz** bei **Codeschloss**.

3) Einrichten der Rufweiterschaltung an OpenScape Business.
   a) Einrichten der Rufweiterschaltung des virtuellen Teilnehmers 22 über den Netzverbund zu OpenScape Business S.
   b) **Experten-Modus**
   c) **Kommende Rufe** > **Rufweiterschaltung**
   d) Virtuellen Teilnehmer 22 auswählen
   e) Weiter zu **Rufweiterschaltung für Teilnehmer parametrieren**
   f) dann an: **externes Ziel** (AutoAttendant Warteschlangen-Rufnummern eingeben z.B. 7410)
   g) **Richtung =** Netzwerk auswählen (Die AutoAttendant Warteschlangen-Rufnummer 7410 muss gezielt im LCR geroutet werden, unter Umgehung der -Z Default Regel 33).

4) Konfigurieren des Routings für OpenScape Business.

Die AutoAttendant Warteschlangen-Rufnummer 7410 muss gezielt im LCR geroutet werden (unter Umgehung der -Z Default Regel 33).

Unter **Wahlplan**:	**Name** einrichten (VSL Queue Pilot)
	Rufnummer unter **Gewählte Ziffern** eingeben (7410)
	Wegetabelle auswählen (XX)
Unter **Wegetabelle** XX:	**Richtung** = Netzwerk auswählen
	Wahlregel zuordnen
	Unter **Dediziertes Gateway** den Eintrag **Erzwungen** auswählen
	GW Knoten ID der OpenScape Business S eintragen
Unter **Wahlregel**:	**Regelname** eintragen
	Wahlregelformat D7410 (Queue Pilot Nummer) eintragen
	Verfahren des Netzanbieters: Corporate Network auswählen
	Type: Unbekannt auswählen

5) Einrichten einer Warteschlange an OpenScape Business S.

a) Einrichten einer Warteschlange (Queue Pilot) mit einer CCV, z.B. **Nebenstellenwahl**, **Nach Name wählen**, **Aktion nach Ziffern**.

6) Einrichtung einer Rufweiterschaltung an OpenScape Business S.

a) Einrichten der Rufweiterschaltung der Queue Pilot 7410 in OpenScape Business S.
b) **Experten-Modus**
c) **Kommende Rufe** > **Rufweiterschaltung**
d) Queue Pilot 7410 auswählen
e) Weiter zu **Rufweiterschaltung für Teilnehmer parametrieren**
f) zuerst an: **externes Ziel** (AutoAttendant Warteschlangen-Rufnummern eingeben z.B. 7410)
g) dann an: **Sprachbox** auswählen

21.8 Presence Manager

Der Presence Manager ermöglicht die netzweite Signalisierung der vermittlungstechnischen Teilnehmerzustände “Frei", “Besetzt" und “Ruf" an den LEDs der HFA-Telefone. Voraussetzung dafür ist eine geschlossene Nummerierung und mindestens ein UC Booster Server am Master-Knoten des Netzverbundes oder eine OpenScape Business S als Master-Knoten. Pro Knoten ist eine Netzwerklizenz erforderlich.

Bei Frei-Zustand ist die entsprechende LED aus, im Belegt-Zustand ist sie dauernd an, im Rufzustand blinkt die LED. Im Rufzustand kann dieser Ruf durch Betätigen der entsprechenden Taste übernommen werden.

Die Signalisierung der vermittlungstechnischen Zustände eines Teilnehmers ist nur möglich, wenn der Presence Manager auf diesen Teilnehmer einen CSTA-Monitorpunkt setzen kann.

Die Konfiguration der Tasten erfolgt durch den Anwender. Bei der Programmierung am Telefon selbst besteht kein Unterschied, ob es sich um eine interne oder netzweite Rufnummer handelt.

Der Presence Manager ist ein Dienst ohne Benutzeroberfläche. Es sind keine Einstellungen vorzunehmen, da alle Daten automatisch durch einen Datenabgleich abgeleitet werden.

Gruppen werden nicht durch Presence Manager unterstützt. Es erfolgt keine LED-Signalisierung und es besteht keine Möglichkeit der Anrufübernahme. MULAPs werden dagegen vom Presence Manager unterstützt.

Presence Manager unterstützt aktiv keine SIP- und S_0-Telefone.

21.9 Synchronisationsstatus im Netzverbund

Bei einem Netzverbund wird der Synchronisationsstatus im Admin-Portal und der Registrationsstatus der einzelnen Knoten durch farbige Buttons angezeigt. Die Anzeige des Synchronisationsstatus gilt für Netzknoten des Kommunikationssystems, nicht für OpenScape 4000 und OpenScape Voice Knoten.

Anzeige des Synchronisationsstatus

Anzeige	Farbe	Bedeutung für den Master	Bedeutung für den Slave
Synchronisations Status (Anzeige auf der Startseite des Admin-Portals)	Rot	-	Die IP-Adresse des Master-Knotens ist konfiguriert aber das Slave-System konnte sich nicht registrieren. In zyklischen Abständen versucht sich der Slave beim Master zu registrieren.
	Gelb	-	Slave ist beim Master registriert, aber die Rufnummern sind nicht konsistent im Netzverbund. Dies kann nach einem Backup/Restore oder nach der ersten Registrierung der Fall sein.
	Grün	Wenn ein Knoten als Master konfiguriert ist, dann erscheint der Status Grün.	
Registrationsstatus der einzelnen Knoten (Anzeige im Dialog Netzwerk>Knotensicht)	Rot	Slave ist konfiguriert; das System hat sich aber noch nie registriert.	Slave ist konfiguriert; das System hat sich aber noch nie registriert.
	Grün	Das System ist registriert.	Das System ist registriert.
Alive (Anzeige im Dialog Netzwerk>Knotensicht)	Rot	Knotenspezifischer Blick auf den Netzverbund: Alle Knoten, die rot markiert sind, können nicht erreicht werden. Die Gründe dafür können Netzwerkprobleme oder ein Ausfall des Kommunikationssystems sein.	
	Grün	Der (fremde) Knoten ist über das Netzwerk erreichbar. Der eigene Knoten wird stets grün dargestellt.	

21.9.1 Manuelle Synchronisierung im Netzverbund

Wenn nach der Konfiguration von Rufnummern / Namen (Interne- oder Durchwahlrufnummern) diese nicht automatisch in den anderen Systemen eines Netzverbundes synchronisiert werden, kann eine manuelle Synchronisierung angestoßen werden. Die manuelle Synchronisierung im Netzverbund funktioniert nur in homogenen Vernetzungen.

Master

Slave

Der Synchronisierungs-Vorgang überträgt ausschließlich Konfigurationsänderungen.

Steht die Statusanzeige im Admin-Portal auf "Rot", kann durch Aktivieren der Synchronisierungs-Schaltfläche versucht werden, die Synchronisierung der Daten an den Master manuell zu starten.

Für den Fall, dass bereits konfigurierte Systeme im Netzwerk untereinander nicht mehr telefonieren können, muss die Ursache für diese Störung anderweitig gesucht werden. Ist der Alive-Status einzelner Knoten "Rot", ist dies ein Hinweis auf Netzwerkprobleme oder es gibt andere Gründe, warum der Knoten im Netzwerk nicht erreichbar ist. In diesen Fällen bringt eine Aktivierung der Synchronisierungs-Schaltfläche keine Abhilfe.

Bei Aktivierung auf dem Master-Knoten werden die Slave-Knoten aufgefordert, Rufnummern und Namen des Systems vom Master zu aktualisieren.

Bei Aktivierung auf einem Slave-Knoten werden die Rufnummern und Namen des Systems an den Master aktualisiert. Gleichzeitig findet ein erneutes Registrieren des Slave-Knotens beim Master-Knoten statt.

21.9.2 Wie Sie eine Synchronisierung manuell starten

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

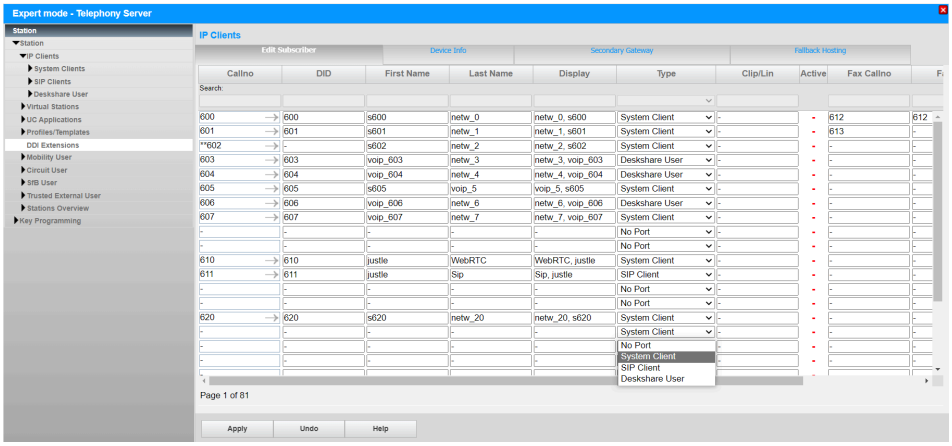
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Aktivieren Sie die Schaltfläche **Sync Network** um die manuelle Synchronisierung zu starten.

21.10 Überlebensfähigkeit

Überlebensfähigkeit ist ein Merkmal innerhalb eines Netzwerks von OpenScape Business-Knoten. Wenn ein OpenScape Business-Knoten ausfällt oder aufgrund von Netzwerkfehlern nicht erreichbar ist, können sich die am OpenScape Business-Knoten angemeldeten Systemtelefone (HFA) stattdessen am anderen OpenScape Business-Knoten des Netzwerks anmelden. Die Telefonnummern der Systemtelefone bleiben nach der neuen Anmeldung erhalten. Dies bietet Kontinuität

für die Basistelefonie; die Merkmale von Anwendungen wie myPortal, Voicemail und CTI sind jedoch vorübergehend nicht verfügbar.



Wenn auf den fehlgeschlagenen OpenScape Business-Knoten wieder sicher zugegriffen werden kann, kehren die Systemtelefone automatisch zum OpenScape Business-Knoten zurück.

Die Zeit für den Wechsel zum Standby-Gateway kann bis zu 30 Minuten dauern.

Wenn der OpenScape Business-Knoten fehlschlägt, wird zunächst versucht, ihn für einen festen Zeitraum (10-Minuten; kann nicht geändert werden) erneut zu erreichen. Erst nach Ablauf dieser Zeit werden die dafür vorgesehenen Systemtelefone am Standby-Gateway registriert. Der aktuelle Status der registrierten Telefone kann in **Expertenmodus** > **Diagnoseprotokolle** angezeigt werden.

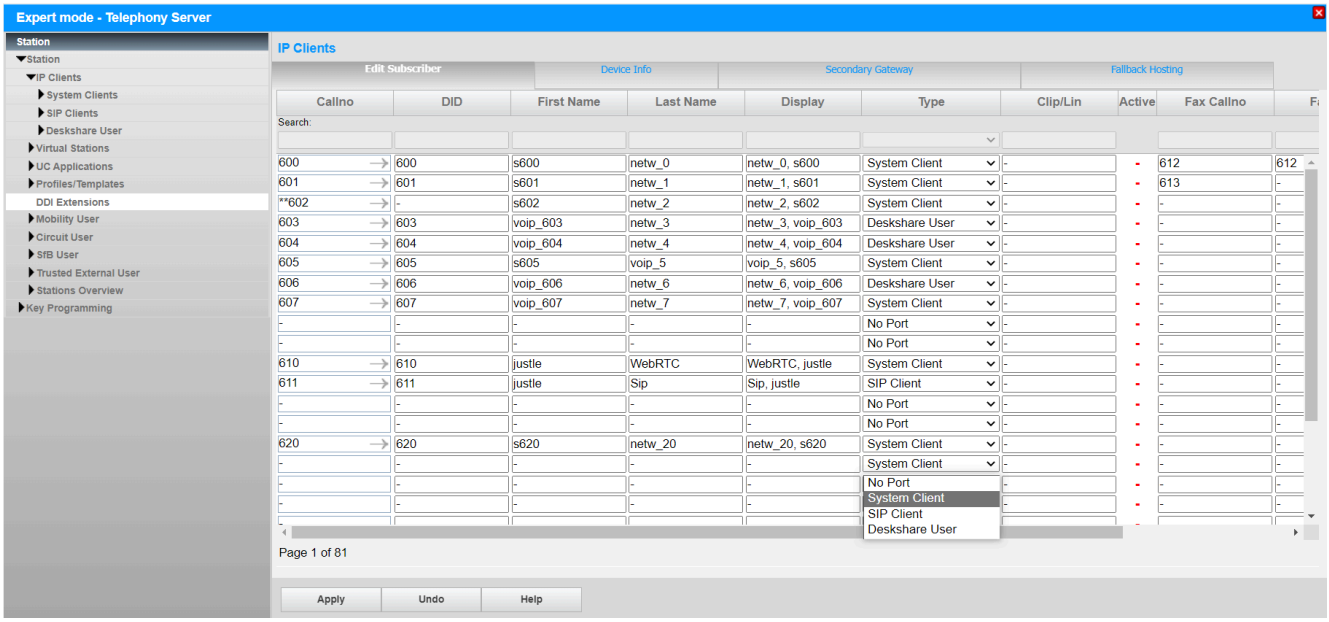
Die Überlebensfähigkeitseinstellungen werden an den Systemtelefonen konfiguriert. Wenn der OpenScape Business-Knoten ausfällt, versuchen die Telefone zunächst mehrmals, ihn erneut zu erreichen. Über die Einstellung "Systemredundanz" im Administrationsmenü der Telefone kann ein Timeout oder wie oft sich das Telefon erneut einloggen versucht konfiguriert werden. Die Standardeinstellung für das Timeout beträgt 30 Sekunden mit einem Wiederholungsversuch. Danach registrieren sich die Telefone am Standby-Gateway. Die automatische Registrierung zurück am OpenScape Business-Knoten muss ebenfalls an den Systemtelefonen konfiguriert werden.

Anmerkung: Das Merkmal der Überlebensfähigkeit erfordert, dass der POSTGRES-Dienst korrekt funktioniert. Wenn die Anwendungsfirewall mit einer Regel für den POSTGRES-Dienst aktiviert ist, müssen Sie sicherstellen, dass die IP-Adressen der anderen vernetzten OpenScape Business-Knoten dieser Regel manuell hinzugefügt werden, andernfalls funktioniert die Überlebensfunktion nicht.

Für die Überlebensfähigkeit müssen die folgenden Voraussetzungen erfüllt sein:

- Für die mit dem OpenScape Business-Knoten verbundenen Systemtelefone, muss am Standby-Gateway eine ausreichende Anzahl freier IP-Ports, die bei Ausfall eines Netzwerkknotens "gespeichert" werden müssen, zur Verfügung stehen.

- Für diese freien Ports am Standby Gateway müssen Stationen ohne Namen und Telefonnummer eingerichtet werden.

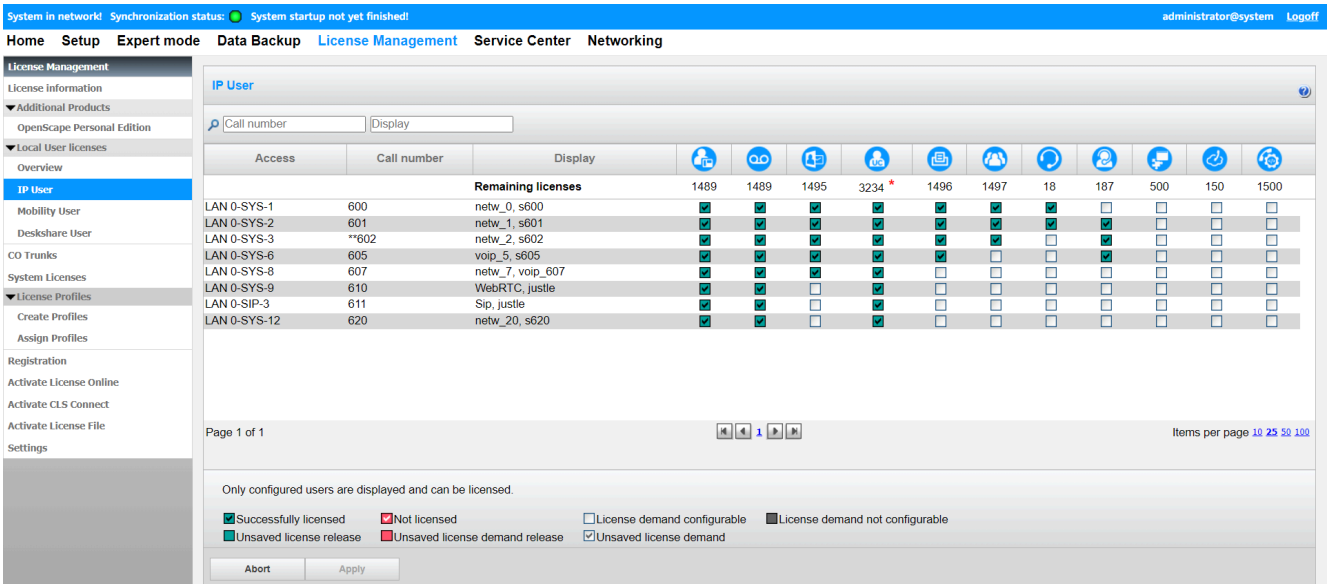


- Die Stationen müssen als Systemtelefone (Systemclients) konfiguriert sein und über eine Fallback-Benutzerlizenz verfügen. Wenn Fallback-Lizenzen in der aktivierten Lizenzdatei nicht verfügbar sind, können stattdessen IP-

Benutzerlizenzen verwendet werden. Im Falle der Überlebensfähigkeit können die Stationen nur Telefonie-Merkmale verwenden.

Anmerkung: Während der Ausfallzeit des Master-Knotens treten Konflikte mit Rufnummern der HFA-Redundanz-Clients auf, bis der Master-Knoten wieder betriebsbereit ist.

Anmerkung: Wenn dem System Fallback-Benutzerlizenzen zugewiesen sind, können IP-Benutzerlizenzen im Fehlerfall nicht verwendet werden.



21.10.1 Wie Sie Survivability konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Navigieren Sie im Menübaum zu **Teilnehmer** > **IP Clients**. Bei einem OpenScape Business Master-System erscheint das Fenster **Secondary Gateway**.
3) Wählen Sie unter **Node ID** die OpenScape Business aus, die im Notfall die Teilnehmer der OpenScape Business S übernehmen soll.
4) Aktivieren Sie das Kontrollkästchen **Emergency** für die Notfallteilnehmer.
5) Die Einträge für **Emergency Call no** und **Call no DID** sind vorgeleistet und können ggf. angepasst werden.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

21.11 Entfernung eines Knotens aus dem Netzverbund

Wenn ein Knoten aus dem Netzverbund entfernt werden soll, ist es wichtig das der Knoten in der Netzwerk-Konfiguration nicht mehr erreichbar ist. Sonst versucht dieser Knoten, sich selbständig wieder im Netzverbund anzumelden, und der Master-Knoten versucht, Daten zu synchronisieren.

Verfahren

Das Löschen eines Knotens erfolgt über den Wizard Vernetzung, wobei immer alle beteiligten Knoten entfernt werden müssen.

- Alle Strecken (Routing) zu den zu entfernenden Knoten unterbrechen.
- Administration des Netzverbundes
- Geben Sie für den betroffenen Slave-Knoten im Netzwerk-Assistenten des Slave-Knotens "Kein Netzwerk" ein.
- Entfernen Sie den Slave-Knoten im Netzwerk-Assistenten des Master-Knotens aus der Registrations-Liste.

Wird der Knoten nicht gelöscht, werden weiterhin Daten von einer OpenScape Business zur anderen übertragen und es kann zu Inkonsistenzen im internen Verzeichnis kommen, d.h. die Benutzer erscheinen nicht im Benutzerverzeichnis und können somit z.B. myPortal for Desktop nicht nutzen.

22 Anschaltungen

Anschaltungen sind externe Geräte (wie z.B. ein Ansagegerät oder eine Türsprechstelle mit Türöffner), die an die Schnittstellen des Kommunikationssystems angeschlossen werden.

22.1 Analoges Ansagegerät

Ein analoges Ansagegerät kann an eine a/b-Schnittstelle angeschlossen werden, um darüber eigene Ansagen abspielen zu können (z.B. für den zentralen AutoAttendant oder als Ersatz für die Wartemusik).

Anmerkung: Stellen Sie vor der Benutzung von Ansagen bzw. Musik aus anderer Quelle sicher, dass Sie keine Copyright-Verletzung begehen.

Pro Kommunikationssystem können bis zu 16 Ansage-Quellen konfiguriert werden, wie z.B. Mediaserver, Announcement Player oder auch analoge Ansagegeräte.

Dabei können die folgenden Typen von Ansagegeräten verwendet werden:

- Ansagegeräte, welche bei Aktivierung stets beim Textanfang starten (z.B. Begrüßungsansage)
- Ansagegeräte, welche über eine Endlos-Wiedergabe verfügen (z.B. für Wartemusik)

Das Ansagegerät muss sich wie ein Teilnehmer verhalten, d.h. sich melden, die Ansage einspielen und das Gespräch vermitteln (in Rückfrage gehen, wählen und auflegen).

Ansage-Varianten

Es sind folgende Ansage-Varianten verfügbar:

- Begrüßungsansage (Ansage vor Melden)

  Einem Anrufer kann vor Annahme des Anrufs eine Begrüßungsansage eingespielt werden.
- AutoAttendant

  Bei aktivem AutoAttendant kann einem Anrufer Musik und/oder weitere Ansagen eingespielt werden, falls er nicht sofort vermittelt werden kann.
- MFV-Durchwahl

  Bei aktiver MFV-Durchwahl wird einem Anrufer über eine Ansage eine Durchwahlmöglichkeit angeboten. Während der Ansage ist ein Codeempfänger aktiv, der die Nachwahl des Anrufers erkennt und weiterleitet.

Alternativen zur a/b-Schnittstelle (SLA-Baugruppen)

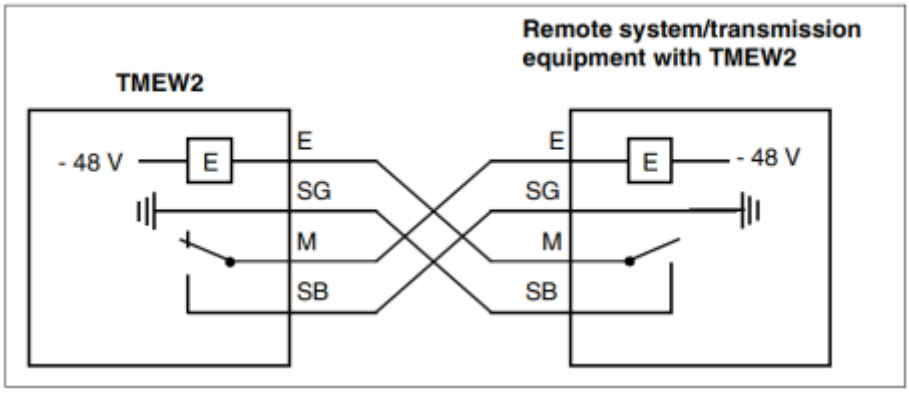
- OpenScape Business X8: TMEW2-Baugruppe
- OpenScape Business X5: STRB-Optionsbaugruppe
- OpenScape Business X3: STRBR-Optionsbaugruppe

Ansageverzögerung

Die Ansageverzögerung gibt an, nach welcher Zeit (0-600s einstellbar) ein wartender Ruf auf ein Ansagegerät weitergeschaltet wird.

Ansagegerät Genius

Für den Anschluss des Ansagegerätes Genius kann die TMEW2-Baugruppe auf Schnittstellentyp 2 eingestellt werden. Die Beschreibung zur TMEW2-Baugruppe sowie die Belegung der SIVAPAC-Stecker auf der Backplane bei Anschluss des Ansagegerätes Genius finden Sie in der Servicedokumentation, Montage der Hardware im Kapitel "Baugruppen".



Die Konfiguration des Ansagegeräts Genius erfolgt mit dem Manager E über **Anlagensicht** > **Einstellungen** > **Anschaltungen** > **Ansage**.

22.1.1 Wie Sie ein analoges Ansagegerät hinzufügen

Voraussetzungen

Das Ansagegerät ist an eine analoge Schnittstelle angeschlossen.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Endgeräte / Teilnehmer**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Analog-Endgeräte** zu starten. Es wird Ihnen eine Liste aller analogen Teilnehmer angezeigt.
4) Tragen Sie in der Zeile des Ansagegeräts Namen und Rufnummern ein.
5) Treffen Sie bei Bedarf in der Zeile des Ansagegeräts weitere Einstellungen.
6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

22.1.2 Wie Sie die Ansageverzögerung ändern

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

Anlagensicht, Menü **Einstellungen** > **Systemparameter** > **Zeitparameter**: in der Tabelle bei dem Eintrag **Verzögerungszeit bis zur Ansage vor Melden aus** die **Basis** und den **Multiplikationsfaktor** der Ansageverzögerung an die eigenen Wünsche anpassen (Standard: 100ms x 20).

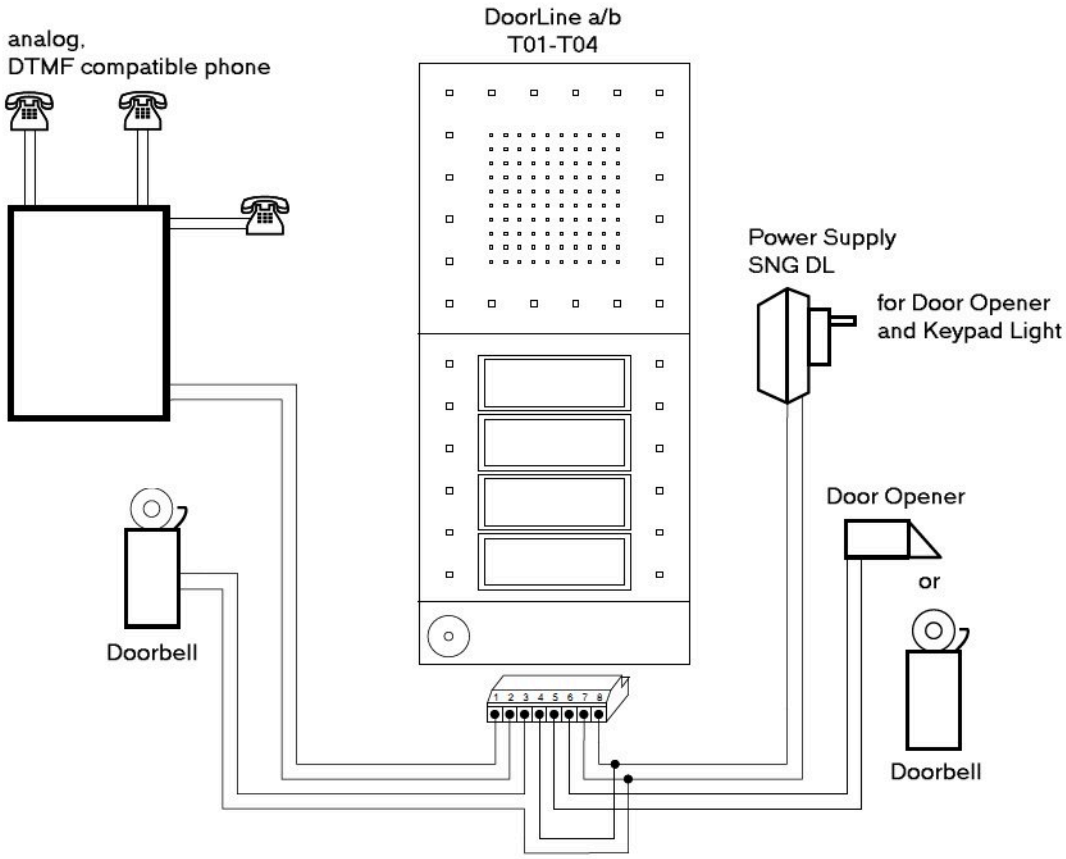
22.2 Türsprechstelle und Türöffner

Türsprechstellen (TFE) werden heute in einer vielfältigen Auswahl von diversen Herstellern angeboten. Dabei sind die Anschlussvarianten ausschlaggebend für die Bedienung und die Funktionalität einer jeden TFE. Beispielhaft ist hier die Doorline a/b T01-T04 beschrieben, wobei sich Türsprechstellen von Behnke, Keil, 2n EntryCom, Auerswald, etc ähneln.

22.2.1 DoorLine a/b T01-T04

Die Türsprechstelle DoorLine a/b T01-T04 wird an eine analoge Schnittstelle angeschlossen. Ausgerüstet mit 1 bis 4 Klingeltastern (je nach Ausführung) können mehrere unabhängige Wohn- und Geschäftsbereiche erreicht werden. Sie kann aber nicht nur von jedem Telefon aus bedient werden, sondern bietet darüber hinaus auch den Anschluss für die Stromversorgung des Türöffners.

Durch die 2-Draht-a/b-Technik ist die DoorLine a/b T01-T04 schnell und einfach zu montieren. Für die Abstimmung zum Kommunikationssystem kann das Wahlverfahren eingestellt und der Sprechweg abgeglichen werden. Die Türöffnung erfolgt über Kennziffer der Doorline (z.B. #9). Ein spezielles Anschaltmodul wie Doorline M02, M03, M06 und M06/1 ist nicht mehr notwendig.



Anmerkung: Für dies Türsprechstelle ist keine weitere Einstellung in OpenScape Business notwendig. Aus Sicherheitsgründen empfiehlt es sich, die Nebenstelle als "Nichtamt" oder als "Halbamt" zu konfigurieren.

22.2.1.1 Wie Sie den Teilnehmerport der Doorline a/b T01-T04 konfigurieren

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Anlagensicht**, Menü **Einstellungen** > **Station einrichten** > **Teilnehmer**: für den Teilnehmerport den Typ **Standard** auswählen.
2) **Teilnehmersicht**, Registerkarte **Flags**: für den Teilnehmerport das Flag **Anklopfschutz ein** aktivieren.
3) **Anlagensicht**, Menü **Einstellungen** > **Systemparameter**, Registerkarte **Flags**: das Flag **DTMF automatisch** aktivieren.

22.2.1.2 Wie Sie die Nebenstelle für die Doorline a/b T01-T04 konfigurieren

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Teilnehmersicht**, Registerkarte **Flags**: für die Nebenstelle das Flag **Anklopfschutz ein** deaktivieren.
2) **Teilnehmersicht**, Registerkarte **Flags**: für die Nebenstelle das Flag **Anruferliste ausgeben** aktivieren.

22.2.2 DoorCom Analog

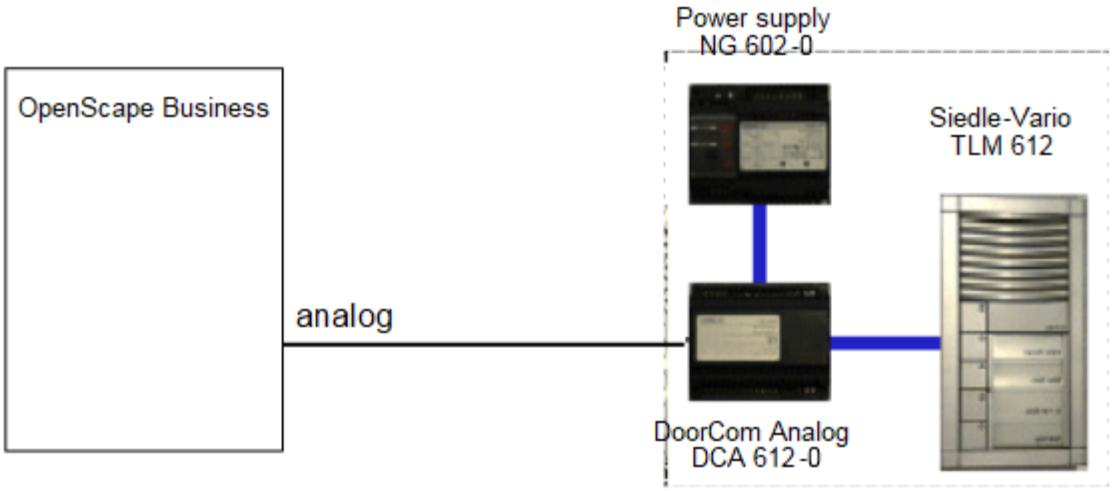
Bei der DoorCom® Analog handelt es sich um eine universelle TFE-Adapterbox für die Tür- und Torsprechstellen der Firma Siedle (zum Beispiel Vario TLM 612).

Die DoorCom® Analog wird an eine analoge Schnittstelle des Kommunikationssystems angeschlossen. Sie verhält sich wie ein analoges Telefon mit MFV-Wahl, MFV-Erkennung und MFV-Steuerung. Die Steuerung ist nur über MFV-Zeichen möglich.

DoorCom Analog ist ausschließlich in Verbindung mit folgenden Komponenten funktionsfähig:

- DoorCom Analog DCA 612-0
- Tür- und Torsprechstelle Siedle-Vario TLM 612
- Schalt-Fernsteuer Interface DCSF 600

  Für die Sprachverbindung von einem internen Teilnehmer zur Tür- und Torsprechstelle. Ohne dieses Modul ist kein Zurückrufen der Tür- und Torsprechstelle möglich, z.B. wenn ein Anruf von der Tür- und Torsprechstelle versehentlich ausgelöst wurde.
- Netzteil NG 602-0



Es besteht die Möglichkeit, die Steuerfunktionen des Gerätes (Tür öffnen, Türsprechstelle anwählen, ...) auf die Prozedurtasten eines Telefons zu programmieren. Die dort gespeicherte MFV-Zeichenfolge wird dann zur Türsprechstelle/Türöffner gesendet.

Anmerkung: Für dies Türsprechstelle ist keine weitere Einstellung in OpenScape Business notwendig. Aus Sicherheitsgründen empfiehlt es sich, die Nebenstelle als "Nichtamt" oder als "Halbamt" zu konfigurieren.

22.2.2.1 Wie Sie den Teilnehmerport der DoorCom Analog konfigurieren

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Anlagensicht**, Menü **Einstellungen** > **Station einrichten** > **Teilnehmer**: für den Teilnehmerport den Typ **Standard** auswählen.
2) **Teilnehmersicht**, Registerkarte **Flags**: für den Teilnehmerport das Flag **Anklopfschutz ein** aktivieren.
3) **Anlagensicht**, Menü **Einstellungen** > **Systemparameter**, Registerkarte **Flags**: das Flag **DTMF automatisch** aktivieren.

22.2.2.2 Wie Sie die Nebenstelle für die DoorCom Analog konfigurieren

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Teilnehmersicht**, Registerkarte **Flags**: für die Nebenstelle das Flag **Anklopfschutz ein** deaktivieren.
2) **Teilnehmersicht**, Registerkarte **Flags**: für die Nebenstelle das Flag **Anruferliste ausgeben** aktivieren.

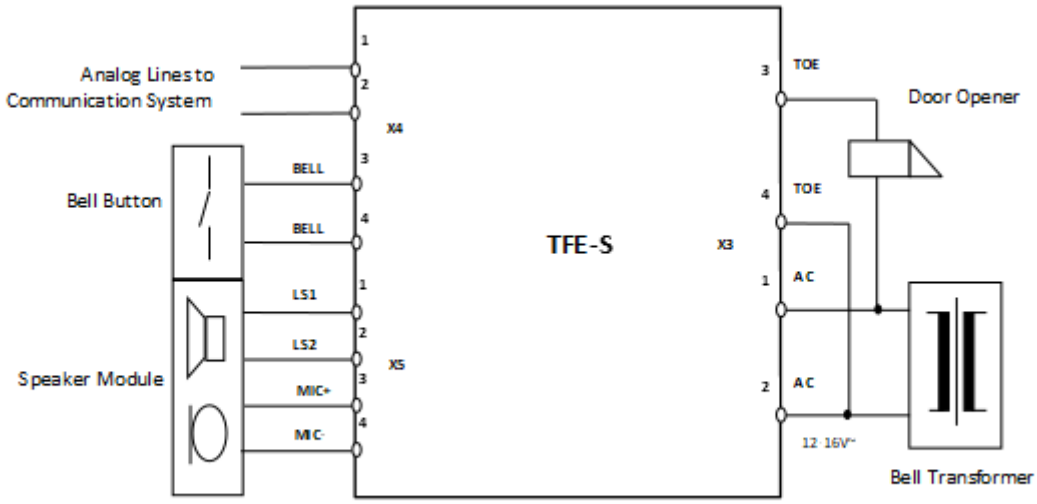
22.2.3 Türfreisprecheinrichtung mit Verstärker (TFE-S)

Das TFE-S Modul (S30122-K7696-T313) verbindet eine analoge Schnittstelle des Kommunikationssystems mit einer Türfreisprecheinrichtung, einem Türöffner und einem Klingeltaster. Die Steuerung erfolgt über das Kommunikationssystem.

Damit ist ein Anschluss an passive Türsprechstellen möglich, die mit folgenden Typen vergleichbar sind:

- Fa. Siedle (TLM511-01, 611-01)
- Fa. Rito (5760)
- Fa. Grothe (TS6216)

Die Verstärkung ist manuell einstellbar. Das TFE-S-Modul benötigt eine eigene Stromversorgung.



Technische Daten

Parameter	Wert
Stromversorgung	Klingeltrafo 12V - 16V AC, 50Hz
Stromaufnahme	Max. 150mA
Schnittstelle OpenScape Business	Analoger Teilnehmer
Abmessungen	100mm x 160mm
Umgebungstemperatur	0°C bis +45°C

Funktionsbeschreibung

Das Betätigen der Türklingel wird einem definierten Teilnehmer (Türrufzielstelle) an seinem Telefon als Anruf signalisiert. Nimmt der Teilnehmer den Anruf an, wird eine Sprechverbindung zur Türsprechstelle aufgebaut. Zusätzlich kann der Teilnehmer an seinem Telefon den Türöffner aktivieren.

Wenn die Türrufzielstelle nicht erreichbar ist, erfolgt ein Abwurf. Ist die Abwurfstelle nicht frei, erfolgt ein Systemsuchlauf über alle Systemtelefone.

Tipp: Bei der Signalisierung eines Türrufs wird die Nachtschaltung nicht berücksichtigt.

Tipp: KWZ ist an der Türsprechstelle nicht nutzbar.

Konfigurationsmöglichkeiten

Folgende Konfigurationsmöglichkeiten stehen zur Verfügung:

- Türöffner:

  Der Türöffner wird über eine a/b-Schnittstelle eingerichtet. Hierfür muss an der Türsprechstelle eine Adapterbox angeschaltet werden. Der Teilnehmer kann dadurch die Tür, durch einen einfachen Tastendruck am Telefon, während der Verbindung mit der Türstelle öffnen.
- MFV (DTMF):

  Hier wird festgelegt, ob der Türöffner mit einem MFV-Sender aktiviert wird (MFV: Mehrfrequenzwahlverfahren), d.h. die Türrufzielstelle kann die Tür durch MFV-Nachwahl öffnen.
- Anrufumleitung (AUL):

  Hier wird festgelegt, ob der Ruf von der Türsprechstelle einer externen Anruf-umleitung der Zielstelle folgen soll.

22.2.3.1 Wie Sie die Türsprechstelle konfigurieren

Mit dem Wizard **Türsprechstelle** können Sie festlegen, welche Teilnehmer den Türöffner betätigen können. Sie können bis zu zehn Türsprechstellen konfigurieren.

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Türsprechstelle** zu starten. Das Fenster **Türsprechstelle ändern** wird angezeigt.
4) Wählen Sie eine bzw. mehrere **Sprechstellen** aus.
5) Geben die **Zielstelle** ein.
6) Aktivieren Sie im Kontrollkästchen die zugehörigen Funktionen wie **Türöffner**, **DTMF** und **AUL**.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.
8) Führen Sie die Schritte 1 bis 7 für jede zu konfigurierende Türsprechstelle aus.

22.2.4 Lautsprecher

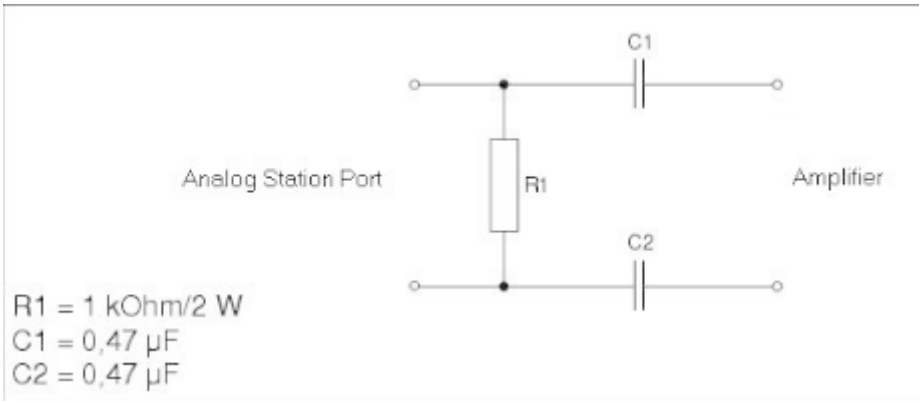
Lautsprecher können über Verstärker an das Kommunikationssystem angeschlossen werden.

Für den Anschluss eines Verstärkers inkl. Lautsprecher bestehen folgende Möglichkeiten:

- **Anschluss des Verstärkers an eine analoge Teilnehmer-Schnittstelle**

  Evtl. ist hierfür eine Pegelanpassung des Verstärkers erforderlich.

Evt. ist zusätzlich ein Schleifenwiderstand nach folgender Schaltung zu verwenden:



- **Anschluss des Verstärkers an das TFE S Modul**

  Ein ein aktiver Verstärker/ Verstärkeranlage lässt sich über das TFE S Modul anschalten. Der Verstärkereingang wird an den Lautsprecherausgang des TFE S Modules angeschlossen.

  Evt. ist noch ein Kontakt der STRB-Baugruppe erforderlich, um den Verstärker einzuschalten oder das Eingangssignal durchzuschalten (Unterdrückung von Störgeräuschen).

22.2.4.1 Wie Sie die analoge Teilnehmer-Schnittstelle für einen Lautsprecher konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Teilnehmer**.
3) Klicken Sie im Menübaum auf **Teilnehmer** > **Analoge Teilnehmer**.
4) Wählen Sie den gewünschten analogen Teilnehmer aus (z.B. 3011).
5) Ändern Sie in der Registerkarte **Teilnehmer-Parameter ändern** die Daten des analogen Teilnehmers wie benötigt.

6) Wählen Sie in der Aufklappliste **Stationstyp** den Eintrag **Lautsprecher** aus.
7) Klicken Sie auf **Übernehmen**.

22.2.4.2 Wie Sie die analoge Teilnehmer-Schnittstelle für den Anschluss eines Verstärker am TFE S Modul konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Türsprechstelle** zu starten. Das Fenster **Türsprechstelle ändern** wird angezeigt.
4) Wählen Sie eine **Sprechstelle** aus.
5) Wählen Sie die **Zielstelle** aus.
6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

22.3 Aktoren

Aktoren sind Steuerausgänge und werden durch Steuersignale des Kommunikationssystems aktiviert oder deaktiviert. Sie bewirken eine Zustandsänderung der angeschalteten Einrichtung und unterstützen Funktionen zum Überwachen, Alarmieren, Steuern und Regeln. Sie werden hauptsächlich in Sicherheits- und Hausverwaltungssystemen eingesetzt (z.B. für Türöffner).

Aktoren sind auf optionalen Steuerrelais-Baugruppen enthalten. Alle Steuerrelais-Baugruppen enthalten 4 Steuerausgänge (Aktoren).

Mögliche Steuerrelais-Baugruppen:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

Die genaue Beschreibung dieser Baugruppen inkl. der Belegungen finden Sie in der Servicedokumentation im Kapitel "Baugruppen".

Für die Steuerung der Aktoren gibt es folgende Möglichkeiten:

- vom Telefon aus über Kennzahlen
- vom Systemtelefon aus über eine Taste
- per Fernzugriff über die Amtsleitung (DISA) durch den der Relaisfunktion zugewiesenen Teilnehmer
- per Fernzugriff über das Leistungsmerkmal "Assoziierte Dienste"

Aktoren können durch folgende Funktionen aktiviert oder deaktiviert werden:

Anmerkung: Die Kennzahlen für die Steuerung finden Sie im Kapitel "Experten-Modus".

- **Ohne Funktion**

  Der Aktor ist entweder nicht in Betrieb oder als zentraler Wecker eingetragen (unter "Einstellungen" - "Kommende Rufe" - "Rufziellisten").
- **Manuell ein und aus**

  Der Aktor kann über Taste oder Kennzahl "Ausgewählter Schalter ein- bzw. ausschalten" aktiviert oder deaktiviert werden. Diese Funktion kann einem Teilnehmer, einer Gruppe oder alle Teilnehmer zugewiesen werden.
- **Autom. nach Zeit aus**

  Der Aktor kann als Zeitschalter über Taste oder Kennzahl "Ausgewählter Schalter ein- bzw. ausschalten" aktiviert oder deaktiviert werden. Diese Funktion kann einem Teilnehmer, einer Gruppe oder alle Teilnehmer zugewiesen werden. Wird als Schaltzeit ein Wert größer als 0 eingegeben, wird der Aktor erst nach Ablauf dieser Schaltzeit deaktiviert.
- **Türöffner**

  Der Aktor kann als Türöffner über Taste oder Kennzahl "Ausgewählter Schalter ein- bzw. ausschalten" aktiviert oder deaktiviert werden. Diese Funktion kann einem Teilnehmer, einer Gruppe oder alle Teilnehmer zugewiesen werden. Wird als Schaltzeit ein Wert größer als 0 eingegeben, wird der Aktor erst nach Ablauf dieser Schaltzeit deaktiviert. Allen zugeordneten Endgeräten wird im Display der Text “Türöffner” angezeigt. Beispiel für den Faktor der Schaltzeit: 30*100ms = 3 sec.
- **Lsp.-Verstärker**

  Der Aktor wird aktiviert, wenn eine Verbindung zur Türsprechstelle/Torstelle/ Lautsprecherbox aufgebaut wird. Er wird deaktiviert, sobald die Verbindung getrennt wird. Hiermit kann ein Türsprechstellenverstärker gesteuert werden, damit dieser nur im Bedarfsfall eingeschaltet wird. Dieser Funktion muss die Türsprechstelle oder der Lautsprecherport zugeordnet werden.
- **Besetztanzeige**

  Der Aktor wird aktiviert, wenn der zugeordnete Teilnehmer den Ruhezustand verlässt (Hörer abgenommen oder Lautsprecher aktiviert oder Endgerät des Teilnehmers wird angerufen). Der Aktor wird deaktiviert, wenn sich der zugeordnete Teilnehmer wieder im Ruhezustand befindet. Der Aktor kann auch direkt über Taste oder Kennzahl "Ausgewählter Schalter ein- bzw. ausschalten" oder eine Taste aktiviert werden. In diesem Fall wird der Status des zugeordneten Teilnehmers ignoriert und der Aktor kann nur mittels Taste oder Kennzahl wieder deaktiviert werden. Dieser Funktion muss ein bestimmter Teilnehmer zugeordnet werden. Beispiel Türbesetztanzeige: Telefoniert der Chef, geht eine Lampe über der Türe des Chefs an, die signalisiert, dass der Chef nicht gestört werden will.
- **Wartemusik**

  Der Aktor wird aktiviert, wenn sich mindestens ein Teilnehmer oder eine Leitung des Kommunikationssystems nicht im Ruhezustand befindet.
  In diesem Fall wird ein Ansagegerät oder ein CD-Player aktiviert.
  Der Aktor wird deaktiviert, wenn alle Teilnehmer und Leitungen des Kommunikationssystems sich im Ruhezustand befinden. Dieser Funktion kann nur allen Teilnehmern zugeordnet sein und darf nur einmal im Kommunikationssystem vorhanden sein. Als Schaltzeit muss ein Wert größer als 0 eingegeben werden (z.B. 600*100ms = 60 sec). Der Aktor ist so lange aktiv und spielt Musik, bis die Schaltzeit abgelaufen ist oder der Aktor per Steuersignal deaktiviert wird.

- **Zweitwecker**

  Der Aktor wird für den zugeordneten Teilnehmer aktiviert, wenn dieser angerufen wird. Mit dem Melden bzw. Rufende wird der Aktor wird deaktiviert. Der Aktor ist nicht getaktet. Dieser Funktion muss ein bestimmter Teilnehmer zugeordnet werden. Wird als Schaltzeit ein Wert größer 0 eingegeben, wird eine Ausschalteverzögerung erreicht. Die Schaltzeit ist ein Vielfaches von 3 Sekunden.
- **Gebühren-Impuls**

  Der Aktor wird anhand der eintreffenden Gebührenimpulse oder Gebührenmeldung(en) entsprechend der Anzahl für den zugeordneten Teilnehmer getaktet. Dieser Funktion muss ein bestimmter Teilnehmer zugeordnet werden. Die Schaltzeit ist mit 150 ms Puls und 150 ms Pause nicht änderbar.
- **Teilnehmer aktiv**

  Der Aktor wird aktiviert, wenn der zugeordnete Teilnehmer aktiv ist (Hörer abgenommen oder Lautsprecher aktiviert). Der Aktor wird deaktiviert, wenn sich der zugeordnete Teilnehmer wieder im Ruhezustand befindet. Dieser Funktion muss ein bestimmter Teilnehmer zugeordnet werden.

Aktornamen

Den Aktoren können beliebige Namen (max. 16 Zeichen) zugewiesen werden.

22.3.1 Wie Sie einen Aktor konfigurieren

Voraussetzungen

Eine Steuerrelais-Baugruppe ist gesteckt.

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Anlagensicht**, Menü **Einstellungen** > **Anschaltungen** > **Aktoren**: unter **Aktoren-Liste** den zu konfigurierenden Aktor auswählen.
2) **Anlagensicht**, Menü **Einstellungen** > **Anschaltungen** > **Aktoren**: unter **Aktor-Typ** die Funktion für den Aktor auswählen.
3) **Anlagensicht**, Menü **Einstellungen** > **Anschaltungen** > **Aktoren**: im Feld **Aktor-Name** einen frei wählbaren Namen für den Aktor eingeben (max. 16 Zeichen).
4) Wenn der Funktion ein Teilnehmer, eine Gruppe oder alle Teilnehmer zugeordnet werden sollen, ist im Bereich **zugeordneter Teilnehmer** in der Liste **Rufnummer** die Rufnummer des Teilnehmers oder die Gruppenrufnummer auszuwählen.

   Für alle Teilnehmer ist der Eintrag **keine** auszuwählen.
5) Wenn die Funktion eine Schaltzeit erfordert, ist im Bereich **Schaltzeit** im Feld **Faktor** der Faktor einzugeben, der mit dem angezeigten Wert multipliziert wird.

   Mögliche angezeigte Werte sind 100ms und 3s.

22.4 Sensoren

Sensoren sind Steuereingänge und erkennen eine Zustandsänderung der angeschalteten Einrichtung. Sie können Funktionen des Kommunikationssystems aktivieren oder deaktivieren und unterstützen somit Funktionen zum Überwachen, Alarmieren, Steuern und Regeln. Sie werden hauptsächlich in Sicherheits- und Hausverwaltungssystemen eingesetzt (z.B. für Temperaturüberwachung oder Bewegungsmelder).

Sensoren sind auf optionalen Steuerrelais-Baugruppen enthalten. Alle Steuerrelais-Baugruppen enthalten 4 Steuereingänge.

Mögliche Steuerrelais-Baugruppen:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

Die genaue Beschreibung dieser Baugruppen inkl. der Belegungen finden Sie in der Servicedokumentation im Kapitel "Baugruppen".

Sensoren können folgende Funktionen aktivieren oder deaktivieren:

Anmerkung: Die Kennzahlen für die Steuerung finden Sie im Kapitel "Experten-Modus".

- Rufsignalisierung an Telefonen
- Displaymeldung an Systemtelefonen
- Ein-/Ausschalten eines Ansagegerätes
- Steuerung eines Anrufbeantworters
- Automatische Wahl mit einer vordefinierten Rufnummer (interne Rufnummer, Gruppenrufnummer oder externe Zielrufnummer)
- Aktivierung der folgenden Dienste für eine Rufnummer (mit Code + Rufnummer):
  - Aktor ein-/aus
  - Anrufschutz
  - Anrufumleitung ein/aus
  - Codeschloss ein/aus
  - Mitteilungstexte senden
  - Mitteilungstexte zurückziehen
  - Nachtbetrieb ein/aus
  - Rufübergabe ein/aus
- Direkte Aktivierung folgender Dienste (nur mit Rufnummer):
  - Aktor ein-/aus
  - Kurzwahlsystem verwenden
- Fehlersignalisierung - möglich ist
  - die Ausgabe einer programmierbaren Fehlermeldung (Sensorname, max. 10 Zeichen: z.B. Temp-Alarm) am Display eines bestimmten Systemtelefons (keine akustische Signalisierung).
  - der Anruf bei einem bestimmten Systemtelefon mit Fehlermeldung im Display während des Anrufs (Zielrufnummer)
  - ein Fehlereintrag in der Error History (Eintrag im Fehlerspeicher = aktivieren)

Zielrufnummer

Ein zugeordneter analoger Port ist für die Sensoren programmierbar. Dieser Port wird vom System gerufen, sobald ein Verbindungsaufbausignal empfangen wird. Der rufende Teilnehmer umgeht daraufhin diesen Anschluss. Über einen an diese Schnittstelle angeschlossenen Anrufbeantworter kann eine Sprachansage angeschaltet werden, die dem angewählten Teilnehmer das Ansprechen des Sensors mitteilt. Ein auf diese Weise programmierter analoger Port kann von außerhalb nicht angesprochen werden. Wurde für einen Sensor eine externe Rufnummer programmiert, für einen analogen Port jedoch nicht, dann wird die externe Verbindung zwar hergestellt, aber kein akustisches Signal im Zusammenhang mit dem Ansprechen des Sensors übermittelt. Erforderlichenfalls kann der gerufene Teilnehmer jedoch anhand der Rufnummer (CLIP) den Ursprung des Anrufs feststellen.

Steuerdateneingabe

Eingabe der Steuerzeichenkette mit maximal 24 Zeichen für das Phonemail-System (Briefkasten-Rufnummer). Sobald die Verbindung hergestellt ist, wird die Steuerzeichenkette an den Ansage-Port übermittelt. Ist kein Ansage-Port verfügbar, wird die Steuerzeichenkette an das Ziel übertragen.

23 Application Connectivity

Application Connectivity unterstützt das System z. B. mit CSTA, TAPI sowie mit Application Launcher.

23.1 CSTA

Die CSTA-Schnittstelle ermöglicht die Anbindung von hochperformanten CTI-, Contact Center- und Unified Communications-Applikationen etc. an OpenScape Business.

CSTA verwendet das Transmission Control Protocol (TCP). Es besteht eine feste Verbindung. Der Verlust von Datenpaketen wird erkannt und automatisch korrigiert.

Standards

Das implementierte CSTA-Protokoll beruht auf:

- ECMA-269 Services for Computer Supported Telecommunications Applications (CSTA) Phase III
- ECMA-285ASN.1 for Computer Supported Telecommunications Applications (CSTA) Phase III
- spezifischen Erweiterungen

Voraussetzungen

Die Nutzung von CSTA erfordert für das mit CSTA-Anwendungen verbundene System entweder UC Booster (Card oder Server) oder OpenScape Business S. Die Anmeldedaten für CSTA-Anwendungen müssen im System konfiguriert sein, um die CSTA-Schnittstelle automatisch zu aktivieren. Externe CSTA-Anwendungen müssen für ihren Zugriff diese Anmeldedaten verwenden.

Leistungsmerkmale

CSTA bietet folgende Leistungsmerkmale:

- Zugriff via Ethernet LAN (TCP/IP)
- CSTA Phase III, ASN.1 codiert
- Unterstützung des CSTA XML Protokolls für zertifizierte Applikationen
- Breite Palette von unterstützten Systemtelefonen
- Netzweites Monitoring und Steuerung aller Ressourcen
- Multiplexing für Monitorpunkte

Unterstützte Geräte

CSTA unterstützt zusätzlich zu den vom System unterstützten Telefonen folgende Geräte:

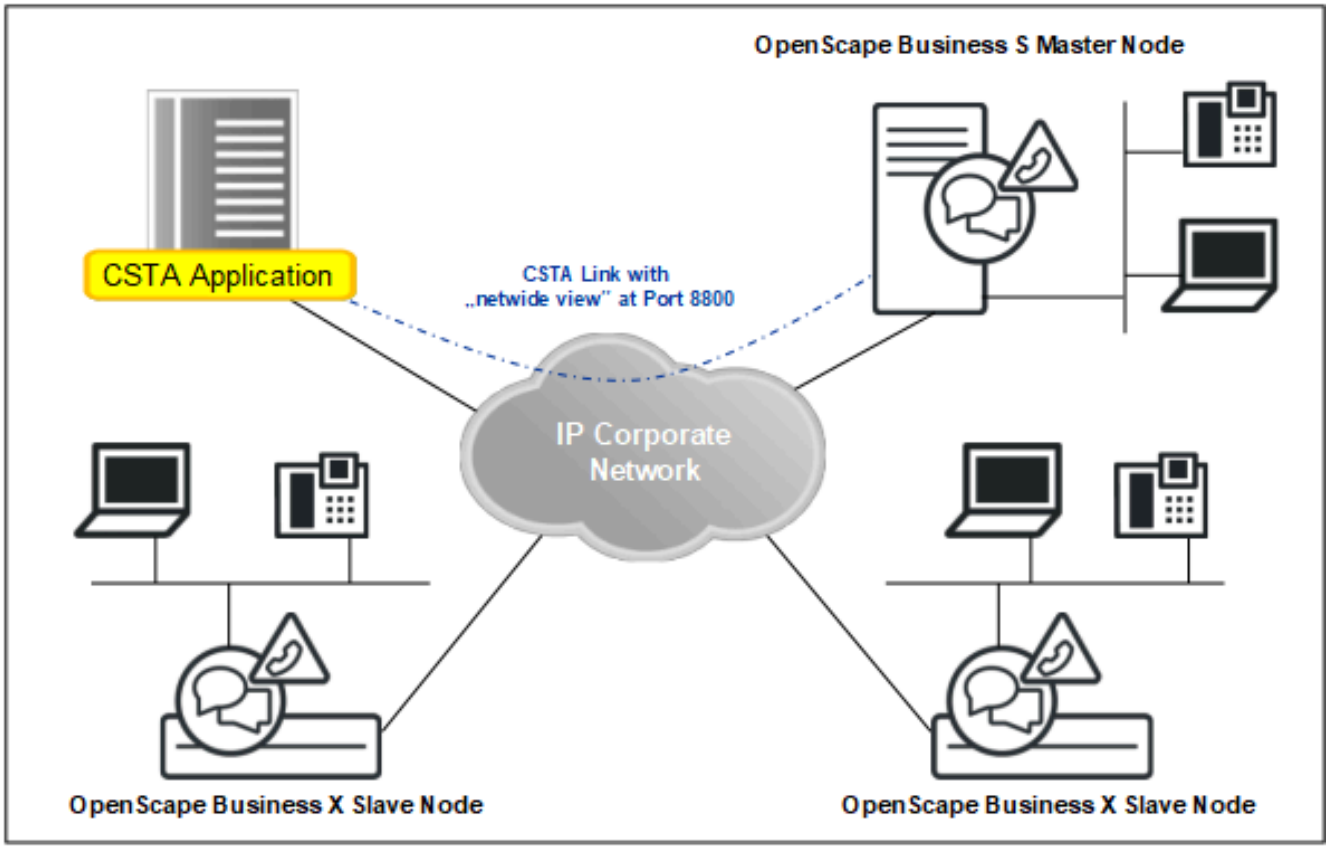
- ITSP

  ermöglicht z.B. die Nutzung von Call Center-Applikationen mit SIP-Amtsleitungen
- ISDN
- Amt analog
- Virtuelle Teilnehmer

- UCD-Gruppen
- MULAPs

Anmerkung: Details zu Leistungsmerkmalen und unterstützten Geräten finden Sie in CSTA Interface Manual.

Anschaltung für netzweite Sicht



Ports

Folgende Portnummern stehen standardmäßig zur Verfügung:

Port	Portnummer	Verwendung
CSP	8800	beliebige CSTA-Anwendung
CMD	8900	Reserviert für TAPI 120 Clients; unabhängig von der Anzahl der Clients wird genau ein logischer CSTA-Link belegt

Externe CSTA-Anwendungen bzw. TAPI 120 Service Provider müssen die IP-Adresse des UC Servers bzw. des Systems mit der entsprechenden Portnummer verwenden um die Verbindung herzustellen. Die entsprechende IP-Adresse wird im WBM unter Applikationsauswahl angezeigt.

CSTA-Links

Standardmäßig steht ein CSTA-Link des CSP Port für externe CSTA-Anwendungen zur Verfügung. Drei weitere CSTA-Links sind standardmäßig folgenden integrierten CSTA-Anwendungen bzw. Diensten zugeordnet:

- CMD (CSTA Message Dispatcher) für TAPI 120 Clients am CMD Port
- DSS (Direct Station Server)
- UC Suite

Falls diese CSTA-Anwendungen bzw. Dienste nicht benötigt werden, können bei Bedarf die entsprechenden CSTA-Links externen CSTA-Anwendungen zugeordnet werden.

Anmerkung: Ein CSTA-Link stellt den TDS-Dienst nur für lokale Geräte zur Verfügung. Kunden benötigen einen CSTA-Link zu jedem Knoten, der den TDS-Dienst bereitstellen soll.

Generell können CSTA-Anwendungen über CSP, über LAS (eine Systemkomponente) oder über PCC (eine LDH-Komponente) an ein OpenScape Business System angeschlossen werden.

Anmerkung: Wenn eine Anwendung über CSP angeschlossen wird, müssen auch die Anmeldeinformationen gegen CSP eingerichtet werden.

Insbesondere:

- Die (externen) Anwendungen UC Suite, OSCC, TAPI 170 und 3rd Party werden über CSP angeschlossen

  Die Anbindung von (externen) CSTA-Anwendungen von Drittanbietern, die Trunk-Informationen benötigen, kann nur im UC Suite-Modus oder durch Abfrage der Trunk-Überwachungspunkte selbst über CSTA in deren eigener Anwendung erfolgen.
- UC Smart wird über LAS angeschlossen

Plus-Produkte

Folgende Flags sind im System stets aktiviert:

- Vorwahl stets mit Rufnummer übertragen
- Erweitertes CSTA-CAUSE Handling
- CSTA CSP Signalisierung
- MULAP Monitoring

Zugehörige Konzepte

Unterstützte Telefone auf Seite 108

23.1.1 Wie Sie die Portnummer für CSTA ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Port-Verwaltung**.
4) Geben Sie in der Zeile für **CSP** im Eingabefeld der Spalte **Port-Nummer** die gewünschte Portnummer ein.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
6) Starten Sie das System neu.

Zugehörige Konzepte

OpenScape Business TAPI 120 auf Seite 1177

23.1.2 Wie Sie den CMD für die Nutzung von TAPI 120 aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Middleware**.
3) Klicken Sie im Menübaum auf **Middleware** > **CSTA Message Dispatcher (CMD)**.
4) Klicken Sie auf die Registerkarte **Einstellungen - CSTA Message Dispatcher (CMD)**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den CMD aktivieren möchten, aktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.
   - Wenn Sie den CMD deaktivieren möchten, deaktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie Auto Registration für Clients nutzen möchten, aktivieren Sie in Bereich **Autom Registrierung** das Kontrollkästchen **Autom. Registrierung des Clients aktiviert**.
   - Wenn Sie Auto Registration für Clients nicht nutzen möchten, deaktivieren Sie in Bereich **Autom Registrierung** das Kontrollkästchen **Autom. Registrierung des Clients aktiviert**.
7) Klicken Sie auf **Übernehmen**.

Zugehörige Konzepte

OpenScape Business TAPI 120 auf Seite 1177

23.1.3 Wie Sie den DSS-Server für die Nutzung von netzweiten DSS-Tasten aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Middleware**.
3) Klicken Sie im Menübaum auf **Middleware** > **DSS-Server**.
4) Klicken Sie auf die Registerkarte **Einstellungen - DSS-Server**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den DSS-Server aktivieren möchten, aktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Der Dienst wird automatisch gestartet**.
   - Wenn Sie den DSS-Server deaktivieren möchten, deaktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Der Dienst wird automatisch gestartet**.
6) Klicken Sie auf **Übernehmen**.

23.1.4 Wie Sie den CSP aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Middleware**.
3) Klicken Sie im Menübaum auf **Middleware** > **CSTA Message Dispatcher (CMD)**.
4) Klicken Sie auf die Registerkarte **Einstellungen - CSTA Service Provider (CSP)**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den CSP aktivieren möchten, aktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**. Geben Sie auch eine CSTA-Benutzer-ID und ein CSTA-Benutzer-Passwort ein, damit eine Applikation CSTA nutzen kann.
   - Wenn Sie den CSP deaktivieren möchten, deaktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.

   Anmerkung: Wenn CSP deaktiviert wird, kann TAPI 120 (über CMD), TAPI 170, DSS-Server und UC Suite nicht betrieben werden!
6) Klicken Sie auf **Übernehmen**.

23.1.5 Wie Sie Media Extension Bridge aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Middleware**.
3) Klicken Sie im Menübaum auf **Middleware** > **Media Extension Bridge (MEB)**.
4) Klicken Sie auf die Registerkarte **Einstellungen - Media Extension Bridge (MEB)**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie Media Extension Bridge nutzen möchten, aktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.
   - Wenn Sie diesen CSTA-Link freigeben möchten, deaktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.
6) Klicken Sie auf **Übernehmen**.

23.2 OpenScape Business TAPI 120/170

OpenScape Business TAPI 120 und OpenScape Business TAPI 170 sind neben CallBridge Collection zwei für die Systemarchitektur und Netzwerktopologie von OpenScape Business optimierte TAPI Service Provider (TSP), die TAPI-basierten Applikationen die Microsoft TAPI Schnittstelle für die Anbindung an das OpenScape Business Kommunikationssystem zur Verfügung stellen.

Die Anschaltung an OpenScape Business erfolgt ausschließlich über LAN. Hardware- und Software-Zusatzkomponenten, wie CSTA Message Dispatcher (CMD) oder CSTA Service Provider (CSP), werden zum Betrieb an OpenScape Business nicht mehr benötigt. Die Lizenzierung ist teilnehmer-bezogen und unterscheidet nicht zwischen OpenScape Business TAPI 120 oder TAPI 170 Teilnehmer. Die Lizenzierungspflicht beginnt mit dem ersten TAPI-Teilnehmer.

Die Wahl des geeigneten TAPI Services Providers hängt im wesenlichen von der Anzahl der anzuschaltenden Client PC mit TAPI-Applikationen und der vorhandenen IT-Infrastruktur sowie den verwendeten Telefonen ab.

- **CallBridge Collection**

  wird als klassischer First Party TAPI Serviceprovider an Systemtelefonen, die eine LAN- oder USB-Schnittstelle besitzen, eingesetzt. Sie eignet sich für Installationen mit nur wenigen PCs. Ein LAN ist für den Betrieb der CallBridge Collection nicht erforderlich. Die CallBridge Collection wird auf jedem PC installiert, auf dem eine TAPI-Applikation betrieben wird. Analoge, Cordless- sowie Systemtelefone ohne USB-/IP-Schnittstelle werden nicht unterstützt.

  TAPI-Anschaltungen über die CallBridge Collection ist nicht lizenziert.

- **OpenScape Business TAPI 120**

  wird vorzugsweise als First Party TAPI Serviceprovider in Microsoft-Netzwerken mit oder ohne Domain Controller eingesetzt, wenn auch analoge, Cordless- oder Systemtelefone ohne USB-/IP-Schnittstelle in Verbindung mit der TAPI-Applikation betrieben werden sollen. Der TAPI 120 Service Provider wird auf jedem PC Client installiert, auf dem eine TAPI-Applikation betrieben wird.

  TAPI-Anschaltungen über OpenScape Business TAPI 120 unterliegen der Lizenzierung innerhalb von OpenScape Business. Zur Anschaltung an OpenScape Business wird abhängig von der Betriebs-/Anschaltungsart entweder ein CSTA Link oder ein Link zum WebServices Interface benötigt - unabhängig davon, wie viele TAPI 120 Clients betrieben werden. Der TAPI-seitige Leistungsumfang hängt von der Betriebs-/Anschaltungsart ab.
- **OpenScape Business TAPI 170**

  ist ein klassischer "Third Party" TAPI Service Provider. Er wird auf einem Server im LAN installiert und zentral an das OpenScape Business System angeschaltet. TAPI 170 kann alternativ zum TAPI 120 eingesetzt werden, wenn ein Domain Controller im Microsoft-Netzwerk vorhanden ist. Bei der Nutzung der sogenannten Remote TAPI Funktion entfällt die Installation des TAPI Service Providers auf den Client PCs. Diese bietet bei Installationen mit vielen Client PCs deutliche Zeitvorteile. In den nachfolgenden Konstellationen ist OpenScape Business TAPI 170 jedoch zwingend zu verwenden.

  – Anbindung von TAPI-Teilnehmern an vernetzte OpenScape Business Systeme, wenn die TAPI-Teilnehmer in verschiedenen Knoten lokalisiert sind.
  – Anbindung von TAPI-Applikationen, die auf einem Terminalserver betrieben werden.
  – Anbindung von serverbasierenden TAPI-Applikationen.

  TAPI-Anschaltungen über OpenScape Business TAPI 170 unterliegen der Lizenzierung innerhalb von OpenScape Business. Zur Anschaltung an OpenScape Business wird ein CSTA Link benötigt, unabhängig davon, wie viele TAPI 170 Teilnehmer betrieben werden.

23.2.1 OpenScape Business TAPI 120

OpenScape Business TAPI 120 ist ein 1st Party Telephony Service Provider, der den Microsoft TAPI V2.1 Funktionsumfang unterstützt. OpenScape Business TAPI 120 ermöglicht Windows-basierten CTI-Applikationen ein an OpenScape Business angeschaltetes Systemtelefon zu monitoren und zu steuern.

OpenScape Business TAPI 120 kann alternativ über die CSTA-Schnittstelle (CSTA Modus) oder über das WebServices Interface WSI (UC Smart Modus) an OpenScape Business angeschaltet werden. Ein Mischbetrieb in der Anschaltung an einem System ist nicht möglich. Ist im OpenScape Business System eine UC Booster Card gesteckt oder ist ein UC Booster Server angeschaltet, kann TAPI 120 nur im CSTA Modus betrieben werden. Die Systemvoraussetzungen, die maximale Anzahl der TAPI-Teilnehmer und der TAPI-seitige Leistungsumfang hängt von den Betriebmodi ab.

OpenScape Business TAPI 120 Anschaltungen

Die OpenScape Business TAPI 120 Software wird auf einem Microsoft Windows Client PC installiert. Die Verbindung zum OpenScape Business System erfolgt über LAN. Eine physikalische Verbindung zwischen dem Windows PC und dem Telefon ist nicht erforderlich.

- **TAPI 120 CSTA Modus**

  Alle TAPI 120 Client PCs werden an denselben CSTA Link von OpenScape Business angeschaltet. OpenScape Business multiplext intern alle TAPI 120 Verbindungen.

  TAPI 120 im CSTA Modus unterstützt OpenScape Business X3/X5/X8 und OpenScape Business S.

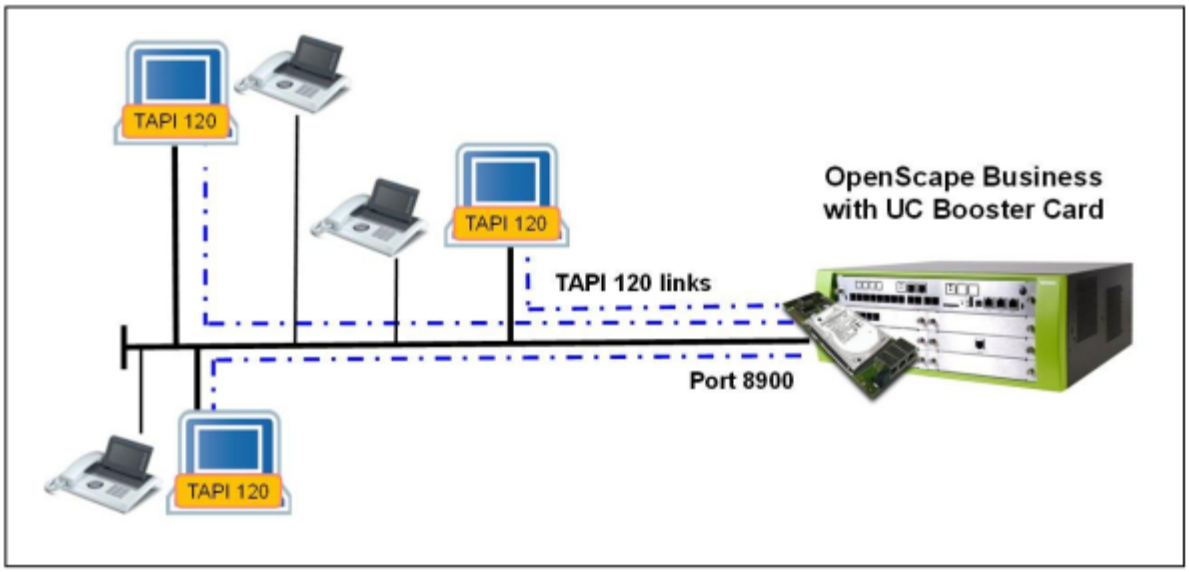


Abbildung 11: TAPI 120 im CSTA Modus mit OpenScape Business X5R und UC Booster Card

- **TAPI 120 UC Smart Modus**

  Alle TAPI 120 Client PCs werden über LAN und WebServer Interface an das Mainboard von OpenScape Business angeschaltet. OpenScape Business multiplext intern alle TAPI 120 Verbindungen.

  TAPI 120 im CSTA Modus unterstützt OpenScape Business X1/X3/X5/X8.

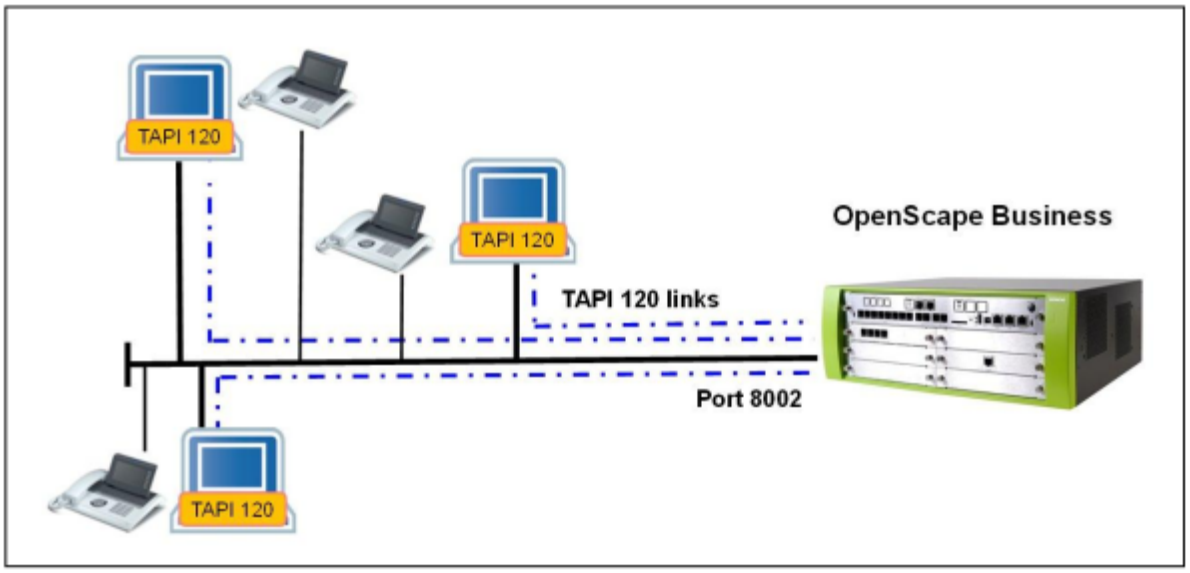


Abbildung 12: TAPI 120 im UC Smart Modus mit OpenScape Business X5R

Leistungsmerkmale

Folgende Leistungsmerkmale werden unterstützt:

Leistungsmerkmal	TAPI 120 CSTA	TAPI 120 UC Smart
Zentral über LAN angeschalteter First-Party TAPI Service Provider	X	X
Kompatibel mit dem Microsoft TAPI 2.1 Standard	X	X
Anschaltung an OpenScape Business Einzelsystemen	X	X
Unterstützung der OpenScape Business CTI Firewall	X	-
Über TAPI unterstützte Funktionen		
Rufsignalisierung kommender und gehender Gespräche mit Identifikation der Rufnummern und der Herkunft des Gespräches	X	X
Zusatzinformationen in der Rufsignalisierung bei umgeleiteten Gesprächen	X	X
Gesprächsannahme interner und externer Anrufe	X	X
gesteuerter Verbindungsaufbau zu internen und externen Gesprächspartnern	X	X
Manuelle Wahl / DTMF Nachwahl	X	X
Auslösung bestehender Gespräche	X	X

Leistungsmerkmal	TAPI 120 CSTA	TAPI 120 UC Smart
Aufbau eines Rückfragegespräches zu internen und externen Gesprächspartnern	X	X
Makeln	X	X
Begleitete Anrufübergabe	X	X
Begleitete Anrufübergabe mit nachfolgender Wahl des Rückfrageziels (One-Step Transfer)	X	X
Unbegleitete Anrufübergabe (Blind-Transfer)	X	-
Anrufumleitung setzen und löschen	X	X
Anrufschutz setzen und löschen	X	X
Konferenz einleiten	X	-
Konferenz erweitern	X	-
Kommenden Ruf weiterleiten	X	-
Gezielte Übernahme (Call Pickup)	X	-
Gruppenrufsignalisierung und Übernahme Gruppenruf (Group Pickup)	X	-
Parken von bestehenden Gesprächen	X	-
Wiederaufnahme geparkter Gespräche	X	-
Manuelles Halten von bestehenden Gesprächen	X	-
Wiederaufnahme manuell gehaltener Gespräche	X	-
Rückruf setzen	X	-
Unterstützung von Code-gesteuerten Funktionen	X	-
gesprächsbezogener Datenaustausch zwischen TAPI-Applikationen	X	-
Steuerung der Tasten bei Systemtelefonen (HFA)	X	-
Steuerung der Mikrofon-Verstärkung bei Systemtelefonen (HFA)	X	-
Steuerung/Auswahl der Nutzung von Handset/ Lautsprechen/Headset bei Systemtelefonen (HFA)	X	-
Steuerung der Lautstärke von Handset/Lautsprecher/ Headset Tastatur bei Systemtelefonen (HFA)	X	-
Zugriff auf optiPoint / OpenStage Displays und den LEDs (mit Limitierung auf 50 aktive Displays pro System)	X	-

Maximalwerte

Die maximal Anzahl von TAPI 120 Client PCs, die an OpenScape Business angeschlossen werden können ist modellabhängig (siehe Vertriebliche Ausbaustufen).

Freigegebene Betriebssysteme

Die aktuell freigegebenen Betriebssysteme für den Microsoft Windows Server, den Terminal-Server und den Remote Client PC sind in der aktellen Vertriebsinformation aufgelistet.

Es können nur Microsoft Windows Betriebssysteme in Verbindung mit TAPI 120 verwendet werden.

Bei Installationen auf Terminal-Servern ist OpenScape Business TAPI 170 anstelle von OpenScape Business TAPI 120 einzusetzen.

Lizenzierung

Die Verwendung von OpenScape Business TAPI 120 ist auf Teilnehmerbasis lizenziert. Die TAPI-Lizenzen werden im OpenScape Business System verwaltet und können für beide Modi von TAPI 120 verwendet werden. Bei Verwendung des Leistungsmerkmals MULAP ist für jeden Teilnehmer innerhalb der MULAP eine TAPI-Lizenz erforderlich.

Anmerkung: Bei TAPI 120 im UC Smart Modus sind keine UC User-Lizenzen erforderlich.

Software-Bereitstellung

Die OpenScape Business TAPI 120 Software wird auf einem eigenen Datenträger ausgeliefert. Sie ist nicht Bestandteil der OpenScape Business System Software.

Hardware-Anforderungen

Der PC muss mindestens den von Microsoft vorgegebenen Systemanforderungen für das eingesetzte Betriebssystem sowie den Anforderungen der TAPI-Applikation entsprechen. Zusätzlich wird ein Ethernet LAN Interface benötigt.

- Bei TAPI 120 CSTA

  Unabhängig von der Anzahl angeschalteter TAPI 120 Clients wird ein CSTA Link von OpenScape Business benötigt. Hierfür ist ein OpenScape Business UC Booster (Card oder Server) Voraussetzung.
- Bei TAPI 120 UC Smart

  Es wird das WebServices Interface benötigt. Es darf kein OpenScape Business UC Booster (Card oder Server) im/am System vorhanden sein.

Unterstützte Geräte

Die unterstützten Endgeräte wie auch die unterstützten Leistungsmerkmale an diesen Endgeräten hängen vom CSTA- bzw vom WSI-Funktionsumfang des eingesetzten OpenScape Business Systems ab. Diese Informationen sind in der OpenScape Business Vertriebsinformation enthalten.

Standardmäßig von TAPI 120 belegter IP-Port/IP-Adresse

In der Betriebsart TAPI 120 CSTA belegt der CSTA Link zur OpenScape Business den IP-Port 8900.

In der Betriebsart TAPI 120 UC Smart belegt der WSI-Link zur OpenScape Business den IP-Port 8802 für eine verschlüsselte Verbindung (HTTPS) oder 8801 für eine unverschlüsselte Verbindung (HTTP).

In der TAPI 120 Konfiguration muss die IP-Adresse des OpenScape Business Systems entsprechend der Betriebsart eingeben werden. Diese IP-Adresse wird im WBM unter **Applikationsauswahl** angezeigt.

Zugehörige Tasks

Wie Sie die Portnummer für CSTA ändern auf Seite 1173
Wie Sie den CMD für die Nutzung von TAPI 120 aktivieren oder deaktivieren auf Seite 1174

23.2.2 OpenScape Business TAPI 170

OpenScape Business TAPI 170 ist ein 3rd Party Telephony Service Provider, der den Microsoft TAPI V2.1 Funktionsumfang unterstützt. TAPI 170 ermöglicht Microsoft Windows basierenden CTI-Applikationen mehrere an OpenScape Business angeschaltete Telefone gleichzeitig zu monitoren und zu steuern.

Leistungsmerkmale

OpenScape Business TAPI 170 bietet folgende Leistungsmerkmale:

- Zentral angeschalteter 3rd Party TAPI Service Provider
- Kompatibel mit dem Microsoft TAPI 2.1 Standard
- Telefonie-Funktionen sind auf jedem angeschalteten PC Client über die TAPI 2.1 Client/Server Architektur verfügbar
- keine zusätzliche TSP Client Software erforderlich
- Unterstützte Telefoniefunktionen:
  - Kommende/gehende Wahl vom PC
  - Übertragung der kommenden Rufnummer, sofern signalisiert
  - Rückfrage und Übergeben
  - Makeln
  - Konferenz
  - Anrufumleitung
  - Anrufer weiterleiten
  - Annehmen eines Anrufs durch die Applikation
  - Auslösen eines Anrufs durch die Applikation
  - Übergabe vor/nach Melden
  - Übertragung von Leistungsmerkmalcodes
  - Monitoring des Telefons (Rufzustände, Ausfall, etc.)
  - Bereitstellung eines ACD-Interfaces
  - Monitoring/Zugriff auf Tastatur bei Systemtelefonen (HFA)
  - Ansteuerung von Display/LED bei Systemtelefonen (HFA)
  - Anschaltung an OpenScape Business Einzelsysteme sowie vernetzte Systeme
  - Unterstützung von MULAP-Teilnehmern/-Rufnummern

OpenScape Business TAPI 170 Anschaltungen

Die OpenScape Business TAPI 170 Software wird auf einem Microsoft Windows Server im Netzwerk installiert. Die Anbindung an OpenScape Business erfolgt über einen CSTA Link. Eine physikalische Verbindung zwischen dem Windows PC und dem Telefon ist nicht erforderlich. OpenScape Business TAPI 170 kann in unterschiedlichen Betriebsarten an Einzelsystemen oder im OpenScape

Business Netzwerk eingerichtet werden. TAPI Server und Clients müssen vom gleichen Netzwerk Domain Controller verwaltet werden.

- **Anschaltung serverbasierter TAPI Applikationen an OpenScape Business über TAPI 170**

  Die Server-Applikation und die TAPI 170 Software werden auf dem sogenannten "Telefonie-Server" im Netzwerk installiert. Die Server-Applikation stellt ihren zugehörigen Clients im Netzwerk die Telefoniefunktionen für die Teilnehmer zur Verfügung, die innerhalb von OpenScape Business TAPI 170 konfiguriert sind. Die TAPI 170 Software wird über LAN an die CSTA Schnittstelle von OpenScape Business angebunden. Für diese Anschaltung wird ein CSTA Link von OpenScape Business sowie je eine TAPI-Lizenz für jeden eingerichteten TAPI-Teilnehmer benötigt.

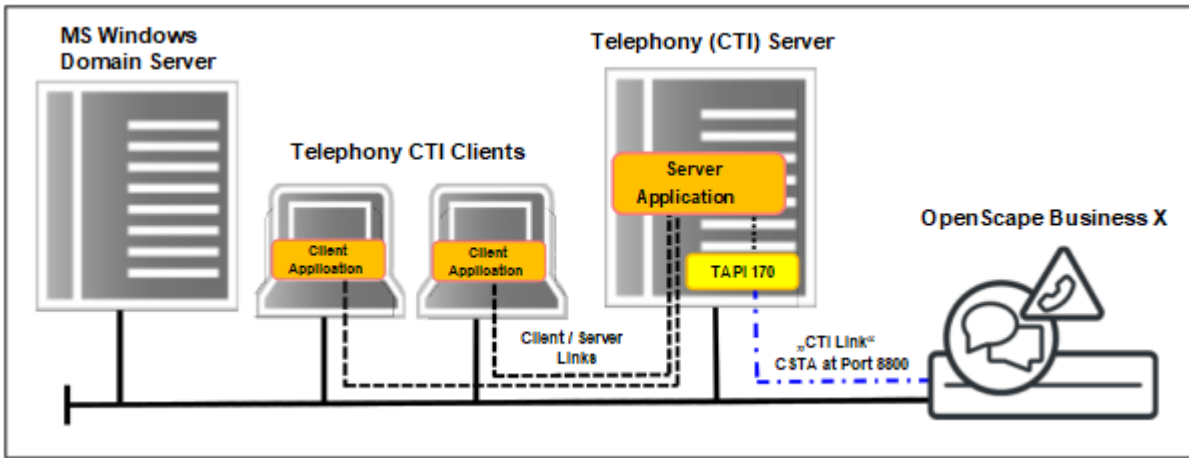


Abbildung 13: Serverbasierte TAPI-Applikation über TAPI 170 an OpenScape Business

- **Anschaltung clientbasierter TAPI-Applikationen an OpenScape Business über TAPI 170 mit "Remote TAPI" Funktion**

  In diesem Szenario wird die OpenScape Business TAPI 170 Software auf einem Server im Netzwerk installiert. Auf den Client PCs mit den TAPI-Applikationen wird sogenannte "Remote TAPI" Funktion freigeschaltet, über die die TAPI-Applikation auf dem Client mit der TAPI 170 Software auf dem Server kommuniziert. Auf den Client muss hierzu keine TAPI 170 Software installiert werden. Die TAPI 170 Software wird über LAN an die CSTA Schnittstelle von OpenScape Business angebunden. Für diese Anschaltung

wird ein CSTA Link von OpenScape Business sowie je eine TAPI-Lizenz für jeden eingerichteten TAPI-Teilnehmer benötigt.

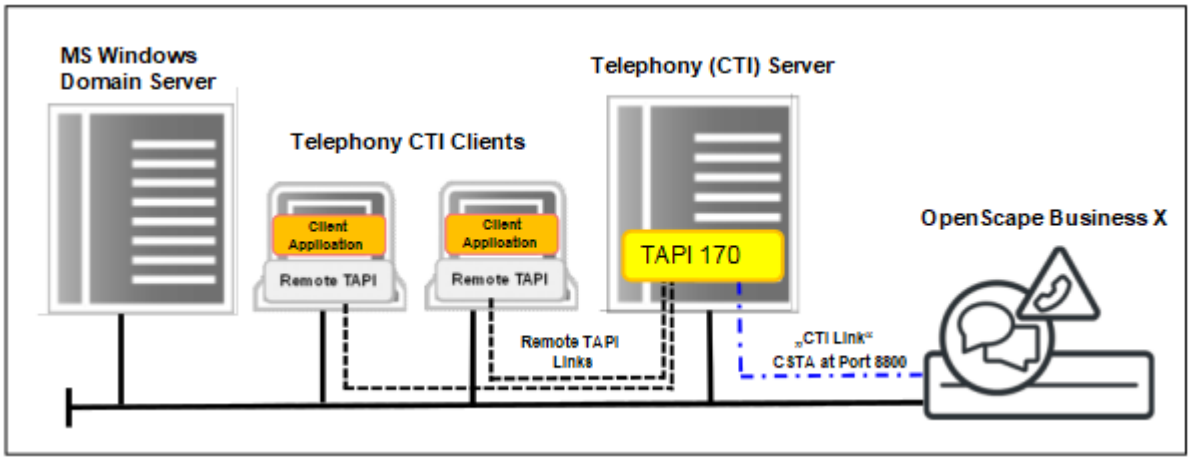


Abbildung 14: Clientbasierte TAPI-Applikation über "Remote TAPI" an OpenScape Business

- **Anschaltung Terminal-Server basierter TAPI-Applikationen an OpenScape Business über TAPI 170**

  In diesem Szenario sind die Client basierten TAPI-Applikationen auf einem oder mehreren Terminal-Servern installiert. Die TAPI 170 Software wird in diesen Fall mit auf dem Terminal-Server installiert. Im Fall eines aus mehreren Terminal-Servern bestehenden Clusters muss die TAPI 170 Software auf jedem Terminal-Server im Cluster installiert werden. Jede installierte TAPI 170 Software wird über LAN an OpenScape Business angebunden. Für jede auf einem Terminal-Server installierte TAPI 170 Software wird ein CSTA Link von OpenScape Business benötigt. Weiterhin ist eine TAPI Lizenz für jeden eingerichteten TAPI Teilnehmer erforderlich.

  Die maximal mögliche Anzahl von OpenScape Business TAPI 170 Servern in Verbindung mit OpenScape Business darf nicht überschritten werden.

  Anmerkung: Es können nur so viele Terminal-Server im Cluster bedient werden wie freie CSTA Links innerhalb von OpenScape Business zur Anschaltung der TAPI 170 Software zur Verfügung stehen. Der Maximalwert der möglichen Anschaltungen verringert sich, wenn die CSTA

Links von OpenScape Business durch andere CSTA Applikationen belegt sind.

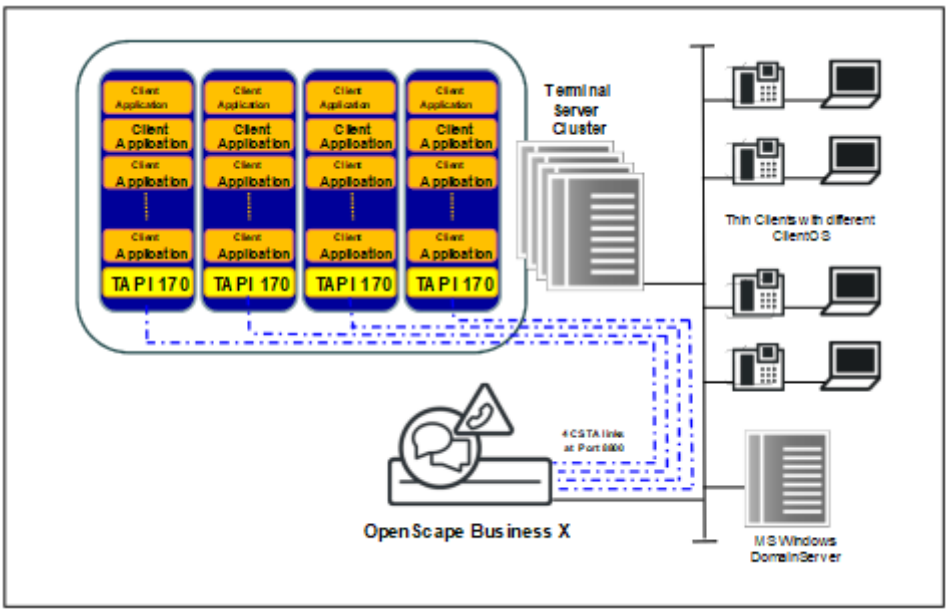


Abbildung 15: Client basierte TAPI Applikation auf Terminal-Server an OpenScape Business

- **Anschaltung von TAPI 170 an vernetzte OpenScape Business Systeme**

  Bei vernetzten OpenScape Business Systemen wird die TAPI 170 Software auf einem Server installiert, der über LAN an die CSTA Schnittstelle des Master-Knotens angeschaltet wird. Diese Anschaltung ist unabhängig von den zuvor erwähnten Betriebsarten des TAPI 170 Service Providers (Remote TAPI oder serverbasierte Anschaltung). Für die Realisierung wird ein CSTA Link von OpenScape Business Master-Konten sowie je eine TAPI Lizenz für jeden TAPI Teilnehmer im Netzwerk benötigt.

  Anmerkung: Über den Master-Knoten erhält der TAPI 170 den netzweiten Zugriff auf alle Teilnehmer im Netzwerk. Bei einer Anschaltung des TAPI 170 an einem Slave-Knoten anstatt am Master-Knoten kann TAPI 170 nur auf die Teilnehmer des Slave-Knotens zugreifen. Bei Einsatz von mehreren TAPI 170 in einem Terminal-Server Cluster

ist für jeden TAPI 170 ein CSTA Link zum Master Knoten erforderlich.

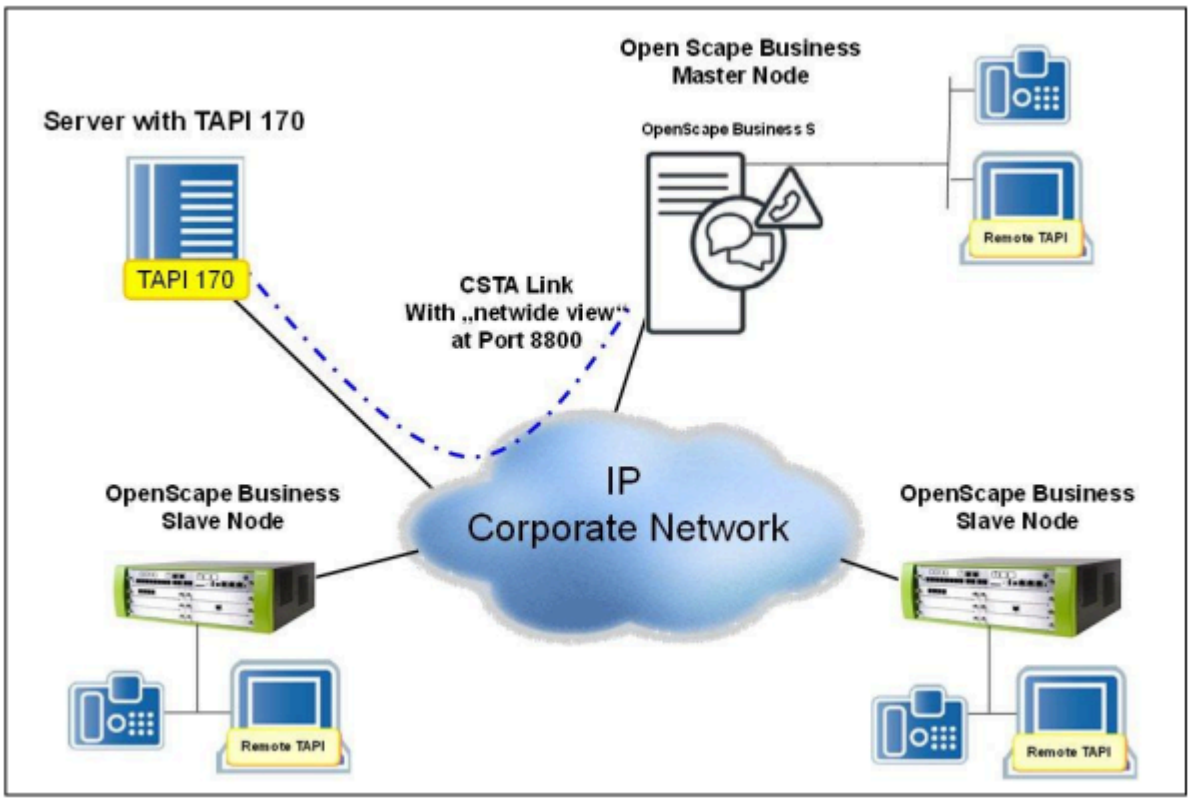


Abbildung 16: Anschaltung von TAPI 170 an vernetzte OpenScape Business Systeme

Ausbaugrenzen

Die maximal Anzahl von TAPI 170 Client PCs, die an OpenScape Business angeschaltet werden können ist modellabhängig. Weitere Informationen hierzu sind im Kapitel 1.3.9.4 enthalten

Freigegebene Betriebssysteme

Die aktuell freigegebenen Betriebssysteme für den Microsoft Windows Server, den Terminal-Server und den Remote Client PC sind in der aktellen Vertriebsinformation aufgelistet.

Es können nur Microsoft Windows Betriebssysteme in Verbindung mit TAPI 170 verwendet werden.

Das Lizenzmodell von Microsoft erfordert neben der Lizenz für das Server Betriebssystem, auch entsprechende Microsoft Device oder User CALs in der für den geplanten Ausbau benötigten Anzahl. Diese CALs sind nicht Bestandteil der Lieferung von OpenScape Business TAPI 170 und müssen immer separat beschafft werden. Unter bestimmten, von Microsoft vorgegebenen Bedingungen, kann für OpenScape Business TAPI 170 auch ein "Windows Server for embedded systems" mit der sogenannten "Embedded Telco Lizenz" verwendet werden.

Lizenzierung

Die Verwendung von OpenScape Business TAPI 170 ist auf Teilnehmerbasis lizenziert. Die Lizenzen werden innerhalb des OpenScape Business Systems verwaltet. Bei Verwendung des Leistungsmerkmals MULAP ist für jeden Teilnehmer innerhalb der MULAP eine TAPI-Lizenz erforderlich.

Software-Bereitstellung

Die OpenScape Business TAPI 170 Software wird auf einem eigenen Datenträger ausgeliefert. Sie ist nicht Bestandteil der OpenScape Business System Software.

Hardware-Anforderungen

Für die Anschaltung von OpenScape Business TAPI 170 wird unabhängig von der Anzahl angeschalteter TAPI 170 Clients ein CSTA Link von OpenScape Office benötigt. Dies gilt auch für vernetzte OpenScape Business Systeme.

Der PC muss mindestens den von Microsoft vorgegeben Systemanforderungen für das eingesetzte Betriebssystem entsprechen, vorausgesetzt dass keine weiteren SW-Applikationen außer TAPI 170 betrieben werden. Zusätzlich wird ein Ethernet LAN Interface benötigt.

Unterstützte Geräte

Die unterstützten Endgeräte wie auch die unterstützten Leistungsmerkmale an diesen Endgeräten hängen vom CSTA- bzw vom WSI-Funktionsumfang des eingesetzten OpenScape Business Systems ab. Diese Informationen sind in der OpenScape Business Vertriebsinformation enthalten.

23.3 Web Services Interface

Das integrierte Web Services Interface ermöglicht das Monitoring und die Steuerung von Telefonie-Ressourcen in einem System mit UC-Benutzern.

Leistungsmerkmale

Das Web Services Interface bietet folgende Leistungsmerkmale:

- Zugriff via Ethernet LAN (TCP/IP)
- Unterstützung von HTTP und HTTPS
- Unterstützung für einzelne Systeme
- Benutzerorientierte, klar strukturierte Funktionen für:
  - Steuerung von Anrufen
  - Steuerung von Geräten
  - Monitoring von Geräten
  - Verzeichnisse
  - Journal der Teilnehmer
  - Anwesenheitsstatus der Teilnehmer

Anmerkung: Abhängig vom verwendeten (Web Services Interface) WSI-Clienttyp muss das Flag Assoziierte Dienste aktiviert werden, um die Ausführung einiger WSI-Befehle zu ermöglichen.

Web Server WebSessions

Die Anzahl der verfügbaren Web Server Sessions gilt für alle entsprechenden Anwendungen gemeinsam, wie z.B. myPortal to go (Web Edition), Application Launcher, OptiClient Attendant (Server) und OptiClient BLF.

Interne Monitorpunkte

Die internen Monitorpunkte sind unabhängig von den Monitorpunkten der CSTA-Schnittstelle. Falls mehrere Anwendungen denselben UC-Benutzer über das Web Services Interface überwachen, verwendet der Webserver dafür nur einen einzigen internen Monitorpunkt.

Ports

Folgende Portnummern stehen zur Verfügung:

Port	Protokoll
8801	HTTP (unverschlüsselt)
8802	HTTPS (verschlüsselt)

23.4 Open Directory Service

Der Open Directory Service (ODS) ist ein offener, integrierter, LDAP-basierter Verzeichnisdienst. Er fungiert als Meta-Verzeichnisdienst und aggregiert die Ergebnisse aus verschiedenen internen und externen Verzeichnisquellen über eine einzige Schnittstelle. Auf den Open Directory Service können verschiedene Arten von Clients, Anwendungen und Kommunikationsgeräten in einem Unternehmen zugreifen.

Der Open Directory Service erfüllt zwei Funktionen:

1) Er ermöglicht den Zugriff auf zusätzliche Kontaktdaten aus externen Quellen über SQL oder ODBC-Datenzugriff auf Datenbanken im Kundennetzwerk, die Verzeichnisdaten enthalten.
2) Er macht sowohl interne als auch externe Verzeichnisse für Clients, Kommunikationsgeräte und Anwendungen zugänglich.

Der Open Directory Service ist standardmäßig deaktiviert. Wenn Sie ihn aktivieren, stellen Sie bitte sicher, dass die Firewalls für das LDAP-Protokoll auf Port TCP/389 geöffnet sind.

Der Open Directory Service auf verschiedenen Varianten von OpenScape Business

Der Open Directory Service wird je nach OpenScape Business-Plattform mit unterschiedlichen Funktionen angeboten:

- OpenScape Business S, OpenScape Business X V3 Advanced-Mainboards, Booster Server oder Booster-Karte:

  Es wird die volle Funktionalität angeboten, sodass sowohl interne als auch externe Datenquellen genutzt werden können.
- OpenScape Business X V3 Basic-Mainboards:

  Die Funktionalität ist auf die internen Standarddatenquellen beschränkt.

- OpenScape Business X V2-Mainboards:

  Für die Nutzung des Open Directory Service ist eine Booster-Karte oder ein Booster-Server erforderlich.

Um über das LDAP-Protokoll eine Verbindung zum Open Directory Service herzustellen, verwenden Sie bitte die im Admin-Portal angezeigte IP-Adresse:

- Auf der rechten Seite der OpenScape Business Assistant-Startseite, unter **Anwendungen**.
- Auf der Seite **Anwendungsauswahl** des Assistenten für die **Erstinstallation** unter **Basis** > **installation einrichten**.

Interne Datenquellen

Die folgenden internen Datenquellen sind standardmäßig im Open Directory Service verfügbar:

- Externes Verzeichnis
- Internes Verzeichnis
- Zentrale Kurzwahlnummern

Für diese internen Datenquellen sind die Feldnamen fest mit dem Datenschema des Open Directory Service verknüpft.

Diese internen Datenquellen können nicht gelöscht oder geändert werden. Um interne Datenquellen über ODS verfügbar zu machen, ist eine „OpenScape Business OpenDirectory Base”-Lizenz erforderlich.

Externe Datenquellen

Als Administrator können Sie Kontaktinformationen aus den folgenden Datenbanktypen als Datenquellen für den schreibgeschützten Zugriff über SQL oder ODBC integrieren.

- Datenquellen mit integrierten Treibern (Microsoft SQL Server, PostgreSQL, Sybase SQL).
- Datenquellen ohne integrierte Treiber erfordern einen installierten und konfigurierten ODBC-Bridge-Server auf dem ODS-Client (kann über das WBM unter **Service Center** > **Software** heruntergeladen werden).

Anmerkung: Für eine erfolgreiche Verbindung ist es erforderlich, einen Wert im Feld **Beschreibung** anzugeben (der Wert kann sich vom Namen der Datenquelle unterscheiden, das Feld darf jedoch nicht leer sein). Bei ODBC-Brücken-Datenquellen für Access, Firebird, Excel und Oracle fügen Sie bitte den Namen der Datenquelle, also „Access“, „Firebird“, „Excel“ bzw. „Oracle“, als Wert in das Feld **Beschreibung** ein.

Anmerkung: Für die Integration von Microsoft Excel- und ODS-Datenbanken wird nur das Dateiformat *.xsl* (jedoch nicht *.xlsx*) unterstützt. Vermeiden Sie es in aktuellen MS Office-Versionen, Excel-Dateien zu bearbeiten oder zu speichern, um die Kodierung der Datei nicht zu beschädigen. Zusätzlich ist ein spezieller ODBC-Bridge-Treiber für Microsoft Excel erforderlich.

Für den Zugriff auf externe Datenquellen aus ODS ist pro verbundener Datenquelle eine „OpenScape Business OpenDirectory Connector”-Lizenz erforderlich.

Maximale Anzahl verschiedener Datenbanktypen: 3

Maximale Anzahl externer Datenquellen: 4

Stellen Sie sicher, dass der Open Directory Service für den Zugriff auf die externe Datenquelle autorisiert ist. Wenden Sie sich vorab an den zuständigen Datenbankadministrator, um dies sicherzustellen. Möglicherweise muss ein separater Benutzer in der externen Datenquelle hinzugefügt werden, damit das System darauf zugreifen kann.

Externe Datenquellen können sowohl für die Verzeichnissuche als auch für die Auflösung von Rufnummern in Namen verwendet werden.

Sie können den direkten Zugriff auf eine Datenbanktabelle aus einer externen Datenquelle oder einer benutzerdefinierten SQL-Abfrage für die Datenquelle konfigurieren.

Jede Spalte, die als ID dient, muss eindeutige und nicht null/nicht leere Werte enthalten. Verwenden Sie die Eigenschaft UNIQUE oder PRIMARY KEY, um sicherzustellen, dass dies der Fall ist.

Bei der Integration externer Datenbanken gelten die folgenden Einschränkungen:

- Die Sonderzeichen ´[]'" werden vom ODS in Tabellennamen und Spaltennamen nicht unterstützt.
- Die Spaltentypen „nchar” und „nvarchar” werden vom ODS nicht unterstützt.
- Die Leerzeichen dazwischen(zumindest in den letzten 4–5 Ziffern) werden vom ODS für Telefondaten nicht unterstützt.

Benutzerdefinierte SQL-Abfragen für externe Datenquellen

Benutzerdefinierte SQL-Abfragen unterstützen auch verwandte Tabellen, z. B.:

```
SELECT * FROM users LEFT OUTER JOIN phonenumbers ON
users.id = phonenumbers.uid;
```

Die Datenstruktur muss vom Typ 1:1 oder n:1 sein, d. h. jeder Datensatz darf nur eine einzige Zeile haben.

Der Zugriff über benutzerdefinierte SQL-Abfragen kann manchmal wesentlich langsamer sein als der direkte Zugriff auf eine Datenbanktabelle.

Benutzerdefinierte SQL-Abfragen mit potenziellen Sicherheitsrisiken werden nicht ausgeführt, zum Beispiel:

- Daten ändern
- SQL-Server stoppen
- Programme über den SQL-Server ausführen
- Benutzerrechte ändern

Benutzerdefinierte SQL-Abfragen mit den folgenden SQL-Befehlen werden daher nicht ausgeführt:

- `CHECKPOINT`
- `CLOSE`
- `CLUSTER`
- `COMMIT`
- `COPY`

- CREATE
- DEALLOCTAE
- DECLARE
- DELETE
- DISCARD
- DO
- DROP
- END
- EXECUTE
- EXPLAIN
- FETCH
- GRANT
- INSERT
- LOAD
- LOCK
- MOVE
- PREPARE
- REASSIGN OWNED
- REINDEX
- RELEASE SAVEPOINT
- RESET
- REVOKE
- SAVEPOINT
- SECURITY LABEL
- SELECT INTO
- SET
- SHOW
- START TRANSACTION
- TRUNCATE
- UNLISTEN
- UPDATE
- VACUUM
- VALUES

Feldzuordnung für Datenquellen

Für diese Datenquellen können Sie die Zuordnung von Feldnamen zum Datenschema des Open Directory Service anpassen. Sie können jedes Feld im Datenschema des Open Directory Service höchstens einem Feld der externen Datenquelle zuordnen. Sie können jedoch ein Feld der externen Datenquelle mehreren Feldern im Datenschema des Open Directory Service zuordnen.

LDAP-Datenausgabezuordnungen

Eine LDAP-Datenausgabezuordnung legt fest, welche Felder im Datenschema des Open Directory Service über LDAP ausgegeben werden sollen, z B. für bestimmte LDAP-Clients oder für verschiedene Gruppen von Abonnenten, die nicht alle Details, sondern nur eine definierte Teilmenge sehen möchten.

Die LDAP-Datenausgabezuordnung **web** ist standardmäßig verfügbar und kann weder gelöscht noch geändert werden. Alle Felder des Datenschemas im Open Directory Service sind dauerhaft der LDAP-Ausgabe darin zugewiesen. Sie können auch andere LDAP- Datenausgabezuordnungen konfigurieren.

LDAP-Clients können über den Parameter „dc“ in der LDAP-Anmeldung auf eine bestimmte LDAP-Datenausgabezuordnung zugreifen, zum Beispiel: `dc=web`.

Normalisierung von Telefonnummern im kanonischen Format

Für jede Datenquelle können Sie die Normalisierung von Telefonnummern im kanonischen Format konfigurieren. Während dieses Vorgangs werden Leerzeichen, Klammern, Bindestriche und Kommas entfernt. Dies ist erforderlich, um den Namen des Anrufers korrekt zu identifizieren und für die Desktop-Wahl. Sie sollten die Normalisierung nicht überspringen, es sei denn, die in der Datenquelle verwendeten Telefonnummern liegen bereits im kanonischen Format vor. Sie können die normalisierungsbezogenen Werte wie die Vorwahl usw. automatisch aus dem System eingeben lassen. Befindet sich die externe Datenquelle an einem anderen Standort als das System, müssen Sie diese Werte möglicherweise anpassen.

Status der Datenquellen

Die Statusanzeige unter **OpenDirectory** > **Datenquellen** hat folgende Bedeutung:

Farbe	Status
grün	aktiv
Rot	Bei ODBC und LDAP stimmt etwas nicht: falsche Konfiguration oder Datenquelle nicht verfügbar
Gelb	Bei LDAP stimmt etwas nicht: Open Directory Service neu starten
grau	Konfiguration unvollständig

Bereitstellen von Verzeichnissen

Die folgenden Arten von Clients, Kommunikationsgeräten und Anwendungen können die vom Open Directory Service bereitgestellten Verzeichnisse nutzen:

- UC-Clients
- Application Launcher
- Systemverzeichnis
- OpenStage mit lokaler LDAP-Unterstützung
- DECT-IP-Telefone (über LDAP)
- SIP-Telefone (über LDAP)
- Anwendungen, z. B. CRM-Suiten des Typs Microsoft Dynamics CRM (über LDAP, ODBC oder OpenLDAP CSV-Export)

Der Open Directory Service kann in den Suchergebnissen die Datenquelle identifizieren, aus der ein Treffer stammt.

Zugehörige Konzepte

Voraussetzungen für Application Launcher auf Seite 1203

23.4.1 Wie Sie Open Directory Service aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Open Directory Service**.
3) Klicken Sie im Menübaum auf **Open Directory** > **Grundeinstellungen**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie Open Directory Service aktivieren möchten, aktivieren Sie das Kontrollkästchen **Aktiv**.
   - Wenn Sie Open Directory Service deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Aktiv**.
5) Klicken Sie auf **Speichern**.
6) Klicken Sie auf **OK**.
7) Klicken Sie auf **OK**.

23.4.2 Wie Sie Open Directory Service neu starten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Open Directory Service ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Open Directory Service**.
3) Klicken Sie im Menübaum auf **Open Directory** > **Wartung**.
4) Klicken Sie auf **Neustart**
5) Klicken Sie auf **OK**.

23.4.3 Kennwort für Zugriff auf Open Directory Service konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Führen Sie die folgenden Schritte durch, um das Kennwort festzulegen, mit welchem Clients, Kommunikationsgeräte und Anwendungen auf Open Directory Service zugreifen können.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Open Directory Service**.
3) Klicken Sie im Menübaum auf **Open Directory** > **Grundeinstellungen**.
4) Geben Sie das gewünschte **LDAP-Kennwort** ein.
5) Klicken Sie auf **Speichern**.
6) Klicken Sie auf **OK**.

23.4.4 ODBC-ODBC Bridge Server konfigurieren

Voraussetzungen

Der ODBC Bridge Server wurde mit dem WBM unter **Service Center** > **Software** heruntergeladen und auf einem Windows-PC (32 Bit oder 64 Bit) mit Datenquellen installiert, die auf relationale oder nicht-relationale Datenbanken zugreifen können. Der ODBC Bridge Server wird benötigt, damit ODBC-Treiber auf die Datenquelle zugreifen können.

Anmerkung:

Aufgrund der jüngsten Windows 10 / Windows Server Updates von Microsoft wurde die ODBC-Schnittstelle des Betriebssystems geändert und daher werden nur 32-Bit-Treiber von der ODBC–ODBC Bridge unterstützt. Es wird dringend empfohlen, 32-Bit-ODBC-Treiber für die Verbindung zu ODBC-Datenquellen zu verwenden.

Dies ist eine vorübergehende Einschränkung.

Die Datenquelle muss über die ODBC-Datenquellen-Administration auf dem ODS-Client als DSN konfiguriert werden.

Der Benutzername und das Kennwort der Datenquelle sind bekannt.

Die Konfiguration des ODBC Bridge Server ist für die Oberflächensprache Englisch beschrieben. Selbstverständlich kann die Konfiguration auch in einer anderen Oberflächensprache durchgeführt werden (Registerkarte **Server Manager** > **Language**).

Schritt für Schritt

1) Klicken Sie mit der rechten Maustaste auf das ODBC Bridge Server-Icon in der Trayleiste und wählen Sie den Menüpunkt **Settings**.

2) Legen Sie die allgemeinen Server-Einstellungen fest:

a) Klicken Sie auf die Registerkarte **Servereinstellungen**.

b) Wählen Sie unter **Verbindungseinstellungen** in der Aufklappliste **Netzwerkschnittst.** die IP-Adresse aus, unter der der ODBC Bridge Server für den ODBC-Client (OpenScape Business) erreichbar sein soll.

Diese IP-Adresse muss im WBM von OpenScape Business bei der ODS-Konfiguration eingegeben werden.

c) Geben Sie unter **Port** den Port an, unter dem die Anfragen des ODBC Clients (OpenScape Business) eingehen sollen.

Dieser Port muss im WBM von OpenScape Business bei der ODS-Konfiguration eingegeben werden.

d) Wenn der Dienst beendet wurde, können Sie den **Dienststatus** aktivieren, indem Sie ihn unter **Dienststeuerung** auf **Ein** setzen oder in der Taskleiste die Option **Dienst starten** auswählen.

e) Wenn der Dienst gestartet ist, können Sie den **Dienststatus** deaktivieren, indem Sie ihn auf **Aus** setzen oder in der Taskleiste die Option **Dienst beenden** auswählen.

f) Unter **Netzwerkeinstellungen** können Sie die Verschlüsselung aktivieren, indem Sie die entsprechende Option auf **Ein** setzen.

g) Geben Sie unter **Netzwerkeinstellungen** die maximale Anzahl der gleichzeitigen Verbindungen zu ODBC-Clients ein (minimal: 1, maximal: 20). Gehen Sie dafür zum Feld **Max. Verbindungen**.

h) Klicken Sie auf **Einstellungen speichern**.

Anmerkung: Nach dem Speichern der Einstellungen ist ein Neustart erforderlich.

---

3) Legen Sie einen Benutzer an für den ODBC Client Zugriff auf die Datenquelle:

a) Klicken Sie auf die Registerkarte **Role Management**.

b) Klicken Sie auf **Benutzer hinzufügen**.

c) Vergeben Sie unter **Benutzername** einen Benutzernamen für den ODBC Client.

d) Geben Sie in den Feldern **Kennwort** und **Kennwort erneut eingeben** ein Kennwort für den ODBC-Client ein.

Die gleichen Benutzerangaben müssen im WBM von OpenScape Business bei der ODS-Konfiguration eingegeben werden.

e) Wählen Sie den DSN aus, auf den der ODBC-Client zugreifen soll, indem Sie das Kontrollkästchen in der Spalte **Access** aktivieren.

f) Geben Sie bei Bedarf **DB-Benutzername** und **Kennwort** ein.

g) Klicken Sie auf **Einstellungen speichern**.

4) Klicken Sie auf die Registerkarte **Überwachung**, um die Verbindungen zu überwachen. Folgende Details werden angezeigt:

- Die Namen und Versionen der installierten ODBC-Treiber.
- Der Name und die IP-Adresse des ODS-Client, die Zeitdauer der letzten aktiven Verbindung sowie die Gesamtdauer aller aktiven Verbindungen.
- Die verfügbaren ODBC-Datenquellen (über den Link **Windows-Datenquellenadministrator öffnen**).

5) Klicken Sie auf die Registerkarte **Protokolle**, um die Erstellung von Protokolldateien zu aktivieren, und bestimmen Sie, welche Trace-Levels protokolliert werden sollen:
   a) Aktivieren Sie die Protokollierung, indem Sie den entsprechenden Wert auf **Ein** setzen.
   b) Wählen Sie die **Protokollebene**: **Alles** für alle Protokolle, **Normal** für Dienstprotokolle oder nur **Warnungen und Fehler**.
   c) Wählen Sie den Protokolltyp aus der Aufklappliste aus. Sie können dabei auswählen, ob die Protokollordner oder die Protokoll-Konsole angezeigt werden soll.
6) Klicken Sie auf die Registerkarte **Darstellung**, um die Darstellung anzupassen:
   a) Wählen Sie ein Design aus (hell oder dunkel).
   b) Wählen Sie einen Stil aus.
   c) Wählen Sie die gewünschte Sprache aus.
   d) Wählen Sie, ob der Dienst automatisch beim Starten ausgeführt werden soll.
   e) Wählen Sie, ob der Dienst in der Taskleiste minimiert werden kann.
7) Klicken Sie auf die Registerkarte **Info**, um sich die Dienstdetails und die verfügbaren Updates anzeigen zu lassen.

Anmerkung: Wenn eine neue Version verfügbar ist, klicken Sie auf **Installieren**, um das Update auszuführen.

---

8) Wählen Sie in der Taskleiste die Option **Beenden**, um die Dienstkonfiguration zu schließen.

23.4.5 Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Die Zugangsdaten der externen Datenbank liegen vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Open Directory Service**.
3) Klicken Sie im Menübaum auf **Datenquelle**.
4) Klicken Sie auf **Hinzufügen**.
5) Klicken Sie auf die Registerkarte **Datenbank**.
6) Geben Sie **Name** der Datenquelle ein.
7) Geben Sie eine **Beschreibung** der Datenquelle ein.

8) Wenn Sie eine SQL-Datenbank hinzufügen möchten:

a) Wählen Sie den Typ **PostgreSQL** oder **Microsoft SQL Server, Sybase SQL** oder **ODBC Bridge** in der Dropdown-Liste **ODBC-Treiber** aus.

b) Geben Sie in **Server-Adresse der Datenbank** die IPv4-Adresse der Datenbank ein.

c) Geben Sie **Server-Port der Datenbank** ein.

d) Geben Sie den **Datenbanknamen** in korrekter Groß-/Kleinschreibung ein.

e) Geben Sie **Datenbank-Login** in korrekter Groß-/Kleinschreibung ein.

f) Geben Sie **Datenbank-Passwort** in korrekter Groß-/Kleinschreibung ein.

g) Wenn Sie den Typ **Microsoft SQL Server, Sybase SQL** in der Dropdown-Liste **ODBC-Treiber** ausgewählt haben, geben Sie auch die **TDS-Protokollversion** ein.

9) Wenn Sie eine Nicht-SQL-Datenbank hinzufügen möchten:

a) Wählen Sie in der Aufklappliste **ODBC-Treiber** den Typ **ODBC Bridge** aus.

b) Geben Sie in **ODBC Bridge Server-Adresse** die IPv4-Adresse der Datenbank ein.

c) Geben Sie **ODBC Bridge Server-Port** ein.

d) Geben Sie den **ODBC Bridge Remote DSN**ein

e) Geben Sie **ODBC Bridge Login**in korrekter Groß-/Kleinschreibung ein.

f) Geben Sie **ODBC Bridge Passwort**in korrekter Groß-/Kleinschreibung ein.

10) Klicken Sie auf **Prüfe Datenbankzugriff**, um den Zugriff zu testen.

11) Klicken Sie auf **Speichern**.

12) Klicken Sie auf die Registerkarte **Datenzugriff**.

13) Wenn Sie eine Datenbanktabelle verwenden möchten:

a) Klicken Sie auf **Einfache Auswahl - Zugriff auf eine Tabelle**.

b) Klicken Sie auf **Datenbanktabellen abfragen** und wählen Sie in der Liste **Datenbanktabellen** die gewünschte Tabelle.

Anmerkung: Diese Funktionalität steht für einige Datenquellen (z. B. Oracle) nicht zur Verfügung. Wenn ja, geben Sie den Namen der Tabelle manuell an.

---

c) Klicken Sie auf **Vorschau der Datenbanktabelle** und navigieren Sie in der Vorschau mit Hilfe der entsprechenden Schaltflächen durch die Datensätze.

14) Wenn Sie eine benutzerdefinierte SQL-Abfrage verwenden möchten:

a) Klicken Sie auf **Benutzerdefinierte SQL-Abfrage**.

b) Geben Sie diese in **SQL-Abfrage** ein.

Anmerkung: Wenn Sie eine neue Datenquelle mit einer SQL-Anweisung definieren, sollten Sie die Abfrage so formulieren, dass die Datensatz-IDs konstant bleiben. Sie müssen die in den jeweiligen Tabellen enthaltenen ID-Attribute verwenden, anstatt die IDs zu berechnen, wenn die Abfrage läuft. Bitte vermeiden Sie jede Anweisung wie "SELECT ROW_NUMBER() OVER As ID", die bei der Ausführung der Abfrage

IDs erzeugt und je nach Sortierung und Anzahl der Datensätze unterschiedliche IDs liefert. Wenn Sie Tabellen mit sich überschneidenden ID-Bereichen mit UNION ALL vereinigen, verringern Sie das Risiko doppelter IDs, indem Sie die vorhandenen Tabellen-IDs für jede zu vereinigende Tabelle mit einer anderen Zahl inkrementieren (z. B. "SELECT (table2.ID+1000) AS ID").

c) Klicken Sie auf **Vorschau des Abfrageergebnisses** und navigieren Sie in der Vorschau mit Hilfe der entsprechenden Schaltflächen durch die Datensätze.

15) Klicken Sie auf die Registerkarte **Feldzuordnungen**.

Anmerkung: Alle Spalten der gewählten Tabelle bzw. alle Spalten welche die benutzerdefinierte SQL-Abfrage zurückliefert, stehen für die Feldzuordnungen zur Verfügung.

16) Klicken Sie auf **Feldzuordnung hinzufügen**.

17) Wählen Sie in der Aufklappliste links jeweils das Feld der externen Datenquelle und in der Aufklappliste rechts in der selben Zeile jeweils das gewünschte zugeordnete Feld im Datenschema von Open Directory Service. Zur Kontrolle wird rechts eine Vorschau auf betreffende Datensätze angezeigt, durch die Sie mit Hilfe der entsprechenden Schaltflächen navigieren können.

Anmerkung: Das Feld **Identifikationsnummer** muss einem Feld der externen Datenquelle zugeordnet werden, welches eindeutig ist.

18) Wenn Sie eine Reihe von Feldzuweisungen entfernen möchten, klicken Sie auf das Papierkorb-Symbol auf der linken Seite.

19) Klicken Sie auf die Registerkarte **Rufnummernkonvertierung**.

a) Aktivieren Sie das Kontrollkästchen **Aktiv**.

b) Klicken Sie auf **Systemeinstellungen auslesen**.

c) Wenn sich die externe Datenbank an einem anderen Standort als dem System befindet Geben Sie **Länderkennzahl**, **OrtskennzahlAmtskennziffer**, **Nationales Prafix**, **Maximale Länge interner Rufnummern** ein

d) Wählen Sie eine der folgenden Optionen:

- Wenn Sie eine in der externen Datenquelle eventuell vorhandene Amtskennziffer entfernen möchten, aktivieren Sie das Kontrollkästchen **Amtskennziffer entfernen**.

- Wenn Sie die Amtskennziffer nicht entfernen möchten, deaktivieren Sie das Kontrollkästchen **Amtskennziffer entfernen**.

20) Klicken Sie auf **Speichern**.

21) Klicken Sie auf **OK**.

Nächste Schritte

Starten Sie Open Directory Service neu, damit die Änderung wirksam wird.

Führen Sie eine Vorschau auf das LDAP-Suchergebnis durch.

23.4.6 Vorschau auf LDAP-Suchergebnis für Open Directory Service durchführen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Führen Sie die folgenden Schritte durch, um zu kontrollieren, ob ein LDAP-Suchergebnis von Open Directory Service Datensätze in der gewünschten Form und mit dem korrekten Rufnummernformat liefert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Open Directory Service**.
3) Klicken Sie im Menübaum unter **Open Directory** > **OpenScape Business-Benutzer** > **Datenquellen** auf die gewünschte Datenquelle.
4) Klicken Sie auf die Registerkarte **LDAP-Test**.
5) Klicken Sie auf **Test starten**. Unter **LDAP Suchergebnis** wird die Vorschau auf das Suchergebnis angezeigt.

Anmerkung: Die Standardgrenze von OpenLDAP für Antworten beträgt 500 Einträge. Die Open Directory Service (ODS)-Backend-Engine schreibt ebenfalls ein Limit von 500 Einträgen für jede Datenquelle vor.

Die LDAP-Testfunktion von Open Directory Service (ODS) führt eine Suchanfrage durch, die eine Obergrenze von 500 Einträgen hat. Der Zweck der LDAP-Testoption ist nicht das Abrufen der Ergebnisse, sondern die Überprüfung, ob die LDAP-Konnektivität korrekt ist.

Wenn mehr als 500 Datensätze vorhanden sind, werden daher Ergänzungen und Änderungen an LDAP-Daten nach Durchführung eines LDAP-Tests möglicherweise nicht über das WBM abgebildet.

23.4.7 Wie Sie eine externe Datenquelle für Open Directory Service löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **Open Directory Service**.
3) Klicken Sie im Menübaum auf **Open Directory** > **Datenquellen**.
4) Klicken Sie im Arbeitsbereich auf die betreffende Datenquelle.
5) Klicken Sie auf **Löschen**.

6) Klicken Sie auf **OK**.

Nächste Schritte

Starten Sie Open Directory Service neu, damit die Änderung wirksam wird.

23.5 Active Directory Integration Service

Active Directory ist ein Microsoft-Verzeichnisdienst für Domänennetzwerke Mit dem angebotenen Active Directory Integration Service kann OpenScape Business die Active Directory Datenbank lesen und Benutzer mit seiner eigenen Datenbank synchronisieren, um die Benutzeradministration zu erleichtern und Konfigurationsaufwand zu verringern.

Voraussetzungen

Damit die Synchronisierung des Active Directory Integration Service stattfinden kann, müssen die folgenden Voraussetzungen erfüllt sein:

- Active Directory Microsoft Server ist vom Kunden bereitgestellt.
- Active Directory wird als zentraler Konfigurationspunkt für Mitarbeiterdaten, und insbesondere Benutzerdaten, verwendet. Folgende Felder werden zwischen Active Directory und OpenScape Business zugeordnet:
  - Vorname
  - Nachname
  - Anzeigename
- Nur dieses Active Directory wird zum Hinzufügen, Ändern oder Löschen von Daten von Mitarbeitern verwendet.
- Es wird erwartet, dass alle Active Directory-Änderungen automatisch auch auf dem Kommunikationssystem gelten.

Synchronisierung

Die eindeutige ID der OpenScape Business Teilnehmer, die für die Synchronisierung verwendet wird, ist die Durchwahlnummer. Diese Nummer wird mit dem Feld telephoneNumber das AD (Active Directory) synchronisiert.

Jede Änderung, die im Active Directory des Unternehmens erfolgt, wird umgehend mit OpenScape Business synchronisiert. Das bedeutet, dass jeder neue Teilnehmer, der zum AD hinzugefügt wird, auch zu OpenScape Business hinzugefügt wird, und dem Teilnehmer eine IP-Teilnehmerlizenz zugewiesen wird.

Alle Änderungen, die im AD an bereits synchronisierten Teilnehmern erfolgen, spiegeln sich umgehend bei OpenScape Business Teilnehmern wider.

Wenn ein synchronisierter Teilnehmer aus dem AD gelöscht wird, werden firstName, sn und displayName des Teilnehmers auch aus OpenScape Business gelöscht und die IP-Teilnehmerlizenz wird freigegeben. Die Durchwahlnummer und die interne Rufnummer werden jedoch nicht aus OpenScape Business und bleiben für die Zuweisung zu einem anderen Teilnehmer verfügbar.

Anmerkung: Der Zugriff auf den Active Directory Service ist schreibgeschützt. Dies bedeutet, dass die Synchronisierung der Benutzerdaten nur von Active Directory zu

OpenScape Business erfolgt. Änderungen in den OpenScape Business Teilnehmerinformationen werden nicht wieder mit Active Directory synchronisiert und bei der nächsten Synchronisierung mit Active Directory Daten überschrieben.

Feldzuordnung

Sie können die Zuordnung der Feldnamen zum Datenschema des Active Directory Service anpassen. Auf diese Weise können Sie kontrollieren, wie Felder in OpenScape Business von Active Directory Daten aktualisiert werden.

Die Standardzuordnung der Felder ist in der folgenden Tabelle angegeben:

OpenScape Business Feld	Active Directory Feld
Vorname	Vorname
Nachname	sn
Anzeigename	displayName
Durchwahl	telephoneNumber

Normalisierung von Durchwahlnummern

Die Gateway-Standortdaten des OpenScape Business Systems werden verwendet, um die Durchwahlnummer eines Teilnehmers in das kanonische Nummernformat umzuwandeln.

Das Format von telephoneNumber in Active Directory muss ebenfalls im kanonischen Format sein, damit eine automatische Synchronisierung möglich ist.

23.5.1 Wie Sie die den Active Directory Service konfigurieren

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den **Active Directory Integration Service**-Wizard zu starten.
4) Markieren Sie das Kontrollkästchen **Aktiv**, um den Active Directory Integration Service zu aktivieren.
5) Stellen Sie die **IP-Adresse** des Active Directory Servers, den **Benutzernamen** und das **Kennwort** für einen gültigen Benutzer ein.

   Der hier geforderte **Benutzername** ist kein OpenScape Business-Benutzername, sondern ein ActiveDirectory-Benutzername, der im X.500 Directory Specification-Format angegeben werden muss. In diesem Format werden Benutzer mit den folgenden Knoten definiert:

CN	Allgemeiner Name
OU	Organisationseinheit

DC	Domain-Komponente

Der Benutzername erschließt sich aus der genaueren Angabe links neben der allgemeineren Information auf der rechten Seite. Jede Informationsangabe erfolgt als Paar, das durch ein Gleichheitszeichen (=) getrennt ist.

Ein Beispiel für einen Benutzernamen ist wie folgt: `CN=Hans.mustermann,OU=Administrator,DC=BeliebigesUnternehmen`.

6) Klicken Sie auf **DNs holen**, um verfügbare DNs zu holen und einen davon als Rootbasis namingContext auszuwählen.

   Sollte ein Problem mit den Benutzeranmeldedaten auftreten, wird ein Fehler `Authentifizierungsfehler! Bitte überprüfen Sie Ihre Anmeldedaten` angezeigt.

7) Bearbeiten Sie die Felder **Container** und **Filter**, falls nötig.

   Der Standardwert für Container ist `cn=Users` und für Filter `(&(objectCategory=person)(objectClass=user))`

8) Klicken Sie auf **Daten holen**.

   Die ersten 1000 Einträge von AD werden, nach Nachname(sn) geordnet, angezeigt.

9) Klicken Sie auf einen Benutzer, um die Details zu prüfen.

10) Klicken Sie auf **OK & Weiter**, um zum Bildschirm **Feldzuordnung** zu gehen.

11) Nehmen Sie die nötigen Änderungen in den Feldzuordnungswerten vor.

    Die Werte in der linken Spalte sind das OpenScape Business Datenbankschema und die Werte, die in der rechten Spalte eingestellt sind, entsprechen den Active Directory Attributen.

    Telefonnummer wird zum Abgleichen der OpenScape Business Durchwahlnummer verwendet.

12) Klicken Sie auf **Fertigstellen**, um die Active Directory Integration abzuschließen.

23.6 Application Launcher

Application Launcher ist eine Java-basierte Windows-Anwendung zur anrufbezogenen Steuerung von Anwendungen, die auf den Client-PCs von UC Suite-Benutzern und myAgent-Benutzern ausgeführt werden. Application Launcher kann z.B. verwendet werden, um in einem CRM-System automatisch das Kontaktformular für den jeweiligen Anrufer zu öffnen.

Application Launcher bietet folgende Leistungsmerkmale:

- Beziehen anrufbezogener Informationen zur Rufnummer (z.B. Rufnummer, Name des Gesprächspartners, Kunden-ID) entweder aus Open Directory Service oder in Verzeichnissen des Systems
- Aufruf von Windows-Anwendungen oder Web-Anwendungen bei ankommenden und gehenden Anrufen
- Übergabe von anrufbezogenen Informationen an Windows-Anwendungen oder Web-Anwendungen
- automatischer Betrieb im Hintergrund bei ankommenden Anrufen

- optionales, konfigurierbares PopUp-Fenster bei ankommenden Anrufen mit anrufbezogenen Informationen und Schaltflächen für Benutzeraktionen
- Anruferliste mit Anruffunktion
- Vorschaufunktionen für Tests während Konfiguration
- einfaches Übernehmen der Konfiguration vom ersten konfigurierten Client in alle weiteren mittels Konfigurationsprofil im System

23.6.1 Voraussetzungen für Application Launcher

Um Application Launcher zu nutzen, muss der Client-PC des jeweiligen Benutzers von UC Suite über geeignete Hardware und Software verfügen.

Die Installation erfordert lokale Administratorrechte auf dem Client-PC, automatische Updates jedoch nicht.

Betriebssystem

Application Launcher kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)

> **Tipp:** Das verwendete Betriebssystem benötigt stets den aktuellen Stand aller verfügbaren Updates (Service Packs und Patches).

Windows Update

Die PCs benötigen stets den aktuellen Stand aller verfügbaren Updates einschließlich Service Packs.

Zusätzliche Software

Auf einem PC muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein (siehe **Service-Center** > **Software**)

Web Services für Mobiltelefone

Web Services für Mobiltelefone muss im System aktiviert sein für die Systemverbindung. An Firewalls im LAN und an Client-PCs müssen die im System konfigurierten Ports geöffnet sein.

Open Directory Service (optional)

Wenn Application Launcher Daten von Open Directory Service nutzen soll, muss Open Directory Service im System konfiguriert sein. An Firewalls im LAN und an Client-PCs muss der im System konfigurierte Port geöffnet sein.

Zugehörige Konzepte

Konfiguration von myPortal to go und Mobility Entry auf Seite 965
Open Directory Service auf Seite 1188

23.6.2 Profil mit Konfigurationsdaten von Application Launcher

Ein Profil mit Konfigurationsdaten von Application Launcher ermöglicht die einfache und schnelle Konfiguration von Application Launcher auf allen Client-PCs.

Das Profil beinhaltet sämtliche Konfigurationsdaten, bis auf die Systemverbindung und die Benutzerdaten. Sobald Application Launcher für einen ersten Benutzer vollständig konfiguriert ist, können Sie als Administrator dessen Profil mit den Konfigurationsdaten von Application Launcher im Kommunikationssystem bereitstellen. Anschließend können alle Benutzer die Konfiguration von Application Launcher durch Importieren dieses Profils durchführen.

23.6.2.1 Wie Sie das Profil mit Konfigurationsdaten von Application Launcher bereitstellen

Voraussetzungen

Application Launcher ist für einen Benutzer vollständig konfiguriert.

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Application Launcher**.
3) Klicken Sie auf **Durchsuchen** und wählen Sie folgende Datei aus: `C:\Documents and Settings\<Windows User Name>\Application Data\Tray_Tool\profile.xml`.
4) Klicken Sie auf **Öffnen**.
5) Klicken Sie auf **Laden**.

Nächste Schritte

Alle Benutzer können dieses Profil in Application Launcher importieren und dadurch die Konfiguration durchführen.

23.7 myPortal for Teams im Überblick

Das myPortal for Teams-Plugin wird verwendet, um die Microsoft Teams-Anwendung mit OpenScape Business zu integrieren.

myPortal for Teams erfordert ein neues OpenScape Business V3-Mainboard oder OpenScape Business S System und wird ab Software-Release V3R1 FR2 unterstützt.

Mit myPortal for Teams sind Sie in der Lage:

- Ihre Anrufhistorie zu filtern und zu verwalten.
- Kontakte anzuzeigen und zu suchen.
- Kontakte in Favoritengruppen zu organisieren.
- E-Mail-Kontakte.

- Ein zugeordnetes Telefon auszuwählen (für MULAP-Benutzer).
- Einen Anruf zu starten.
- Einen Anruf anzunehmen, abzulehnen oder weiterzuschalten.
- Einen Anruf zu halten.
- Einen Anruf zu übergeben.
- Einen Rückfrageanruf zu tätigen.
- Zwischen Anrufen zu wechseln.
- Ein Gespräch zu übergeben.

Anmerkung: Die Suche nach Kontakten in externen Verzeichnissen, wie z. B. LDAP, ist nicht verfügbar.

Anmerkung: Die VoIP-Funktionalität wird für myPortal for Teams nicht unterstützt.

23.7.1 myPortal for Teams konfigurieren

Voraussetzungen

- Offizielles und vertrauenswürdiges Microsoft-Zertifikat, das in OpenScape Business WBM importiert werden kann
- Microsoft-Anwendungs-ID, die vor der Konfiguration von myPortal for Teams erstellt werden muss

Schritt für Schritt

1) Navigieren Sie zu **Setup > Cloud-Dienste**.
2) Klicken Sie neben dem **Microsoft Teams Client-Plugin** auf Bearbeiten.
3) Der Domänenname und die Portnummer im **URL-Feld** sind bereits ausgefüllt.

   Der Domänenname ist die Domäne Ihres OpenScape Business-Systems.

   Der Standardwert für die Portnummer ist 8805. Sie können die Domänen-ID und die Portnummer ändern, wenn Sie möchten.
4) Geben Sie die **Anwendungs-ID** ein.

   Die Anwendungs-ID wird vom Administrator des Microsoft Azure-Portals generiert.
5) Klicken Sie auf **OK & Download**.

   Das Plugin wird in Form einer Zip-Datei heruntergeladen. Die heruntergeladene Datei ist ein an Ihre Systemkonfiguration angepasstes Plugin.

   Anmerkung:

   Die Registerkarte Microsoft Teams verhindert das Laden von Webinhalten von einem Server, der selbstsignierte Zertifikate verwendet. Dies ist ein Sicherheitsaspekt, und die Verwendung von selbstsignierten Zertifikaten ist im Grunde

eine unsichere Praxis, da diese Schnittstelle dem Internet ausgesetzt ist.

Daher muss ein vertrauenswürdiges Microsoft-Zertifikat im System installiert sein. Für weitere Informationen siehe Kapitel Server-Zertifikat importieren (PKCS#12) auf Seite 1048.

23.7.2 So laden Sie myPortal for Teams in den Teams-Speicher hoch

Voraussetzungen

Sie müssen über Administratorrechte für die Anwendung Microsoft Teams verfügen.

Schritt für Schritt

1) Klicken Sie in der linken Navigation der Microsoft Teams-Anwendung auf **Apps**.
2) Klicken Sie auf **Eine benutzerdefinierte App hochladen** und wählen Sie **Für meine Org hochladen**.

   Wählen Sie die Datei, die Sie vom WBM heruntergeladen haben, und laden Sie sie hoch.

Nächste Schritte

Sobald das myPortal for Teams-Plugin hochgeladen ist, steht es den Benutzern zur Verfügung, um es in ihre Microsoft Teams-Anwendung einzufügen.

23.8 Unify Phone

Für OpenScape Business-Benutzer ist es möglich, über den Unify Phone Client Telefonanrufe zu tätigen. Diese Funktionalität ist sowohl über den Unify Phone Client als auch über das Gerät verfügbar. Dazu müssen Sie die Unify Phone-Konnektivität mit OpenScape Business konfigurieren und die Unify Phone-Benutzer hinzufügen.

Die verfügbare Unify Phone-Funktionalität umfasst:

- Anrufe durchführen/annehmen
- Anrufe löschen/abweisen
- Anrufe halten/wiederaufnehmen
- Anruf weiterschalten/verschieben
- DTMF-Unterstützung
- Anruf tauschen
- Anrufumleitung
- Alternative Nummer
- Anruf-Routing
- Zugriff auf Verzeichnis und Journal
- Anrufsteuerung von Drittanbietern über die folgenden Onboard-UC-Clients: myPortal @work, myPortal for Desktop, myPortal for Outlook, myAttendant, my Agent und myPortal for Teams.

Neben den oben genannten Merkmalen werden keine weiteren Merkmale veröffentlicht, insbesondere Funktionscodes.

Anmerkung: Die Anrufsteuerung von Drittanbietern (CTI-Steuerung) ist derzeit nur für Unify Phone Desktop Client möglich. Die Steuerung erfolgt immer über den Unify Phone Desktop Client (Web/PWA) und ist nicht für den Unify Phone Mobile Client vorgesehen. Es ist möglich, einen Anruf nach Annahme des Anrufs auf den Unify Phone Mobile Client zu verschieben. Außerdem ist die Anrufsteuerung von Drittanbietern nicht für die Verwendung in Verbindung mit einem aktiven Unify Phone-Merkmal "alternative Nummer" vorgesehen.

23.8.1 Unify Phone-Konnektivität konfigurieren

Voraussetzungen

Sie haben den Wert **Upstream bis zu (Kbps)** unter **Einrichtung** > **Wizards** > **Grundinstallation** > **Grundinstallation** > **Upstream Ihrer Internetverbindung** eingetragen, um gleichzeitige Gespräche führen zu können. Geben Sie zum Beispiel '256' für 2 gleichzeitige Gespräche ein.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie neben der Option **Unify Phone-Konnektivität** auf **Bearbeiten**, um die Einstellungen für einfache Verbindungen zu konfigurieren.
4) Aktivieren Sie das Kontrollkästchen **Unify Phone aktivieren** , um die Unify Phone-Konnektivität zu aktivieren.
5) Geben Sie unter **Unify Phone Domain Zugangsdaten** folgende Details ein:
   a) Wählen Sie aus der Aufklappliste die verfügbare **Domäne** aus.

      Folgende Möglichkeiten bestehen:

      - phoneapp.unify.com
      - Benutzerdefiniert

      Anmerkung: Wenn „Benutzerdefiniert“ ausgewählt ist, füllen Sie das Feld **Benutzerdefinierte Domäne** aus.

   b) Geben Sie den API-Schlüssel, der für Ihren Mandanten generiert wurde, in das Feld **Unify Phone API-Schlüssel** ein.
6) Wählen Sie unter **Gleichzeitige Unify Phone-Anrufe** in der Aufklappliste die Anzahl der gleichzeitigen Unify Phone-Anrufe aus. Diese Zahl hängt von dem zuvor konfigurierten Upstream-Wert ab.

   Anmerkung: Wenn die Anrufqualität sich verschlechtert, muss die Anzahl der gleichzeitigen Anrufe reduziert werden.
7) Klicken Sie auf **OK & Weiter**.

8) Wählen Sie im Fenster **Unify Phone-Standortnummer** , welches Nummerierungsschema Sie verwenden möchten. Diese Auswahl betrifft das Format der SIP- und WSI-Nummern.

   - Um internationale Nummern zu verwenden, aktivieren Sie das Kontrollkästchen **Internationale Nummerierung verwenden** .

     Wenn internationale Nummern gewählt werden, fordert der Assistent dazu auf, fehlende Standortnummern der Unify Phone-Route, die zur Bildung der internationalen Nummer verwendet werden sollen, zu konfigurieren. Außerdem werden die Unify Phone-Routenparameter für die Art der Nummer entsprechend der Auswahl aktualisiert.
   - Internrufnummern

9) Klicken Sie auf **OK & Weiter**.

10) Klicken Sie im Pop-up-Fenster auf **Funktion ausführen**, um einen SIP-Trunk für Unify Phone zu erstellen.

11) Klicken Sie auf **OK & Weiter** gefolgt von **Fertigstellen**.

Anmerkung: Es wird empfohlen, die Konfigurationsdaten über die Option **Datensicherung** > **Backup - Sofort** im Hauptmenü zu speichern.

Nächste Schritte

Wenn Sie die Unify Phone-Konnektivität deaktivieren möchten, müssen Sie zunächst alle Unify Phone-Benutzer löschen, wie in Wie entfernen oder löschen Sie Unify Phone-Benutzer auf Seite 1211beschrieben.

Anmerkung: Es ist wichtig, aktive Unify Phone-Benutzer vor z.B. Systemmigrationen zu löschen, um kritische Diskrepanzen zwischen der OpenScape Business-Datenbank und der Cloud-Datenbank zu vermeiden.

23.8.2 Wie konfigurieren Sie die Unify Phone-Benutzerinstanz

Voraussetzungen

Unify Phone-Konnektivität ist konfiguriert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie bei der Option **Unify Phone-Benutzerinstanz** auf **Bearbeiten**.
4) Klicken Sie auf **OK und Weiter** und dann auf **Fertigstellen**.

23.8.3 Unify Phone-Benutzer verwalten

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie bei der Option **Unify Phone-Benutzerinstanz** auf **Bearbeiten**.

   Für das bestimmte System wird eine Liste mit den konfigurierten Unify Phone-Benutzern angezeigt.

   Anmerkung: Wenn es bereits registrierte Unify Phone-Benutzer gibt, werden Sie aufgefordert, den Unify Phone-Konnektivität-Wizard auszuführen, ohne die Konfiguration zu ändern.

23.8.3.1 Wie Sie Unify Phone-Benutzer erstellen

Voraussetzungen

Unify Phone-Konnektivität ist konfiguriert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie bei der Option **Unify Phone-Benutzerinstanz** auf **Bearbeiten**. Die verfügbaren Unify Phone-Benutzer werden angezeigt.
4) Klicken Sie auf **Erstellen** neben **Einen neuen Benutzer für Unify Phone erstellen**.
5) Gehen Sie auf der Seite **Unify Phone-Benutzererstellung** wie folgt vor:
   a) Der **Trunk-Zugangscode + Unify Phone-Benutzerrufnummer** ist schreibgeschützt und wird automatisch entsprechend dem ausgewählten Nummerierungsschema (international oder intern) generiert.
   b) Geben Sie die **Rufnummer des Unify Phone-Benutzers** ein.
   c) Geben Sie die **Unify Phone-Benutzer-Durchwahl** ein.
   d) Geben Sie den **Vornamen**ein.
   e) Geben Sie den **Nachnamen**ein.
   f) Geben Sie die **E-Mail-Adresse**des Unify Phone-Benutzers ein.
6) Klicken Sie auf **OK & Weiter**.
7) Klicken Sie auf **Fertig**.
   Nach erfolgreichem Abschluss dieses Vorgangs wird eine E-Mail an die eingegebene E-Mail-Adresse gesendet, mit der der Unify Phone-Benutzer die Konfiguration abschließen kann.
8) Wiederholen Sie die Schritte 4 bis 6, um weitere Unify Phone-Benutzer hinzuzufügen.

23.8.3.2 Wie fügen Sie bestehende Unify Phone-Benutzer hinzu

Voraussetzungen

Unify Phone-Konnektivität ist konfiguriert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie bei der Option **Unify Phone-Benutzerinstanz** auf **Bearbeiten**. Die verfügbaren Unify Phone-Benutzer werden angezeigt.
4) Klicken Sie auf **Hinzufügen** neben **Bestehende Benutzer zu Unify Phone hinzufügen**.
5) Auf der Seite **Unify Phone-Benutzerzuweisung** werden die verfügbaren Benutzer als Symbole angezeigt. Um einen bestehenden Benutzer hinzuzufügen, gehen Sie wie folgt vor:
   a) Der **Trunk-Zugangscode + Unify Phone-Benutzerrufnummer** ist schreibgeschützt und wird automatisch entsprechend dem ausgewählten Nummerierungsschema (international oder intern) generiert.
   b) Geben Sie die **Rufnummer des Unify Phone-Benutzers** ein.
   c) Geben Sie die **Unify Phone-Benutzer-Durchwahl** ein.
   d) Sie können einen Benutzer nach **Name** oder **E-Mail**suchen.
   e) Wählen Sie einen Unify Phone-Benutzer mit den verfügbaren Symbolen aus.

      Für Unify Phone-Benutzer gibt es drei Symbole:

      - Grüne Symbole: Verfügbare Benutzer, die aktiv sind.
      - Ausgegraute grüne Symbole: Nicht verfügbare Benutzer, die nicht aktiv sind.
      - Ausgegrautes grünes Symbol im roten Rahmen: Nicht verfügbare Benutzer, die nicht aktiv sind und bereits mit einer Nummer in Unify Phone konfiguriert sind.

      Die Felder **Vorname** und **Nachname** des Unify Phone-Benutzers werden automatisch ausgefüllt.
6) Klicken Sie auf **OK & Weiter**.
7) Wiederholen Sie die Schritte 4 bis 6, um weitere Unify Phone-Benutzer hinzuzufügen.

Nächste Schritte

Weisen Sie den Unify Phone-Benutzern Lizenzen zu, wie unter Teilnehmer lizenzieren (Standalone) auf Seite 319 oder Wie Sie Teilnehmer lizenzieren (Netzverbund) auf Seite 330 beschrieben.

Wenn Sie einen Unify Phone-Benutzer in ein Team (MULAP) integrieren, beachten Sie Folgendes:

- Es kann nur ein IP- oder TDM-Desk Phone in das Team mit dem Unify Phone-Benutzer aufgenommen werden. Die Routing-Funktion in Unify Phone wird verwendet, um zu bestimmen, welches Endgerät zur Signalisierung eines eingehenden Anrufs verwendet werden soll.
- Das Desk Phone im Team mit Unify Phone kann weiterhin von externen Anwendungen über TAPI, WSI oder CSTA gesteuert werden. Dies gilt auch, wenn Unify Phone über Drittanwendungen gesteuert wird.
- Cordless-Teilnehmer sind in Verbindung mit Unify Phone nicht zugelassen.

23.8.3.3 Unify Phone-Benutzerdetails bearbeiten

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie neben dem entsprechenden Unify Phone-Benutzer auf **Bearbeiten**.
4) Sie können folgende Details bearbeiten:
   a) Die **Kennzahl zur Amtsholung + Rufnummer des Unify Phone-Benutzers** ist schreibgeschützt und wird automatisch entsprechend dem ausgewählten Nummerierungsschema (international oder intern) generiert.
   b) Die **Rufnummer des Unify Phone-Benutzers**.
   c) Die **Unify Phone-Benutzer-DuWa**.
   d) **Vorname** des Unify Phone-Benutzers.
   e) **Nachname** des Unify Phone-Benutzers.

   Anmerkung: Das Feld Ausgewählter Unify Phone-Benutzer, das die E-Mail-Adresse des Benutzers enthält, ist schreibgeschützt.
5) Klicken Sie auf **OK & Weiter**.

23.8.3.4 Wie entfernen oder löschen Sie Unify Phone-Benutzer

Es gibt Szenarien, in denen das Löschen von Unify Phone-Benutzern aus Ihrem OpenScape Business-System unbedingt erforderlich ist. Zum Beispiel:

- Bei der Migration von einem Testlaborsystem auf ein echtes/Live-System.
- Beim Austausch einer Hauptplatine von V2 H/W auf V3 H/W oder aufgrund von H/W-Fehlern.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie bei der Option **Unify Phone-Benutzerinstanz** auf **Bearbeiten**.
4) Klicken Sie neben dem entsprechenden Unify Phone-Benutzer auf **Bearbeiten**.
5) Klicken Sie auf **Entfernen** oder **Löschen**.
6) Wiederholen Sie die Schritte 1-5, um weitere Unify Phone-Benutzer zu löschen.

   Denken Sie daran, dass das Löschen von Admin-Benutzern unterscheidet sich vom Löschen von Unify Phone-Benutzern, die keine Admins sind:

   Wenn Unify Phone-Benutzer, ob mit oder ohne Administratorrolle, aus dem System entfernt werden, werden sie nicht aus dem Unify Phone-Mandanten,

zu dem sie gehören, entfernt. Diese Benutzer existieren noch, aber ihnen ist keine Telefonnummer mehr zugewiesen.

Wenn Unify Phone-Benutzer ohne Administratorrolle aus dem System gelöscht werden, werden sie auch aus dem Mandanten, zu dem sie gehören, entfernt.

Wenn Unify Phone-Benutzer mit Administratorrolle aus dem System gelöscht werden, werden sie nicht aus dem Mandanten, zu dem sie gehören, entfernt. Diese Benutzer existieren noch, aber ihnen ist keine Telefonnummer mehr zugewiesen.

Anmerkung: Wird ein neues System durch Klonen oder Datenwiederherstellung (Migration) eingerichtet, bei dem das ursprüngliche System einen Unify Phone Connector-Zugang konfiguriert hatte, muss sichergestellt werden, dass Diskrepanzen zwischen dem UP-Cloud-Status und dem der OSBiz-Datenbank vermieden werden. Aus diesem Grund ist es wichtig, alle UP-Benutzer zu entfernen und dann den Unify Phone Connector zu deaktivieren, bevor das ursprüngliche System geklont/gesichert wird.

23.8.3.5 Wie Sie alternative Nummern und Anruf-Routing für das Unify Phone-Interworking einrichten

Damit die Funktionen alternative Nummer und Anruf-Routing von Unify Phone in OpenScape Business unterstützt werden, müssen Sie im Experten-Modus die folgende Einstellung vornehmen.

Schritt für Schritt

1) Klicken Sie im **Experten-Modus** auf **Telefonie-Server** > **Eingehende Anrufe** > **Anrufumleitung**.
2) Klicken Sie auf die Registerkarte **Rufzielliste - Definition**.
3) Nehmen Sie unter **Anrufumleitung bearbeiten** die folgenden Konfigurationen vor.
   a) Wählen Sie als **Ziel 1** `* Gerufener Teilnehmer`.
   b) Wählen Sie als **Ziel 2** `** Benutzerdefiniert`.
   c) Wählen Sie als **Ziel 3** die Option `Anzahl der Voicemail` (optional).

23.9 Let's Encrypt-Dienst

Let's Encrypt ist eine automatische Zertifizierungsstelle, die kostenlose TLS/SSL-Zertifikate über das ACME-Protokoll (Automatic Certificate Management Environment) anbietet. Der Dienst verifiziert die Domäneneigentümerschaft mithilfe eindeutiger Token und Herausforderungen, wie z. B. die HTTPS-Herausforderung. Nach der Überprüfung bieten Let's Encrypt-Server signierte Zertifikate für die sichere Kommunikation zwischen Servern und Benutzern.

Für V2-Hauptplatinensysteme, die OCAB oder Booster Server verwenden, wird das Let's Encrypt-Zertifikat mit dem Booster Server synchronisiert. Um die Aktivierung zu erleichtern, wird ein Mechanismus in die Java-Anwendung

integriert. Der Aktivierungsprozess von V2-Hauptplatinensystemen kann zusätzliche Zeit in Anspruch nehmen, da das Zertifikat innerhalb des Boosters (entweder Karte oder Server) übertragen und aktiviert werden muss. Aufgrund dieses Synchronisierungsvorgangs sollten Sie mit einer leichten Verzögerung der Aktivierungszeit rechnen. Wenn das Merkmal deaktiviert ist, wird das Standardserverzertifikat entweder für den OCAB- oder den Booster-Server aktiviert.

23.9.1 Wie konfigurieren Sie den Let's Encrypt-Dienst

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie auf **Bearbeiten** next to **Let's Encrypt-Dienst**.
4) Geben Sie unter **Konfiguration des Domänennamens**die folgenden Details ein:
   - Geben Sie den Domänennamen in das Feld **Primärer Domänenname** ein.
   - Geben Sie optional eine zweite Domäne in das Feld **Sekundärer Domänenname (Optional)** ein.
5) Unter **Konfiguration der automatischen Zertifikatsaktualisierung**, legen Sie im Feld **Automatische Aktualisierungszeit** die Zeit fest, zu der die automatische Aktualisierung durchgeführt werden soll.

   Anmerkung: Das System wird nach einer automatischen Aktualisierung neu gestartet.

6) Klicken Sie auf **Aktivieren** , um den Dienst zu aktivieren, oder **Deaktivieren** , um ihn zu deaktivieren.
7) Unter **Let's Encrypt-Dienststatus** finden Sie detaillierte Informationen über den Dienst und seinen Status:
   - **Dienststatus** zeigt, ob der Dienst derzeit `aktiv` oder `inaktiv`ist.
   - **Zertifikatsaktivierungsdatum** zeigt das Datum, an dem das Zertifikat aktiviert wurde.
   - **Erneuerungsdatum** zeigt das Fälligkeitsdatum für die automatische Zertifikatserneuerung.
   - **Erneuerungsstatus** zeigt den Status des automatischen Erneuerungsprozesses an.

     Anmerkung: Das Let's Encrypt-Protokoll verwendet den HTTP-Port TCP/80 für die HTTP-Herausforderung bei der ersten Zertifikatserstellung oder bei der Zertifikatsaktualisierung.

   Auf der WBM-Startseite wird eine Meldung angezeigt, die Systemadministratoren darüber informiert, wann das Zertifikat abläuft (X Tage) und wann der Versuch einer Zertifikatsaktualisierung fehlgeschlagen ist.

23.10 CloudLink Service

CloudLink aktiviert die Kommunikation zwischen lokalen OpenScape Business-Systemen und cloudbasierten Mitel-Anwendungen.

SIP-Verbindung

Die SIP-Verbindungsfunktion wird verwendet, um OpenScape Business mit Cloud-Diensten wie Workflow Studio zu verbinden.

Informationen zum Aktivieren dieser Funktion finden Sie im Kapitel Konfigurieren des SIP-Connectors.

Tipp: Stellen Sie zuvor sicher, dass der Upstream Ihrer Internetverbindung konfiguriert ist (siehe Konfigurieren des Internetzugangs über einen externen Internetrouter).

Containerunterstützung in OpenScape Business

In OpenScape Business ist eine Container-Laufzeitumgebung verfügbar, die den CAS-Container (Cloudlink Gateway) unterstützt. Aufgrund von Leistungs-/Kapazitätsbeschränkungen ist sie nur in den folgenden OpenScape Business Varianten verfügbar:

- V3-Mainboards mit angeschlossenem NVMe-Laufwerk (eingebettete Systeme)
- OpenScape Business S Systeme (Servervarianten)

Auf eingebetteten Systemen ist die Container-Laufzeitumgebung als Teil des OpenScape Business Software Images für V3 HW vorinstalliert. Sie wird beim Booten standardmäßig nicht gestartet, um Systemressourcen zu sparen. Sie wird erst aktiviert, wenn der Administrator die Containerunterstützung in der Cloudlink-Weboberfläche aktiviert.

Bei Servervarianten muss die Container-Laufzeitumgebung (Docker-Paket) vom Administrator bei der Installation des Betriebssystems SLES15 installiert werden.

Informationen zur Konfiguration des Containerunterstützungsdienstes finden Sie im Kapitel Konfigurieren der CloudLink Daemon-Weboberfläche.

23.10.1 So konfigurieren Sie den Cloud Link-Dienst

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie auf **Bearbeiten** neben **CloudLink Service**.
4) Klicken Sie auf das Kontrollkästchen neben **CloudLink Service aktivieren**.
5) Klicken Sie bei Bedarf auf das Kontrollkästchen neben **Proxy verwenden**.
6) Geben Sie die IP-Adresse und den Port des Proxys in die Felder **HTTP-Proxy** und **HTTP-Proxy Port** ein.

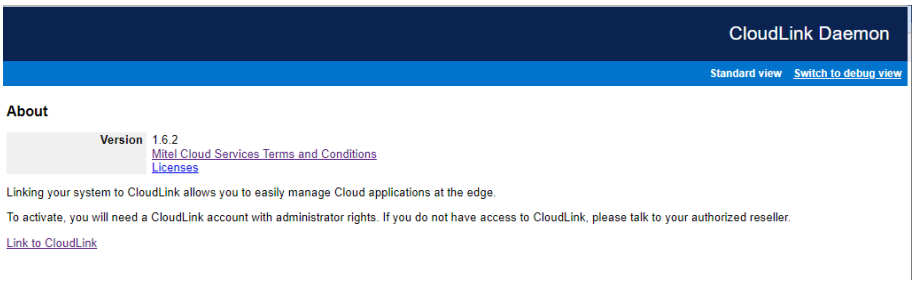
7) Geben Sie Ihre Anmeldeinformationen in die Felde **Benutzername** und **Passwort** ein.
8) Falls erforderlich, aktivieren Sie bitte das Kontrollkästchen neben **SIP-Connector aktivieren**.
9) Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern.
10) Klicken Sie auf die **CloudLink**- Schaltfläche, um das CloudLink Dämon-Webschnittstelle-Fenster zu öffnen.

23.10.2 So öffnen Sie die CloudLink Daemon-Webschnittstelle

CloudLink Daemon-Webschnittstelle ermöglicht die Konfiguration und Integration von Cloud- und On-Premise-Systemen, wodurch die Funktionen von OpenScape Business-Kommunikationsanwendungen erweitert werden.

Schritt für Schritt

1) Klicken Sie auf **Link zu CloudLink**.



   Sie werden zum CloudLink Portal weitergeleitet.
2) Geben Sie Ihren **Benutzernamen** und Ihr **Passwort** an, um sich beim CloudLink-Portal anzumelden.
3) Starten Sie eine Verbindung.

23.10.3 So konfigurieren Sie die CloudLink Dämon-Webschnittstelle

Sie können die folgenden Aktionen in der Standardansicht oder der Debug-Ansicht ausführen. Um zwischen den Ansichten zu wechseln, klicken Sie auf **Zur Debug-Ansicht wechseln** oder **Zur Standardansicht wechseln**.

Schritt für Schritt

1) Klicken Sie auf **Allgemeine Geschäftsbedingungen für Mitel Cloud Services**, um die Allgemeinen Geschäftsbedingungen anzuzeigen.
2) Klicken Sie auf **Lizenzen**, um die zugehörigen Lizenzen anzuzeigen.
3) Klicken Sie auf **CloudLink Portal**.

   Sie werden zum CloudLink Portal weitergeleitet.
4) Klicken Sie auf **Von CloudLink trennen**, um die Verbindung zum Dienst zu trennen.
5) Ändern Sie den Tag und die Stunde für automatische Updates und klicken Sie auf **Neu planen**.
6) Klicken Sie auf **Pause**, um das nächste Update anzuhalten.

7) Klicken Sie auf **Alle Tunnel starten** und **Alle Tunnel stoppen**, um konfigurierte Tunnel zu starten oder zu stoppen.
8) Klicken Sie auf **Starten** oder **Stoppen**, um den Fernzugriff über das CloudLink Gateway-Portal zu starten oder zu stoppen.
9) Für V3-Mainboards OCCe mit NVMe und OpenScape Business S Systemen können Sie die Container-Unterstützungsfunktion wie folgt konfigurieren:
   a) Klicken Sie auf **Containerunterstützung aktivieren**.
   b) Klicken Sie im Popup-Bestätigungsfenster auf **Ja**.
   c) Klicken Sie bei Bedarf auf **Neustart** or **Container-Unterstützung deaktivieren**, um den Dienst neu zu starten bzw. zu beenden.

23.10.4 So aktivieren/konfigurieren Sie den SIP-Connector für die Verbindung mit Workflow Studio

Voraussetzungen

Die Upstream-Verbindung Ihres Internetzugangs ist konfiguriert (siehe So konfigurieren Sie den Internetzugang über einen externen Internetrouter).

Ein CloudLink-Konto ist erforderlich, und es muss eine Verbindung zu CloudLink hergestellt werden (siehe So konfigurieren Sie die CloudLink Daemon-Webschnittstelle).

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie auf **Bearbeiten** neben **CloudLink Service**.
4) Klicken Sie auf das Kontrollkästchen neben **CloudLink Service aktivieren**.
5) Klicken Sie bei Bedarf auf das Kontrollkästchen neben **Proxy verwenden**.
6) Geben Sie die IP-Adresse und den Port des Proxys in die Felder **HTTP-Proxy** und **HTTP-Proxy Port** ein.
7) Geben Sie Ihre Anmeldeinformationen in die Felde **Benutzername** und **Passwort** ein.
8) Falls erforderlich, aktivieren Sie bitte das Kontrollkästchen neben **SIP-Connector aktivieren**.
   a) Wählen Sie einen Wert aus der Dropdown-Liste für das Feld **Anzahl gleichzeitiger CloudLink-Anrufe** aus.
9) Klicken Sie auf **OK & Weiter**.
   Die Trunks werden hinzugefügt (für die Trunks sind keine Lizenzen erforderlich). CloudLink wird konfiguriert und eine Verbindung wird hergestellt.
10) Klicken Sie auf „Fertigstellen“. Klicken Sie auf **Fertig**.

23.11 CloudLink-Pilotnummern

Durch Anrufen einer konfigurierten CloudLink-Pilotnummer wird der Anruf zur weiteren Bearbeitung an Wokflow Studio weitergeleitet.

Die Pilotnummern für die Cloudlink services pro OpenScape Business-System sind auf 60 pro OpenScape Business-System begrenzt.

Die Anzahl der Fernleitungen pro OpenScape Business-System ist auf insgesamt 250 begrenzt.

Darüber hinaus sind Fernleitungen durch die im Basisinstallationsassistenten definierte Upstream-Bandbreite (128 Kbit/s pro Leitung) begrenzt.

Die Cloudlink-Fernleitungsverbindung belegt eine von zehn dedizierten ITSP/ native SIP-Routen in einem OpenScape Business System.

23.11.1 So konfigurieren Sie CloudLink-Pilotnummern

Voraussetzungen

Der CloudLink-Assistent ist konfiguriert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Cloud-Dienste**.
3) Klicken Sie auf **Bearbeiten** neben **CloudLink-Pilotnummern**.
4) Klicken Sie auf **Hinzufügen**.
5) Geben Sie in der Spalte **CloudLink-Pilotnummern** die erforderlichen Nummern ein.
6) Geben Sie für jede Nummer einen Namen in die Spalte **Anzeigename** ein.
7) Klicken Sie auf **OK & Weiter**.
8) Falls erforderlich, klicken Sie auf **Löschen** oder **Alle löschen** m einen einzelnen oder alle Einträge zu löschen, und bestätigen Sie anschließend mit **OK**.
9) Klicken Sie auf **OK & Weiter** gefolgt von **Fertigstellen**.

24 Accounting

Accounting umfasst die Erfassung von Verbindungsdaten, Projektkennzahlen, die Übertragung und Anzeige von Verbindungsdaten sowie Kostenkontrolle und Accounting Tools.

24.1 Verbindungsdaten

Verbindungsdaten umfassen die Erfassung von Verbindungsdaten sowie Projektkennzahlen.

24.1.1 Erfassung von Verbindungsdaten

Das System kann die Verbindungsdaten seiner genutzten Leitungen protokollieren.

Für jede beendete Verbindung bzw. bei jeder kommenden Verbindung wird ein Verbindungsdatensatz aufgezeichnet. Für einen neuen zeitlichen Abschnitt einer Verbindung (z.B. durch Übergabe oder Weiterleitung an einen anderen Teilnehmer) wird ein eigener Verbindungsdatensatz aufgezeichnet. Interne Verbindungen werden nicht protokolliert.

Der Administrator kann für die Erfassung von Verbindungsdaten folgende Optionen aktivieren:

- Erfassung ein bzw. aus
- Verbindungsdauer
- Geldbeträge oder Tarifeinheiten:

  Die Umrechnung von Tarifeinheiten in Geldbeträge erfolgt anhand des konfigurierbaren Tariffaktors (Währungsbetrag pro Tarifeinheit).
- Dezimalformat

  Teilt den Geldbetrag durch 100, um z.B. 6 Cent als 0,06 darzustellen
- Letzte vier Ziffern von Zielrufnummern unterdrücken
- Kommende Verbindungen protokollieren
- Gehende Anrufe ohne Verbindung:

  Hierdurch erhält der Teilnehmer z.B. einen Nachweis für die Nichtannahme eines Anrufs durch den Zielteilnehmer (gekennzeichnet durch Verbindungsdauer 00:00:00). Die Option gilt für ISDN-Verbindungen und für alle Teilnehmer.
- Verbindungsprotokoll

  Protokoll bereits bei Anrufbeginn
- MSN protokollieren
- Ausgabe der LCR Nummer gehend oder der gewählten Rufnummer kommend
  - Gehend:

    die von LCR tatsächlich zum PSTN gesendete Rufnummer
  - Kommend:

    die ursprünglich gewählte interne Rufnummer

Entstehen Verbindungskosten bereits vor dem Verbindungsaufbau (wie z.B. in Österreich), werden diese erfasst, unabhängig davon, ob die Protokollierung gehender Anrufe ohne Verbindung aktiviert ist.

Das System berücksichtigt Verbindungen über QSIG-Leitungen nur, wenn für diese eine Leitungskennzahl konfiguriert ist.

Es erfolgt keine Protokollierung bei:

- vorzeitigem Abbruch des Wahlversuchs
- unzulässigen Verbindungen (LCR, Verbotslisten).

Zugehörige Konzepte

Projektkennzahlen auf Seite 1223

24.1.1.1 Wie Sie die Erfassung von Verbindungsdaten aktivieren oder deaktivieren

Mit dem Wizard **Gesprächsdatenerfassung** können Sie die Erfassung von Verbindungsdaten aktivieren.

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Gesprächsdatenerfassung** zu starten.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Erfassung von Verbindungsdaten aktivieren möchten, aktivieren Sie das Kontrollkästchen **Gebührenerfassung einschalten**.
   - Wenn Sie die Erfassung von Verbindungsdaten deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Gebührenerfassung einschalten**.
5) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

24.1.1.2 Wie Sie die Protokollierung der Verbindungsdauer aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.

4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Anrufdauerprotokollierung ein**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Anrufdauerprotokollierung ein**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.1.3 Wie Sie die Protokollierung von Geldbeträgen oder Tarifeinheiten konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie möchten, dass das System Geldbeträge protokolliert, aktivieren Sie das Kontrollkästchen **Beträge statt Einheiten ausgeben**.
   - Wenn Sie möchten, dass das System Tarifeinheiten protokolliert, deaktivieren Sie das Kontrollkästchen **Beträge statt Einheiten ausgeben**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.1.4 Wie Sie Tariffaktor, Währung und Rechengenauigkeit konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Faktoren**.
4) Geben Sie für jede betreffende Richtung in den Feldern **Multiplikator** und **Multipl. ISDN** die entsprechenden Werte ein.
5) Geben Sie im Feld **Währung** am unteren Ende des Formulars den entsprechenden Wert ein.

6) Wählen Sie für jede betreffende Richtung mit dem QSIG-Protokoll in Übereinstimmung mit dem verbundenen Kommunikationssystem eine der folgenden Möglichkeiten:
   - Wenn Währungsbeträge empfangen und gesendet werden sollen, aktivieren Sie das Kontrollkästchen **Währungsbetrag**.
   - Wenn Tarifeinheiten empfangen und gesendet werden sollen, deaktivieren Sie das Kontrollkästchen **Währungsbetrag**.
7) Geben Sie in jeder Zeile mit einer Richtung mit QSIG-Protokoll, welche Tarifeinheiten empfängt und sendet, in **Währung** ein Leerzeichen ein.
8) Wählen Sie aus der Aufklappliste **Rechengenauigkeit** den Eintrag **Keine Nachkommastelle**, **1 Nachkommastelle**, **2 Nachkommastellen**, **3 Nachkommastellen** oder **Über Gebührenimpulse**.
9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.1.5 Wie Sie die Protokollierung der letzten vier Ziffern aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Letzte 4 Ziffern unterdrücken**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Letzte 4 Ziffern unterdrücken**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.1.6 Wie Sie die Protokollierung gehender Anrufe ohne Verbindung aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.

4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Gehend ohne Verbindung**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Gehend ohne Verbindung**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.1.7 Wie Sie die Protokollierung kommender Verbindungen aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Kommende Gespräche protokollieren**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Kommende Gespräche protokollieren**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.1.8 Wie Sie das Verbindungsprotokoll aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Anrufprotokoll ein**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Anrufprotokoll ein**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.1.9 Wie Sie die Protokollierung der MSN aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Ausgabe der MSN ein**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Ausgabe der MSN ein**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.1.10 Wie Sie das Dezimalformat aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Dezimalformat**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Dezimalformat**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.2 Projektkennzahlen

Projektkennzahlen (PKZ) ermöglichen die projektbezogene Zuordnung von Verbindungsdaten und -kosten. Das System protokolliert hierfür in den entsprechenden Verbindungsdatensätzen die von den Teilnehmern am Telefon eingegebenen Projektkennzahlen.

PKZ wird in Verbindung mit der Erfasung von Verbindungsdaten genutzt und steht jedem Teilnehmer zur Verfügung.

Der Teilnehmer kann eine PKZ am Telefon vor Wahlbeginn oder nach Wahlende eingeben. Die Wahl aus einem Client bei aktivierter PKZ ist nicht möglich.

Eine während einer Konferenz mit externen Teilnehmern eingegebene PKZ wird allen beteiligten Verbindungen bzw. Leitungen zugeordnet.

Der Administrator kann einstellen, ob eine PKZ für die Wahlwiederholung gespeichert werden kann.

Das persönliche Telefonbuch kann in einem Eintrag die Kennzahl für das Leistungsmerkmal PKZ + eine PKZ + eine Rufnummer gemeinsam speichern.

PKZ-Eingabeverfahren

Der Administrator legt das PKZ-Eingabeverfahren im LCR-Wahlplan fest:

- Erzwungen

  Die PKZ muss vor Verbindungsbeginn (vor oder nach Belegen einer Richtung) eingegeben werden.
- Freiwillig

  Die PKZ kann freiwillig vor Verbindungsbeginn eingegeben werden. An IP-Telefonen Clients ist die Eingabe zusätzlich während einer Verbindung möglich, auch kommend.

PKZ-Prüfverfahren

Das System kann die Gültigkeit einer eingegebenen PKZ auf folgende Arten prüfen:

- Listenprüfung

  Gültig sind nur vordefinierte PKZ. Nach Eingabe einer gültigen PKZ kann der Teilnehmer unmittelbar weiter wählen. Das System weist eine ungültige PKZ ab. Im Display erscheint "Falscher Eintrag" und es ertönt ein negativer Quittungston.
- Prüfung der Stellenzahl

  Gültig sind alle theoretisch möglichen PKZ mit der konfigurierten Stellenanzahl. Nach Eingabe einer gültigen PKZ durch den Teilnehmer kann unmittelbar weiter gewählt werden.
- Keine Prüfung

  Die PKZ wird nicht auf ihre Gültigkeit hin überprüft. PKZ mit weniger als 11 Stellen muss der Teilnehmer durch Wahl von “#” von den weiteren gewählten Ziffern abgrenzen. Bei ISDN-Endgeräten erfordert diese Variante immer 11-stellige PKZ, ansonsten wird die Wahl nicht ausgeführt.

Wenn der Teilnehmer während einer Verbindung feststellt, dass die einer Verbindung zugeordnete PKZ nicht korrekt ist, kann er eine andere eingeben. Das System überschreibt die aktuell gesetzte PKZ. Die Erfassung von Verbindungsdaten erstellt nach jedem Segment einen Verbindungsdatensatz. Daher werden zuvor abgeschlossene Verbindungsabschnitte mit der alten PKZ gekennzeichnet.

Zugehörige Konzepte

Erfassung von Verbindungsdaten auf Seite 1218

24.1.2.1 Wie Sie eine Projektkennzahl konfigurieren

Mit dem Wizard **Gesprächsdatenerfassung** können Sie Projektkennzahlen konfigurieren.

Voraussetzungen

Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Gesprächsdatenerfassung** zu starten.
4) Geben Sie im Bereich **Projekt-Kennzahlen** in den Eingabefeldern die Projektkennzahlen in der vom Wizard beschriebenen Weise ein.
5) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

24.1.2.2 Wie Sie ein PKZ-Prüfverfahren konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Projekt Kennzahlen**.
4) Wählen Sie in der Zeile der betreffenden PKZ-Liste in der Aufklappliste **Prüfverfahren** den gewünschten Eintrag: **Keine Prüfung**, **Listen-Prüfung** oder **Prüfung der Stellenzahl**.
   a) Wählen Sie ggf. in der Aufklappliste **Anzahl der zu prüfenden Stellen** den gewünschten Wert.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.2.3 Wie Sie die Wahlwiederholung mit PKZ aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Wahlwiederholung mit PKZ**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Wahlwiederholung mit PKZ**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.2 Anzeige und Übertragung von Verbindungsdaten

Die Anzeige und Übertragung von Verbindungsdaten umfasst verschiedene Möglichkeiten der Anzeige im Display der Systemtelefone und zur Dateiübertragung.

24.2.1 Übermittlung von Geldbeträgen (nicht für USA)

Das System kann den vom Netzbetreiber übermittelten Geldbetrag zur aktuellen externen Verbindung im Display des Telefons anzeigen.

Der Netzbetreiber muss die Übermittlung von Geldbeträgen beim Leistungsmerkmal Advice Of Charge (AOC-D oder AOC-S) unterstützen. Das System kumuliert die Beträge der entsprechenden Tarifeinheiten.

Der Geldbetrag kann grundsätzlich zu folgenden Zeiten übermittelt werden:

- Bei Verbindungsbeginn und gegebenenfalls während der Verbindung (AOC-S)
- während der Verbindung (AOC-D)

Über den Parameter Rechengenauigkeit kann der Administrator Ungenauigkeiten bei der Aufzeichnung der Verbindungsdaten vermeiden. Die Rechengenauigkeit bestimmt

- die Anzahl der Nachkommastellen für die Verbindungsdatenauswertung (kleinster Geldbetrag)
- die maximale Summe der kumulierten Geldbeträge.

Die eingestellte Rechengenauigkeit muss mindestens jener von ISDN entsprechen. Falls die maximal möglichen drei Nachkommastellen nicht ausreichen, wird automatisch gerundet. Rechengenauigkeit kann folgende Werte annehmen:

Rechengenauigkeit	kleinster Geldbetrag	Größter Geldbetrag
Keine Nachkommastellen	1	ca. 4,3 Milliarden
1 Nachkommastelle	0,1	ca. 430 Millionen
2 Nachkommastellen (z.B. für Euro)	0,01	ca. 43 Millionen
3 Nachkommastellen (z.B. für Engl. Pound Sterling)	0,001	ca. 4,3 Millionen

24.2.1.1 Wie Sie die Übermittlung von Geldbeträgen konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Faktoren**.
4) Wählen Sie je gewünschter Richtung in der Aufklappliste **Gebührenmode** den Eintrag **während der Verbindung**, **am Ende der Verbindung**, **während / am Ende der Verbindung** oder **keine Gebühren**.
5) Wählen Sie in der Aufklappliste **Rechengenauigkeit** am unteren Ende des Formulars die Anzahl der zu berücksichtigenden Nachkommastellen.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.2.2 Anzeige der Verbindungskosten am Telefon

Das System kann Informationen zu den Kosten einer bestehenden externen Verbindung im Display des Telefons als Geldbetrag anzeigen.

Das System kumuliert die Beträge der entsprechenden Tarifeinheiten. Der Geldbetrag berechnet sich aus den Tarifeinheiten und dem konfigurierten Tariffaktor. Der Service-Provider muss das Leistungsmerkmal Advice Of Charge (AOC) unterstützen.

Die Information zu den Verbindungskosten kann zu folgenden Zeiten übermittelt werden:

- Bei Verbindungsbeginn und gegebenenfalls während der Verbindung (AOC-S)
- Während der Verbindung (AOC-D)
- Bei Verbindungsende (AOC-E)

Bei Verbindungsende zeigt das Display die endgültigen Verbindungskosten für ca. 5 Sekunden an, sofern der Teilnehmer nicht eine andere Aktion startet.

Beim Makeln werden immer die Verbindungskosten für die aktuelle Verbindung angezeigt.

Bei nicht erfolgreicher Übergabe vor Melden wird der Gesamtbetrag angezeigt und berechnet.

Einem Teilnehmer, dem eine Verbindung übergeben wird, werden nur die Verbindungskosten ab diesem Zeitpunkt belastet und angezeigt.

24.2.3 Anzeige der Verbindungsdauer am Telefon

Das System kann die Dauer gehender und kommender externer Verbindungen im Display des Telefons anzeigen.

Das Format ist HH:MM:SS.

Ist die Verbindungsdaueranzeige deaktiviert, zeigt das Display am Telefon stattdessen die Information zu den Verbindungskosten des PSTN an. Ist keine Information zu den Verbindungskosten vorhanden, zeigt das Display die Rufnummer des Gesprächspartners, sofern bekannt.

24.2.3.1 Wie Sie die Anzeige der Verbindungsdauer aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Display**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Gesprächsdauer anzeigen**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Gesprächsdauer anzeigen**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.2.4 Übertragung von Verbindungsdaten

Das System kann Verbindungsdaten in einer Datei über HTTPS übertragen.

Sie können übertragene Datei mit einem geeigneten Programm auswerten.

Eine fortlaufende Ausgabe der Verbindungsdaten ist ausschließlich via CSTA möglich.

Der Administrator kann für Verbindungsdaten zwischen folgenden Formaten (ASCII 8-bit) wählen:

- Komprimiertes Format
- Unkomprimiertes Format

Komprimiertes Format, Standard

Ein Verbindungsdatensatz im komprimierten Format enthält folgende durch | getrennte Felder, wobei CRLF jeden Verbindungsdatensatz abschließt:

Feldpositi	Länge	Beschreibung
1	8	Datum (bei Verbindungsende)
2	8	Uhrzeit (bei Verbindungsende)
3	3	Belegte Amtsleitungsnummer
4	16	Interne Teilnehmernummer
5	8	Klingeldauer der kommenden Verbindung
6	8	Dauer der Verbindung
7	Max. 25	Gewählte oder empfangene externe Rufnummer
8	11	Tarifeinheit/Betrag
9	2	Zusätzliche Informationen, (z.B. kommend, gehend, übergebene Verbindung, Konferenz, DISA, Kosten für Verbindungsaufbau)
10	Max. 11	PKZ

Feldpositi	Länge	Beschreibung
11	Max. 11	Nur bei Mehrgeräteanschluss: benutzte MSN
12	6	Access Code LCR, Amtskennzahl
13	2	Benutzte LCR Route, Wahlregel
14	25	Gewählte oder empfangene Rufnummer (optional)

Beispiele für Verbindungsdatensätze:

- Abgehende Verbindung:

```
13.02.13|14:18:02|201|33388|00:02|00:00:07|0123456789||
1||||||
```

- Ankommende Verbindung:

```
13.02.13|14:28:02|202|33388|00:05|00:00:12|0123456789||
1|||||
```

Komprimiertes Format, USA-spezifisch

Ein Verbindungsdatensatz im komprimierten Format enthält folgende durch | getrennte Felder, wobei CRLF jeden Verbindungsdatensatz abschließt:

Feldpositi	Länge	Beschreibung
1	8	Datum (bei Verbindungsende)
2	8	Uhrzeit (bei Verbindungsende)
3	3	Belegte Amtsleitungsnummer
4	16	Interne Teilnehmernummer
5	8	Klingeldauer der kommenden Verbindung
6	8	Dauer der Verbindung
7	Max. 25	Gewählte oder empfangene externe Rufnummer
8	11	Tarifeinheit/Betrag
9	2	Zusätzliche Informationen, (z.B. kommend, gehend, übergebene Verbindung, Konferenz, DISA, Kosten für Verbindungsaufbau)
10	Max. 11	PKZ
11	Max. 11	Nur bei Mehrgeräteanschluss: benutzte MSN
12	6	Access Code LCR, Amtskennzahl
13	2	Benutzte LCR Route, Wahlregel
14	2	PRI Nodal Service
15	1	PRI WATS-Band
16	3	PRI CIC
17	25	Gewählte oder empfangene Rufnummer (optional)

Anmerkung: In *HKEY_LOCAL_MACHINE\SOFTWARE* muss in den Registrierungsschlüsseln für *Accounting Tool*

der Wert von **DateFormat DWORD** auf 1 festgelegt werden, um das nordamerikanische Datumsformat (MM.TT.JJ) zu erhalten. Standardwert ist 0 und steht für das in Europa und Lateinamerika verwendete Datumsformat (TT.MM.JJ).

Anmerkung: Die Datensätze von Accounting Manager in komprimierter Form sind durch das Trennzeichen | getrennt. Dies kann nur über Manager E konfiguriert werden.

Unkomprimiertes Format

Das unkomprimierte Format eignet sich für Ausdrucke. Außerdem wird eine Kopfzeile und Seitenvorschub ausgegeben. Ein Verbindungsdatensatz im komprimierten Format enthält folgende durch | getrennte Felder:

Feldposition	Zeichenposition, Länge	Beschreibung
1	1-8 (8)	Datum bei Verbindungsende: TT.MM.JJ (TT = Tag: Wertebereich 01 ... 31, MM = Monat: Wertebereich 01 ... 12, JJ = Jahr: Wertebereich 00 ... 99)
2	9-16 (8)	Uhrzeit am Ende des Verbindungsabschnittes bzw. eines nicht beantworteten kommenden Rufes: hh:mm:ss (hh = Stunden: Wertebereich 00 ... 23, mm = Minuten: Wertebereich 00 ... 59, ss = Sekunden: Wertebereich 00 ... 59)
3	17-19 (3)	Leitung: Leitungsnummer Wertebereich: 1 ... 250
4	20-35 (16)	Teilnehmer: interne Teilnehmernummer Bei nicht beantworteten Anrufen wird immer der zuletzt gerufene Teilnehmer ausgegeben (z.B. Sammelanschluss, Anrufumleitung, Rufweiterschaltung). Beim Gruppenruf ist dies der zuletzt eingetragene Teilnehmer. Bei abgefragten Rufen wird der Teilnehmer angegeben, der den Ruf angenommen hat. Ein programmiertes RNR-Präfix (nur bei Vernetzung) wird nicht ausgegeben. Wurde die interne Nummerierung auf einen max. 7-stelligen Rufnummernplan umgewertet, wird die umgewertete Rufnummer ausgegeben. Der internen Teilnehmerrufnummer kann eine maximal 7-stellige Knotenrufnummer vorangestellt werden. Ist die Summe aus Knotenrufnummer und Teilnehmerrufnummer größer als sieben, so werden nur die letzten sieben Ziffern der Nummer ausgegeben.

Feldposition	Zeichenposition, Länge	Beschreibung
5	36-40 (5)	Rufdauer einer kommenden Verbindung: mm:ss (mm = Minuten: Wertebereich 00 ... 59, ss= Sekunden: Wertebereich 00 ... 59) Die Anzeige erfolgt bei allen kommenden Rufen, sofern im System die Ausgabe der "Rufdauer" konfiguriert ist. Bei einem Überlauf des Zählers (Dauer > 59:59) erfolgt die Ausgabe von "59:59". Dies kann z. B. bei einer Datums- oder Uhrzeitumstellung während des Betriebs der Anlage vorkommen. Bei einem kommenden Ruf auf einen besetzten Teilnehmer hat die Rufdauer den Wert „00:00“.
6	41-48 (8)	Dauer der Verbindung bzw. des Verbindungsabschnittes: hh:mm:ss (hh = Stunden: Wertebereich 00 ... 23, mm = Minuten: Wertebereich 00 ... 59, ss = Sekunden: Wertebereich 00 ... 59) Ist bei einem ankommenden Anruf keine Verbindung zustande gekommen, werden 8 Leerzeichen ausgegeben. Bei einem Überlauf des Zählers (Dauer > 23:59:59) erfolgt die Ausgabe von “23:59:59”.
7	49-73 (25)	Gewählte oder, wenn vorhanden, die empfangene externe Rufnummer: nnnnnnnnnnnnnnnnnnnnnnnnn (n = gewähltes oder empfangenes Zeichen: Wertebereich 0 ... 9, *, #, ?) Die Ausgabe erfolgt bei kommenden und gehenden Rufen, sofern vorhanden. Bei gehenden Rufen wird die gewählte Rufnummer bzw. wenn vorhanden, die über COLP übermittelte Rufnummer angezeigt. Bei aktiver Datenschutzfunktion werden die letzten vier gewählten Zeichen ersetzt durch "????" Ist keine Information über die Rufnummer vorhanden, werden 25 Leerzeichen ausgegeben.
8	74-84 (11)	Tarifeinheiten für einen Verbindungsabschnitt: zzzzzzzzzzz (z = Ziffer: Wertebereich 0 ... 9) Es kann zwischen Tarifeinheiten und Geldbeträgen gewählt werden. Die Umrechnung der Tarifeinheiten in Geldbeträge erfolgt anhand des Tariffaktors, der als Währungsbetrag (inklusive eines notwendigen Aufschlags) pro Tarifeinheit definiert ist. Für die Einstellung des Tariffaktors gilt: • Mit Rechengenauigkeit: Tariffaktor = 100% + evtl. notwendiger Aufschlag • Ohne Rechengenauigkeit: Tariffaktor = Betrag/Einheit + evtl. notwendiger Aufschlag In Abhängigkeit von der Rechengenauigkeit erfolgt die Erfassung der Verbindungskosten mit oder ohne Aufschlag: Die Ausgabe erfolgt immer, wenn für den Verbindungsabschnitt Verbindungskosten anfallen (z.B. auch bei übergebenen Verbindungen).

Feldposition	Zeichenposition, Länge	Beschreibung
9	85-86 (2)	Informationselement: zusätzliche Information Wertebereich 0 ... 9 Bedeutung: • 1 = kommende Verbindung (Voice / 3.1 kHz Audio Call) • 2 = gehende Verbindung (Voice / 3.1 kHz Audio Call) • 3 = kommende Verbindung (Sonstige Services) • 4 = gehende Verbindung (Sonstige Services) • 5 = kommende Verbindung weitervermittelt • 6 = gehende Verbindung weitervermittelt • 7 = int/ext/ext Konferenz mit kommender Verbindung / Transit durch Übergabe nach extern • 8 = Konferenz mit gehender Verbindung / Transit durch Übergabe nach extern • 9 = gehende Verbindung über Anrufumleitung zu externem Ziel • 0 = Verbindungs-Info (Ruferliste), wird sofort bei Eintreffen eines kommenden Anrufes ausgegeben (Ausgabe kann unterdrückt werden). Kann z.B. für eine Datenbanksuche von einem PC genutzt werden. Bei mehreren gerufenen Teilnehmern wird für jeden einzelnen Teilnehmer eine Zeile ausgegeben (ohne Rufdauer, Verbindungsdauer und Gebühreninfo). • +10 = Offset als Kennung für Anrufe in Blacklist • +20 = Offset als Kennung für Kosten für den Verbindungsaufbau (ohne Verbindungsdauer) • +30 = Offset als Kennung für einen Folgedatensatz bei – Verbindungsdauer > 24 h. – zusammenhängenden Verbindungsabschnitten mit gleicher Leitungs-/ Teilnehmernummer (z.B. nach dem Übergeben einer Verbindung, nach dem Aufheben einer Konferenz). • +40 = Offset für einen Datensatz mit Transitkennung (durch eine Nebenstelle der Unteranlage). Kann in Kombination mit Offset +30 auftreten. • +50 = Offset als Kennung für DISA-Verbindungen • +70 = Kombination der Offsets +30 und +40
10	87-97 (11)	Vom Benutzer für diese Verbindung eingegebene Projektkennzahl PKZ: pppppppppp (p = Ziffer der PKZ: Wertebereich 0 ... 9) Fehlende Ziffern werden durch Leerzeichen ersetzt.
11	98-108 (11)	Benutzte MSN: mmmmmmmmmm (m = Ziffer der MSN: Wertebereich 0 ... 9) Die Anzeige erfolgt, sofern der Teilnehmer eine MSN-Taste programmiert hat. Bei gehenden Verbindungen eines MULAP-Teilnehmers wird die Rufnummer der belegten MULAP ausgegeben. Fehlende Ziffern werden durch Leerzeichen ersetzt.

Feldposition	Zeichenposition, Länge	Beschreibung
12	109-113 (5)	Benutzte Belegungskennzahl, Access Code: bbbbb (b = Ziffer der Belegungskennzahl: Wertebereich 0 ... 9)
13	114-115 (2)	Benutzte LCR-Route: rr (r = Ziffer der gewählten Route: Wertebereich 0 ... 9)

Kommunikationsablauf

Die Übertragung von Verbindungsdaten kann angefordert werden (Download Request), woraufhin das System entsprechend reagiert (Download Response).

Anschließend kann die Löschung von Verbindungsdaten angefordert werden (Delete Request), woraufhin das System entsprechend reagiert (Download Response).

Download Request – Definition

Element	Inhalt
HTTP-Kopf	Anforderungsmethode = GET
URL	https://<IP-Adresse des Systems>/management/portlet
Parameter	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=get
	username=<username>
	password=<password>

Anmerkung: Beim Zugriff auf Gebührendaten mit der referenzierten Schnittstelle gelten die Einschränkungen der HTTP GET-Anforderung. Die folgenden Sonderzeichen dürfen nicht als Passwort verwendet werden, wenn jemand versucht, Daten über eine URL-Anfrage zu erhalten:

:/?#[]@ !$&'()*+,;=

Beispiel:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Download Response – Definition

Element	Inhalt
HTTP-Kopf	ContentType = "text/plain"
Parameter	attachment filename = "<charging file>"

Element	Inhalt
	data=<content of the charging file>

Response-Code	Bedeutung
SC_OK(200)	Erfolgreich
SC_BAD_REQUEST(400)	Fehlender Parameter in Request
SC_UNAUTHORIZED(401)	Anmeldung fehlgeschlagen oder username bzw. password falsch
SC_INTERNAL_SERVER_ERROR(500)	Interner Fehler

Delete Request – Definition

Element	Inhalt
HTTP-Kopf	Anforderungsmethode = POST
URL	https://<IP-Adresse des Systems>/management/portlet
Parameter	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=delete
	username=<username>
	password=<password>

Beispiel:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Delete Response – Definition

Response-Code	Bedeutung
SC_OK(200)	Erfolgreich
SC_BAD_REQUEST(400)	Fehlender Parameter in Request
SC_UNAUTHORIZED(401)	Anmeldung fehlgeschlagen oder username bzw. password falsch
SC_INTERNAL_SERVER_ERROR(500)	Interner Fehler

Zugehörige Konzepte

Accounting-Tools auf Seite 1237

24.2.4.1 Wie Sie das Format auswählen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie das Komprimierte Format wünschen, aktivieren Sie das Kontrollkästchen **Komprimiertes Ausgabeformat**.
   - Wenn Sie das Unkomprimierte Format wünschen, deaktivieren Sie das Kontrollkästchen **Komprimiertes Ausgabeformat**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.2.4.2 Wie Sie die Übertragung von Verbindungsdaten über HTTPS aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gebühren** > **Gebühren Ausgabe**.
4) Wählen Sie in der Aufklappliste **Ausgabe** eine der folgenden Möglichkeiten:
   - Wenn Sie das Leistungsmerkmal aktivieren möchten, wählen Sie den Eintrag **HTTPS**.
   - Wenn Sie das Leistungsmerkmal deaktivieren möchten, wählen Sie den Eintrag **Keine**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.3 Kostenkontrolle

Kostenkontrolle umfasst die Leistungsmerkmale Hinweis auf teure Verbindungswege und Schutz vor Gebührenbetrug.

24.3.1 Hinweis auf teure Verbindungswege

Ist ein Anrufziel momentan nicht über den preisgünstigsten Verbindungsweg erreichbar, kann das Telefon dem Teilnehmer einen Hinweis auf den teureren Verbindungsweg geben.

Der Teilnehmer kann so entscheiden, ob er die Verbindung trotz des teureren Verbindungsweges zu diesem Zeitpunkt führen will. Der Hinweis kann auf verschiedene Weise erfolgen:

- Text im Display
- Ton
- Text im Display und Ton

Das System weist auf den teuren Verbindungsweg hin, wenn in der Wegetabelle eine entsprechende Warnung konfiguriert ist und es nicht die Richtung von Index 1 der Wegetabelle benutzt.

Der Hinweis im Display wird nur angezeigt, wenn für die zugehörige Wahlregel kein Name konfiguriert ist. Ist ein Name konfiguriert, wird dieser angezeigt.

24.3.1.1 Wie Sie einen Hinweis auf einen teuren Verbindungsweg konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **LCR**.
3) Klicken Sie im Menübaum auf **Routing** > **LCR** > **Wegetabelle** und auf die betreffende Wegetabelle.
4) Wählen Sie für jeden teuren Verbindungsweg (Spalte **Richtung**) in der Aufklappliste **Warnung** den gewünschten Eintrag: **Ton**, **Display** oder **Display + Ton**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.3.2 Schutz vor Gebührenbetrug

Das System kann Verbindungen überwachen, um einen potenziellen Gebührenbetrug zu erkennen (Toll Fraud Monitoring). Dies betrifft Verbindungen, die über eine Amtsleitung ankommen und wieder über eine Amtsleitung abgehen.

Der erste Teilnehmer signalisiert die Überschreitung der konfigurierten Verbindungsdauer und ermöglicht so, die Verbindung bei Bedarf zu trennen. Als Administrator können Sie konfigurieren ob bzw. nach welcher Verbindungsdauer eine derartige Verbindung signalisiert werden soll.

24.3.2.1 Wie Sie den Schutz vor Gebührenmissbrauch aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Zeitparameter**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie Schutz vor Gebührenmissbrauch aktivieren möchten, wählen Sie für **Timer für Toll Fraud Monitoring** in der Aufklappliste **Basis** den gewünschten Eintrag und geben Sie im Feld **Faktor** einen von 255 abweichenden Wert ein. **Basis** * **Faktor** ergibt dann die Verbindungsdauer, nach welcher eine potenziell betrügerische Verbindung signalisiert wird.
   - Wenn Sie Schutz vor Gebührenmissbrauch deaktivieren möchten, geben Sie für **Timer für Toll Fraud Monitoring** im Feld **Faktor** 255 ein.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.4 Accounting-Tools

Accounting Tools bietet Accounting Manager und Teledata Office.

Zugehörige Konzepte

Service Center – Dokumente auf Seite 127
Übertragung von Verbindungsdaten auf Seite 1228

24.4.1 Accounting Manager

Accounting Manager ist eine Windows-Anwendung zum Abruf von Verbindungsdaten über HTTPS und zu deren Auswertung in Tabellen und Grafiken.

Accounting Manager beinhaltet eine eigene Dokumentation. Accounting Manager ruft Verbindungsdaten von einzelnen Netzknoten ab. Sie können Accounting Manager auch zum Testen der Schnittstelle für Verbindungsdaten verwenden. Sie können Accounting Manager im **Service Center** des WBM herunterladen. Accounting Manager erfordert lokale Administrationsrechte und die Aktivierug von TLS 1.2 in Microsoft Internet Explorer.

24.4.2 Teledata Office

Teledata Office ist eine Windows-Anwendung für die Auswertung von Verbindungsdaten.

25 Wartung

Das System bietet vielfältige Maintenance-Möglichkeiten. Dazu gehören das Ändern von Telefonie-Einstellungen, das Sichern und Wiederherstellen der Konfigurationsdaten, das Aktualisieren der Software durch Update und Upgrade und Restart-/Reload-Funktionen. Darüber hinaus stehen Funktionen zur Statusermittlung, Überwachung und Wartung zur Verfügung. Durch verschiedene Remote Services ist ein Fernzugriff auf das System möglich.

Wartung des UC Booster Servers

Wird zusätzlich zum Kommunikationssystem ein UC Booster Server betrieben, so bietet auch der UC Booster Server einige Maintenance-Möglichkeiten. Für die Wartung des UC Booster Servers gibt der Administrator beim Aufruf des WBM nicht die IP-Adresse des Kommunikationssystems an, sondern die IP-Adresse des Linux-Servers.

25.1 Telefonie-Konfiguration

Das Kommunikationssystem bietet verschiedene Konfigurationsmöglichkeiten für Telefonie, z.B. Datum und Uhrzeit, SNTP, Kundenindividuelle Displayanzeige, und Wartemusik.

25.1.1 Datum und Uhrzeit

Das Kommunikationssystem enthält eine Systemuhr mit Datum und Uhrzeit. myPortal und jedes Display eines Endgerätes zeigt diese Systemzeit.

Sie können die Systemzeit grundsätzlich auf folgende Weise festlegen bzw. synchronisieren:

- Über einen Zeitserver mittels SNTP
- Über eine ISDN-Amtsleitung durch einen gehenden Anruf
- Durch manuelle Einstellung

Nach Aktivierung eines SNTP-Servers ist keine systemindividuelle Einstellung der Systemzeit mehr möglich.

Sollte ein SNTP-Server einmal nicht erreichbar sein und HFA-Systemtelefone eine andere Zeitquelle als das System nutzen, so kann die dort angezeigte Zeit von der Systemzeit abweichen.

Eine nach dem Anlagenhochlauf manuell eingestellte Systemzeit wird immer beim ersten gehenden ISDN-Gespräch durch die ISDN-Zeitinformation überschrieben, vorausgesetzt, der Netzbetreiber übermittelt diese Information. Liegt bei laufender Anlage die Differenz einer manuell eingestellten Systemzeit zur ISDN-Zeitinformation zwischen 2 und 70 Minuten, wird die ISDN-Zeitinformation übernommen. Anderenfalls wird die manuell eingestellte Systemzeit beibehalten.

Für die Darstellung des Datums im Telefondisplay kann der Administrator eines der folgenden Formate auswählen. Das Format ist zusätzlich abhängig vom Typ des Telefons:

Datumformat	OpenStage	OptiPoint 410, OptiPoint 420
Europa	Di 20.11.07	20. NOV 07
USA	Di 11/20/07	Di NOV 20.07
International1	Di 20.11.07	DI 20 NOV 07
International2	Di 20.11.07	DI 20.11.07

Wenn Sie als Administrator versehentlich ein Datum vor 2007 einstellen, können Sie anschließend nicht mehr auf das WBM zugreifen. Dies ist erst nach einem Restart wieder möglich, der das Datum auf 01.01.2007 zurücksetzt.

25.1.1.1 Wie Sie Datum und Uhrzeit manuell konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Führen Sie die folgenden Schritte durch, wenn das System Datum und Uhrzeit und weder über digitale Amtsleitungen noch über SNTP bezieht.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbereich auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Datum und Uhrzeit** > **Datum und Uhrzeit**.
4) Geben Sie **Datum und Uhrzeit** ein.
5) Klicken Sie auf **Übernehmen**.
6) Klicken Sie auf **Abmelden**.
7) Melden Sie sich am WBM ab und erneut an.

25.1.1.2 Wie Sie die Zeitzone einstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbereich auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Datum und Uhrzeit** > **Zeitzonen-Einstellungen**.
4) Wählen Sie in der Aufklappliste die **Zeitzone**.
5) Klicken Sie auf **Übernehmen**.
6) Melden Sie sich am WBM ab und erneut an.

25.1.1.3 Wie Sie das Datumsformat konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbereich auf **Telephony Server** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Display**.
4) Wählen Sie in der Aufklappliste das **Datumsformat**.
5) Klicken Sie auf **Übernehmen**.

25.1.2 SNTP

Über SNTP können Sie Datum und Uhrzeit Ihrer Systeme netzweit mit NTP-Zeitservern synchronisieren.

SNTP (Simple Network Time Protocol) ist eine vereinfachte Version des NTP (Network Time Protocol), ein Standard zur Synchronisierung von Datum und Uhrzeit über paketbasierte Kommunikationsnetze. Um Datum und Uhrzeit zu synchronisieren, benötigt Ihr System eine Verbindung zu einem NTP-Server. Dieser kann sich in Ihrem lokalen Netzwerk oder im Internet befinden. Im Internet gibt es frei zugängliche NTP-Server, aus denen Sie sich einen in Ihrer Zeitzone gelegenen auswählen können. Beachten Sie die Nutzungsbedingungen des entsprechenden Servers und fragen Sie um Erlaubnis, wenn dies nötig ist.

25.1.2.1 Wie Sie das Datum und die Uhrzeit von einem SNTP-Server beziehen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbereich auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Datum und Uhrzeit** > **SNTP-Einstellungen**.
4) Geben Sie **IP-Adresse / DNS-Name des externen Zeitservers** ein, z.B. `0.de.pool.ntp.org`.
5) Wählen Sie in der Aufklappliste **Administrativer Betriebszustand des SNTP-Servers** den Eintrag **Aktiviert**.
6) Wählen Sie in der Aufklappliste **Pollzeit für externen Zeitserver** das gewünschte Zeitintervall für das Beziehen von Datum und Uhrzeit vom SNTP-Server.
7) Klicken Sie auf **Übernehmen**.
8) Melden Sie sich am WBM ab und erneut an.

25.1.3 Telefon-Logos

Systemtelefone mit Display können ein kundenindividuelles Logo als Hintergrund der Telefonie-Oberfläche anzeigen.

Als Administrator können Sie Telefon-Logos für Systemtelefone mit Display importieren, zuweisen oder aus dem System löschen. Unterschiedliche Typen von Systemtelefonen können unterschiedliche Telefon-Logo verwenden.

Zugehörige Konzepte

Update der Systemtelefone auf Seite 1269

25.1.3.1 Telefon-Logo ins System laden

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Die Bilddatei mit dem Telefon-Logo erfüllt die Voraussetzungen:

Telefon	Format	Farbe
OpenStage 40	112 x 32, BMP	monochrom
OpenStage 60 OpenStage 80	240 x 71, JPEG	monochrom oder farbig
OpenScape Desk Phone CP 400 OpenScape Desk Phone CP 400T/405T	112 x 32, BMP	monochrom
OpenScape Desk Phone CP 600/700/700X OpenScape Desk Phone CP 710	220 x 70, PNG	24-Bit mit Alpha (Transparenz)
OpenScape Desk Phone CP 600E	220 x 70, PNG	24-Bit mit Alpha (Transparenz) oder 256 Graustufen mit Alpha

Sie haben Zugriff auf die Bilddatei mit dem Telefon-Logo im Dateisystem des Administrations-PCs.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Logo-Images** > **Laden**.
4) Klicken Sie auf **Durchsuchen**, um eine entsprechende Bilddatei auszuwählen.
5) Klicken Sie auf **Laden**.

25.1.3.2 Wie Sie ein Telefon-Logo an Systemtelefone verteilen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Logo-Images** > **Verteilen**.
4) Aktivieren Sie in der Zeile des zu verteilenden Telefon-Logos das Kontrollkästchen **Verteilen**.
5) Wählen Sie in der Aufklappliste **An Workpoints folgenden Typs verteilen** den gewünschten Systemtelefontyp aus.
6) Klicken Sie auf **Übernehmen**.

25.1.3.3 Wie Sie ein Telefon-Logo löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Sie haben Zugriff auf die Bilddatei mit dem Telefon-Logo im Dateisystem des Administrations-PCs.

Um ein Telefon-Logo aus dem Kommunikationssystem zu löschen führen Sie folgende Schritte durch:

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Logo-Images** > **Laden**.
4) Aktivieren Sie in der Zeile des zu löschenden Telefon-Logos das Kontrollkästchen **Löschen**.
5) Wenn Sie weitere Telefon-Logos löschen wollen, wiederholen Sie den vorherigen Schritt.
6) Klicken Sie auf **Löschen**. Alle markierten Telefon-Logos werden aus dem Kommunikationssystem gelöscht.

25.1.4 Kundenindividuelle Displayanzeige

Kundenindividuelle Displayanzeige ermöglicht die Anzeige z.B. des Firmennamens im Display von Systemtelefonen im Ruhezustand.

Veränderbar ist ausschließlich der rechte Teil (max. 18 Zeichen) der zweiten Displayzeile, der standardmäßig mit „OpenScape“ belegt ist. Der Text wird linksbündig zum Datum eingerückt, soweit die Länge des Textes dies zulässt:

```
16:30       FR 29.FEB 08         123456  Hotel zur Post >
```

25.1.4.1 Wie Sie die kundenindividuelle Displayanzeige (System-Name) ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **Gateway**.
4) Geben Sie im Feld **System-Name** den anzuzeigenden Namen ein.

   Anmerkung: Verwenden Sie keine anderen Zeichen als A-Z, a-z und 0-9.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.1.5 Mehrsprachige Textausgabe

Die Sprache für Displaymeldungen lässt sich systemweit oder auch teilnehmerindividuell auswählen.

Verfügbare Sprachen: Chinesisch, Dänisch, Deutsch, Englisch, Estnisch, Finnisch, Französisch, Griechisch, Italienisch, Katalanisch, Lettisch, Litauisch, Niederländisch, Norwegisch, Polnisch, Portugiesisch, Russisch, Schwedisch, Serbokroatisch, Slowakisch, Slowenisch, Spanisch, Deutsch (Telekom), Tschechisch, Türkisch, Ungarisch, Englisch (US), Serbisch, Bulgarisch, Rumänisch und Mazedonisch.

Die grundsätzliche Spracheinstellung wird beim Systemhochlauf durch die Länderinitialisierung vorgenommen.

Zugehörige Konzepte

Konfiguration der Teilnehmer auf Seite 454

Zugehörige Tasks

Wie Sie IP- und SIP-Teilnehmer konfigurieren auf Seite 199

25.1.6 Flexible Menüs

Flexible Menüs ermöglichen die kundenindividuelle Anpassung der Menüpunkte im Display der Systemtelefone.

Als Administrator können Sie die Menüpunkte einzeln aus- oder einblenden.

25.1.6.1 Wie Sie das flexible Menü ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen** > **System** > **Flexible Menüs**.
4) Bearbeiten Sie die **Ausblendliste** wie folgt:
   - Um einen Menüpunkt auszublenden, aktivieren Sie dessen Kontrollkästchen.
   - Um einen Menüpunkt einzublenden, deaktivieren Sie dessen Kontrollkästchen.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.1.7 Wartemusik

Das Kommunikationssystem kann wartenden Teilnehmern während Vermittlungsvorgängen Wartemusik (Music On Hold, MOH) einspielen. Anrufer hören die Wartemusik, während sie gehalten, geparkt oder übergeben werden. Dies gilt auch für Anrufer in der Warteschlange der Anrufverteilung.

Das System kann Wartemusik aus folgenden Quellen einspielen:

- Wartemusik (MOH)
- EXMR

  Siehe Installation OpenScape Business X1/X1W, Service Dokumentation oder Installation OpenScape Business X3/X5/X8, Service Dokumentation.
- MUSIC Einsteckmodul

  Siehe Installation OpenScape Business X1/X1W, Service Dokumentation oder Installation OpenScape Business X3/X5/X8, Service Dokumentation.
- Baugruppe MPPI-USB EXM Modul (nur für OpenScape Business X3/X5)

  Siehe Installation OpenScape Business X3/X5/X8, Service Dokumentation.

Audio-Dateien

Der Administrator kann Audio-Dateien für die interne Wartemusik vom PC in das Kommunikationssystem übertragen als alternative interne Wartemusik.

Anmerkung: Bitte vergewissern Sie sich vorher, dass Sie mit der Benutzung von Ansagen oder Wartemusik keine Copyright-Verletzungen begehen.

Wichtig: Wenn der gehaltene Teilnehmer ein IP Workpoint Client oder ein IP-Trunk ist, wird die interne MOH verwendet. Externe MOH ist für IP nicht vorgesehen.

Die Audio-Dateien müssen als `Wave`-Dateien vorliegen mit folgenden Eigenschaften:

- 16 bit PCM
- Mono oder Stereo
- Mögliche Abtastraten: 8 / 22,05/ 24 / 32 / 40 / 44,1 oder 48 kHz.

- Länge des Audio-Dateinamens maximal: 30 Zeichen

Empfohlen: **16 bit PCM - Mono - 8 kHz, Länge ca. 2 min**

Wartemusik (MOH)

Für Tag - und Nachtbetrieb (Nachtschaltung) kann unterschiedliche Wartemusik konfiguriert werden.

Anmerkung: Bei UC Suite gibt es keinen Unterschied zwischen Tag- und Nachtdateien. Die **Wartemusik-Datei - Tag** wird verwendet.

Der Administrator kann folgende Funktionen konfigurieren:

- Wartemusik mit Rufton (Freiton):

  Der gehaltene Teilnehmer hört während der Rückfrage zunächst die Wartemusik. Nach Übergeben des gehaltenen Teilnehmers an das Ziel ertönt an Stelle der Wartemusik der Rufton.
- Wartemusik ohne Rufton (Freiton):

  Der gehaltene Teilnehmer hört die Wartemusik, bis der gerufene Teilnehmer den Anruf annimmt.
- Keine Wartemusik:

  Der gehaltene Teilnehmer hört nichts (Stille). Wird ein externes Gespräch durch Übergabe vor Melden übergeben, hört der Anrufer das Freizeichen.

25.1.7.1 Wie Sie interne Wartemusik importieren

Mit dem Wizard **Wartemusik / Ansagen** können Sie Audiodateien als interne Wartemusik in das Kommunikationssystem importieren.

Voraussetzungen

Sie sind am WBM angemeldet.

Die einzuspielenden Audio-Dateien liegen als WAVE-Dateien im geforderten Format vor.

Anmerkung: Stellen Sie vor der Benutzung sicher, dass Sie keine Copyright-Verletzung begehen.

Anmerkung: Bei UC Suite gibt es keinen Unterschied zwischen Tag- und Nachtdateien. Die **Wartemusik-Datei - Tag** wird verwendet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards** > **Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Wartemusik / Ansagen** zu starten.

4) Klicken Sie für Tagbetrieb bei **Wartemusik-Datei - Tag** und/oder für Nachtbetrieb bei **Wartemusik-Datei - Nacht** auf **Durchsuchen**.
5) Wählen Sie eine Audio-Datei aus und klicken Sie auf **Öffnen**. Der Pfad zur gewählten Audio-Datei wird bei **Wartemusik-Datei - Tag** und/oder **Wartemusik-Datei - Nacht** angezeigt.
6) Klicken Sie auf **Laden**.
7) Bestätigen Sie den Hinweis mit **OK** und klicken Sie auf **OK & Weiter**.
8) Klicken Sie auf **Fertig**.

25.1.7.2 Wie Sie die Funktion der internen Wartemusik konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Die Länge des Wartemusik-Dateinamens beträgt maximal 30 Zeichen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Anschaltungen**.
3) Klicken Sie im Menübaum auf **Anschaltungen** > **Ansage / Interne Wartemusik**.
4) Wählen Sie im Bereich **Interne Wartemusik** in der Aufklappliste **MOH Typ** den Eintrag **Kein Music On Hold**, **MOH ohne Rufton** oder **MOH mit Rufton**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.1.7.3 Wie Sie die interne Wartemusik für jede VBZ-Gruppe ändern

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Anschaltungen**.
3) Klicken Sie im Menübaum auf **Anschaltungen > Ansage / Interne Wartemusik**.
4) Klicken Sie auf die Registerkarte **Wartemusik bearbeiten**.
5) Wählen Sie in der Zeile der der entsprechenden Verkehrsbeziehungsgruppe in der Aufklappliste Audiodatei die gewünschte Wartemusik.
6) Wenn einer VBZ-Gruppe keine Wartemusik zugeordnet ist, gilt für diese die interne Wartemusik
7) Geben Sie in der Zeile der entsprechenden Verkehrsbeziehungsgruppe eine Beschreibung ein.
8) Klicken Sie auf **Übernehmen**.
9) Klicken Sie auf **OK**.

Anmerkung: Diese Funktionalität gilt nur für OpenScape Business S Systeme und wird von OpenScape Business X nicht unterstützt.

25.1.8 Ansagen

Das Kommunikationssystem bietet die Möglichkeit, vor der Beantwortung eines Anrufs sowie bei der Anrufverteilung und der MFV-Direktwahl eine Warteschleifenansage für den Anrufer abzuspielen. Sie können auch die Wartemelodie in bestimmten Situationen durch eine Ansage ersetzen, z. B. wenn ein Teilnehmer in die Warteschleife gelegt wird oder wenn ein Teilnehmer besetzt ist oder weitergeleitet wird.

Das System kann Ansagen aus den folgenden Quellen importieren:

- Interne Ansagen
- Ansage-Player (nur mit UC Booster-Funktionalität)

  Der Ansage-Player ist ein internes Softwareprogramm, das zusammen mit der UC Booster-Funktionalität (UC Booster Card oder UC Booster Server) verfügbar ist. Beim Anruf eines Teilnehmers spielt der Ansage-Player zunächst die gewünschte Ansage ab und erstellt dann die Verbindung zum Teilnehmer.
- Analoges Ansagegerät

  Siehe Abschnitt Hilfsmittel - Analoges Ansagegerät in der *OpenScape Business, Administratoren-Dokumentation*.
- MPPI-USB-EXM-Modul (nur für OpenScape Business X3/X5)

  Weitere Informationen finden Sie unter *Installation von OpenScape Business X3/X5/X8, Service-Dokumentation*.

Der Administrator kann Ansagen für die einmalige (Start/Stopp) oder kontinuierliche Wiedergabe konfigurieren.

Ein externes Ansagegerät muss sich wie ein Teilnehmer verhalten, d. h. sich selbst ansagen, die Ansage abspielen und das Gespräch vermitteln (Rückfrage halten, wählen und auflegen).

Audiodateien

Der Administrator kann Audiodateien mit Ansagen vom PC auf das Kommunikationssystem übertragen.

Anmerkung: Bitte vergewissern Sie sich vorher, dass Sie mit der Benutzung von Ansagen oder Wartemusik keine Copyright-Verletzungen begehen.

Die Audiodateien müssen als `Wave`-Dateien mit den folgenden Eigenschaften verfügbar sein:

- 16 Bit PCM
- Mono oder Stereo
- Mögliche Abtastraten: 8 / 22,05 / 24 / 32 / 40 / 44,1 oder 48 kHz
- Maximale Länge für den Namen der Audiodatei: 30 Zeichen

Empfohlen: **16 Bit PCM - Mono - 8 kHz, Länge ca. 2 min**

25.1.8.1 So konfigurieren Sie die Ansagen (UC Suite & UC Booster)

Der Assistent für **Wartemusik / Ansagen** kann zur Konfiguration von Ansagen verwendet werden.

Voraussetzungen

- Aktivieren Sie im **Expertenmodus > Middleware > Ansage-Player** das Kontrollkästchen **Service wird automatisch gestartet**, um den Ansage-Player zu aktivieren.
- Eine Ansage-Player-Rufnummer sollte im **Expertenmodus > Grundeinstellungen > Voicemail / Ansage-Player** eingestellt sein.
- Vergewissern Sie sich, dass die Nummer im **Expertenmodus > LCR > Wahl-Plan** unter dem Feld **Ansage-Player** korrekt konfiguriert ist.
- Die zugehörige **Routing-Tabelle** ist auf **12** gesetzt, **UC Suite** ist für **Route** und **MEB** ist für **Wahl-Regel**eingestellt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Assistenten** > **Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Assistenten für **Wartemusik / Ansagen** zu starten.

4) Überspringen Sie die Auswahl von **Wartemusikdateien über HTTP-Dateien laden**, indem Sie auf **OK & Weiter** klicken.

Anmerkung: Stellen Sie vor der Benutzung sicher, dass Sie keine Copyright-Verletzung begehen.

---

5) Um eine Audiodatei an das Kommunikationssystem zu übertragen, gehen Sie wie folgt vor:

a) Klicken Sie auf **Datei auswählen**.
b) Wählen Sie eine Audiodatei aus.
c) Klicken Sie auf **Öffnen**.
d) Klicken Sie auf **Laden**.
e) Bestätigen Sie die Nachricht mit **OK**.
f) Wenn Sie weitere Audiodateien in das System laden möchten, wiederholen Sie diese Schritte.

6) Klicken Sie auf **OK & Weiter**.

Tipp: Die Konfigurationsparameter für **Ansagen** sind ebenfalls beschrieben und können über **Expertenmodus > Hilfsausrüstung > Ansagen** konfiguriert werden.

---

7) Wählen Sie in der Spalte **Typ** den Typ der abzuspielenden Ansage aus.

8) Wählen Sie in der Spalte **Zugang** den Anschluss, an dem das Gerät angeschlossen ist. Über externe Ziele können Ansagegeräte in einem anderen Systemknoten angesprochen werden.

9) Wählen Sie eine Ansagedatei aus der Dropdown-Liste in der Spalte **Wave-Datei** aus (nur für den Typ **Ansage-Player** und im UC Suite-Modus).

10) Wählen Sie den Typ der Wiedergabe aus der Dropdown-Liste in der Spalte **Modus**.

11) Klicken Sie auf **OK & Weiter** gefolgt von **Fertigstellen**.

25.1.8.2 So konfigurieren Sie die Ansagen (UC Smart)

Der Assistent für **Wartemusik / Ansagen** kann zur Konfiguration von Ansagen verwendet werden.

Voraussetzungen

Analoge Ports, die als Ansage-Ports eingerichtet sind, müssen unter **Durchwahl-Typ** den Wert **Anrufbeantworter** zugewiesen bekommen.

EVM-Ports, die als Ansage-Ports eingerichtet sind, sollten:

- unter **Durchwahl-Typ** den Wert **Standard** zugewiesen bekommen.
- aus dem Sammelanschluss der Sprachbox entfernt werden.
- der Rufnummer des Ports im Expertenmodus eine Sprachbox zugewiesen werden**Expertenmodus > Zusatzgeräte > Smart VM**.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Assistenten** > **Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Assistenten für **Wartemusik / Ansagen** zu starten.
4) Überspringen Sie die Auswahl von **Wartemusikdateien über HTTP-Dateien laden**, indem Sie auf **OK & Weiter** klicken.

Tipp: Die Konfigurationsparameter für **Ansagen** sind beschrieben und können über Expertenmodus > Hilfsausrüstung > Ansagen konfiguriert werden.

---

5) Wählen Sie in der Spalte **Typ** den Typ der abzuspielenden Ansage aus.
6) Wählen Sie in der Spalte **Zugang** den Anschluss, an dem das Gerät angeschlossen ist. Über externe Ziele können Ansagegeräte in einem anderen Systemknoten angesprochen werden.
7) Wählen Sie eine Ansagedatei aus der Dropdown-Liste in der Spalte **Wave-Datei** aus (nur für den Typ **Ansage-Player** und im UC Suite-Modus).
8) Wählen Sie den Typ der Wiedergabe aus der Dropdown-Liste in der Spalte **Modus**.
9) Klicken Sie auf **OK & Weiter** gefolgt von **Fertigstellen**.

25.1.9 Teilnehmer-zu-Teilnehmer Zeichengabe

Das Kommunikationssystem ermöglicht die transparente Übertragung von Nachrichten zwischen Endgeräten (User to User Signalling, UUS). Unterstützt wird die Variante UUS1 für den Austausch von Informationen in Steuernachrichten des Verbindungsauf- und Abbaus.

Bei einem Mehrgeräte-Anschluss ist zu gewährleisten, dass maximal ein Endgerät auf einen ankommenden Ruf eine Nachricht übermittelt.

25.1.10 Sprachkanal-Signalisierungsschutz

Das Kommunikationssystem bietet einen durch den Administrator einrichtbaren Schutz vor Datenverfälschung durch unerwünschte Toneinblendungen in den Sprachkanal. Aufschalten auf eine so geschützte Verbindung ist nicht möglich. Jeder als Fax konfigurierte Teilnehmer hat diesen Signalisierungsschutz automatisch.

Wiederanrufe werden bis zum Freiwerden der Nebenstelle zurückgestellt.

Ein gehaltener Teilnehmer hat immer Signalisierungsschutz.

25.1.11 Zeitparameter

Das Kommunikationssystem bietet dem Administrator Einstellmöglichkeiten für diverse Zeitparameter, wie z.B. für die Dauer des Rückrufes oder die Zeit für automatische Wahlwiederholung.

Die Zeitparameter sind im Kommunikationssystem voreingestellt und müssen in der Regel nicht verändert werden.

25.1.12 Steuerung von Centrex-Leistungsmerkmalen

Zur Steuerung von Centrex-Leistungsmerkmalen müssen die Wählzeichen * und # ins ISDN und zu ITSP übertragen werden.

Als Administrator können Sie dieses Leistungsmerkaml aktivieren oder deaktivieren.

Die Eingabe einer Kennzahl muss im Wahlzustand erfolgen (zum Beispiel nach Eingabe der Leitungskennzahl). Die Eingabe beginnt immer mit * oder #, gefolgt von einer Ziffer oder Ziffernkombination und endet mit #.

25.1.12.1 Wie Sie die Steuerung von Centrex-Leistungsmerkmalen aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Grundeinstellungen**.
3) Navigieren Sie im Menübaum zu **System** > **System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Steuerung von Centrex-Leistungsmerkmalen aktivieren möchten, aktivieren Sie das Kontrollkästchen **Wahl von * und # auf Leitungsschnittstellen**.
   - Wenn Sie die Steuerung von Centrex-Leistungsmerkmalen deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Wahl von * und # auf Leitungsschnittstellen**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.2 Sichern und Wiederherstellen

Die Konfigurationsdaten des Kommunikationssystems können gesichert und wiederhergestellt werden.

Die Konfigurationsdaten werden in einem Backup-Set abgespeichert. Jede Sicherung erzeugt ein eigenes Backup-Set. Die Sicherung kann sofort manuell oder automatisch zu bestimmten Zeitpunkten durchgeführt werden.

Anmerkung: Es wird dringend empfohlen, die Konfigurationsdaten regelmäßig als Backup-Sets zu sichern.

Bei einem Update auf ein neues Minor Release ist es erforderlich, ein neues Backup-Set zu erstellen.

Jedes Backup wird mit einem systemspezifischen Schlüssel verschlüsselt.

Ein verschlüsseltes Backup-Set kann nur für die Wiederherstellung des Systems verwendet werden, von dem das Backup verschlüsselt wurde.

Es kann auf unterschiedliche Backup-Medien gesichert werden (wie z.B. auf ein USB-Medium, ein Netzlaufwerk oder die Festplatte der UC Booster Card).

Abhängig von der Systemkonfiguration, der Nutzung des Kommunikationssystems und der Art des Backup-Mediums kann eine Sicherung oder Wiederherstellung eine längere Zeit in Anspruch nehmen - bei Systemen mit UC Suite im Einzelfall bis zu drei Stunden. Dieser Vorgang sollte nicht manuell oder durch einen System-Neustart abgebrochen werden.

Der Abbruch einer Datenwiederherstellung kann zu einer inkonsistenten Systemkonfiguration führen, in der ein fehlerfreier Betrieb des Systems nicht gewährleistet ist. Eine abgebrochene Wiederherstellung sollte unbedingt wiederholt werden, bis diese erfolgreich abgeschlossen ist. Andernfalls kann eine vollständige Neueinrichtung des Systems erforderlich werden. Falls die Wiederherstellung mehrfach fehlschlägt, verständigen Sie bitte den Service-Support und stellen Sie zwischenzeitlich sicher, dass ihre Datensicherung nicht durch neue Backups überschrieben wird. Dazu muss die automatische Datensicherung vorübergehend deaktiviert werden.

Backup-Set für Diagnosezwecke

Für Diagnosezwecke können "kleinere" Backup-Sets erzeugt werden, die Daten für die Fehlersuche durch den Service-Support enthalten. Im Gegensatz zu den normalen Backup-Sets werden wesentlich kleinere Datenmengen erzeugt und damit zum Beispiel ein einfaches Versenden per E-Mail ermöglicht. Diagnose-Backup-Sets enthalten unter anderem die Konfigurationsdaten des Kommunikationssystems und der installierten UC-Lösung. Sprachnachrichten, Faxnachrichten und Ansagen sind nicht enthalten.

Backup-Verzeichnis "Hard disk" (nur bei UC Booster Card)

Ist die UC Booster Card gesteckt, können die Konfigurationsdaten des Kommunikationssystems in einer eigenen Partition der Festplatte der UC Booster Card im Backup-Verzeichnis gespeichert werden. Dieses Backup-Verzeichnis ist als Standard-Archiv "Harddisk" bereits vorgeleistet.

Sicherung der Konfigurationsdaten des UC Booster Servers

Wird zusätzlich zum Kommunikationssystem ein UC Booster Server betrieben, so sollte bei einer Sicherung der Konfigurationsdaten des Systems auch die Konfigurationsdaten des UC Booster Servers gesichert werden. Der Sicherung der Daten des UC Booster Servers erfolgt identisch zum Sicherung der Daten des Kommunikationssystems, nur dass der Administrator beim Aufruf des WBM nicht die IP-Adresse des Kommunikationssystems angibt, sondern die IP-Adresse des Linux-Servers.

25.2.1 Backup-Sets

Die Konfigurationsdaten des Kommunikationssystems werden in einem Backup-Set gesichert.

Zusätzlich zum Backup-Set ist eine zu dem Backup-Set gehörige Text-Datei zu speichern. Sie enthält Informationen über Datum und Uhrzeit der Sicherung und unter welcher Software-Version die Sicherung durchgeführt wurde. Die Text-Datei ist notwendig für die Wiederherstellung des Backup-Sets.

Übersteigt die Anzahl der gespeicherten Backup-Sets den eingestellten Wert, so werden die ältesten Backup-Sets gelöscht.

Backup-Set-Daten

Folgende Daten zu einem Backup-Set werden angezeigt:

- **Archivname**: Name des Backup-Set
- **Größe**: Größe des Backup-Sets in Byte.
- **Datum**: Datum, an dem das Backup-Set erstellt wurde.
- **Kommentar**: Kommentar, der bei der Erstellung des Backup-Sets mit angegeben wurde (optional).

Ausgegraut dargestellte Backup-Sets können nicht wiederhergestellt werden.

25.2.1.1 Wie Sie sich Backup-Sets anzeigen lassen

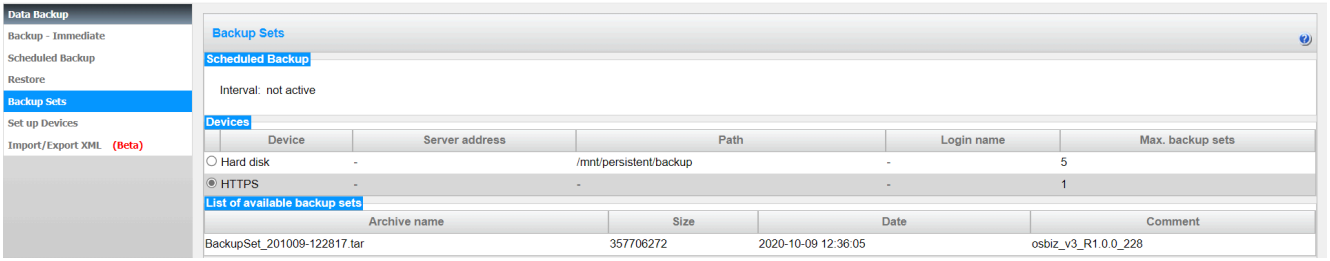
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup-Sets**.

3) Aktivieren Sie im Bereich **Geräte** das Backup-Medium, dessen Backup-Sets Sie sich anzeigen lassen wollen. Sie erhalten eine Liste aller auf diesem Medium verfügbaren Backup-Sets.



25.2.1.2 Wie Sie Backup-Sets löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup Sets**.
3) Aktivieren Sie im Bereich **Geräte** das Backup-Medium, dessen Backup-Sets Sie sich anzeigen lassen wollen. Sie erhalten eine Liste aller auf diesem Medium verfügbaren Backup-Sets.
4) Aktivieren Sie das Kontrollkästchen des Backup-Sets, das Sie löschen wollen und klicken Sie auf **Löschen**. Das Backup-Set wird gelöscht.

25.2.2 Backup-Medien

Auf den Backup-Medien werden die Backup-Sets gesichert.

Für die Sicherung können folgende Backup-Medien verwendet werden:

- Gestecktes USB-Medium
- Network drive
- Client-PC über HTTPS (nur möglich bei sofortiger Sicherung)
- Festplatte der UC Booster Card
- FTP-/FTPS-Server

Für jedes Backup-Medium kann festgelegt werden, wie viele Backup-Sets maximal in dem Verzeichnis abgelegt werden dürfen.

USB-Medium

Um ein USB-Medium (z.B. USB-Festplatte oder USB-Stick) für das Backup zu verwenden, muss das USB-Medium an der USB-Server-Schnittstelle des Kommunikationssystems gesteckt sein, damit es für die Sicherung zur Verfügung steht. Zusätzlich muss das USB-Medium mit FAT-32 formatiert sein. Aufgrund der Dateisystembeschränkung darf die maximale Größe des Backup-Sets 4 GB nicht überschreiten. In solchen Fällen müssen alternative Backup-Medien ausgewählt werden. Von einem NTFS-formatierten USB-Medium kann

nur gelesen werden. Sind mehrere Partitionen vorhanden, ist eine Sicherung nur auf der ersten Partition möglich!

Ein bootfähiges USB-Medium wird nicht unterstützt.

Bei OpenScape Business S und OpenScape UC Booster Server wird das USB-Medium in die USB-Schnittstelle des Linux-Servers gesteckt.

FTP-/FTPS-Server und Netzlaufwerke

FTP-/FTPS-Server und Netzlaufwerke können als neue Medien hinzugefügt, bearbeitet oder gelöscht werden. FTP-/FTPS-Server und Netzlaufwerke können auch mehrfach angegeben werden, wenn dabei unterschiedliche Verzeichnisse genutzt werden. Als verschlüsseltes File-Transfer-Protokoll (FTPS) wird TLS 1.2 unterstützt.

Der Benutzer muss für die Sicherung der Konfigurationsdaten auf einem FTP-/FTPS-Server Schreibrechte für sein Root-Verzeichnis haben. Für die Sicherung auf einem Netzlaufwerk reichen Schreibrechte für das gewünschte Verzeichnis.

Ist die Übertragungsgeschwindigkeit zum FTPS-Server zu niedrig, kann es zu einer Fehlfunktion bei der Datensicherung kommen. In diesem Fall muss die Datensicherung neu gestartet werden.

Bei FTPS werden Zertifikate bis 2048 Bit unterstützt. Diese Zertifikate sind für die Authentifizierung am FTPS-Server erforderlich.

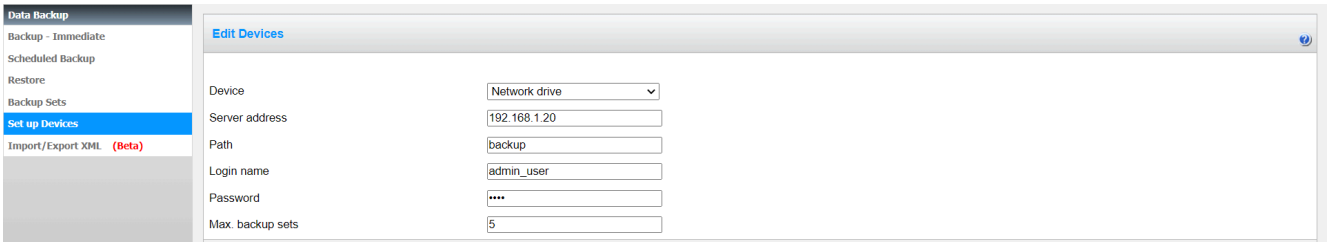
25.2.2.1 Backup-Medium hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Einrichtung Geräte**.
3) Klicken Sie auf **Hinzufügen**.



4) Wählen Sie in der Aufklappliste in der Spalte **Gerät** das gewünschte Backup-Medium aus.
   - Wenn Sie auf einem FTP-/FTPS-Server sichern wollen, wählen Sie **(S)FTP** aus.
   - Wenn Sie auf einem Netzlaufwerk sichern wollen, wählen Sie **Netzlaufwerk** aus.

Anmerkung: Die unterstützte Samba-Version ist SMB2.

5) Geben Sie unter **Server-Adresse** den Hostnamen oder die IP-Adresse des Mediums ein.
6) Geben Sie unter **Verzeichnis** den Pfad an, in dem das Backup-Set gespeichert werden soll.
7) Wenn Sie auf einem FTP-/FTPS-Server sichern wollen, geben Sie **Benutzername** und **Passwort** für den Zugang zum FTP-/FTPS-Server ein.

Anmerkung: Folgende Zeichen sind für das Passwortfeld zulässig: `0-9 A-Z a-z ~ ! @ # $ % ^ _ - + = ? / , . :`

Die maximale Passwortlänge beträgt 64 Zeichen.

---

8) Wenn Sie auf einem Netzlaufwerk sichern wollen, das gesichert ist, geben Sie **Benutzername** und **Passwort** für den Zugang zum Netzlaufwerk ein.

Anmerkung: Standardmäßig wird eine leere Domäne für die Authentifizierung verwendet. Wenn Sie die Domäne bereitstellen möchten, verwenden Sie im Feld **Login-Name** den Vorwärtsschrägstrich (/) als Trennzeichen. Zum Beispiel: `Domäne/Benutzer`.

---

9) Geben Sie unter **Max. Backup-Sets** die Anzahl der Backup-Sets ein, die maximal in dem Verzeichnis gespeichert werden sollen.
10) Klicken Sie auf **OK & Weiter**. Das neu angelegte Backup-Medium erscheint in der Liste der verfügbaren Backup-Medien.
11) Klicken Sie im Navigationsbaum auf **Backup-Sets**.
12) Aktivieren Sie im Bereich **Geräte** das Backup-Medium, das Sie gerade hinzugefügt haben. Ist in der Liste der verfügbaren Backup-Sets kein roter Balken mit einer Fehlermeldung zu sehen, ist das Backup-Medium korrekt eingerichtet.
13) Wird eine Fehlermeldung angezeigt, überprüfen Sie nochmals Ihre Eingaben (siehe Backup-Medium bearbeiten auf Seite 1255

25.2.2.2 Backup-Medium bearbeiten

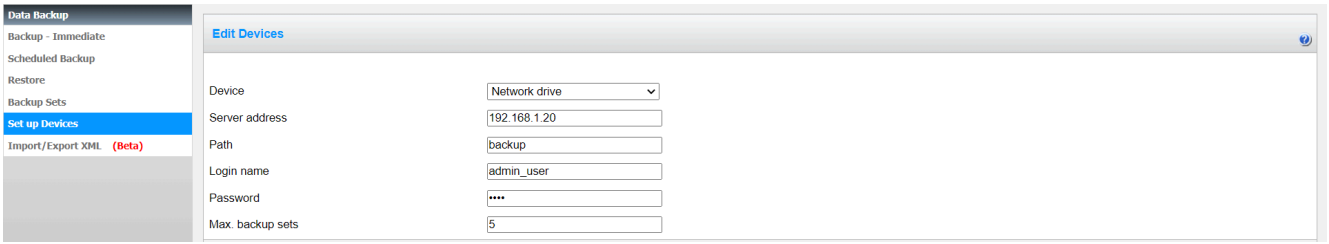
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Einrichtung Geräte**.

3) Aktivieren Sie das zu bearbeitende Backup-Medium und klicken Sie auf **Bearbeiten**.



4) Ändern Sie die gewünschten Werte.
5) Klicken Sie auf **OK & Weiter**.

25.2.2.3 Wie Sie ein Backup-Medium löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Einrichtung Geräte**.
3) Wählen Sie das zu löschende Backup-Medium aus und klicken Sie auf **Löschen**.

   Es können auch mehrere Backup-Medien zum Löschen ausgewählt werden.
4) Bestätigen Sie die Abfrage mit **OK**. Das Backup-Medium ist aus der Liste der verfügbaren Backup-Medien gelöscht.

25.2.3 Sofortiges Sichern

Die Konfigurationsdaten können manuell sofort gesichert werden.

Die Sicherung kann auf unterschiedlichen Backup-Medien erfolgen. Standardmäßig ist das Backup-Medium **HTTPS** eingerichtet. Damit können Sie das Backup-Set an allen Speicherorten ablegen, auf die der Client-PC Zugriff hat, mit dem Sie sich am WBM angemeldet haben. Der gewählte Speicherort muss auch bei der Wiederherstellung des Backup-Sets zugänglich sein. Ist ein USB-Medium am Kommunikationssystem angeschlossen, wird als zusätzliches Backup-Medium **USB-Device** angezeigt. Ist die UC Booster Card inkl. Festplatte gesteckt, wird ein weiteres Backup-Medium **Local hard disk** angezeigt.

Der Name des Backup-Sets wird bei der Sicherung automatisch vergeben. Er beinhaltet u.a. das Datum, an dem die Sicherung durchgeführt wird. Zusätzlich sind diese Daten auch in einer Text-Datei enthalten, die ebenfalls abgespeichert werden muss. Um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können, kann ein Kommentar angegeben werden.

Zugehörige Konzepte

Zeitgesteuertes Sichern auf Seite 1258

Zugehörige Tasks

Wie Sie das eigene Administratorpasswort ändern auf Seite 121

25.2.3.1 Wie Sie ein Backup-Set sofort sichern

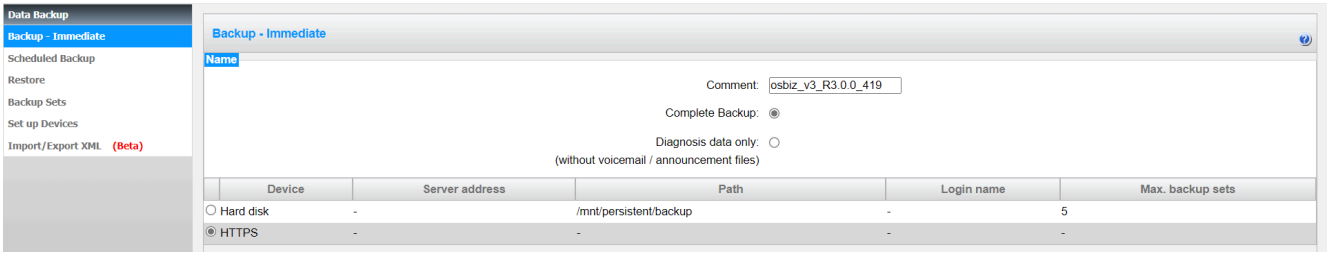
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Nur bei Verwendung von UC Suite: UC Suite wurde korrekt gestartet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup – Sofort**.



3) Geben Sie im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.
4) Wenn Sie ein Backup-Set inkl. Sprachnachrichten und Ansagen erstellen wollen, aktivieren Sie die Option **Vollständiges Backup**.
5) Wenn Sie ein Backup-Set ohne Sprachnachrichten und Ansagen erstellen wollen, aktivieren Sie die Option **Nur Diagnose-Daten**.
6) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.
7) Klicken Sie auf **OK & Weiter**. Der Fortschritt des Backup-Vorgangs wird in einem separaten Fenster angezeigt.

Anmerkung: Falls die Schaltfläche **OK & Weiter** ausgegraut ist, sind nicht alle Applikationen (z.B. UC Suite) korrekt gestartet, deren Daten gesichert werden sollen.

Falls Sie für das ausgewählte Archiv-Verzeichnis keine Berechtigung haben, erhalten Sie eine Fehlermeldung. Wählen Sie ein anderes Ziellaufwerk aus oder ändern Sie den Pfad für das Archiv.

Falls auf dem Ziellaufwerk nicht genügend Speicherplatz für das Backup-Set vorhanden ist, erhalten Sie eine Fehlermeldung. Wählen Sie ein anderes Ziellaufwerk oder löschen Sie ein Backup-Set und starten Sie die Datensicherung erneut.

---

8) Die Sicherung war erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt!** erscheint. Es wird **100 %** angezeigt.

9) Wenn Sie als Backup-Medium **HTTPS** ausgewählt haben, müssen Sie das Backup-Set und die zum Backup-Set gehörige Text-Datei an einem Speicherort Ihrer Wahl sichern. Bei den anderen Backup-Medien geschieht dies automatisch. Das Browser-Fenster muss solange geöffnet bleiben, bis der Speichervorgang für Backup-Set und Text-Datei abgeschlossen ist.

Anmerkung: Wenn Sie als Backup-Medium ein USB-Medium verwenden, warten Sie ab, bis die LED des USB-Mediums aufhört zu blinken. Erst dann ist die Sicherung erfolgreich auf dem USB-Medium gespeichert. Entfernen Sie anschließend das USB-Medium.

10) Klicken Sie auf **Beenden**.

25.2.4 Zeitgesteuertes Sichern

Über eine Zeitsteuerung können die Konfigurationsdaten automatisch gesichert werden. Zeitpunkt, Intervall und Ort der automatischen Sicherung ist einstellbar.

Die zeigesteuerte Datensicherung kann täglich oder wöchentlich für eine feste Uhrzeit geplant werden und startet dann automatisch. Dieser "Sicherungsauftrag" kann für ein internes oder externes Sicherungsmedium eingerichtet werden. Die Einrichtung mehrerer Sicherungsaufträge ist nicht möglich.

Zugehörige Konzepte

Sofortiges Sichern auf Seite 1256

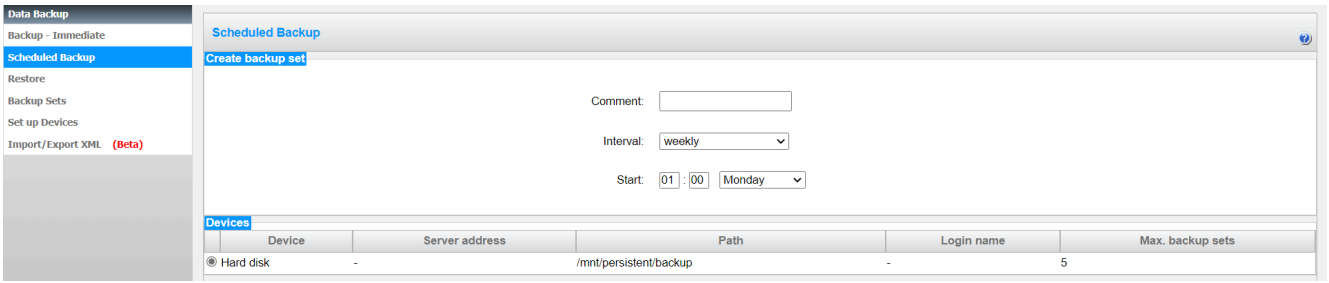
25.2.4.1 Wie Sie ein Backup-Set zeitgesteuert sichern

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup - zeitgesteuert**.



3) Geben Sie im Bereich **Backup-Set erstellen** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.

4) Legen Sie das Intervall für die Sicherung fest:
   - Tägliche Datensicherung: Wählen Sie in der Aufklappliste **Intervall** den Eintrag **Täglich** und geben Sie bei **Backup - Zeitpunkt** an, wann die Datensicherung jeden Tag starten soll.
   - Wöchentliche Datensicherung: Wählen Sie in der Aufklappliste **Intervall** den Eintrag **Wöchentlich** und geben Sie bei **Backup - Zeitpunkt** an, an welchem Wochentag und um welche Zeit die Datensicherung starten soll.
5) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.
6) Klicken Sie auf **OK & Weiter**. Die Datensicherung wird täglich oder wöchentlich zum angegebenen Zeitpunkt automatisch gestartet.

25.2.5 Wiederherstellen

Die Wiederherstellung der Konfigurationsdaten erfolgt manuell über die Backup-Sets.

Die Wiederherstellung kann von allen unterstützten Backup-Medien erfolgen.

25.2.5.1 Wie Sie ein Backup-Set wiederherstellen

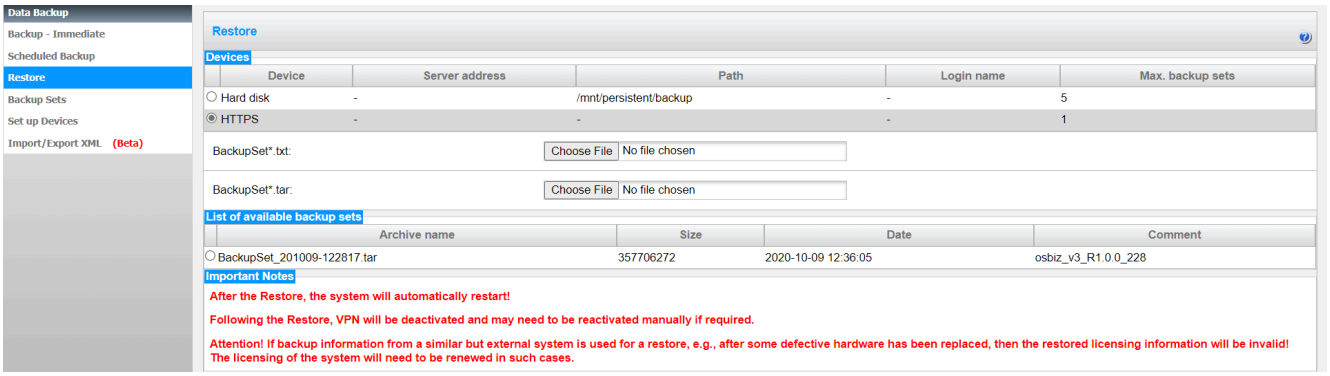
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Nur bei Verwendung von UC Suite: UC Suite wurde korrekt gestartet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Restore**.



3) Aktivieren Sie im Bereich **Geräte** das Medium, das das wiederherzustellende Backup-Set enthält.
4) Wenn Sie als Backup-Medium **HTTPS** aktiviert haben, navigieren Sie zu dem Speicherort des Backup-Sets und wählen das Backup-Set aus. Navigieren Sie anschließend zum Speicherort der Text-Datei und wählen Sie diese aus.
5) Wenn Sie ein anderes Backup-Medium als **HTTPS** aktiviert haben, aktivieren Sie im Bereich **Liste der verfügbaren Backupsets** das Backup-Set, das die wiederherzustellenden Konfigurationsdaten enthält.

6) Warten Sie bis die Dateien auf das System geladen wurden und klicken Sie anschließend auf **OK & Weiter**. Die Wiederherstellung der Konfigurationsdaten wird gestartet. Es wird Ihnen der Fortschritt der Wiederherstellung angezeigt.
7) Nachdem die Meldung **Restore erfolgreich ausgeführt!** erscheint, führt das System automatisch einen Neustart durch. Die Wiederherstellung ist erfolgreich abgeschlossen, wenn das System wieder betriebsbereit ist.

25.3 Updates

Mit Hilfe von Updates wird die Software der Systemkomponenten innerhalb einer Version aktualisiert.

Um Updates installieren zu können, benötigen Sie den 3 jährigen Software-Support.

Die Version der installierten Software und das Ablaufdatum des Software-Supports werden auf der Startseite des WBM angezeigt. Ist eine aktuellere Software verfügbar, wird dies dort mitgeteilt.

Anmerkung: Bei einem Update auf ein neues Minor Release ist es erforderlich, ein neues Backup-Set zu erstellen.

Die Software-Aktualisierung wird mit dem WBM durchgeführt. Bei einem Hardwaremodell gibt es zusätzlich die Möglichkeit, die Software direkt über einen USB-Medium ohne WBM-Zugriff zu aktualisieren. Bei einem Kommunikationssystem mit UC Booster Server werden Hardwaremodell und UC Booster Server separat aktualisiert.

Mit Hilfe des WBM kann die Software über den Internet-Webserver, einen lokalen Webserver oder direkt über Image-Dateien aktualisiert werden.

Folgende Systemkomponenten werden aktualisiert:

- Software des Kommunikationssystems
- Software der UC Clients
- Software der Systemtelefone (Aktualisierung auch einzeln möglich)
- Dokumentation

Zusammen mit der Software des Kommunikationssystems wird die Software der UC Clients aktualisiert. Liegt eine aktuellere Software vor, erhalten die Benutzer der UC Clients über das Auto-Update eine Nachricht, dass ein Update zur Verfügung steht und installiert werden kann.

Die Software-Aktualisierung der IP-Systemtelefone erfolgt automatisch zusammen mit der Aktualisierung des Kommunikationssystems, kann aber auch manuell durchgeführt werden. Für die UP0-Systemtelefone erfolgt die Aktualisierung manuell mit dem Manager E.

Das Software-Update kann sofort gestartet werden oder die Zeitpunkte für die Software-Übertragung und Software-Aktivierung können getrennt voneinander festgelegt werden. Die Aktualisierung sollte außerhalb der Kundengeschäftszeiten durchgeführt werden, da das Kommunikationssystem und/oder die Systemtelefone neu gestartet werden und bestehende Gespräche und die Nutzung der UC Clients unterbrochen werden.

Ist die Software auf das Kommunikationssystem übertragen worden, wird die Software zum gewählten Zeitpunkt aktiviert. Anschließend wird automatisch das aktuellste Telefon-Image auf die IP-Systemtelefone geladen. Nach einem Neustart des Kommunikationssystems und der IP-Systemtelefone ist die neu geladenen Software aktiv.

Anmerkung: Das Software-Update muss nicht gleichzeitig auf allen Systemen und in verschiedenen Software-Versionen durchgeführt werden.

Image-Dateien

Für die Aktualisierung der Systemkomponenten werden Image-Dateien benötigt, die die Software der Systemkomponenten enthalten. Diese Image-Dateien können z.B. vom Software-Server (Internet-Webserver) heruntergeladen und eigenständig auf einem lokalen Webserver oder im internen Netz oder auf einem USB-Stick abgelegt werden. Es gibt eine eigene Image-Datei für das Kommunikationssystem ohne UC Booster Card und eine eigene Image-Datei für ein System mit UC Booster Card. Beide Image-Dateien enthalten auch die Software für die Systemtelefone. Zusätzlich gibt es aber auch für jeden Systemtelefontyp eine eigene Image-Datei, falls die Systemtelefone separat aktualisiert werden sollen.

Es gibt folgende Typen von Image-Dateien:

- **tgz**: für die Software des Kommunikationssystems. In der tgz-Datei befindet sich eine tar-Datei. Die tar-Datei muss mit einem Entpacker wie z.B. WinZip oder 7-zip aus der tgz-Datei entpackt werden. Die tgz-Datei wird deshalb zum Download angeboten, weil damit beim Herunterladen vom Software-Server überprüft werden kann, ob die Datei beschädigt ist oder nicht.
- **tar**: für die Software des Kommunikationssystems. Sie enthält die gepackten Dateien für die einzelnen Systemkomponenten.
- **app**: für die Software des Systemtelefons.

Lokaler Webserver

Bei der Software-Aktualisierung über einen Webserver wird standardmäßig auf den Software-Server (Internet-Webserver) zugegriffen.

Es ist aber auch möglich für die Aktualisierung einen lokalen Webserver zu verwenden. Dafür muss die Image-Datei auf dem lokalen Webserver abgelegt sein und der Pfad zum lokalen Webserver im WBM konfiguriert sein.

Speed-Upgrade

Ein Speed-Upgrade wie bei der HiPath 3000 ist nicht möglich.

Wichtig: Ein Ziehen der SDHC-Karte während des Betriebs führt zu Datenverlust!

Netzwerk – Lizenzierung

Bei Upgrade und Migration von Systemen in einem Netzwerk, in dem der Master-Knoten für die Lizenzierung der Slave-Knoten verwendet wird, beginnen Sie bitte mit den Slave-Knoten, bevor Sie mit dem Master-Knoten fortfahren.

25.3.1 Nutzung eines lokalen Webservers

Die Software kann über einen lokalen Webserver aktualisiert werden.

Die aktuellen Image-Dateien müssen auf dem lokalen Webserver abgelegt sein. Zusätzlich sind die Zugangsdaten des lokalen Webservers im WBM einzutragen. Diese Änderung kann nur von einem Administrator mit dem Profil **Expert** durchgeführt werden. Sind die Zugangsdaten des lokalen Webservers eingetragen, werden diese als Standard gesetzt und für alle weiteren Updates des Kommunikationssystems wird jetzt anstelle des Internet-Webservers der lokale Webserver verwendet.

25.3.1.1 Wie Sie den Zugang zum lokalen Web-Server konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Eine Verbindung zum lokalen Webserver ist vorhanden.

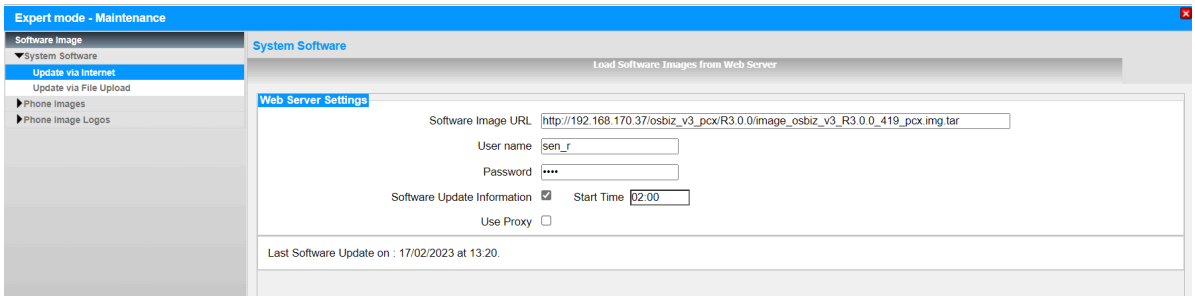
Sie benötigen die Web-Adresse (URL) und die Zugangskennung des lokalen Webservers sowie den Namen der Image-Datei.

Die Image-Datei ist als tar-Datei auf dem lokalen Webserver gespeichert und der Ablageort ist bekannt. Evtl. mus die tar-Datei aus der gespeicherten tgz-Datei entpackt werden.

Wenn Sie für die Aktualisierung einen Proxy-Server verwenden, benötigen Sie noch dessen Daten (evtl. auch Benutzername und Passwort).

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Software-Image**.
3) Klicken Sie im Menübaum auf **System-Software**.
4) Klicken Sie auf **Update via Internet**.



5) Richten Sie den Zugang zum lokalen Webserver ein:
   a) Geben Sie unter **Software-Image URL** die Adresse des lokalen Webservers inkl. dem Pfad und dem Namen der Image-Datei ein.

      Anmerkung: Mit der Schaltfläche **Voreinstellung** können Sie die eingegebenen Werte wieder auf die Standardwerte zurücksetzen.

   b) Geben Sie im Feld **Benutzername** den Benutzernamen und im Feld **Passwort** das Passwort für den Zugriff auf den lokalen Webserver ein.
   c) Aktivieren Sie das Kontrollkästchen **Software Update Information** und geben Sie unter Startzeit einen **Zeitpunkt** an, zu der auf dem oben angegebenen Server nach einer neueren Software gesucht werden soll.
   d) Wenn Sie für die Übertragung einen Proxy-Server verwenden, aktivieren Sie das Kontrollkästchen **Proxy verwenden** und geben Sie die Daten für den Proxy-Server ein.
6) Klicken Sie auf **Übernehmen**. Die eingegebenen Zugangsdaten des lokalen Webservers werden als Standard übernommen.

   Liegt auf dem lokalen Webserver bereits eine neue Image-Datei, wird die Software-Aktualisierung eingeleitet und es erscheint die Lizenzvereinbarung (siehe Wie Sie das System über einen Webserver aktualisieren). Der Start der Software-Aktualisierung kann aber bei Bedarf noch verhindert werden.

25.3.2 Update des Kommunikationssystems

Mit dem Update des Kommunikationssystems wird die Software des Kommunikationssystems aktualisiert und zusätzlich die auf dem Kommunikationssystem gespeicherten Software-Images der Systemtelefone. Damit ist ein komplettes Update aller Systemkomponenten schnell und einfach durchzuführen.

Vor jeder Software-Aktualisierung sollten die Konfigurationsdaten des Kommunikationssystems gesichert werden (Sicherung und Wiederherstellung).

Aktualisierung über Webserver

Bei der Software-Aktualisierung über einen Webserver wird standardmäßig auf den Software-Server (Internet-Webserver) zugegriffen.

Wird ein lokaler Webserver verwendet, muss die Image-Datei auf dem lokalen Webserver abgelegt sein.

Für ein Kommunikationssystem ohne UC Booster Card ist es egal, ob eine Image-Datei für ein System ohne oder mit UC Booster Card verwendet wird. Es werden nur die benötigten Komponenten installiert.

Nachdem automatisch eine Verbindung zum Webserver aufgebaut wurde, wird geprüft, ob neue Software-Updates vorliegen. Einzelne Pakete des Software-Updates können bei Systemen ohne UC Booster abgewählt werden, um die Downloadzeit zu verringern. Es werden auch nur die Pakete übertragen, die sich gegenüber der installierten Software-Version geändert haben. Startzeitpunkt der Software-Übertragung und Startzeitpunkt der Software-Aktivierung können ausgewählt werden. Wird der Zeitpunkt der Software-Aktivierung erreicht, obwohl das Software-Update noch nicht komplett auf das

System übertragen ist, wird die Aktivierung nicht automatisch durchgeführt. Es muss manuell ein neuer Aktivierungszeitpunkt festgelegt werden.

Aktualisierung über USB-Medium

Die Image-Datei ist auf einem USB-Medium gespeichert. Das USB-Medium wird in die USB-Server-Schnittstelle des Kommunikationssystems gesteckt. Diese Art der Aktualisierung kann nur von einem Administrator mit dem Profil **Expert** durchgeführt werden und ist nicht möglich für OpenScape Business S und OpenScape Business UC Booster Server.

Aktualisierung über Datei-Upload

Die Image-Datei befindet sich in einem Verzeichnis im internen Netz oder auf dem Admin-PC.

Aktualisierung über USB-Medium ohne WBM-Zugriff

Das Kommunikationssystem kann direkt ohne WBM-Zugang über ein USB-Medium aktualisiert werden. Dazu muss das USB-Medium in der USB-Server-Schnittstelle des Systems gesteckt werden und die Image-Datei auf der obersten Verzeichnisebene des USB-Mediums liegen. Wird bei gestecktem USB-Medium ein Reset des Kommunikationssystems durchgeführt, wird automatisch das Software-Update gestartet. Diese Art der Aktualisierung ist nicht möglich bei OpenScape Business S. Bei einem System mit OpenScape Business UC Booster Server muss der Server zusätzlich aktualisiert werden.

Aktualisierung des UC Booster Servers

Wird zusätzlich zum Kommunikationssystem ein UC Booster Server betrieben, so muss bei einem Update der System-Software auch die Kommunikationssoftware des UC Booster Servers aktualisiert werden. Die Software des Kommunikationssystems und des UC Booster Servers sollten immer auf dem gleichen Stand sein. Der Software-Update des UC Booster Servers erfolgt identisch zum Software-Update des Kommunikationssystems, nur dass der Administrator beim Aufruf des WBM nicht die IP-Adresse des Kommunikationssystems angibt, sondern die IP-Adresse des Linux-Servers.

25.3.2.1 Wie Sie das System über einen Webserver aktualisieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Auf der Startseite des WBM wird angezeigt, dass eine neue Softwareversion vorliegt.

Ein Zugang zum Webserver ist vorhanden. Standardmäßig wird die Verbindung zum Internet-Webserver aufgebaut. Stattdessen kann ein lokaler Webserver konfiguriert werden. (siehe Nutzung eines lokalen Webservers).

Wird das Update über einen lokalen Webserver ausgeführt, muss die aktuellste Image-Datei auf dem lokalen Webserver abgelegt sein.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Startseite** und zuerst auf den Link **Zum Inhalt können Sie sich hier informieren**: **Link**. Es öffnet sich eine PDF-Datei mit wichtigen Hinweisen zu der neuen Softwareversion. Lesen

Sie sich die Informationen durch und berücksichtigen Sie die Informationen zur Hochrüstung des Systems. Schließen Sie das Fenster anschließend.

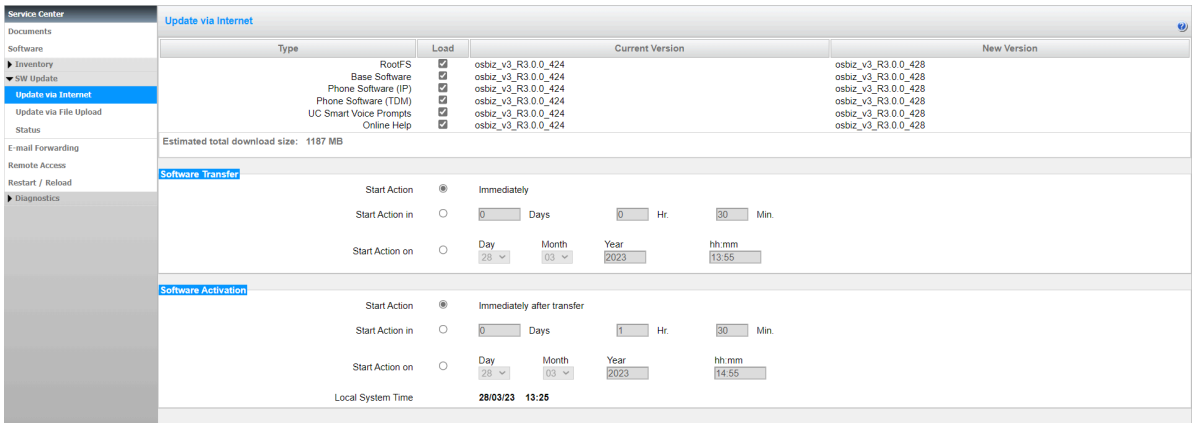
2) Klicken Sie in der Navigationsleiste auf **Service-Center**.

3) Klicken Sie im Navigationsbaum auf **Software Update** > **Update via Internet**. Es wird Ihnen die aktuell installierte Softwareversion angezeigt.

4) Klicken Sie auf **OK & Weiter**.

5) Lesen Sie sich die Lizenzvereinbarung (EULA) durch und aktivieren Sie anschließend das Optionsfeld **Ich stimme der Lizenzvereinbarung zu**.

6) Klicken Sie auf **OK & Weiter**.



7) Deaktivieren Sie bei Bedarf in der Spalte **Laden** die Pakete, die nicht aktualisiert werden sollen. Das ist z.B. sinnvoll bei langsamen Internet-Verbindungen oder Software-Aktualisierungen über ISDN.

8) Wählen Sie die Zeitpunkte für Software-Übertragung und Software-Aktivierung aus:

- **Start der Aktion - Sofort/Sofort nach der Übertragung**: Die Software wird sofort übertragen und danach aktiviert. Das Software-Update wird im Hintergrund in das Kommunikationssystem geladen. Nach zwei Neustarts ist die Software aktualisiert.
- **Start der Aktion in**: Die Software wird nach Ablauf einer bestimmten Zeit übertragen bzw. aktiviert. Geben Sie dazu den Zeitraum in Tagen, Stunden und Minuten an.
- **Start der Aktion am**: Die Software wird zu einem bestimmten Zeitpunkt übertragen bzw. aktiviert. Geben Sie dazu Datum und Uhrzeit des Zeitpunkts an.

Anmerkung: Wird der Zeitpunkt der Software-Aktivierung erreicht, obwohl das Software-Update noch nicht komplett auf das System übertragen ist, wird die Aktivierung nicht automatisch durchgeführt. Es muss manuell ein neuer Aktivierungszeitpunkt festgelegt werden.

---

9) Klicken Sie auf **OK & Weiter**. Das Software-Update wird zu den von Ihnen konfigurierten Zeitpunkten im Hintergrund in das System geladen und

aktiviert. Zum Zeitpunkt der Software-Aktivierung werden automatisch hintereinander zwei Neustarts durchgeführt.

Anmerkung: Sie können das Browser-Fenster jederzeit schließen.

10) Den aktuellen Status des Updates können Sie mit dem WBM unter **Service-Center** > **Software-Update** > **Status** abfragen.

25.3.2.2 Wie Sie das System über ein USB-Medium aktualisieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

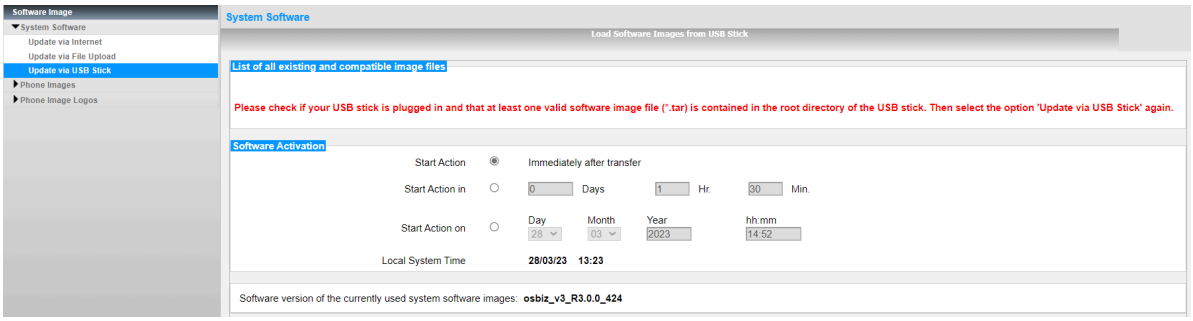
Das USB-Medium muss mit FAT32 formatiert sein.

Eine aktuelle Image-Datei ist als tar-Datei auf dem USB-Medium gespeichert. Es können auch mehrere Image-Dateien in unterschiedlichen Verzeichnissen abgelegt sein.

Hat das USB-Medium mehrere Partitionen, muss die Image-Datei in der ersten Partition abgelegt sein.

Schritt für Schritt

1) Stecken Sie das USB-Medium in die USB-Server-Schnittstelle des Mainboards.
2) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
3) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.
4) Klicken Sie im Menübaum auf **System-Software**.
5) Klicken Sie auf **Update via USB Stick**. Es werden Ihnen alle auf dem USB-Medium gespeicherten, gültigen Image-Dateien mit Versionsnummer und Dateiname angezeigt.



6) Wenn mehrere Image-Dateien gespeichert sind, wählen Sie die gewünschte Image-Datei aus, ansonsten ist die Image-Datei automatisch markiert.
7) Wählen Sie den Zeitpunkt für die Software-Aktivierung aus:
   - **Start der Aktion - Sofort nach der Übertragung**: Die Software wird sofort nach der Übertragung in das Kommunikationssystem aktiviert.
   - **Start der Aktion in**: Die Software wird sofort in das Kommunikationssystem übertragen. Nach Ablauf einer bestimmten

Zeit wird die Software aktiviert. Geben Sie dazu den Zeitraum in Tagen, Stunden und Minuten an.

- **Start der Aktion am**: Die Software wird sofort in das Kommunikationssystem übertragen. Zu einem bestimmten Zeitpunkt wird die Software aktiviert. Geben Sie dazu Datum und Uhrzeit des Zeitpunkts an.

8) Klicken Sie auf **Laden**. Die Image-Datei wird in das Kommunikationssystem übertragen und auf Konsistenz überprüft. Für beide Vorgänge werden mehrere Minuten benötigt. Während dieser Zeit muss das USB-Medium gesteckt bleiben.

9) Ziehen Sie das USB-Medium, sobald das WBM Sie darauf hinweist, und klicken Sie auf **Beenden**. Zum angegebenen Zeitpunkt der Software-Aktivierung werden automatisch hintereinander zwei Neustarts durchgeführt.

10) Den aktuellen Status des Updates können Sie mit dem WBM unter **Service-Center** > **Software-Update** > **Status** abfragen.

25.3.2.3 System über einen Datei-Upload aktualisieren

Voraussetzungen

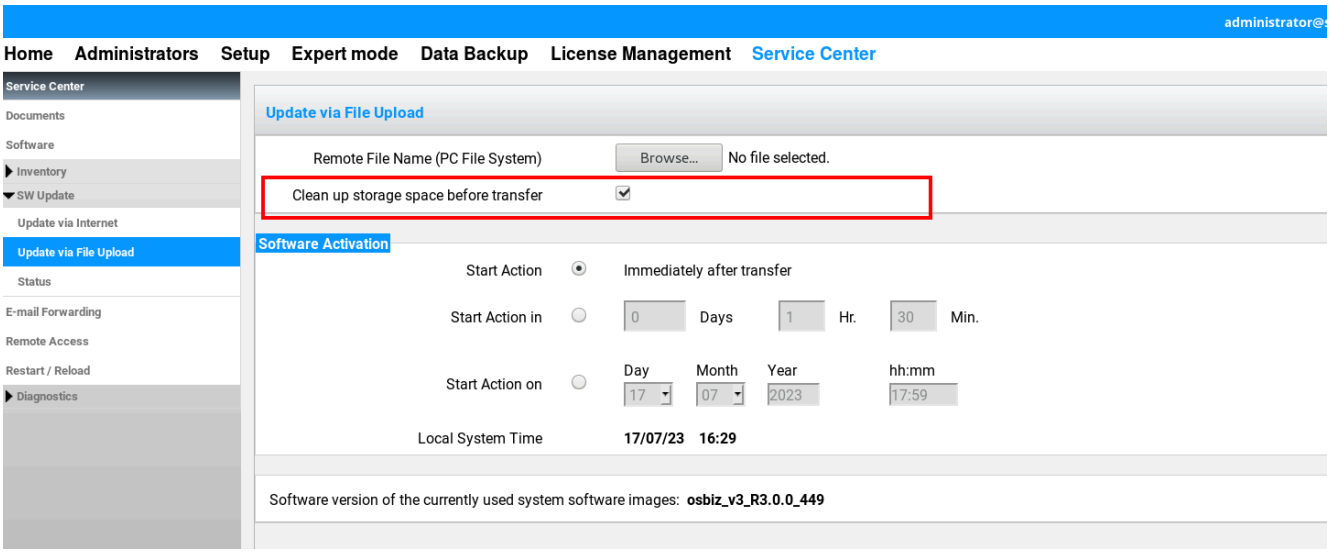
Die Image-Datei ist als tar-Datei im internen Netz oder direkt auf dem Admin-PC gespeichert und der Ablageort ist bekannt. Ist eine tgz-Datei gespeichert, muss die tar-Datei aus der tgz-Datei entpackt werden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Software Update** > **Update via File Upload**. Es wird Ihnen die aktuell installierte Softwareversion angezeigt.

3) Klicken Sie auf **OK & Weiter**.



4) Navigieren Sie mit der Schaltfläche **Durchsuchen** zum Ablageort der Image-Datei (`*.tar`).

5) Das Flag **Speicherplatz vor der Übertragung freigeben** ist standardmäßig aktiviert. Die folgenden Aktionen werden ausgelöst, um Speicherplatz zur Vorbereitung des Software-Datei-Uploads freizugeben.
   - Alle Protokolle und Traces werden gelöscht.
   - Alle Telefon-Software-Images werden gelöscht.
   - Alle TCP-Dumps werden gelöscht.
6) Wählen Sie den Zeitpunkt für die Software-Aktivierung aus:
   - **Start der Aktion - Sofort nach der Übertragung**: Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach zwei Neustarts ist die Software aktualisiert.
   - **Start der Aktion in**: Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach Ablauf einer bestimmten Zeit wird die Software aktiviert. Geben Sie dazu den Zeitraum in Tagen, Stunden und Minuten an.
   - **Start der Aktion am**: Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Zu einem bestimmten Zeitpunkt wird die Software aktiviert. Geben Sie dazu Datum und Uhrzeit des Zeitpunkts an.
7) Klicken Sie auf **OK & Weiter**.
8) Die Image-Datei wird in das Kommunikationssystem übertragen und auf Konsistenz überprüft. Für beide Vorgänge werden mehrere Minuten benötigt.

   Anmerkung: Wenn Sie das Browser-Fenster während des Software-Transfers schließen, wird der Vorgang abgebrochen. Während des Konsistenz-Checks können Sie mit dem WBM weiterarbeiten oder es schließen.
9) Soll die Software sofort aktiviert werden, werden nach erfolgreicher Konsistenz-Prüfung automatisch hintereinander zwei Neustarts durchgeführt.
10) Soll die Software nicht sofort aktiviert werden, klicken Sie nach erfolgreicher Übertragung auf **Beenden**. Zum Zeitpunkt der Software-Aktivierung werden automatisch hintereinander zwei Neustarts durchgeführt.
11) Den aktuellen Status des Updates können Sie mit dem WBM unter **Service-Center** > **Software-Update** > **Status** abfragen.

25.3.2.4 Wie Sie das System über ein USB-Medium ohne WBM-Zugriff aktualisieren

Voraussetzungen

Das USB-Medium muss mit FAT32 formatiert sein.

Eine aktuelle Image-Datei ist als tar-Datei in der obersten Verzeichnisebene des USB-Mediums gespeichert. Dort darf nur eine Image-Datei abgelegt sein.

Hat das USB-Medium mehrere Partitionen, muss die Image-Datei in der ersten Partition abgelegt sein.

Die Software-Version der Image-Datei muss neuer sein als die Software-Version des Systems. Vorsicht: es wird auch auf ältere Software-Versionen aktualisiert.

Das Kommunikationssystem ist gestartet.

Schritt für Schritt

1) Stecken Sie das USB-Medium in die USB-Server-Schnittstelle des Mainboards.
2) Drücken Sie den Reset-Knopf zwischen 1 bis 4 Sekunden lang. Das System fährt herunter und beginnt einen Neustart.

   Während des Hochlaufs wird die Software geprüft. Enthält das USB-Medium eine geeignete Image-Datei, wird die Datei auf das Kommunikationssystem geladen. Die rote LED blinkt dabei im 1Hz-Takt (0,5s an / 0,5s aus). Ist der Kopiervorgang beendet, wird die Software entpackt und die Kundendaten automatisch übernommen. Dabei blinkt die rote LED im 5Hz-Takt (100ms an / 100ms aus).
3) Entfernen Sie das USB-Medium, wenn die rote LED im 5Hz-Takt blinkt.
4) Abschließend führt das System hintereinander automatisch zwei Neustarts durch. Wenn die grüne LED im 1Hz-Takt blinkt (0,5s an / 0,5s aus), ist das System wieder betriebsbereit.

25.3.3 Update der Systemtelefone

Die Software der Systemtelefone wird über eine Image-Datei aktualisiert. Für jeden Systemtelefontyp gibt es eine eigene Image-Datei, die die Telefon-Software dieses Typs enthält. Diese Image-Dateien sind in der Software des Kommunikationssystems enthalten und werden beim Update automatisch auf das Kommunikationssystem geladen.

Die IP-Systemtelefone werden standardmäßig automatisch mit der aktuellen Software versorgt. Wird ein IP-Systemtelefon im WBM umkonfiguriert (von einem System Client zu einem SIP Client oder umgekehrt) wird automatisch über den DLI die passende, im Kommunikationssystem gespeicherte Software auf das IP-Systemtelefon geladen. Bei IP-Systemtelefonen, die bereits am System oder an einem anderen System in Betrieb waren, müssen zuerst die Werkseinstellungen wiederhergestellt werden (Factory Reset), bevor die automatische Software-Aktualisierung durchgeführt werden kann.

Eine vom Standard abweichende Telefon-Software kann der Administrator über das WBM manuell auf alle einem Typ zugehörigen IP-Systemtelefone übertragen. Das Update der Software für die UP0-Systemtelefone wird mit dem Manager E durchgeführt.

Ist eine Telefon-Software (Image-Datei) im WBM als Standard markiert, wird dieses Image automatisch auf jedes diesem Typ zugehörige IP-Systemtelefon übertragen, wenn es sich zum ersten Mal am System anmeldet.

Achten Sie bei einer manuellen Aktualisierung darauf, dass die Software der Systemtelefone zur Software-Version des Kommunikationssystems kompatibel ist (siehe Release Note).

Zugehörige Konzepte

Telefon-Logos auf Seite 1241

25.3.3.1 Wie Sie die Telefonsoftware ins System laden

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Die Image-Dateien sind im lokalen Netz gespeichert und der Ablageort ist bekannt. Für jeden Systemtelefontyp wird eine eigene Image-Datei benötigt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Images**.
4) Klicken Sie auf **Laden**. Es wird Ihnen eine Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien angezeigt.
5) Navigieren Sie unter **Remote-Dateiname (PC-Dateisystem)** mit **Durchsuchen** zum Ablageort der Image-Datei (`*.app`).
6) Klicken Sie auf **Laden**. Die Image-Datei wird geladen und auf Fehler geprüft.

Anmerkung: Bei einem Fehler erhalten Sie eine Fehlermeldung. Prüfen Sie Ihre Eingaben und wiederholen Sie die Schritte 5 bis 6.

---

7) Bestätigen Sie bei erfolgreicher Prüfung mit **OK**. Die Image-Datei wird in die Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien aufgenommen.
8) Wenn Sie weitere Image-Dateien für andere Systemtelefontypen laden wollen, wiederholen Sie die Schritte 5 bis 7.

25.3.3.2 Wie Sie die Telefonsoftware an Systemtelefone verteilen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Images**.
4) Wenn Sie ein Telefon-Image an alle Systemtelefone eines Typs verteilen wollen:
   a) Klicken Sie auf **Verteilen**. Es wird Ihnen eine Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien angezeigt.
   b) Aktivieren Sie das Kontrollkästchen **Verteilen** bei dem oder den gewünschten Telefon-Images.
5) Wenn Sie ein Telefon-Image an ein bestimmtes Systemtelefon verteilen wollen:
   a) Klicken Sie auf **Verteilen pro Endgerät**. Es wird Ihnen eine Liste der Systemtelefone angezeigt.
   b) Wählen Sie aus der Aufklappliste **verteilbare Software** für das oder die gewünschten Systemtelefone das Telefon-Image aus.

6) Klicken Sie auf **Übernehmen**.

25.3.3.3 Wie Sie die Telefonsoftware löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Images**.
4) Klicken Sie auf **Laden**. Es wird Ihnen eine Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien angezeigt.
5) Aktivieren Sie in der Zeile des zu löschenden Telefon-Images das Kontrollkästchen **Löschen**.
6) Wenn Sie weitere Telefon-Images löschen wollen, wiederholen Sie den vorherigen Schritt.
7) Klicken Sie auf **Löschen**. Alle markierten Telefon-Images werden aus dem Kommunikationssystem gelöscht.

25.3.3.4 Wie Sie die automatische Verteilung der Telefonsoftware aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Images**.
4) Klicken Sie auf **Verteilen**. Es wird Ihnen eine Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien angezeigt.
5) Wenn die Telefonsoftware automatisch an die Systemtelefone übertragen werden soll, aktivieren Sie in der Zeile der gewünschten Image-Datei das Kontrollkästchen **Standard** (Standardeinstellung).
6) Wenn die Telefonsoftware nicht automatisch an die Systemtelefone übertragen werden soll, deaktivieren Sie in der Zeile der gewünschten Image-Datei das Kontrollkästchen **Standard**.
7) Klicken Sie auf **Übernehmen**.

25.3.3.5 Automatisches Reflashing konfigurieren

Automatisches Reflashing ist eine einfache Methode zum Reflashing der HFA-Software bei den neuwertigen oder in den Lieferzustand zurückgesetzten Geräten OpenScape Desk Phone IP 35G Eco und OpenScape Desk Phone

CP 100/110/200/205/210/400/600/600E/700/700X/710 unter Zuhilfenahme des System-DLI-Servers.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Anmerkung: Automatisches Reflashing ist nur möglich bei Geräten, die sich im Liefer- bzw. Werkszustand befinden. Geräte, die sich nicht im Werkszustand befinden, müssen zunächst auf die Werkseinstellungen zurückgesetzt werden, erst dann ist ein automatisches Reflashing möglich.

Schritt für Schritt

1) Konfiguration des Geräts mit einer Rufnummer und als System-Client:
   a) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
   b) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer > IP Clients**.
   c) Geben Sie im Feld **Rufnummer** die interne Rufnummer ein.
   d) Geben Sie im Feld **Durchwahl** die öffentliche Rufnummer ein.
   e) Geben Sie einen Namen für das Gerät ein.
   f) Wählen Sie im Aufklappmenü **Typ** den Eintrag **System-Client** aus.
   g) Klicken Sie auf **Übernehmen**.

2) Richten Sie den DHCP-Server so ein, dass die IP-Adresse des DLI über die DHCP-Option gesendet wird:
   a) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
   b) Klicken Sie im Navigationsbaum auf **Telefonie > Netzwerkschnittstellen > DHCP > DHCP-Server > Globale Parameter ändern**.
   c) Aktivieren Sie die Option **Internes DLI verwenden** im Bereich **DNS-Server**.

3) Schließen Sie das Gerät an und geben Sie nach dem Hochfahren des Telefons die Rufnummer (Terminal Number) ein.

4) Das Telefon wird auch in der DLI-Datenbank registriert. So überprüfen Sie die Registrierung des Geräts:
   a) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
   b) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.
   c) Klicken Sie im Menübaum auf **Telefon-Images**.
   d) Klicken Sie auf **Verteilen pro Endgerät**.

5) Das automatische Reflashing beginnt und die im Kommunikationssystem gespeicherte HFA-Software wird auf das Gerät geladen.

Anmerkung: Das Gerät darf während dieses Prozesses nicht getrennt werden.

Das Gerät ist jetzt konfiguriert.

Anmerkung: Wenn das Gerät (unter **Telefonie > Teilnehmer > IP Clients**) als SIP-Gerät definiert wurde, erfolgt eine Aktualisierung auf die neueste SIP-Software,

allerdings nur dann, wenn das Update in der entsprechenden Softwareversion verfügbar ist.

Wenn ein SIP-Client in System-Client geändert wird, ist ein manueller Neustart des Telefons erforderlich, um die HFA-Software zu laden.

Anmerkung: Wenn der Reflashing-Prozess fehlschlägt, muss das Gerät wieder in den Werkszustand zurückgesetzt werden.

25.3.4 Software-Status

Der Software-Status gibt Auskunft über den Softwarestand und die Aktualisierung der Software.

Folgende Stati können angezeigt werden:

- aktuelle Version der Software
- Aktuellere Version liegt zur Aktualisierung vor
- Zeitpunkt, zum die Software-Aktualisierung durchgeführt wird
- neue Software wird gerade in das System geladen
- Ladevorgang war erfolgreich oder fehlerhaft

25.3.4.1 Wie Sie den Software-Status abfragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

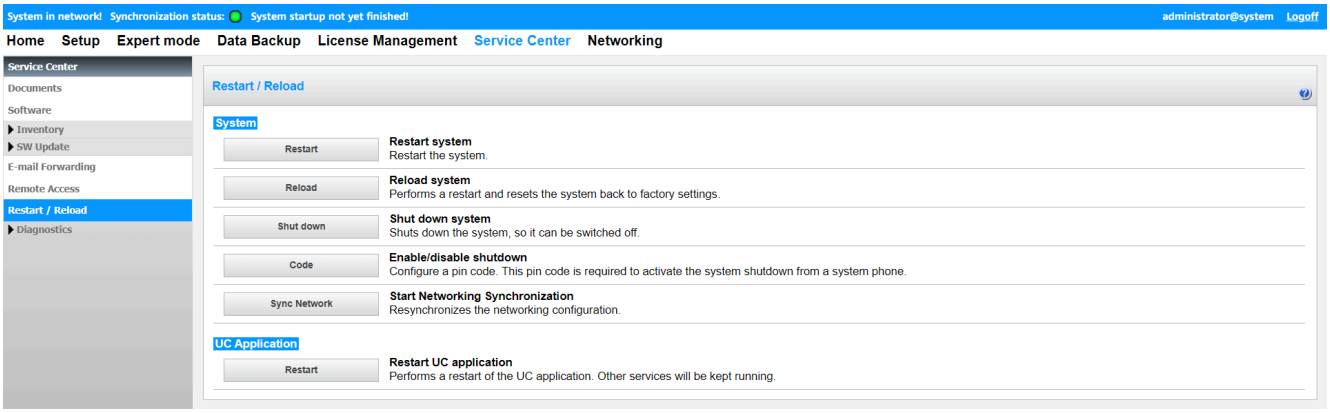
1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Software Update** > **Status**. Es wird Ihnen die aktuelle Version der Software angezeigt. Diese Information wird Ihnen auch auf der Startseite des WBM angezeigt.

   Falls im Hintergrund gerade ein Software-Update läuft, wird Ihnen das hier mitgeteilt.

   Falls ein neues Software-Update auf dem Webserver vorliegt, wird Ihnen das hier mitgeteilt. Diese Information wird Ihnen auch auf der Startseite des WBM angezeigt.

25.4 Restart, Reload, Shutdown

Über die zugehörigen Funktionen kann ein Restart (Neustart) und ein Reload des OpenScape Business Kommunikationssystems oder der UC Booster Card ausgelöst werden sowie OpenScape Business X kontrolliert herunterfahren werden (Shutdown). Darüber hinaus kann ein Restart (Neustart) der UC Applikation (UC Smart oder UC Suite) ausgelöst werden. Um das kontrollierte Herunterfahren von OpenScape Business X über ein Systemtelefon zu ermöglichen, kann eine PIN definiert werden.



Restart und Reload des UC Booster Servers

Wird zusätzlich zum Kommunikationssystem ein UC Booster Server betrieben, so kann auch die Kommunikationssoftware des UC Booster Servers neu gestartet oder reloadet werden. Der Restart/Reload des UC Booster Servers erfolgt identisch zum Restart/Reload des Kommunikationssystems, nur dass der Administrator beim Aufruf des WBM nicht die IP-Adresse des Kommunikationssystems angibt, sondern die IP-Adresse des Linux-Servers.

Anmerkung: Siehe auch Wie entfernen oder löschen Sie Unify Phone-Benutzer auf Seite 1211.

25.4.1 Restart (Neustart) von OpenScape Business

Über die Funktion **System neu starten** kann ein kontrollierter Restart (Neustart) von OpenScape Business ausgelöst werden.

Folgende Unterschiede sind zu beachten:

- OpenScape Business S und OpenScape Business X

  Es erfolgt ein kontrollierter Restart (Neustart) des Kommunikationssystems. Nach dem Hochlauf ist das Kommunikationssystem wieder betriebsbereit.

  Die Hochlaufzeit ist abhängig vom Systemausbau und dem OpenScape Business-Vernetzungsszenario.

  Ist OpenScape Business X3/X5/X8 mit einer UC Booster Card (Application Board OCAB) bestückt, erfolgt auch ein kontrollierter Restart (Neustart) der UC Applikation (UC Smart oder UC Suite).
- OpenScape Business UC Booster Server (Application Server)

  Es erfolgt ein kontrollierter Restart (Neustart) des OpenScape Business-Anteils und der UC Applikation (UC Suite). Nach dem Hochlauf ist die UC Applikation wieder betriebsbereit.

Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

25.4.1.1 Wie Sie einen Restart (Neustart) von OpenScape Business auslösen

Mit der Funktion **System neu starten** können Sie einen Restart (Neustart) von OpenScape Business auslösen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Tipp: Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **System neu starten** und anschließend auf **OK**. OpenScape Business führt einen Restart (Neustart) durch.

   OpenScape Business S und OpenScape Business X: Nach dem Hochlauf ist das Kommunikationssystem wieder betriebsbereit.

   OpenScape Business UC Booster Server: Nach dem Hochlauf ist die UC Applikation (UC Suite) wieder betriebsbereit.

25.4.2 Reload von OpenScape Business

Über die Funktion **System-Reload ausführen** kann ein Reload von OpenScape Business ausgelöst werden.

Folgende Unterschiede sind zu beachten:

- OpenScape Business S und OpenScape Business X

  Es erfolgt ein Reload des Kommunikationssystems. Nach dem anschließenden Hochlauf befindet sich das Kommunikationssystem im Grundzustand.

  – Alle länder- und kundenspezifischen Einstellungen wurden gelöscht (System-Länderkennzeichen = Deutschland).
  – Das Kommunikationssystem hat die Standard-IP-Adresse 192.168.1.2 und den internen IP-Adressbereich 192.168.3.xxx.
  – Die Lizenzierung bleibt erhalten.

  Die Hochlaufzeit ist abhängig vom Systemausbau.
- OpenScape Business UC Booster Server

  Es erfolgt ein Reload des OpenScape Business-Anteils. Nach dem anschließenden Hochlauf befindet sich der OpenScape Business-Anteil im Grundzustand.

  – Alle kundenspezifischen Einstellungen des OpenScape Business-Anteils (zum Beispiel das Benutzerverzeichnis) wurden gelöscht.
  – Die Lizenzierung bleibt erhalten.

  Das Betriebssystem wird nicht zurückgesetzt.

25.4.2.1 Wie Sie einen Reload von OpenScape Business auslösen

Mit der Funktion **System-Reload ausführen** können Sie einen Reload von OpenScape Business auslösen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

OpenScape Business S und OpenScape Business X: Die Konfigurationsdaten des Kommunikationssystems wurden in einem Backup-Set gesichert.

Anmerkung:

Durch einen Reload wird das Kommunikationssystem in den Grundzustand versetzt. Alle länder- und kundenspezifischen Einstellungen werden gelöscht (System-Länderkennzeichen = Deutschland). Das Kommunikationssystem erhält die Standard-IP-Adresse 192.168.1.2.

OpenScape Business UC Booster Server: Die Konfigurationsdaten des OpenScape Business-Anteils wurden in einem Backup-Set gesichert.

Anmerkung:

Durch einen Reload wird der OpenScape Business-Anteil in den Grundzustand versetzt. Alle kundenspezifischen Einstellungen des OpenScape Business-Anteils (zum Beispiel das Benutzerverzeichnis) werden gelöscht.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **System-Reload ausführen** und anschließend auf **OK**. OpenScape Business führt einen Reload durch.

Tipp: OpenScape Business S und OpenScape Business X: Nach dem anschließenden Hochlauf befindet sich das Kommunikationssystem im Grundzustand. Nach Konfiguration der Grundeinstellungen über den Wizard **Erstinstallation** können die gesicherten länder- und kundenspezifischen Daten wieder geladen werden. Informationen zur Vorgehensweise siehe Wiederherstellen .

OpenScape Business UC Booster Server: Nach dem anschließenden Hochlauf befindet sich der OpenScape Business-Anteil im Grundzustand. Die gesicherten kundenspezifischen Daten können wieder geladen werden. Informationen zur Vorgehensweise siehe Wiederherstellen .

25.4.3 Shutdown (Herunterfahren) von OpenScape Business X

Über die Funktion **System herunterfahren** kann ein kontrolliertes Herunterfahren der Kommunikationssysteme OpenScape Business X veranlasst werden.

25.4.3.1 Wie Sie OpenScape Business X herunterfahren

Mit der Funktion **System herunterfahren** können Sie ein kontrolliertes Herunterfahren der Kommunikationssysteme OpenScape Business X veranlassen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **System herunterfahren** und anschließend auf **OK**. Das Kommunikationssystem wird kontrolliert heruntergefahren.

Tipp: OpenScape Business X1/X3/X5: Das anschließende Hochfahren des Kommunikationssystems ist ausschließlich durch Ziehen und anschließendes Stecken des Netzsteckers möglich.

OpenScape Business X8: Das anschließende Hochfahren des Kommunikationssystems ist ausschließlich durch Ausschalten und anschließendes Wiedereinschalten aller Stromversorgungen LUNA2 möglich.

25.4.4 PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X

Die Aktivierung des Shutdowns über ein Systemtelefon ist PIN-geschützt.

Bei der Aktivierung über ein Systemtelefon muss immer die im Kommunikationssystem konfigurierte PIN eingegeben werden. Die Konfiguration dieser PIN erfolgt durch einen Administrator mit dem Profil **Advanced**.

25.4.4.1 Wie Sie eine PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X konfigurieren

Die PIN gilt für die Aktivierung eines Shutdowns über ein Systemtelefon.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **Shutdown aktivieren/deaktivieren**.
4) Geben Sie im Feld **PIN** die gewünschte sechsstellige PIN ein.
5) Klicken Sie auf **Sichern** und anschließend auf **OK**.

Nächste Schritte

Die Aktivierung eines Shutdowns über ein Systemtelefon erfolgt durch Eingabe der entsprechenden Kennzahl (Standardkennzahl = *997) und anschließender Eingabe der sechsstelligen PIN.

- Bei IP-Telefonen: Sie können das kontrollierte Herunterfahren von den beiden zuerst konfigurierten Geräten aus starten.
- Bei UP0-Telefonen: Sie können das kontrollierte Herunterfahren von den beiden zuerst konfigurierten Geräten aus starten. In diesem Fall haben die IP Clients keine Berechtigung, einen Shutdown auszuführen.

25.4.5 Restart (Neustart) der UC Booster Card (Application Board OCAB)

Über die Funktion **Application Board neu starten** können Sie als Administrator einen kontrollierten Restart (Neustart) des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite) auslösen.

Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Darüber hinaus werden die CSTA-Schnittstelle, der Presence Manager, das Wiedergabegerät für Ansagen, die Media Extension Bridge und der Open Directory Service ebenfalls neu gestartet.

25.4.5.1 Wie Sie einen Restart (Neustart) der UC Booster Card (Application Board OCAB) auslösen

Mit der Funktion **Application Board neu starten** können Sie einen kontrollierten Restart (Neustart) des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite) auslösen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Tipp: Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **Application Board neu starten** und anschließend auf **OK**. Die UC Booster Card (Application Board OCAB) führt einen Restart (Neustart) durch.

25.4.6 Reload der UC Booster Card (Application Board OCAB)

Über die Funktion **UC Booster Card Reload ausführen** kann ein Reload des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite) ausgelöst werden.

Der Reload der UC Booster Card dient dazu, die Karte auf die Werkseinstellungen zurückzusetzen und sie anschließend aus dem System zu entfernen. Dies kann z.B. notwendig werden, wenn die Karte nicht mehr in diesem System verwendet werden soll, weil auf den UC Booster Server umgestiegen oder die Karte in einem anderen/neuen OpenScape Business System eingesetzt werden soll.

Alle kundenspezifischen Daten und alle Diagnose-Daten werden auf der UC Booster Card gelöscht und das System wird heruntergefahren. Anschließend wird das System vom Stromnetz genommen und die UC Booster Card entfernt.

Nachdem die UC Booster Card entfernt und das System neu hochgefahren wurde, ist ein neues Backup-Set zu erstellen, da sich die Konfigurationsdaten geändert haben und das alte Backup-Set nicht mehr kompatibel ist. Wurde vorher die Festplatte der UC Booster Card als Backup-Medium verwendet, muss nun ein anderes Backup-Medium ausgewählt werden, wie z.B. ein Netzlaufwerk, ein USB-Medium oder ein FTP-/FTPS-Server (siehe auch Sichern und Wiederherstellen).

25.4.6.1 Wie Sie einen Reload der UC Booster Card (Application Board OCAB) auslösen

Mit der Funktion **UC Booster Card Reload ausführen** können Sie einen Reload des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite) auslösen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **UC Booster Card Reload ausführen** und anschließend auf **OK**. Sie werden vom WBM abgemeldet. Die Karte wird auf die Werkseinstellungen zurückgesetzt und das System anschließend heruntergefahren.
4) Sobald die grüne RUN LED des Mainboards und die Controller-LEDs der UC Booster Card komplett erloschen sind, nehmen Sie das System vom

Stromnetz und entfernen Sie die UC Booster Card (siehe Sichern und Wiederherstellen).

25.4.7 Restart (Neustart) der UC Applikation

Über die Funktion **UC Applikation neu starten** können Sie als Administrator einen kontrollierten Restart (Neustart) der UC Applikation (UC Smart oder UC Suite) auslösen.

Bei einem Restart der UC Applikation werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

25.4.7.1 Wie Sie einen Restart (Neustart) der UC Applikation auslösen

Mit der Funktion **UC Applikation neu starten** können Sie einen Restart (Neustart) der UC Applikation (UC Smart oder UC Suite) auslösen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Tipp: Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **UC Applikation neu starten** und anschließend auf **OK**. Die UC Applikation führt einen Restart (Neustart) durch.

25.5 Inventory-Management

Unter Inventory-Management versteht man die Ermittlung des aktuellen Status der Kommunikationssysteme OpenScape Business Xund OpenScape Business S und der Hardware-Konfiguration der Kommunikationssysteme OpenScape Business X.

25.5.1 Systemstatus

Den aktuellen Status der Kommunikationssysteme OpenScape Business X und OpenScape Business S kann ein Administrator mittels WBM ermitteln. Abgerufen werden können Informationen über den Status der Teilnehmer, des Verbindungsaufbaus, der ITSPs und der VPNs und die Liste der konfigurierten IP-Adressen.

Teilnehmer-Status

Der Teilnehmer-Status ermöglicht die Abfrage folgender Informationen über die eingerichteten Teilnehmer:

- Rufnummer
- Name
- Gerätetyp
- IP-Adresse (Zusätzlich wird bei Systemtelefonen ein Link angezeigt, über den das WBM des Telefons geöffnet werden kann.)
- MAC-Adresse
- Aktuelle SW-Version
- HW Version
- Status (Aktiviert/Deaktiviert)

Verbindungsaufbau-Status

Der Verbindungsaufbau-Status ermöglicht die Abfrage von Informationen über die bestehenden Verbindungen zu PSTN-Partnern (Public Switched Telephone Network-Partner, wie zum Beispiel öffentliche oder private Telekommunikationsnetzte) des Kommunikationssystems OpenScape Business X.

ITSP Status

Der ITSP-Status ermöglicht die Abfrage von Informationen über den aktuellen Status der vorkonfigurierten und eventuell hinzugefügten Internet-Telefonie-Service-Provider (ITSP). Angezeigt wird darüber hinaus, welche Teilnehmer für welchen ITSP eingerichtet wurden.

Die Status jedes ITSPs werden durch die Farbe des zugehörigen Rechtecks angezeigt (grün = OK, orange = Mindestens ein Teilnehmer wurde nicht fehlerfrei eingerichtet.).

VPN-Status

Der VPN-Status ermöglicht die Abfrage von Informationen über die eingerichteten VPN-Tunnel des Kommunikationssystems OpenScape Business X.

Übersicht IP-Adressen

Angezeigt werden die im Kommunikationssystem OpenScape Business X konfigurierten IP-Adressen.

Darüber hinaus wird angezeigt, über welchen Wizard und über welche Menüs im Experten-Modus die IP-Adressen konfiguriert werden können.

Es wird außerdem eine Statusübersicht der Booster Card und Mainboard Ethernet-Schnittstellen angezeigt.

25.5.1.1 Wie Sie den Teilnehmer-Status abfragen

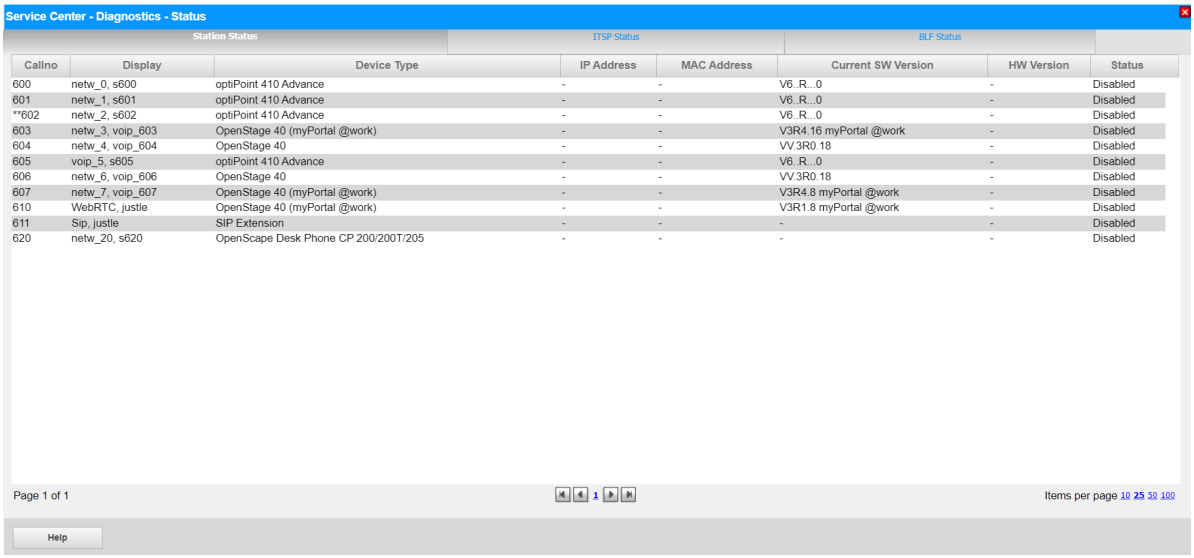
Mit dem Wizard **Status** können Sie den aktuellen Status aller eingerichteten Teilnehmer ermitteln.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Status**.
3) Klicken Sie auf die Registerkarte **Teilnehmer Status**. Es wird Ihnen der Status aller eingerichteten Teilnehmer angezeigt.



4) Klicken Sie auf **Beenden**.

25.5.1.2 Wie Sie den Verbindungsaufbau-Status abfragen

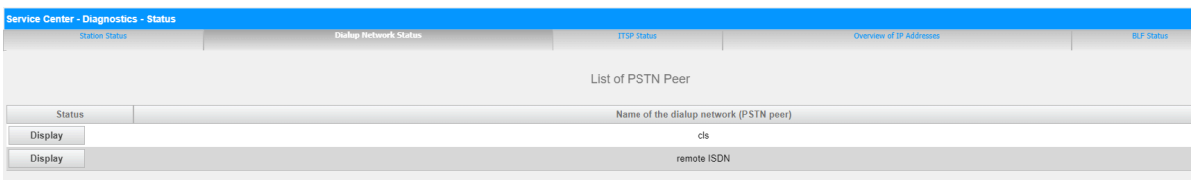
Mit dem Wizard **Status** können Sie den aktuellen Status der PSTN-Partner eines Kommunikationssystems OpenScape Business X ermitteln.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Status**.
3) Klicken Sie auf die Registerkarte **Status Verbindungsaufbau**. Es wird Ihnen die Liste der PSTN-Partner angezeigt.
4) Klicken Sie in der Zeile der gewünschten Verbindung (PSTN-Partner) auf **Anzeigen**. Es wird Ihnen der aktuelle Status dieser Verbindung (PSTN-Partner) angezeigt.



5) Wenn Sie die Statusinformationen einer weiteren Verbindung (PSTN-Partner) abrufen möchten, fahren Sie wie unter Schritt 3 beschrieben fort.
6) Klicken Sie auf **OK** und anschließend auf **Beenden**.

25.5.1.3 Wie Sie den ITSP-Status abfragen

Mit dem Wizard **Status** können Sie den aktuellen Status der Internet-Telefonie-Service-Provider (ITSP) ermitteln.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Status**.
3) Klicken Sie auf die Registerkarte **ITSP Status**. Der aktuelle Status der vorkonfigurierten Internet-Telefonie-Service-Provider (ITSPs) und eventuell hinzugefügter ITSPs mit aktivem Status wird angezeigt.
4) Klicken Sie auf **Diagnose**, um zusätzliche Informationen zur SIP-Verbindung zu erhalten.
5) Klicken Sie auf **Beenden**.

25.5.1.4 Wie Sie IP-Adressen anzeigen

Mit dem Wizard **Status** können Sie eine Übersicht der in einem Kommunikationssystem OpenScape Business X konfigurierten IP-Adressen aufrufen. Darüber hinaus wird angezeigt, über welchen Wizard und über welche Menüs im Experten-Modus die IP-Adressen konfiguriert werden können.

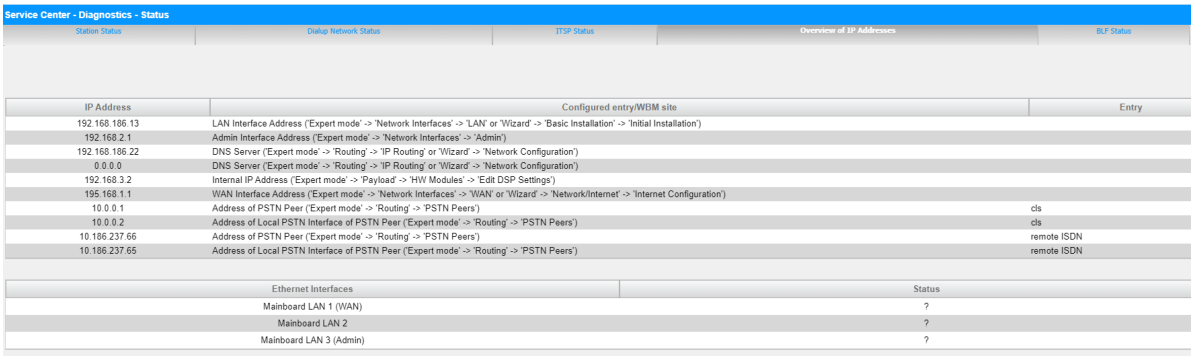
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Status**.

3) Klicken Sie auf die Registerkarte **Übersicht IP-Adressen**. Es wird Ihnen eine Übersicht der im Kommunikationssystem konfigurierten IP-Adressen angezeigt.



4) Klicken Sie auf **Beenden**.

25.5.2 Inventar

Das Inventar ermöglicht es einem Administrator, Informationen über die Hardware und Software von OpenScape Business X sowie die Software von OpenScape Business S abzurufen.

OpenScape Business X

Die folgenden Details können abgerufen werden:

- Kommunikationssystem

  Unter anderem werden folgende Informationen angezeigt:

  – Grafische Darstellung des Kommunikationssystems und der Baugruppe
  – Teilenummer des Mainboards, MAC-Adresse, IP-Adresse, Hostname und Softwareversion
  – Typ der CPU und RAM (in GB) des Systems
  – Details zu Speichergrößen, einschließlich des verfügbaren und belegten Speicherplatzes auf der SDHC-Karte
  – Status aller Anwendungen
- Baugruppen

  Die angezeigten Informationen umfassen Folgendes: Steckplatz, Typ, Teilenummer und Status aller installierten Baugruppen.
- UC-Booster-Karte (Anwendungskarte OCAB), falls verfügbar

  Unter anderem werden folgende Informationen angezeigt:

  – MAC-Adresse, IP-Adresse, Hostname und Softwareversion
  – Details zu Speichergrößen, einschließlich des verfügbaren und belegten Festplattenspeichers.
  – Status aller Anwendungen
  – Übersicht über alle Booster-Karten-Schnittstellen

  Der Link **UC Booster Karte verfügbar** auf der Startseite von WBM leitet den Benutzer zur detaillierten Ansicht der **Service Center > Inventar > Booster-Karte** weiter. Der Link ist auch dann vorhanden, wenn ein Problem

mit der Booster-Karte vorliegt und der Text **UC Booster-Karte nicht verfügbar**.

Je nach Fehler werden auf der Startseite von WBM die folgenden Fehlermeldungen angezeigt:

1) Inter-Integrierte-Schaltung – Verbindung mit Booster-Karte nicht möglich
2) Internetprotokoll V6 – Verbindung zur Booster-Karte nicht möglich
3) Internetprotokoll V4 – Verbindung zur Booster-Karte nicht möglich
4) Secure Socket Shell – Verbindung zur Booster-Karte nicht möglich
5) Netzwerkdateisystem – Verbindung zur Booster-Karte nicht möglich
6) Eine oder mehrere Ethernet-Schnittstellen befinden sich im Halbduplex-Modus – Vollduplex dringend empfohlen

OpenScape Business S

Die folgenden Details können abgerufen werden:

- Software

  Unter anderem werden folgende Informationen angezeigt: MAC-Adresse, IP-Adresse, Hostname und Softwareversion.
- Informationen zur Festplatte

  Details zur Speichergröße, einschließlich des verfügbaren und belegten Speichers.
- Anwendungen

  Alle Anwendungen und ihre jeweiligen Status werden angezeigt.

25.5.2.1 Wie Sie das Inventory von OpenScape Business X abfragen

Mit dem Wizard **Inventory** können Sie den aktuellen Status der Hardware und der Software der Kommunikationssysteme OpenScape Business X ermitteln.

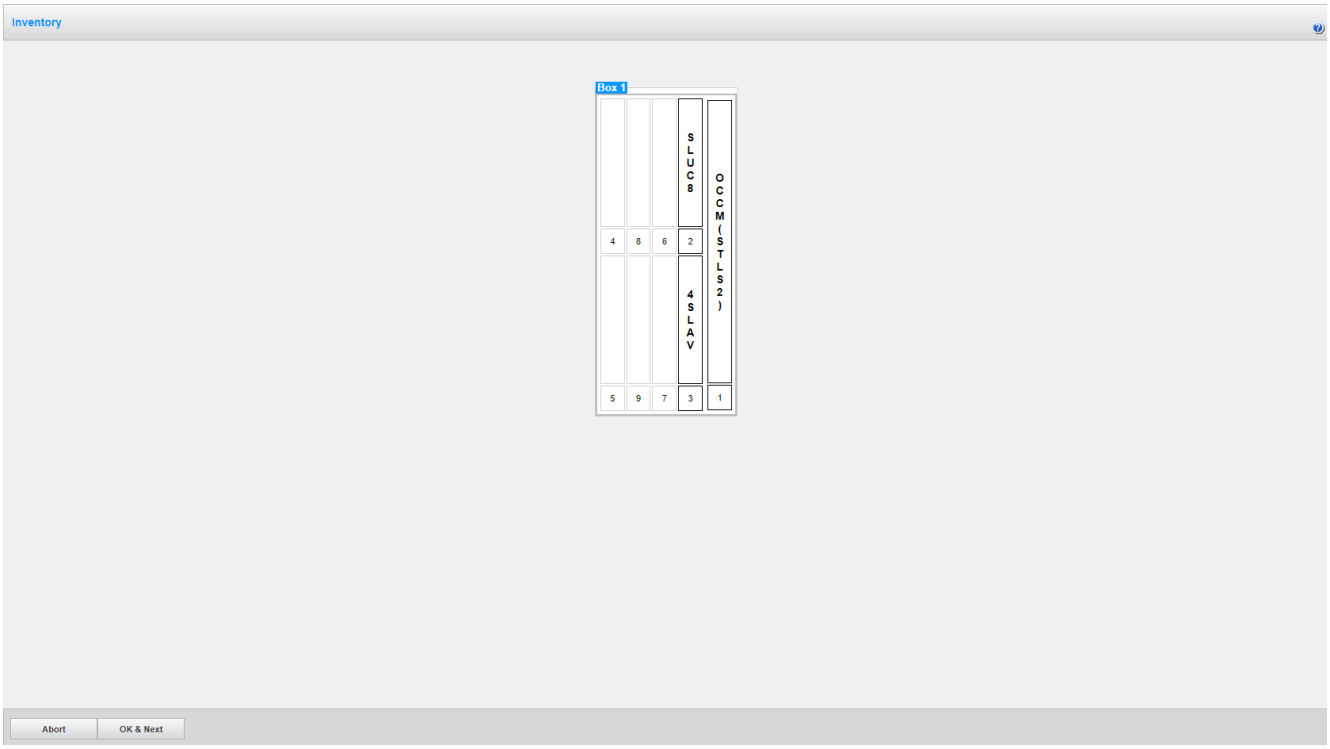
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

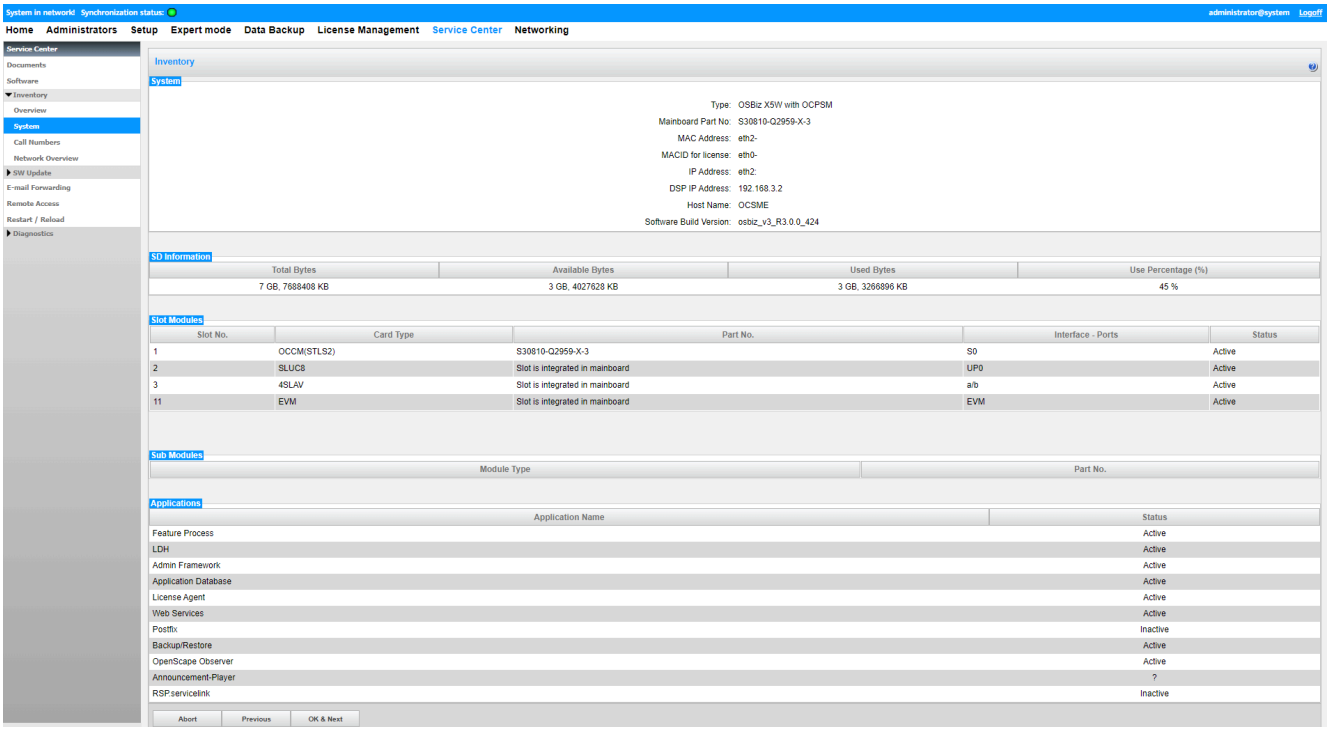
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Inventory** > **Überblick**. Es wird Ihnen eine grafische Darstellung des Kommunikationssystems und der Baugruppen angezeigt.



3) Klicken Sie auf **OK & Weiter**. Es werden Ihnen Informationen über das Kommunikationssystem, über den verfügbaren und den belegten Speicher der SDHC-Karte, über die Baugruppen und über den Applikationsstatus angezeigt.



4) Klicken Sie auf **OK & Weiter**. Die anschließend angezeigten Informationen sind abhängig davon, ob das Kommunikationssystem mit einer UC Booster Card (Application Board OCAB) bestückt ist:
   a) Wenn Ihr Kommunikationssystem nicht mit einer UC Booster Card ausgestattet ist: Es werden Ihnen Informationen über die Zuordnung der Rufnummern zu den Baugruppen angezeigt.
   b) Wenn Ihr Kommunikationssystem mit einer UC Booster Card ausgestattet ist: Es werden Informationen zur OCAB-Baugruppe, zum verfügbaren und belegten Speicherplatz auf der Festplatte sowie zum Anwendungsstatus und zum Status der Booster Card-Schnittstellen angezeigt.

      Klicken Sie auf **OK & Weiter**. Es werden Ihnen Informationen über die Zuordnung der Rufnummern zu den Baugruppen angezeigt.
5) Klicken Sie auf **Beenden**.

25.5.2.2 Wie Sie das Inventory von OpenScape Business S abfragen

Mit dem Wizard **Inventory** können Sie den aktuellen Status der Software von OpenScape Business S ermitteln.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Inventory**. Es werden Ihnen Informationen über die Software des Kommunikationssystems, über den verfügbaren und den belegten Speicher der Festplatten und über den Applikationsstatus angezeigt.

25.6 Automatische Aktionen

Über diese Funktion können einmalig oder regelmäßig durchzuführende Aktionen definiert werden. Diese Aktionen werden dann zum eingestellten Zeitpunkt automatisch durch das Kommunikationssystem ausgeführt.

25.6.1 Automatische Aktion Garbage Collection

Durch die automatische Aktion Garbage Collection kann regelmäßig eine automatische Speicherbereinigung auf dem Kommunikationssystem durchgeführt werden. Nach Abschluss jeder Speicherbereinigung führt das Kommunikationssystem einen Restart (Neustart) durch.

Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status der Aktion (grün = Aktion aktiviert, rot = Aktion nicht aktiviert).

Durch Auswahl von **Aktion starten/stoppen** kann eine nicht aktive Aktion (roter Listenpunkt) aktiviert/gestartet und eine aktive Aktion (grüner Listenpunkt) deaktiviert/gestoppt werden.

In der Standardeinstellung ist die automatische Aktion Garbage Collection nicht aktiviert.

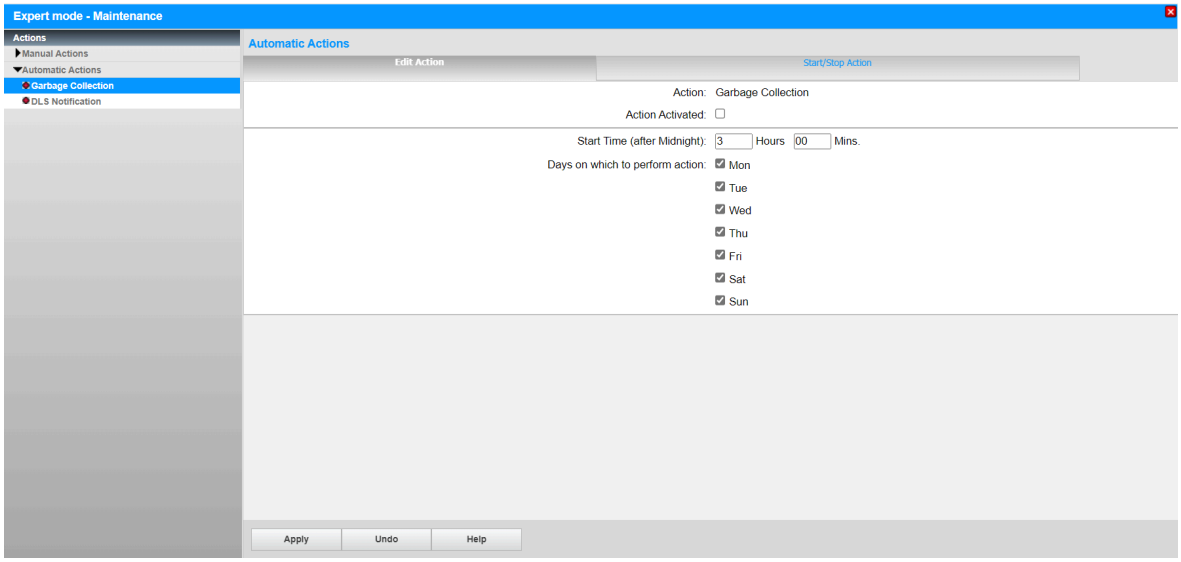
25.6.1.1 Wie Sie die automatische Aktion Garbage Collection ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Aktionen**.
3) Klicken Sie im Menübaum auf **Aktionen** > **Automatische Aktionen** > **Garbage Collection**.
4) Klicken Sie auf die Registerkarte **Aktion ändern**.



5) Wählen Sie die gewünschte Einstellung aus:
   - Wenn die Aktion Garbage Collection durchgeführt werden soll, aktivieren Sie das Kontrollkästchen **Aktion aktiviert**.
   - Wenn die Aktion Garbage Collection nicht durchgeführt werden soll, deaktivieren Sie das Kontrollkästchen **Aktion aktiviert**.
6) Ändern Sie bei Bedarf den **Startzeitpunkt nach Mitternacht**.

   Geben Sie im Feld **Std.** die Stunden und im Feld **Min.** die Minuten ein, nach deren Ablauf die Aktion gestartet werden soll.

   Beispiel: Im Feld **Std.** wurde `3` und im Feld **Min.** `30` eingegeben. Das bedeutet, die Aktion Garbage Collection wird morgens um 3:30 Uhr durchgeführt.
7) Ändern Sie bei Bedarf die Wochentage über **Aktion an folgenden Wochentagen ausführen**.

   Aktivieren Sie die Kontrollkästchen der Wochentage, an denen die Aktion durchgeführt werden soll. Deaktivieren Sie die Kontrollkästchen der Wochentage, an denen die Aktion nicht durchgeführt werden soll.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.6.1.2 Wie Sie die automatische Aktion Garbage Collection starten (aktivieren)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Aktionen**.
3) Klicken Sie im Menübaum auf **Aktionen** > **Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt. Nicht aktivierte Aktionen sind durch einen roten Listenpunkt gekennzeichnet. Aktivierte Aktionen sind durch einen grünen Listenpunkt gekennzeichnet.
4) Klicken Sie im Menübaum auf **Garbage Collection**.
5) Klicken Sie auf die Registerkarte **Aktion starten/stoppen**.
6) Klicken Sie auf **Start** und anschließend auf **OK**.

25.6.1.3 Wie Sie die automatische Aktion Garbage Collection stoppen (deaktivieren)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Aktionen**.
3) Klicken Sie im Menübaum auf **Aktionen** > **Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt. Nicht aktivierte Aktionen sind durch einen roten Listenpunkt gekennzeichnet. Aktivierte Aktionen sind durch einen grünen Listenpunkt gekennzeichnet.
4) Klicken Sie im Menübaum auf **Garbage Collection**.
5) Klicken Sie auf die Registerkarte **Aktion starten/stoppen**.
6) Klicken Sie auf **Stop** und anschließend auf **OK**.

25.6.2 Automatische Aktion DLS Notification

Durch die automatische Aktion DLS Notification kann die automatische Anmeldung an einem externen DLS-Server beim Hochlauf des Kommunikationssystems initiiert werden.

Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status der Aktion (grün = Aktion aktiviert, rot = Aktion nicht aktiviert).

Durch Auswahl von **Aktion starten/stoppen** kann eine nicht aktive Aktion (roter Listenpunkt) aktiviert/gestartet und eine aktive Aktion (grüner Listenpunkt) deaktiviert/gestoppt werden.

In der Standardeinstellung ist die automatische Aktion DLS Notification nicht aktiviert.

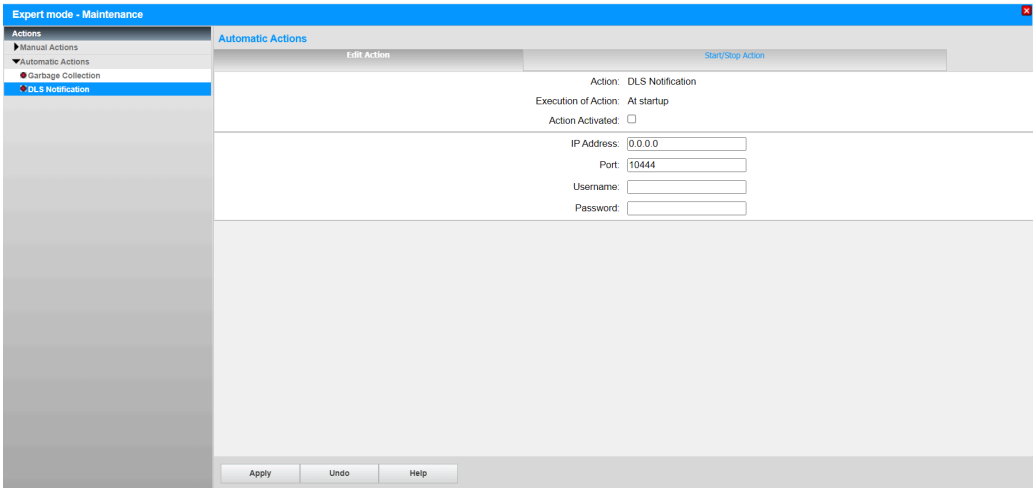
25.6.2.1 Wie Sie die automatische Aktion DLS Notification ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Aktionen**.
3) Klicken Sie im Menübaum auf **Aktionen** > **Automatische Aktionen** > **DLS Notification**.
4) Klicken Sie auf die Registerkarte **Aktion ändern**.



5) Wählen Sie die gewünschte Einstellung aus:
   - Wenn die Aktion DLS Notification durchgeführt werden soll, aktivieren Sie das Kontrollkästchen **Aktion aktiviert**.
   - Wenn die Aktion DLS Notification nicht durchgeführt werden soll, deaktivieren Sie das Kontrollkästchen **Aktion aktiviert**.
6) Ändern Sie bei Bedarf im Feld **IP-Adresse** die IP-Adresse des externen DLS-Servers.
7) Ändern Sie bei Bedarf im Feld **Port** den Port des externen DLS-Servers.
8) Ändern Sie bei Bedarf im Feld **Benutzername** den Benutzernamen für die Anmeldung am externen DLS-Server.
9) Ändern Sie bei Bedarf im Feld **Passwort** das Passwort für die Anmeldung am externen DLS-Server.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.6.2.2 Wie Sie die automatische Aktion DLS Notification starten (aktivieren)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Aktionen**.

3) Klicken Sie im Menübaum auf **Aktionen** > **Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt. Nicht aktivierte Aktionen sind durch einen roten Listenpunkt gekennzeichnet. Aktivierte Aktionen sind durch einen grünen Listenpunkt gekennzeichnet.
4) Klicken Sie im Menübaum auf **DLS Notification**.
5) Klicken Sie auf die Registerkarte **Aktion starten/stoppen**.
6) Klicken Sie auf **Start** und anschließend auf **OK**.

25.6.2.3 Wie Sie die automatische Aktion DLS Notification stoppen (deaktivieren)

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Aktionen**.
3) Klicken Sie im Menübaum auf **Aktionen** > **Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt. Nicht aktivierte Aktionen sind durch einen roten Listenpunkt gekennzeichnet. Aktivierte Aktionen sind durch einen grünen Listenpunkt gekennzeichnet.
4) Klicken Sie im Menübaum auf **DLS Notification**.
5) Klicken Sie auf die Registerkarte **Aktion starten/stoppen**.
6) Klicken Sie auf **Stop** und anschließend auf **OK**.

25.6.3 Warnmechanismus für SDHC-Kartenlebensdauer

Die automatische Aktion Warnmechanismus für die SDHC-Lebensdauer ist eine Möglichkeit, Informationen über den Zustand der SDHC-Karten mit einer Dateisystemprüfung während des Startvorgangs abzurufen. Ein WBM-Wizard wird gestartet und führt den Techniker durch die Festlegung einer Zeit, zu der das System einen Neustart durchführen und die Prüfung ausführen soll.

Anmerkung: Falls bei der Überprüfung keine Dateisystemfehler gefunden werden, wird **SDHC-Integritätsstatus** wieder auf grün oder gelb gesetzt, auch wenn zuvor Fehler gemeldet wurden.

Alle Informationen werden im Kunden-Trace protokolliert. In der Standardeinstellung ist die automatische Aktion Warnmechanismus für SDHC deaktiviert.

Anmerkung: Diese Option löst einen Neustart des Systems aus, während die folgende Warnung angezeigt wird "`Hinweis: Das System wird neu gestartet, nachdem Sie "OK" drücken.`"

Die WBM-Startseite erkennt zwei Zustände:

- Wenn die Informationen im System verfügbar sind, wird ein Text auf dem Startbildschirm angezeigt, der über den allgemeinen Status der Karte informiert: **SDHC-Integritätsprüfung** (grün, gelb, rot oder grau).

  Die allgemeine Lebensdauer der Karte wird basierend auf den Herstellerspezifikationen und den durchschnittlichen Schreibzyklen des Systems berechnet. Es sind unterschiedliche Werte für die Lebensdauer der Karte möglich. Diese Informationen werden zusammen mit anderen Informationen auf der Seite „SDHC-Integritätsprüfung“ im WBM angezeigt.

  Eine geschätzte Lebensdauer von 4 Jahren für Standardkarten und 10 Jahren für Karten mit hoher Ausdauer wird innerhalb des Systems gespeichert.

  Anmerkung: Die geschätzten Werte für die Lebensdauer sind nur die Basis für den Warnmechanismus der integrierten SDHC-Integritätsprüfung. Diese Werte implizieren nicht automatisch, dass eine Karte nach Ablauf dieser Zeit defekt ist.

  Ein grüner Integritätsstatus zeigt an, dass die Karte ihre geschätzte Lebensdauer nicht erreicht hat und es ein Problem mit dem Dateisystem gibt.

  Ein gelber Integritätsstatus zeigt an, dass die Karte ihre geschätzte Lebensdauer erreicht.

  Ein roter Integritätsstatus zeigt an, dass mehr als 50 Dateisystemfehler gefunden wurden.

  Ein grauer Integritätsstatus zeigt an, dass die Karte entweder nicht unterstützt wird oder keine Informationen für die Karte abgerufen werden können. Die SDHC-Karte muss durch einen unterstützten Typ ersetzt werden.

  Der Warnmechanismus für den gelben Integritätsstatus basiert auf dem Herstellungsdatum und der geschätzten Lebensdauer der Karte. Da Karten länger vorrätig sein können, bis sie in OpenScape Business verwendet werden, wird das Erstellungsdatum des Dateisystems ebenfalls im Berechnungsalgorithmus berücksichtigt.

  Im Folgenden wird eine Berechnungstabelle für die SDHC-Integritätsprüfung mit einer geschätzten Lebensdauer von 4 Jahren angezeigt.

Faktor	**Jahre und Gewichtung**									
Herstellungsdatum	< 4 Jahre	< 5 Jahre		< 6 Jahre		< 7 Jahre		< 8 Jahre		> 8 Jahre
Dateisystem erstellt	< 4 years	< 4 years	4-5 Jahre	< 4 years	4 - 6 Jahre	< 3 Jahre	3-7 Jahre	< 2 Jahre	2 - 8 Jahre	-
SDHC-Integritätsstatus	Grün	Green	Gelb	Green	Yellow	Green	Yellow	Green	Yellow	Yellow

- Falls die Informationen nicht verfügbar sind, erhält der Benutzer die folgende Meldung: **Card Health Status unknown**.

Anmerkung: Ist das Dateisystem beschädigt, muss das entsprechende System-SW-Image von SWS heruntergeladen und mit dem Card Manager Tool auf die SDHC-Karte kopiert werden. Nach dem Start des Systems mit der neuen SDHC-Karte kann die Konfiguration mit der neuesten Sicherung wiederhergestellt werden.

Der Text „**Card Health Status**“ enthält auch einen Link, der zur Seite "Aktionen" führt.

25.6.3.1 Benachrichtigung bei Fehlern in SDHC-Karte festlegen

Falls die integrierte Dateiprüffunktion einige Fehler meldet, die den angegebenen Schwellenwert (50 Fehler) überschreitet, oder das System bei normalem Betrieb nicht mehr von der/auf die SDHC-Karte lesen/schreiben kann, sendet das System eine Benachrichtigung mit einer E-Mail oder einem SNMP-Ereignis.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Ereignisse**.
3) Klicken Sie im Menübaum auf **Ereignisse** > **Reaktionstabelle**. Im Menübaum werden die Namen der Reaktionstabelle angezeigt.
4) Wählen Sie im Menübaum **FP_EVT_HW_067** aus.
5) Wählen Sie eine der folgenden Optionen aus:
   a) SNMP-Trap senden.
   b) E-Mail senden.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Anmerkung:

Die E-Mail-Adresse muss unter **Experten-Modus > Wartung > Ereignisse > E-Mail** konfiguriert werden.

25.6.3.2 Automatische Aktion Warnmechanismus für SDHC-Lebensdauer starten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Speichern Sie das System mit der Sicherungsfunktion auf einem externen Medium.
2) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
3) Klicken Sie im Navigationsbaum auf **Wartung** > **Aktionen**.

4) Klicken Sie im Menübaum auf **Aktionen** > **Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt.
5) Klicken Sie im Menübaum auf **SDHC-Integritätsprüfung**.

   Datum und Uhrzeit für **Lokale Systemzeit** und **Letzte Integritätsprüfung** werden angezeigt. Der Inhalt der **Protokolldatei** wird ebenfalls angezeigt.
6) Wählen Sie eine der folgenden Optionen aus:
   a) Integritätscheck sofort beginnen.
   b) Integritätscheck an einem bestimmten Datum beginnen.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.6.3.3 SDHC-Karte klonen und wechseln

SDHC-Karten haben generell eine begrenzte Lebensdauer. Die Lebensdauer hängt hauptsächlich von der Anzahl der Schreibzyklen der SDHC-Karte ab. OpenScape Business unterstützt den integrierten Erkennungsmechanismus „SDHC-Integritätsstatus“ für die Lebensdauer der SDHC-Karte und eine integrierte Funktion für SDHC-Datensicherung, die im Folgenden zum Wechseln der erschöpften SDHC-Karte und die Erstellung einer neuen und voll funktionsfähigen Karte beschrieben wird.

Anmerkung: Die Funktion für SDHC-Datensicherung bietet die Möglichkeit, den Inhalt der in der Anlage eingesteckten SDHC-Karte zu kopieren, ohne die Anlage herunterzufahren. Siehe auch Wie entfernen oder löschen Sie Unify Phone-Benutzer auf Seite 1211.

Die relevanten Daten können an verschiedenen Speicherorten und auf unterschiedlichen Datenträgern gesichert werden, z. B.:

- An die Anlage angeschlossener USB-Stick
- An die Anlage angeschlossener USB SDHC Card Reader
- NFS-Laufwerk (Network File System)
- NFS-Laufwerk (Network File System) über USB

Anmerkung: Die Optionen mit USB-Stick oder USB SDHC Card Reader sind für OpenScape Business X1 nicht verfügbar. In diesem Fall muss die SDHC-Datensicherung auf einem NFS-Laufwerk gespeichert werden.

Wenn ein USB Card Reader verwendet wird, kann nicht ausgeschlossen werden, dass dieser nicht auch die SDHC-Karte zugreifen oder sie formatieren kann. In diesem Fall sollte ein anderer USB Card Reader oder ein USB-Stick verwendet werden.

Falls ein USB Card Reader mit der neuen eingelegten SDHC-Karte verwendet und direkt mit der Anlage verbunden ist, erstellt die integrierte Funktion für SDHC-Datensicherung eine voll funktionsfähige SDHC-Karte. In allen anderen Fällen wird eine sogenannte TAR-Datei erstellt, die alle System- und Konfigurationsdaten enthält.

Anmerkung: Die TAR-Datei kann nicht von der Wiederherstellungsfunktion der Anlage verwendet werden.

Wie groß die SDHC-Datensicherung (TAR-Datei) ist, hängt von den spezifischen Daten der Anlage ab und kann mehrere GB erreichen, wenn Mediendateien (Voicemails, Gesprächsdatensätze usw.) gespeichert werden.

Um eine SDHC-Karte in einer laufenden Anlage zu klonen und zu wechseln, müssen Sie wie folgt vorgehen:

1) Erstellen Sie auf einem geeigneten Datenträger eine Datei für die SDHC-Datensicherung (siehe Datei für SDHC-Datensicherung erstellen).
2) Erstellen Sie eine neue betriebsbereite SDHC-Karte mit allen Systemdaten (siehe Kommunikationssoftware mit dem Card Manager auf die SDHC-Karte schreiben auf Seite 1359).
3) Schalten Sie das System aus, wechseln Sie die SDHC-Karte und schalten Sie es wieder ein (siehe Kommunikationssoftware mit dem Card Manager auf die SDHC-Karte schreiben auf Seite 1359).

25.6.3.4 Datei für SDHC-Datensicherung erstellen

Voraussetzungen

Ein USB-Stick mit mindestens der gleichen Kapazität wie die SDHC-Karte der Anlage oder ein USB Card Reader, in den eine neue SDHC-Karte mit mindestens der gleichen Größe wie die Karte des Systems eingelegt ist, oder ein NFS-Laufwerk (Network File System) ist von der Anlage aus zugänglich.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **SDHC-Datensicherung** > **Datensicherung**.

3) Wählen Sie eine der folgenden Optionen aus, je nachdem, welche Speicherorte und Datenträger verfügbar sind:

a) NFS

Eine gültige Serveradresse, der relevante Pfad und gültige Login-Daten müssen konfiguriert sein.

Klicken Sie auf **Speichern & prüfen**.

Anmerkung: Ein geplantes Backup ist verfügbar. Es kann nur jeweils eine Aktion geplant sein, und der Benutzer kann sie ändern oder abbrechen.

---

b) Card Reader

Diese Option erstellt eine voll funktionsfähige Kopie der SDHC-Karte ohne Trace- und Protokolldateien.

Ein USB SDHC Card Reader mit eingelegter SDHC-Karte muss vor dem Kopiervorgang in die Anlage eingesteckt werden.

Nach Beginn des Vorgangs wird die eingelegte SDHC-Karte formatiert und alle relevanten Dateien werden auf die eingelegte SDHC-Karte übertragen.

Anmerkung: Entfernen Sie weder den USB SDHC Card Reader noch die eingelegte SDHC-Karte, bevor der Vorgang abgeschlossen ist.

Anmerkung: Die neue SDHC-Karte ist voll funktionsfähig und kann sofort in der OpenScape Business-Anlage

---

verwendet werden. Die neue Karte enthält alle Dateien und Daten außer Protokoll- und Tracedateien.

Anmerkung: Ein geplantes Backup ist verfügbar. Es kann nur jeweils eine Aktion geplant sein, und der Benutzer kann sie ändern oder abbrechen.

c) NFS über USB

Eine gültige Serveradresse, der relevante Pfad und gültige Login-Daten müssen konfiguriert sein.

Klicken Sie auf **Speichern & prüfen**.

Anmerkung: Ein geplantes Backup ist verfügbar. Es kann nur jeweils eine Aktion geplant sein, und der Benutzer kann sie ändern oder abbrechen.

d) USB

Ein FAT32-formatiertes leeres USB-Gerät muss an die Anlage angeschlossen werden.

Anmerkung: Entfernen Sie den USB-Stick nicht, bevor der Vorgang abgeschlossen ist.

Anmerkung: Die kopierte Datendatei für das SDHC-Backup (TAR-Datei) kann im Card Manager Tool verwendet werden, um eine voll funktionsfähige SDHC-Karte für die Anlage zu erstellen.

Anmerkung: Ein geplantes Backup ist verfügbar. Es kann nur jeweils eine Aktion geplant sein, und der Benutzer kann sie ändern oder abbrechen.

4) Klicken Sie auf **OK & Weiter**. Der Fortschritt des Backup-Vorgangs wird in einem separaten Fenster angezeigt.

Anmerkung: Eine Fehlermeldung wird angezeigt, wenn die NFS-Freigabe oder der USB-Stick nicht gemountet werden kann oder wenn der Datenträger nicht formatiert werden kann.

5) Die Meldung **Backup-Aufgabe wurde erfolgreich abgeschlossen** wird angezeigt, nachdem die Sicherungsdatei erfolgreich kopiert wurde.

6) Klicken Sie auf **Beenden**.

Anmerkung: Je nach gewähltem Speicherort und Datenträger unterscheidet sich das weitere Vorgehen.

Bei Verwendung des SDHC Card Readers mit SDHC-Karte kann die neue SDHC-Karte sofort verwendet werden.

In allen anderen Fällen muss die generierte Backup-Datei für die SDHC-Karte in Kombination mit dem Card Manager Tool verwendet werden, um eine neue SDHC-Karte zu generieren.

Nächste Schritte

Befolgen Sie die Anweisungen zum Erstellen einer neuen funktionsfähigen SDHC-Karte und zum Wechseln der SDHC-Karte in der laufenden Anlage (siehe Kommunikationssoftware mit dem Card Manager auf die SDHC-Karte schreiben auf Seite 1359).

25.6.3.5 Austausch der SDHC-Karte

Voraussetzungen

Sie sind am WBM mit dem Profil **Erweitert** angemeldet.

Nur bei Verwendung von UC Suite: UC Suite wurde korrekt gestartet.

Ein Downgrade auf die vorherige Softwareversion wird nicht unterstützt. Wenn eine Karte mit V2-Software installiert ist, können nur ältere Unterversionen von V2 wiederhergestellt werden.

Um Nebeneffekte zu vermeiden, muss die aktuelle Software-Version verwendet werden.

Anmerkung: Falls die SDHC-Karte defekt und das System heruntergefahren ist, sollte eine vorherige Sicherung verwendet und die ersten 10 Schritte der folgenden Prozedur sollten ignoriert werden. Siehe auch Wie entfernen oder löschen Sie Unify Phone-Benutzer auf Seite 1211.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup – Sofort**.
3) Geben Sie im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.
4) Wenn Sie ein Backup-Set inkl. Sprachnachrichten und Ansagen erstellen wollen, aktivieren Sie die Option **Vollständiges Backup**.
5) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.

6) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt des Backups angezeigt.

Anmerkung: Falls die Schaltfläche **OK & Weiter** ausgegraut ist, sind nicht alle Applikationen (z.B. UC Suite) korrekt gestartet, deren Daten gesichert werden sollen.

Falls Sie für das ausgewählte Archiv-Verzeichnis keine Berechtigung haben, erhalten Sie eine Fehlermeldung. Wählen Sie ein anderes Ziellaufwerk aus oder ändern Sie den Pfad für das Archiv.

Falls auf dem Ziellaufwerk nicht genügend Speicherplatz für das Backup-Set vorhanden ist, erhalten Sie eine Fehlermeldung. Wählen Sie ein anderes Ziellaufwerk oder löschen Sie ein Backup-Set und starten Sie die Datensicherung erneut.

Anmerkung: Wenn Sie als Backup-Medium ein USB-Medium verwenden, warten Sie ab, bis die LED des USB-Mediums aufhört zu blinken. Erst dann ist die Sicherung erfolgreich auf dem USB-Medium gespeichert. Entfernen Sie anschließend das USB-Medium.

Anmerkung: Zusätzlich zum Backup-Set ist eine zu dem Backup-Set gehörige Text-Datei zu speichern. Sie enthält Informationen über Datum und Uhrzeit der Sicherung und unter welcher Software-Version die Sicherung durchgeführt wurde.

---

7) Die Sicherung war erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt! erscheint. Es wird 100 %** angezeigt.

8) Wenn Sie als Backup-Medium **HTTPS** ausgewählt haben, müssen Sie das Backup-Set und die zum Backup-Set gehörige Text-Datei an einem Speicherort Ihrer Wahl sichern. Bei den anderen Backup-Medien geschieht dies automatisch. Das Browser-Fenster muss solange geöffnet bleiben, bis der Speichervorgang für Backup-Set und Text-Datei abgeschlossen ist.

9) Klicken Sie auf **Fertig**.

10) Schalten Sie das System aus.

11) Entfernen Sie die installierte SDHC-Karte.

12) Installieren Sie die neue SDHC-Karte.

13) Schalten Sie das System ein.

Wenn eine neue SDHC-Karte installiert wird, wird automatisch die auf der Karte enthaltene Softwareversion mit der Standardkonfiguration auf dem System installiert. Nach dem Start erhält das System seine Standard-IP-Adresse.

14) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

15) Klicken Sie im Navigationsbaum auf **Restore**.

16) Aktivieren Sie im Bereich **Geräte** das Medium, das das wiederherzustellende Backup-Set enthält.

17) Wenn Sie als Backup-Medium **HTTPS** aktiviert haben, navigieren Sie zu dem Speicherort des Backup-Sets und wählen das Backup-Set aus. Navigieren Sie anschließend zum Speicherort der Text-Datei und wählen Sie diese aus.
18) Wenn Sie ein anderes Backup-Medium als **HTTPS** aktiviert haben, aktivieren Sie im Bereich Liste der verfügbaren Backupsets das Backup-Set, das die wiederherzustellenden Konfigurationsdaten enthält.
19) Warten Sie bis die Dateien auf das System geladen wurden und klicken Sie anschließend auf **OK & Weiter**. Die Wiederherstellung der Konfigurationsdaten wird gestartet. Es wird Ihnen der Fortschritt der Wiederherstellung angezeigt.
20) Nachdem die Meldung **Restore erfolgreich ausgeführt!** erscheint, führt das System automatisch ein Neustart durch. Die Wiederherstellung ist erfolgreich abgeschlossen, wenn das System wieder betriebsbereit ist.

Anmerkung: Nach der Wiederherstellung muss das Gerät auf dem RSP-Server gelöscht und dann neu konfiguriert werden.

25.7 Power Management

Das Power-Management versetzt das Kommunikationssystem abhängig von der Auslastung des Systems automatisch in einen Energiesparzustand. Dadurch wird der Energieverbrauch des Systems gesenkt und ein Beitrag zum Umweltschutz geleistet. Die Zeitspanne, in der das System in den Energiesparzustand wechseln darf, ist einstellbar (z.B. nachts).

Das Power-Management kann nur aktiviert werden, wenn sich die LAN-Schnittstellen des Systems im Ethernet-Link-Modus **Auto** befinden.
Im Energiesparzustand wechseln die LAN-Schnittstellen des Systems automatisch in den 100Mbit/s-Vollduplex-Modus. Die LAN-Schnittstellen der angeschlossenen Infrastruktur sollten sich ebenfalls im Autosense-Modus befinden.

Betriebszustände

- Aktivzustand (Active Mode)

  Im Aktivzustand werden Funktionen des Kommunikationssystem genutzt und es findet zwischen dem System und der angeschlossenen Infrastruktur signifikanter Datentransfer statt.
- Bereitschaftszustand (Idle Mode)

  Im Bereitschaftszustand werden kaum Funktionen des Kommunikationssystem genutzt und es findet zwischen dem System und der angeschlossenen Infrastruktur kein signifikanter Datentransfer statt. Wird eine Funktion eingeleitet, wechselt das System vom Bereitschaftszustand in den Aktivzustand.
- Energiesparzustand (Low Power Mode)

  Der Energiesparzustand hat gegenüber dem Bereitschaftszustand einen reduzierten Energiebedarf. Das System befindet sich im 100Mbit/s-Vollduplex-Modus.

Es besteht auch die Möglichkeit, das System permanent im Ethernet-Link-Modus 100Mbit/s-Vollduplex oder 100Mbit/s-Halbduplex zu betreiben.

25.7.1 Wie Sie das Power-Management aktivieren oder deaktivieren

Voraussetzungen

Die LAN-Schnittstelle des Mainboards, über die das System an die LAN-Infrastruktur angeschlossen ist, befindet sich im Ethernet-Link-Modus **Auto**.

Nur wenn eine UC Booster Card gesteckt ist: Die LAN-Schnittstelle der UC Booster Card, über die die UC Booster Card an die LAN-Infrastruktur angeschlossen ist, befindet sich im Ethernet-Link-Modus **Auto**.

Die LAN-Schnittstellen der angeschlossenen Infrastruktur (z.B. IP-Telefone) befinden sich im Autosense-Modus.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Power Management** zu starten.
4) Wenn Sie das Power-Management aktivieren möchten:
   a) Aktivieren Sie das Kontrollkästchen **Power Management ein-/ausschalten**.
   b) Geben Sie unter **Beginn des LowPowerModes** und **Ende des LowPowerModes** die Zeitspanne an, in der das Kommunikationssystem in den Energiesparmodus wechseln soll.
5) Wenn Sie das Power-Management deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Power Management ein-/ausschalten**.
6) Klicken Sie auf **OK & Weiter**. Ihre Einstellungen werden übernommen.
7) Klicken Sie auf **Beenden**.

25.7.2 Wie Sie den Ethernet-Link-Modus der LAN-Schnittstellen ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie** > **Netzwerkschnittstellen**.

3) Wählen Sie den Ethernet-Link-Modus für die LAN-Schnittstelle des Mainboards aus:

a) Klicken Sie im Menübaum auf **Mainboard** > **LAN 2**. Über die LAN 2-Schnittstelle ist das System an die LAN-Infrastruktur angeschlossen.

b) Wenn Sie das Power-Management aktivieren wollen, wählen Sie in der Aufklappliste **Ethernet-Link-Modus** den Eintrag **Auto** aus.

c) Wenn Sie das System permanent in den Energiesparzustand setzen wollen, wählen Sie in der Aufklappliste **Ethernet-Link-Modus** den Eintrag **100HDX** oder **100FDX** aus.

Anmerkung:

Für die Ethernet-Link-Modi **100HDX**, **100FDX** und **1000FDX** kann das Power-Management kann nicht aktiviert werden.

---

d) Klicken Sie auf **Übernehmen**.

4) Nur falls eine UC Booster Card gesteckt ist: wählen Sie den Ethernet-Link-Modus für die LAN-Schnittstelle der UC Booster Card aus:

a) Klicken Sie im Menübaum auf **Application Board** > **LAN 2** oder **LAN 1**, je nachdem, über welche LAN-Schnittstelle die UC Booster Card an die LAN-Infrastruktur angeschlossen ist (zu erkennen an dem Häkchen im Kontrollkästchen **Schnittstelle aktiviert**).

b) Wenn Sie das Power-Management aktivieren wollen, wählen Sie in der Aufklappliste **Ethernet-Link-Modus** den Eintrag **Auto** aus.

c) Wenn Sie das System permanent in den Energiesparzustand setzen wollen, wählen Sie in der Aufklappliste **Ethernet-Link-Modus** den Eintrag **100HDX** oder **100FDX** aus.

Anmerkung:

Für die Ethernet-Link-Modi **100HDX**, **100FDX** und **1000FDX** kann das Power-Management kann nicht aktiviert werden.

---

d) Klicken Sie auf **Übernehmen**.

25.8 Überwachung und Wartung von OpenScape Business

OpenScape Business bietet verschiedene Funktionen, um den aktuellen Status des Systems zu überwachen und um Fehler zu finden und zu beheben.

25.8.1 Prüfen einer Netzwerkverbindung von OpenScape Business X

Durch eine ICMP (Internet Control Message Protocol)-Anforderung kann die Netzwerkverbindung zwischen einem Kommunikationssystem OpenScape Business X und der Ziel-Adresse mit Hilfe von Echoanforderungspaketen überprüft werden.

Echoanforderungspakete können sowohl über die Funktion **Ping** als auch über die Funktion **Traceroute** versendet werden. Die Antwortquittungen werden zusammen mit den Umlaufzeiten angezeigt.

Über die Funktion **Traceroute** werden die Echoanforderungspakete mit unterschiedlichen, ansteigenden TTL (Time-To-Live)-Werten gesendet.

25.8.1.1 Wie Sie Ping senden

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **IP-Diagnose**.
3) Navigieren Sie im Menübaum zu **Mainboard** > **ICMP-Anforderung** > **Ping**.
4) Geben Sie im Feld **Ziel-Adresse** die IP-Adresse des gewünschten Ziels ein.
5) Geben Sie im Feld **Anzahl zu sendender Echoanforderungen** die gewünschte Anzahl ein (Standardwert = 3).
6) Klicken Sie auf **Senden**.

   Anschließend werden Ihnen die Antwortquittungen zusammen mit den Umlaufzeiten angezeigt.

25.8.1.2 Wie Sie Traceroute testen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **IP-Diagnose**.
3) Navigieren Sie im Menübaum zu **Mainboard** > **ICMP-Anforderung** > **Traceroute**.
4) Geben Sie im Feld **Ziel-Adresse** die IP-Adresse des gewünschten Ziels ein.
5) Geben Sie im Feld **TOS-Byte** den gewünschten Wert ein (Standardwert = 0).
6) Klicken Sie auf **Senden**.

   Anschließend werden Ihnen die Antwortquittungen zusammen mit den Umlaufzeiten angezeigt.

25.8.2 SNMP (Simple Network Management Protocol)

Das Simple Network Management Protocol (SNMP) ist ein Netzwerkprotokoll, über das Netzwerkkomponenten (zum Beispiel Router, Server, Switches, Drucker, PC) von einer zentralen Station (Managementkonsole) aus überwacht und gesteuert werden können. Das Protokoll regelt hierbei die Kommunikation zwischen den überwachten Komponenten und der Überwachungsstation.

SNMP beschreibt den Aufbau der Datenpakete, die gesendet werden können, und den Kommunikationsablauf. SNMP wurde so ausgelegt, dass jedes

netzwerkfähige Gerät in die Überwachung aufgenommen werden kann. Zu den Aufgaben des Netzwerkmanagements über SNMP gehören

- die Überwachung von Netzwerkkomponenten,
- die Fernsteuerung und Fernkonfiguration von Netzwerkkomponenten,
- die Fehlererkennung und Fehlerbenachrichtigung.

Zur Überwachung werden sogenannte Agenten eingesetzt. Dabei handelt es sich um Programme, die direkt auf den überwachten Komponenten laufen. Diese Programme sind in der Lage, den Zustand der Komponente zu erfassen und auch selber Einstellungen vorzunehmen oder Aktionen auszulösen. Mit Hilfe von SNMP ist es möglich, dass die zentrale Managementkonsole mit den Agenten über ein Netzwerk kommunizieren kann.

Anmerkung: OpenScape Business unterstützt SNMPv2c, reagiert aber auch auf SNMPv1 snmpget Anfragen.

Management-Informationsdatenbanken MIB

Der Umfang der Daten, die über SNMP verwaltet werden können, wird in Management-Informationsdatenbanken (MIBs) festgelegt. MIBs sind Datenmodelle, die zu verwaltende Netzwerkkomponenten in vorgegebener Weise beschreiben. Die MIB der Kommunikationssysteme OpenScape Business X kann über das WBM (Service-Center) heruntergeladen werden.

Die Kommunikationssysteme verfügen über einen eigenen SNMP-Agenten, der den Zugriff auf eine Reihe von Systemdaten ermöglicht, die in seiner Management-Informationsdatenbank MIB gespeichert sind. Die MIB liefert grundlegende Systeminformationen, Statusinformationen, ereignisbezogene Daten sowie Informationen zu installierter Hardware (Slots) und eingerichteten Verbindungen (Ports).

SNMP ermöglicht die zentrale Überwachung und Administration der Netzwerkkomponenten - inklusive der Kommunikationssysteme selbst. Möglich ist damit

- das Ansprechen eines Kommunikationssystems über TCP/IP.
- der Datenzugriff über externe Management-Applikationen.
- die Realisierung von Fernwartungsaufgaben.
- die Visualisierung des Betriebszustands des Kommunikationssystems.
- die Übermittlung servicerelevanter Fehler (Traps).

Communities

Der Zugriff auf die SNMP-Daten (MIBs) wird durch Communities geregelt. Dabei wird zwischen der lesenden, schreibenden und der Trap-Community unterschieden. Hinter einer Community verbirgt sich jeweils eine IP-Adresse.

Um zum Beispiel einem PC den lesenden Zugriff auf die SNMP-Daten (MIBs) zu ermöglichen, muss die IP-Adresse dieses PCs in die Liste der lesenden Communities eingetragen werden. Um lesenden und schreibenden Zugriff zu erhalten, muss die IP-Adresse in die Liste der schreibenden Communities eingetragen werden.

Über Trap-Communities werden die Empfänger von Fehlermeldungen (Traps) verwaltet.

Traps

Bei Problemen eines Kommunikationssystems werden Traps erzeugt, um über Fehler und Ausfälle zu informieren. Es gibt folgende Arten von Traps:

- System-Traps = Systemfehler, die sofortige Maßnahmen zur Behebung erfordern.
- Leistungs-Traps = Informationen zu Leistungsproblemen, die jedoch keine Behebung erfordern.

Traps sind nach ihrer Auswirkung klassifiziert und können durch einen Administrator mit dem Profil **Expert** über das WBM abgerufen werden. Angezeigt wird eine Liste aller empfangenen Traps mit folgenden Informationen:

Tabellenspalte	Bedeutung
VarBind1 (Severity)	Auswirkungsklasse des Traps Folgende Einträge sind möglich: Kritisch: Fehlermeldung Der Fehler hat problematische Auswirkungen. Major: Fehlermeldung. Der Fehler kann problematische Auswirkungen haben. Minor: Fehlermeldung. Der Fehler hat keine problematischen Auswirkungen. Warning: Meldung über einen möglicherweise problematischen Vorgang oder Zustand, jedoch keine Fehlermeldung. Gelöscht Information: Reine Statusmeldung, keine Fehlermeldung. Intermediate status Other traps
VarBind2 (Name)	Name des Traps
Generischer Name	Allgemeine Bezeichnung, wie zum Beispiel Enterprise Specific
Spezifischer Name	Typ des Traps (1 = Software, 2 = Hardware)
Enterprise	–
Uhrzeit	Zeitpunkt des Fehlers
Index	Listennummer

Die Anzeige der Traps wird alle 30 Sekunden aktualisiert. Die Sortierung der Traps erfolgt in der Reihenfolge ihres Auftretens.

Durch Klicken auf einen Trap-Namen werden die Detaildaten des Traps angezeigt.

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
Fehlerklasse 01 - Allgemeine Meldungen				

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
	Restart des Systems	Harter Neustart (Reset) des gesamten Systems mit aktuellem KDS.	Keine	
FP_EVT_ADM_002	Nachladen des signierten Slots	Nachladen des signierten Slots		
FP_EVT_ADM_003	Restart des Systems	Restart des Systems		
FP_EVT_ADM_010	Restart des SNMP Systems	Harter Neustart des gesamten Systems über SNMP.	Keine	
FP_EVT_ADM_014	SNMP lokale DB-Änderungen	Vor-Ort-Änderungen an der Datenbank.	Keine	
FP_EVT_ADM_015	SNMP Remote-DB-Änderungen	„Remote“-Änderungen an der Datenbank.	Keine	
FP_EVT_ADM_016	SNMP APSXF-Ergebnis	APS-Übertragungsbestätigungsnachricht über SNMP.	Keine	
FP_EVT_ADM_017	SNMP-Authentifizierung fehlgeschlagen	Unerlaubter Zugriffsversuch.	Überprüfen Sie die Firewall-Einstellungen in OpenScape Business/ Manager E (Netzwerk Firewall).	
FP_EVT_ADM_019	Sensor-Alarm	Die Temperatur im OpenScape Business-Gehäuse ist zu hoch.	Überprüfen Sie das Gebläse und die Luftzufuhr im 19-Zoll-Gehäuse. Beachten Sie die Umgebungstemperatur.	
FP_EVT_ADM_020	CDR-Puffergrenze erreicht	Überlauf im CDR-Puffer (CDR-Informationen).	Prüfen Sie, ob die Schnittstellen (V.24, LAN), Ports und die Verbindung funktionieren oder lesen Sie die Rufdaten aus.	
FP_EVT_ADM_024	unautorisierte Applikation	Versuchter Zugriff über eine nicht autorisierte Applikation.	Überprüfen Sie die Firewall-Einstellungen in OpenScape Business/ Manager E (Netzwerk Firewall).	
FP_EVT_ADM_025	Manual Switchback aus HiPath Manager			
Fehlerklasse 02 - Meldungen zur Lizenzverwaltung				
Fehlerklasse 09 - Hardware-Modul-Meldungen				
FP_EVT_HW_034	Verlust des Rahmens ein (STMD)	Verlust des Rahmens ein (STMD)		

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_HW_035	Verlust des Rahmens aus (STMD)	Verlust des Rahmens aus (STMD)		
FP_EVT_HW_036	Schlupf erkannt ein (STMD)	Auf einer ISDN-Leitung ist ein Bitfehler aufgetreten.	Überprüfen Sie die S0-Leitung. Falls erforderlich, laden Sie die Baugruppe neu oder führen Sie einen harten Neustart durch. Wenn der Fehler weiterhin besteht, richten Sie einen ISDN-Trace ein.	Das Problem kann durch asynchrone interne und externe Taktraten verursacht werden. Datenverlust möglich/ Verbindung kann unterbrochen werden.
FP_EVT_HW_039	Alarmanzeige Signalfehler aus (TMS2M)	Alarmanzeige: Der S2M-Fehler ist korrigiert worden.	Keine	
FP_EVT_HW_040	degradierter Minutenfehler ein (TMS2M)	degradierter Minutenfehler ein (TMS2M)		
FP_EVT_HW_041	degradierter Minutenfehler aus (TMS2M)	degradierter Minutenfehler aus (TMS2M)		
FP_EVT_HW_042	kein Signalfehler ein (TMS2M/STMD)	Alarmanzeige: Ein S2M-Fehler ist aufgetreten. Keine physische Verbindung vorhanden.	Überprüfen Sie die S2M-Leitung und die Baugruppe. Falls erforderlich, laden Sie die Baugruppe neu oder führen Sie einen harten Neustart durch. Wenn der Fehler weiterhin besteht, richten Sie einen ISDN-Trace ein.	
FP_EVT_HW_043	kein Signalfehler aus (TMS2M/STMD)	Alarmanzeige: Der S2M-Fehler ist korrigiert worden.	Keine	
FP_EVT_HW_046	schwer fehlerhafte Sekundenfehler ein(TMS2M)	schwer fehlerhafte Sekundenfehler ein(TMS2M)		
FP_EVT_HW_047	schwer fehlerhafte Sekundenfehler aus (TMS2M)	schwer fehlerhafte Sekundenfehler aus (TMS2M)		
FP_EVT_HW_052	Uhr kann als Ref. verwendet werden (TMS2M/STMD)	Uhr kann als Ref. verwendet werden (TMS2M/STMD)		

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_HW_053	Uhr kann nicht als Referenz verwendet werden	Uhr kann nicht als Referenz verwendet werden		
FP_EVT_HW_060	Zugriff auf Einspeisefehler ein (SLMO)	Zugriff auf Einspeisefehler ein (SLMO)		
FP_EVT_HW_063	ELIC-Fehler ein (SLMO/SLMC)	ELIC-Fehler ein (SLMO/SLMC)		
FP_EVT_HW_064	ELIC-Fehler aus (SLMO/SLMC)	ELIC-Fehler aus (SLMO/SLMC)		
FP_EVT_HW_067	OCTAT-Fehler ein (SLMC)	OCTAT-Fehler ein (SLMC)		
FP_EVT_HW_096	unbekannter Fehler von LW	unbekannter Fehler von LW		
Fehlerklasse 11 - Allgemeine Meldungen				
FP_EVT_DEV_041	L1 asynchron ein	L1 asynchron ein		
FP_EVT_DEV_042	L1 asynchron aus	L1 asynchron aus		
FP_EVT_DEV_043	Überlastungsfehler ein	Überlastungsfehler ein		
FP_EVT_DEV_044	Überlastungsfehler aus	Überlastungsfehler aus		
FP_EVT_DEV_045	Alive-Check-Fehler ein	Alive-Check-Fehler ein		
FP_EVT_DEV_046	optiPoint-Informationen	optiPoint-Informationen		
FP_EVT_DEV_048	Layer-2-Fehler erkannt	Layer-2-Fehler erkannt		
FP_EVT_DEV_049	Layer-3-Fehler erkannt	Layer-3-Fehler erkannt		
FP_EVT_DEV_052	Andere Fehler	Andere Fehler		
FP_EVT_DEV_057	KEIN TEI verfügbar	KEIN TEI verfügbar		
FP_EVT_DEV_058	Zu viele L1-Fehler	Zu viele Layer-1-Fehler.	Überprüfen Sie die Leitungen, das Endgerät und den Anschluss. Möglicherweise ist ein Kurzschluss aufgetreten.	
FP_EVT_DEV_059	Zugang nicht konfiguriert	Zugang nicht konfiguriert		
Fehlerklasse 16 - Betriebssystem-Meldungen				

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_GEN_002	Fehler im Freigabepool	Fehler im Freigabepool	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_004	Fehler in OSF-Send	Fehler in OSF-Send	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_005	Fehler im OSF-Timer	Fehler im OSF-Timer	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_010	RESTARTED: manueller Reset	RESTARTED: manueller Reset	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_GEN_011	RESTARTED: manueller Reload	RESTARTED wegen manuellem Reload	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_012	RESTARTED: Ausschalten	RESTARTED aufgrund eines Stromausfalls	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_013	KDS-Sicherung nicht durchgeführt	KDS-Sicherung nicht durchgeführt	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_014	RESTARTED: unbekannter Rest. Nichtübereinst. HW-Angabe	RESTARTED wegen unbekanntem Rest. Nichtübereinst. HW-Angabe	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_GEN_015	Allgemeines Fehlerprotokoll	Allgemeines Fehlerprotokoll	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_020	CSTA: Länge außerhalb des Bereichs	CSTA: Länge außerhalb des Bereichs	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_024	Leerlauf nach Neustart eingetroffen	Leerlauf nach Neustart eingetroffen	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_030	Überschreit. CSTA-Monitor-Pkte.	Überschreit. CSTA-Monitor-Pkte.	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
Fehlerklasse 19 - Meldungen der Netzwerkdienste				
FP_EVT_NWS_011	SNTP-Client am PCS kann nicht aktiviert werden	SNTP-Client am PCS kann nicht aktiviert werden		
Fehlerklasse 20 - Meldungen der Anrufverarbeitung				

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_CP_002	RS232: DSR nicht bereit	Die RS232/V.24-Schnittstelle ist defekt.	Überprüfen Sie die Schnittstelle, die Leitung und die Applikation.	
FP_EVT_CP_013	nicht verbundene Wege	Die maximal zulässige Anzahl von Verbindungswegen wurde überschritten.	Verwenden Sie das Projektierungswerkzeug, um die Systemkonfiguration zu testen. Richten Sie einen Trace mit Informationen von BLS ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
Fehlerklasse 21 - Geräte-Handler-Meldungen				
FP_EVT_DH_004	Port außer Betrieb	Port außer Betrieb		
FP_EVT_DH_005	Port betriebsbereit	Port betriebsbereit		
FP_EVT_DH_016	Name in S0/S2M msg verwerfen	Name in S0/S2M msg verwerfen		
FP_EVT_DH_017	Meldung zu lang L3S int->ext	Meldung zu lang L3S int->ext		
FP_EVT_DH_018	Meldung zu lang L3S ext->int	Meldung zu lang L3S ext->int		
FP_EVT_DH_022	Auto PRI-Erkennung DMS250-Prot	Auto PRI-Erkennung DMS250-Prot		
FP_EVT_DH_023	Auto PRI-Erkennung NI2-Prot		Auto PRI-Erkennung NI2-Prot	I
FP_EVT_DH_024	Automatische PRI-Erkennung 4ESS-Protokoll		Automatische PRI-Erkennung 4ESS-Protokoll	
FP_EVT_DH_026	Überlauf des Schlüsselmoduls	Überlauf des Schlüsselmoduls		
FP_EVT_DH_027	B-chan-Grenze erreicht	B-chan-Grenze erreicht		
Fehlerklasse 23 - Geräte-Handler-Meldungen				

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_NW_060	Systemhalt, kein Puffer verfügbar	Systemhalt, kein freier Puffer mehr verfügbar.	Richten Sie einen Trace mit Informationen von BLS ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
Fehlerklasse 26 - Meldungen der Baugruppenadministration				
FP_EVT_PR_001	Karte außer Betrieb	Die angegebene Baugruppe ist außer Betrieb.	Keine	
FP_EVT_PR_003	anderer Kartentyp als alter Kartentyp	Inkompatibler Kartentyp. Der Steckplatz ist bereits mit einem anderen Baugruppentyp vorbelegt.	Tauschen Sie die Baugruppe aus oder löschen Sie mit dem Assistenten T den voreingestellten Baugruppentyp, damit die neue Baugruppe erkannt wird.	
FP_EVT_PR_004	Karte betriebsbereit	Die angegebene Karte ist betriebsbereit.	Keine	
FP_EVT_PR_005	Fehler beim Lesen der Datenbank	Fehler beim Lesen der Datenbank		
Fehlerklasse 28 - Wiederherstellungsmeldungen				
FP_EVT_RC_008	Fehlende APS im EventLog B	Fehlende APS im EventLog B	Keine	Die aktuelle APS-Version wird beim Kopieren des EventLogs B eingetragen. Dies erleichtert die Analyse.
Fehlerklasse 30 - Board-Software-Meldungen				
FP_EVT_LW_095	keine USBS-Verbindung zum System	keine USBS-Verbindung zum System		
Meldungen zum Ressourcenmanager				
FP_EVT_RM_001	Resource Manager Fehlerkonfiguration	Resource Manager Fehlerkonfiguration		
Nachrichten zum UPM				
FP_EVT_UPM_010	UPM: neu gestartet	UPM: neu gestartet		

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
MSG_DLSC_BOOTSTRAP_OK	DLS-Client erfolgreich gebootstrapt.	DLS-Client erfolgreich gebootstrapt.		
MSG_STRC_STOP	Sicherer Trace gestoppt.	Sicherer Trace gestoppt.		
MSG_STRC_START	Sicherer Trace gestartet für Protokolle.	Sichere Traces wurden vom Benutzer für die genannten Protokolle aktiviert.		
MSG_SPE_CERT_MISSING	SPE-Zertifikat fehlt.	Kein SPE-Zertifikat installiert.	SPE-Zertifikat und privaten Schlüssel importieren (Datei PKCS#12).	
MSG_SPE_CERT_AVAIL	SPE-Zertifikat vorhanden.	SPE-Zertifikat ist jetzt verfügbar.		
MSG_SPE_CERT_UPDATED	Das SPE-Zertifikat wurde erfolgreich aktualisiert.	Das SPE-Zertifikat wurde erfolgreich aktualisiert.		
MSG_SPE_CERT_EXPIRED	SPE-Zertifikat abgelaufen.	Die Gültigkeitsdauer des installierten SPE-Zertifikats ist abgelaufen.	Installieren Sie ein neues gültiges Zertifikat.	
MSG_SPE_CRL_EXPIRED	Die SPE CRL für eine bestimmte CA ist abgelaufen.	CDP unzugänglich oder abgerufene CRL ist abgelaufen.	Importieren Sie ein in CDP konfiguriertes SPE CA-Zertifikat mit gültigen CRLs.	
MSG_SPE_CRL_UPDATED	Die SPE CRL für CA wurde erfolgreich aktualisiert.	Die SPE CRL für CA wurde erfolgreich aktualisiert.		
MSG_SPE_ALL_CRLS_UPTODATE	Alle SPE CRLs sind wieder auf dem neuesten Stand.	Alle SPE CRLs sind wieder auf dem neuesten Stand.		
MSG_MIKEY_REBOOT	Mikey Stack: Durchsetzung gescheitert.	Mikey Stack: Durchsetzung gescheitert.		
MSG_IPSEC_REBOOT	Fataler Fehler im IPSec-Stack.	Fataler Fehler im IPSec-Stack.		
MSG_CAT_H323_REBOOT		Neustart mit H.323		
MSG_CAT_HSA_REBOOT		Neustart mit HAS		
MSG_GW_SUCCESSFULLY_STARTED				
MSG_IP_LINK_FAILURE				
MSG_IP_LINK2_FAILURE		IP-Link 1 auf/ab		
MSG_IP_LINK3_FAILURE				
MSG_NEW_SW_AVAILABLE				

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
MSG_ADMIN_NEUSTART		Neustart mit WBM/ CLI-Admin, Software-Upgrade oder Datenwiederherstellung		
MSG_SYSTEM_NEUSTART		Automatischer Neustart, zum Beispiel mit Garbage Collection		
MSG_EXCEPTION_REBOOT		Neustart mit SW-Ausnahme		
MSG_GW_OBJ_MEMORY_EXHAUSTED		Kein Speicherplatz vorhanden		
MSG_TLS_POOL_SIZE_EXCEEDED		Keine internen Pools mehr		
MSG_OAM_RAM_THRESHOLD_REACHED		RAM-Grenze erreicht		
MSG_OAM_DMA_RAM_THRESHOLD_REACHED		DRAM-Grenze erreicht		
MSG_OAM_THRESHOLD_REACHED		Limit erreicht, zum Beispiel für Flash-Speicher oder IP-Pools		
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION		Temperaturgrenze erreicht (zu heiß)		
MSG_HACKER_AUF_SNMP_PORT_TRAP		Unerlaubter Zugriff auf SNMP-Port		
MSG_DVMGR_LAYER2_SERVICE_TRAP		B-Kanal auf/ab		
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	Mehr als 2 Call-Legs: nicht unterstützt! CSID: %x/%x	Es sind nicht mehr als zwei Call-Legs pro Sitzung erlaubt. Dies hat dazu geführt, dass die Software instabil geworden ist. Der notwendige Neustart wird durchgeführt.		
MSG_SSM_SESSION_CREATION_FAILED	Sitzungserstellung fehlgeschlagen	Eine Signalisierung ist nicht mehr möglich, da eine Sitzung nicht aufgebaut werden konnte. Der notwendige Neustart wird durchgeführt. Es wird ein SNMP-Trap erzeugt.		
MSG_IPNCV_STARTUP_ERROR	IPNCV Startup: Erstellen des IPNCV-Managers fehlgeschlagen	IPNCV konnte nicht gestartet werden. Es wird ein SNMP-Trap erzeugt.	Einen TR/MR erstellen	

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
MSG_IPNCV_STARTUP_SHUTDOWN	IPNCV Start/Stopp: IPNCV-Manager erfolgreich erstellt oder IPNCV starten/ stoppen: IPNCV Manager erfolgreich heruntergefahren	IPNCV wurde erfolgreich gestartet oder gestoppt, ein SNMP-Trap wird erzeugt		
MSG_IPNCV_INTERNAL_ERROR	Interner IPNCV-Fehler: %s	Software-Fehler: ungültige interne Daten gefunden. Es wird ein SNMP-Trap mit dem Profil IPNCV- Detailed generiert.		
MSG_IPNCV_MEMORY_ERROR	IPNCV-Speicher: %s	Speicherüberlauf: Es wird ein SNMP-Trap erzeugt.	Gateway neu starten. Einen TR/MR erstellen.	
MSG_IPNCV_SIGNALING_ERROR	IPNCV-Signalfehler: %s	Softwarefehler: ungültige interne Daten gefunden.		
MSG_CAR_ALIVE_IP_CONNECTION_LOST	CAR: Alive: ip-Verbindung %d.%d. %d.%d verloren	CAR: Alive: IP-Verbindung verloren.		
MSG_LIC_DATA_ACCEPTED		Lizenzdaten akzeptiert		
MSG_LIC_DATA_CORRUPTED		Lizenzdaten unvollständig		
MSG_LIC_DATA_NOT_ACCEPTED		Lizenzdaten akzeptiert		
MSG_SPE_CERT_MISSING	Kein SPE-Zertifikat installiert!	SPE-Zertifikat fehlt.	SPE-Zertifikat installieren.	

Anmerkung: Es gibt SNMP-Events, die in diesem Leitfaden nicht dokumentiert sind.

25.8.2.1 Wie Sie alle Communities anzeigen

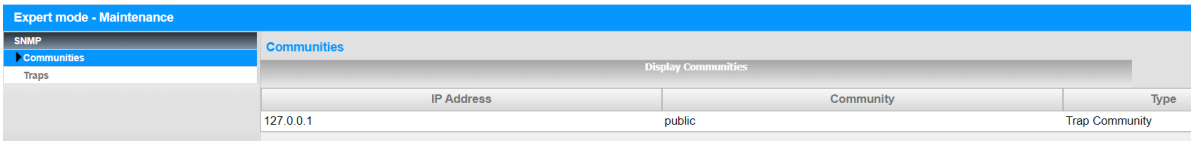
Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **SNMP**.

3) Klicken Sie im Menübaum auf **SNMP** > **Communities**. Es wird Ihnen eine Liste aller Communities mit den zugehörigen Daten (IP-Adresse, Community, Typ) angezeigt.



25.8.2.2 Wie Sie eine Community hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **SNMP**.
3) Wählen Sie die gewünschte Community aus:
   - Wenn Sie eine lesende Community hinzufügen möchten, klicken Sie im Menübaum auf **SNMP** > **Communities** > **Lesende Communities**. Klicken Sie auf die Registerkarte **Lesende Community hinzufügen**.
   - Wenn Sie eine schreibende Community hinzufügen möchten, klicken Sie im Menübaum auf **SNMP** > **Communities** > **Schreibende Communities**. Klicken Sie auf die Registerkarte **Schreibende Community hinzufügen**.
   - Wenn Sie eine Trap-Community hinzufügen möchten, klicken Sie im Menübaum auf **SNMP** > **Communities** > **Trap Communities**. Klicken Sie auf die Registerkarte **Trap Community hinzufügen**.
4) Geben Sie im Feld **IP-Adresse** die IP-Adresse der neuen Community ein.
5) Geben Sie im Feld **Community** den Namen der neuen Community ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.2.3 Wie Sie eine Community ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **SNMP**.
3) Navigieren Sie im Menübaum unter **SNMP** > **Communities** > **...** zur gewünschten Community.
4) Klicken Sie auf die Registerkarte **Community ändern**.
5) Ändern Sie die Community.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.2.4 Wie Sie eine Community löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **SNMP**.
3) Navigieren Sie im Menübaum unter **SNMP** > **Communities** > **...** zur gewünschten Community.
4) Klicken Sie auf die Registerkarte **Community löschen**.
5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

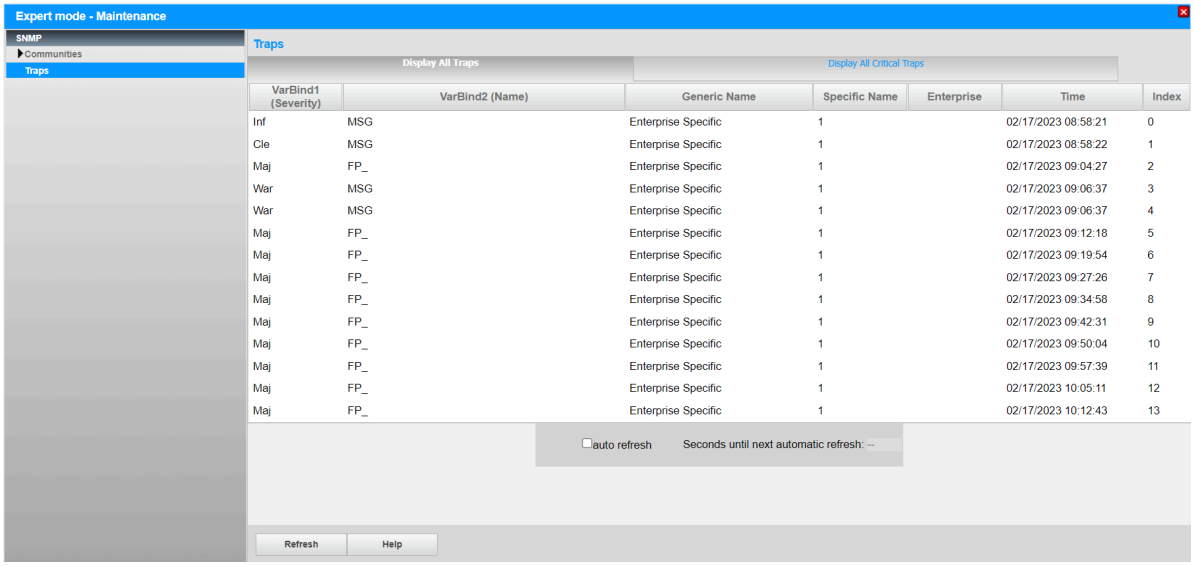
25.8.2.5 Wie Sie Traps anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **SNMP**.
3) Klicken Sie im Menübaum auf **SNMP** > **Traps**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Liste aller Traps angezeigt werden soll, klicken Sie auf die Registerkarte **Alle Traps anzeigen**.



   - Wenn die Liste aller kritischen Traps angezeigt werden soll, klicken Sie auf die Registerkarte **Alle kritischen Traps anzeigen**.

25.8.2.6 Wie Sie Details eines Traps anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **SNMP**.
3) Klicken Sie im Menübaum auf **SNMP** > **Traps**.
4) Klicken Sie auf die Registerkarte **Alle Traps anzeigen**. Es wird Ihnen eine Liste aller Traps mit den zugehörigen Daten angezeigt.
5) Klicken Sie auf den Namen des gewünschten Traps. Es werden Ihnen die Detaildaten dieses Traps angezeigt.
6) Klicken Sie auf die Registerkarte **Alle Traps anzeigen**, um die Liste aller Traps wieder aufzurufen.

25.8.3 Manuelle Aktionen

Durch manuelle Aktionen können verschiedene Protokolldaten (Diagnosedaten / Diagnose-Protokolle) geladen werden.

Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Trace** Diagnosedaten (Diagnose-Protokolle) laden.

Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** Diagnose-Protokolle laden.

Folgende Protokolle können geladen werden:

Protokoll	Erklärung	Anwendungsfall
Trace-Protokoll	Standard-Trace-Datei, wenn Trace-Profile aktiviert werden. Zwischen folgenden Optionen kann gewählt werden: • **Gesamtes Protokoll**: Die gesamten vorhandenen Systemtrace-Protokolldateien werden heruntergeladen. • **Protokoll von heute**: Die Systemtrace-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • **Eigene Auswahl**: **Von:** XXX **Bis:** YYY: Die Systemtrace-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen.	Keine spezielle Anwendung
Event-Protokoll	Aktionen/Events des Kommunikationssystems (Reset, Ein-/Ausschalten usw.)	Keine spezielle Anwendung
Admin-Protokoll	Meldungen über Administrationsvorgänge am Kommunikationssystem (Login-Versuche usw.)	Keine spezielle Anwendung
Lizenz-Protokolle	Meldungen über lizenzierungspflichtige Komponenten des Kommunikationssystems	Probleme bei der Lizenzierung (Lizenzdatei kann nicht aktiviert werden usw.)

Protokoll	Erklärung	Anwendungsfall
Kunden-Trace	Meldungen für den Kunden-Trace werden in ausführlicherer Form dargestellt, als zum Beispiel im Trace-Protokoll (Remote-Login, ITSP-Login usw.).	Probleme mit der ITSP (Internet Telefonie Service Provider)-Anbindung oder beim Remote-Login
Framework-Protokoll	Meldungen des WBM	Probleme bei der Lizenzierung, beim Sichern (Backup), beim Wiederherstellen (Restore) oder mit dem WBM
Diagnose-Protokoll	Diagnose Logs des Kommunikationssystems (FP/LDH)	Absturz oder unkontrolliertes Herunterfahren des Kommunikationssystems
UC Suite-Protokolle	Meldungen der UC Suite des Kommunikationssystems (UC Suite-, CSP- und MEB-Protokolle) Zwischen folgenden Optionen kann gewählt werden: • **Gesamtes Protokoll**: Alle vorhandenen UC Suite-, CSP- und MEB-Protokolldateien werden heruntergeladen. • **Protokoll von heute**: Die UC Suite-, CSP- und MEB-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • **Eigene Auswahl**: **Von:** XXX **Bis:** YYY: Die UC Suite-, CSP- und MEB-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst. Für die OpenScape Business-Protokolle gelten folgende Dateibezeichnungen: UC Suite-Protokolldateien = `vs_jjjj_mm_tt.log`, CSP-Protokolldateien = `csptrace_jjjj_mm_tt.log`, MEB-Protokolldateien = `mebtrace_jjjj_mm_tt.log`. ***INFO***: Diagnosedaten können nur beim Betrieb mit UC Booster Card OCAB heruntergeladen werden. Bei Einsatz des OpenScape Business UC Booster Servers müssen Diagnosedaten über den Server selbst heruntergeladen werden.	Probleme mit der UC Suite und/oder den Clients (myPortal for Desktop, myAttendant usw.)

Protokoll	Erklärung	Anwendungsfall
Applikationsprotokolle	Meldungen des Applikationsanteils des Kommunikationssystems (zum Beispiel CSP-Protokolle) Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** zwischen folgenden Optionen wählen: • **Gesamtes Protokoll**: Alle vorhandenen Protokolldateien werden heruntergeladen • **Protokoll von heute**: Die Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • **Eigene Auswahl**: **Von:** XXX **Bis:** YYY: Die Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst.	Probleme mit dem Applikationsanteil des Kommunikationssystems
System-Diagnose-Protokolle	Diagnose Logs des Kommunikationssystems	Keine spezielle Anwendung
PPP-Protokoll	Meldungen zum Point-to-Point-Protokoll	Probleme bei Einwahl (Dial-In)- oder Auswahl (Dial-Out)-Verbindungen
CoreLog-Protokoll	CoreLogs werden bei Resets usw. erstellt (wie Memory Dumps bei einem PC).	Absturz oder unkontrolliertes Herunterfahren von OpenScape Business

Nach Auswahl der gewünschten Protokolle wird eine komprimierte Datei erzeugt und in einem anzugebenden Verzeichnis gespeichert.

25.8.3.1 Wie Sie Diagnosedaten / Diagnose-Protokolle herunterladen

Mit dem Wizard **Trace** können Sie Diagnosedaten (Diagnose-Protokolle) der Kommunikationssysteme herunterladen.

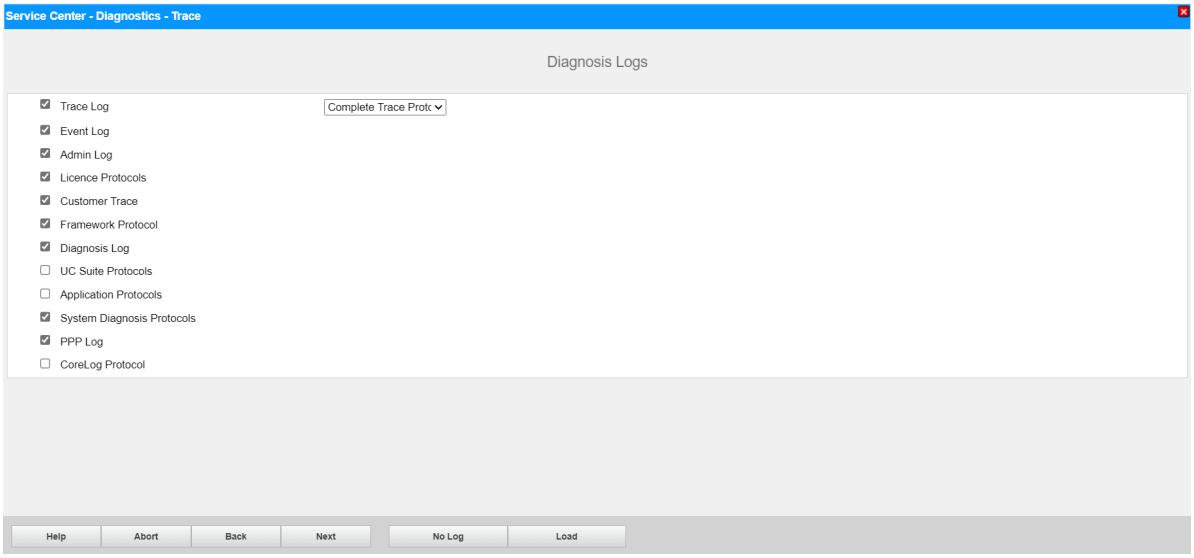
Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Trace**.

3) Klicken Sie auf **Diagnosedaten**.



4) Aktivieren Sie die Kontrollkästchen der Protokolle, die Sie herunterladen wollen. Deaktivieren Sie die Kontrollkästchen der Protokolle, die Sie nicht herunterladen wollen.
5) Klicken Sie auf **Laden** und auf **OK**. Es erscheint das Dateidownload-Fenster.
6) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.
7) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

25.8.4 Traces

Anhand von Traces können Programmschritte und ihre Resultate während eines Programmablaufs aufgezeichnet werden. In Verbindung mit weiteren Diagnosedaten kann damit ein fehlerhaftes Programm bis zur Fehlerursache zurückverfolgt werden. Über die Trace-Profile und Trace-Komponenten wird konfiguriert, welche Traces in welcher Detailtiefe aufgezeichnet werden.

Tipp: Das Aktivieren von Traces wirkt sich negativ auf die System-Performance aus und darf nur durch erfahrene Administratoren und nur in Absprache mit dem zuständigen Service-Support erfolgen.

Insbesondere der Konsolen-Trace belegt wesentliche System-Ressourcen und beeinträchtigt dadurch die Leistung des Kommunikationssystems.

Vernetzung

Für die Diagnose von vernetzten Kommunikationssystemen müssen die Trace-Daten jedes einzelnen Knotens separat erfasst werden. Die zentrale Erfassung von Trace-Daten vernetzter Kommunikationssysteme ist nicht möglich.

Trace-Format-Konfiguration

Über die Funktion Trace-Format-Konfiguration kann ein Administrator mit dem Profil **Expert** definieren, welche Header-Daten in der Trace-Ausgabe enthalten sein sollen und wie die Trace-Daten formatiert werden sollen.

Header-Daten für die Trace-Ausgabe (In der Standardeinstellung sind alle Optionen aktiviert.):

- Globale Trace-Header Format-Einstellungen

  Ist diese Option aktiviert, können die Optionen für die folgenden Header-Daten aktiviert oder deaktiviert werden.
- Subsystem-ID
- Task-Name
- Task-ID
- Uhrzeit
- Modulname
- Zeilennummer

Aufbereitung der Trace-Daten (Formatierung):

- Volle Formatierung mit Parameterexpansion (Standard) = großes Datenvolumen, normale Trace-Performance. Standardeinstellung
- Eingeschränkt (Meldungstypen binär, speziell für X-Tracer) = mittleres Datenvolumen, schnelle Trace-Performance.
- Eingeschränkt (nur Expansion elementarer Datentypen) = geringes Datenvolumen, sehr schnelle Trace-Performance.
- Performanceoptimierter Trace ohne Parameterexpansion = sehr geringes Datenvolumen, extrem schnelle Trace-Performance.

Tipp:

Zu beachten ist, dass zusätzliche Trace-Header-Daten und eine umfangreichere Trace-Daten-Formatierung die Gesamt-Performance eines Traces reduzieren.

Trace-Ausgabe-Interfaces

Über diese Funktion kann ein Administrator mit dem Profil **Expert** die Schnittstellen für die Trace-Ausgabe definieren. Möglich ist entweder die Aktivierung des Datei-Trace oder des Trace über LAN oder die Deaktivierung beider Schnittstellen.

Trace-Ausgabe-Interface	Erläuterung	Standardeinstellung
Datei-Trace	**Datei-Trace aktivieren** Trace-Meldungen werden im Kommunikationssystem in eine Protokolldatei eingetragen. Bei aktivierter Option gelten folgende Einstellungen: **Max. Trace-Quote (kByte)**: Gibt die maximale Größe des Trace-Speichers an **Strategie bei Erreichen der max. Quota**: Ausgewählt werden kann zwischen **Wrap Around (Lösche älteste Datei)** und **Datei-Trace wird temporär gestoppt**. **Zeit, nach der jeweils eine neue Trace-Datei angelegt wird (s)** 900 **Zeitraum für den Trace-Dateien verfügbar sind** Die aktuelle Zeit wird angegeben.	Aktiviert
Trace über LAN	**Trace über LAN aktivieren** Trace-Meldungen werden über die LAN-Schnittstelle übertragen. Stationen, Expertenmodus **Timer-Wert** = 25 s (Verzögerungszeit, bis Daten übertragen werden.)	Nicht aktiviert

Trace-Protokoll

Ist das Trace-Ausgabe-Interface Datei-Trace aktiviert, kann ein Administrator mit dem Profil **Expert** die resultierenden Protokolldateien über diese Funktion auf einen PC übertragen oder löschen.

Digitales Loopback

Digitale Prüfschleifen werden zur Leitungsüberprüfung von B-Kanälen der S_0-, S_{2M}- und T1-Schnittstellen eventuell vorhandener Baugruppen eingesetzt. Die Aktivierung digitaler Prüfschleifen sollte nur nach Aufforderung durch den Service-Provider erfolgen.

Die Konfiguration von digitalen Prüfschleifen ist ausschließlich mit Manager E möglich.

Event Viewer / Kunden-Trace-Protokoll

Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Event Viewer** die Ereignis-Anzeige (Kunden-Trace) starten. Darüber hinaus kann die Kunden-Trace-Protokolldatei auf einen PC übertragen oder gelöscht werden.

Beschrieben ist die Vorgehensweise für folgende Funktionen, die über den Wizard gestartet werden können:

- Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll anzeigen oder ändern
- Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll herunterladen oder öffnen
- Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll löschen

Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** die Anzeige der Kunden-Trace-Protokolldatei starten. Darüber hinaus kann die Kunden-Trace-Protokolldatei auf einen PC übertragen oder gelöscht werden.

M5T-Trace-Komponenten

Diese Funktion dient zur Überwachung des SIP-Stacks durch einen Administrator mit dem Profil **Expert**. Für jede M5T-Trace-Komponente kann die Detailtiefe der Aufzeichnung über Trace-Levels (0 = geringste Detailtiefe bis 4 = größte Detailtiefe) definiert werden.

Secure Trace

Diese Funktion wird von einem Administrator mit dem **Expertenprofil** verwendet, um verschlüsselte VoIP-Nutzlast und Signalisierungsdatenströme aufzuzeichnen.

Bei aktiviertem Leistungsmerkmal Signaling and Payload Encryption (SPE) werden VoIP-Nutz- und Signalisierungsdatenströme vom und zum Kommunikationssystem und zwischen IP-Telefonen verschlüsselt.

Um im Fehlerfall eine Analyse zu gewährleisten, können für einen begrenzten Zeitraum zusätzliche Trace-Informationen (**Secure Trace**) im LAN übertragen werden. Dabei werden asymmetrisch verschlüsselte Secure-Trace-Dateien erzeugt, deren Entschlüsselung und Analyse nur durch die Entwicklung möglich ist.

Um die Nutzung der Secure-Trace-Funktion einzuschränken, wurden folgende Sicherheitsmerkmale implementiert:

- Ein Servicetechniker muss einen sogenannten öffentlichen Schlüssel (Zertifikat) in das betroffene Kommunikationssystem importieren. Das Zertifikat ist Teil einer X.509-Datei und Voraussetzung dafür, dass ein Secure Trace erzeugt werden kann. Die X.509-Datei wird durch die Entwicklung bereitgestellt. Das enthaltene Zertifikat ist maximal einen Monat gültig.
- Das Starten und Stoppen des Secure Trace ist durch ein besonderes Passwort (Passphrase) geschützt. Dieses Passwort ist nur dem Kunden bekannt.

Somit ist das Zertifikat der Schlüssel des Servicetechnikers und das Passwort (Passphrase) der Schlüssel des Kunden. Beide Schlüssel sind notwendig, um die Secure-Trace-Funktion zu aktivieren.

Ablauf für die Erzeugung eines Secure Trace:

1) Ein Servicetechniker stellt ein Problem im Kunden-LAN fest. Zusammen mit der zuständigen Entwicklung wird die Notwendigkeit erkannt, einen Secure Trace zu erzeugen.

2) Der Kunde wird über die Notwendigkeit informiert und muss bestätigen, dass er informiert wurde. Anschließend gibt der Kunde eine Bestellung zur Erzeugung eines Secure Trace auf, in der Datum und Uhrzeit des Beginns und des Endes der Überwachung genannt werden.

3) Ein Entwickler erstellt ein Schlüsselpaar, das aus dem öffentlichen Schlüssel und dem privaten Schlüssel besteht. Mit diesem Schlüsselpaar kann

nur ein einziger Secure Trace erzeugt werden. Die Zertifikate werden folgendermaßen verwendet

- Das Zertifikat mit dem privaten Schlüssel ist streng geheim und kann nur von autorisierten Entwicklern benutzt werden.

  Der private Schlüssel ist zur Entschlüsselung der Secure-Trace-Dateien erforderlich.
- Das Zertifikat mit dem öffentlichen Schlüssel wird dem Servicetechniker in Form einer X.509-Datei im PEM- oder im Binärformat übergeben.

  Der Import dieses Zertifikats in das betroffene Kommunikationssystem ist Voraussetzung dafür, dass ein Secure Trace erzeugt werden kann.

4) Der Servicetechniker informiert den Kunden über den bevorstehenden Beginn der Secure-Trace-Erzeugung. Der Kunde muss die betroffenen Teilnehmer informieren.

Anmerkung: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Strafttatbestand, falls die betroffenen Teilnehmer nicht darüber informiert wurden.

---

5) Der Servicetechniker importiert das Zertifikat mit dem öffentlichen Schlüssel in das betroffene Kommunikationssystem.

6) Der Kunde startet den Secure Trace durch Eingabe des Passworts (Passphrase). Die Secure-Trace-Dateien werden erzeugt.

Start und der Stopp des Secure Trace werden durch das Kommunikationssystem protokolliert.

7) Nach Abschluss der Secure-Trace-Erzeugung wird der Kunde über das Ende der Secure-Trace-Aktivitäten informiert. Der Servicetechniker entfernt das Zertifikat vom Kommunikationssystem.

8) Die Secure-Trace-Dateien werden der Entwicklung zur Verfügung gestellt.

9) Ein Entwickler entschlüsselt den Secure-Trace-Dateien mit Hilfe des privaten Schlüssels. Anschließend erfolgt die Analyse der entschlüsselten Daten.

Anmerkung: Nach dem Ende der Analyse müssen alle relevanten Daten auf eine sichere Art und Weise zerstört werden. Das beinhaltet auch das Zerstören des privaten Schlüssels, damit eine eventuell angefertigte unerlaubte Kopie der Secure-Trace-Dateien nicht mehr entschlüsselt werden kann.

H.323-Stack-Trace

Über diese Funktion ist die Einstellung H.323-Stack-Trace-Konfiguration durch einen Administrator mit dem Profil **Expert** möglich. Die Detailtiefe der Aufzeichnung kann über Trace-Levels (0 = geringste Detailtiefe bis 4 = größte Detailtiefe) definiert werden. Für die H.323-Stack-Trace-Ausgabe können folgende Einstellungen gewählt werden:

Trace-Ausgabe-Interface	Erläuterung	Standardeinstellung
Konsolen-Trace	**Konsolen-Trace aktivieren** H.323-Stack-Trace-Meldungen werden auf der Konsole ausgegeben.	Nicht aktiviert

Trace-Ausgabe-Interface	Erläuterung	Standardeinstellung
Datei-Trace	**Datei-Trace aktivieren** H.323-Stack-Trace-Meldungen werden in eine Protokolldatei eingetragen. Bei aktivierter Option gelten folgende Einstellungen: Max. Größe des Trace-Buffers = 50000 Byte (Menge der Daten, die im Zwischenspeicher gehalten wird.) Max. Größe der Trace-Datei = 1000000 Byte (Maximale Größe der Protokolldatei.) Trace-Timer = 60 s (Verzögerungszeit, bis Daten in die Protokolldatei geschrieben werden.)	Nicht aktiviert

Durch das Aktivieren und/oder Deaktivieren von H.323-Modulen wird definiert, für welche Komponenten der H.323-Stack-Trace die Prozess- und Zustandsinformationen aufzeichnen soll. Der Status jedes H.323-Moduls wird durch die Farbe des zugehörigen Listenpunkts angezeigt (grün = H.323-Modul aktiviert, rot = H.323-Modul nicht aktiviert).

Das H.323-Stack-Trace-Protokoll kann auf einen PC übertragen oder gelöscht werden.

Lizenz-Komponenten-Trace

Diese Funktion dient zur Überwachung des systeminternen Lizenzagenten CLA (Customer License Agent) durch einen Administrator mit dem Profil Expert. Die Detailtiefe der Aufzeichnung kann über Trace-Levels (Niedrig = geringste Detailtiefe (Standardeinstellung), Standard = mittlere Detailtiefe, Alles = größte Detailtiefe) eingestellt werden.

In der Standardeinstellung ist der Lizenz-Komponenten-Trace aktiviert (Trace-Level = Niedrig).

Eine Änderung des Trace-Levels wirkt sich negativ auf die System-Performance aus und darf nur durch erfahrene Administratoren und nur in Absprache mit dem zuständigen Service-Support erfolgen.

Trace-Profile

Trace-Profile legen fest, welche Daten in welcher Detailtiefe aufgezeichnet werden sollen. Einem Trace-Profil werden Trace-Komponenten zugewiesen. Auf diese Weise wird festgelegt, für welche Systemkomponenten ein Trace-Profil die Prozess- und Zustandsinformationen aufzeichnen soll.

Es stehen vordefinierte Trace-Profile zur Verfügung, die alle Standardszenarios adressieren. Zusätzlich kann ein Administrator mit dem Profil **Expert** eigene Trace-Profile anlegen. Durch Starten eines Trace-Profils wird die Aufzeichnung über dieses Profil aktiviert und durch Stoppen deaktiviert.

- Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Trace** Trace-Profile starten und/oder stoppen. Der Status jedes Trace-Profils wird durch die Farbe des zugehörigen Listenpunkts angezeigt (grün = Trace-Profil aktiviert, rot = Trace-Profil nicht aktiviert). Durch Auswahl von **Start/**

Stop kann ein nicht aktives Trace-Profil (roter Listenpunkt) aktiviert/gestartet und ein aktives Trace-Profil (grüner Listenpunkt) deaktiviert/gestoppt werden

Über **Trace laden** können die resultierenden Protokolldateien auf einen PC übertragen oder geöffnet werden.

Über **Trace löschen** können die resultierenden Protokolldateien gelöscht werden.

Beschrieben ist die Vorgehensweise für folgende Funktionen, die über den Wizard gestartet werden können:

– Wie Sie eine Systemtrace-Protokolldatei herunterladen
– Wie Sie eine Systemtrace-Protokolldatei löschen
– Wie Sie alle Trace-Profile anzeigen
– Wie Sie ein Trace-Profil starten oder stoppen
– Wie Sie Diagnosedaten / Diagnose-Protokolle herunterladen

- Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** alle Trace-Profile gemeinsam stoppen und Trace-Profile einzeln starten und/oder stoppen.

  Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status des Trace-Profils (grün = Trace-Profil aktiviert, rot = Trace-Profil nicht aktiviert). Durch Auswahl von **Start/Stop Trace-Profil** kann ein nicht aktives Trace-Profil (roter Listenpunkt) aktiviert/gestartet und ein aktives Trace-Profil (grüner Listenpunkt) deaktiviert/gestoppt werden

  Durch die Auswahl von **Trace-Profil anzeigen** können Sie die Details des gewünschten Trace-Profils anzeigen: Diese beinhalten neben dem Profilnamen, Angaben zum Schreibschutz und zum Status des Profils auch Informationen darüber, bei welchen Problemen dieses Trace-Profil verwendet werden sollte. Angegeben ist auch, welche Trace-Komponenten zum Trace-Profil gehören.

Trace-Profil	Anwendungsfall
Actors_Sensors_Door-Opener	Information liegt noch nicht vor!
Basic	Information liegt noch nicht vor!
Calls_with_Analog_Subscriber_Trunks	Information liegt noch nicht vor!
Calls_with_ISDN_Subscriber_Trunks	Information liegt noch nicht vor!
Calls_with_System_Device_HFA	Information liegt noch nicht vor!
Calls_with_System_Device_Upn	Information liegt noch nicht vor!
CDR_Charging_data	Information liegt noch nicht vor!
CMI	Information liegt noch nicht vor!
CSTA_application	Information liegt noch nicht vor!
Display_problems	Information liegt noch nicht vor!
Gateway_Stream_detailed	Information liegt noch nicht vor!
Gateway_Stream_overview	Information liegt noch nicht vor!
IP_Interfaces	Information liegt noch nicht vor!
License_problem	Information liegt noch nicht vor!
Network_Call_Routing_LCR	Information liegt noch nicht vor!

Trace-Profil	Anwendungsfall
Peripheral_cards	Information liegt noch nicht vor!
RAS_or_Internal_access	Information liegt noch nicht vor!
Ressources_MOH_Conferencing	Information liegt noch nicht vor!
SIP_Interconnection_Subscriber_ITSP	Information liegt noch nicht vor!
SIP_Registration	Information liegt noch nicht vor!
Smart_VM	Information liegt noch nicht vor!
UC_Smart	Information liegt noch nicht vor!
Voice_fax_connection	Information liegt noch nicht vor!
VPN	Information liegt noch nicht vor!
Web_based_Assistant_Expert_Mode	Information liegt noch nicht vor!

Trace-Komponenten

Anhand von Trace-Komponenten werden die Prozess- und Zustandsinformationen einzelner Komponenten des Kommunikationssystems aufgezeichnet.

Alle Trace-Komponenten können durch einen Administrator mit dem Profil **Expert** gemeinsam gestoppt und einzeln gestartet oder gestoppt werden. Durch Starten einer Trace-Komponente wird die Aufzeichnung aktiviert und durch Stoppen deaktiviert. Die Detailtiefe der Aufzeichnung kann über Trace-Levels (0 = geringste Detailtiefe bis 9 = größte Detailtiefe) eingestellt werden.

Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status der Trace-Komponente (grün = Trace-Komponente aktiviert, rot = Trace-Komponente nicht aktiviert). Durch Auswahl von **Start/Stop Trace-Komponente** kann ein nicht aktives Trace-Profil (roter Listenpunkt) aktiviert/gestartet und ein aktives Trace-Profil (grüner Listenpunkt) deaktiviert/gestoppt werden

Bei der Anzeige einer Trace-Komponente werden der Subsystem-Name, der Trace-Komponenten-Index, das eingestellte Trace-Level sowie die Statusinformation angezeigt, ob die Trace-Komponente aktuell gestartet ist oder nicht. Soll eine Trace-Komponente bearbeitet werden, kann neben der Änderung des Trace-Levels auch ein Start oder Stopp der Trace-Komponente vorgenommen werden.

25.8.4.1 Wie Sie eine Systemtrace-Protokolldatei herunterladen

Mit dem Wizard **Trace** können Sie Systemtrace-Protokolldateien herunterladen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Trace**.
3) Klicken Sie auf **Diagnosedaten**.

4) Klicken Sie auf **Kein Protokoll**, um die Kontrollkästchen aller Protokolle zu deaktivieren.
5) Aktivieren Sie das Kontrollkästchen **Trace-Protokoll**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie das gesamte vorhandene Systemtrace-Protokoll herunterladen möchten, wählen Sie in der Aufklappliste **Gesamtes Protokoll** aus.
   - Wenn Sie das Systemtrace-Protokoll des heutigen Tages herunterladen möchten, wählen Sie in der Aufklappliste **Protokoll von heute** aus.
   - Wenn Sie das Systemtrace-Protokoll eines bestimmten Zeitraums herunterladen möchten, wählen Sie in der Aufklappliste **Eigene Auswahl** aus. Wählen Sie in der Aufklappliste **Von:** den Anfang und in der Aufklappliste **Bis:** das Ende des gewünschten Zeitraums aus.
7) Klicken Sie auf **Laden** und auf **OK**. Es erscheint das Dateidownload-Fenster.
8) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.
9) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

25.8.4.2 Wie Sie eine Systemtrace-Protokolldatei löschen

Mit dem Wizard **Trace** können Sie Systemtrace-Protokolldateien löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Trace**.
3) Klicken Sie auf **Trace löschen** und anschließend auf **OK**.
4) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

25.8.4.3 Trace-Einstellungen auf Standardwerte festlegen

Mit dem Wizard **Trace** können Sie System-Trace-Protokolldateien auf den Auslieferungszustand setzen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** oder **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Trace**.
3) Klicken Sie auf die Schaltfläche **Standard-Trace-Einstellungen** und anschließend in der nächsten Popup-Meldung, die Sie darüber informiert, dass die Aktion erfolgreich abgeschlossen wurde, auf **OK**.

4) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

Anmerkung: Erweitertes Tracen erhöht die allgemeine Systemauslastung und sollte nicht dauerhaft aktiviert sein. Die Trace-Einstellungen sollten auf den Standardwert zurückgesetzt werden, indem Sie auf die Schaltfläche **Standard-Trace-Einstellungen** klicken, sobald die erforderlichen Traces erfolgreich erstellt **wurden.**

Anmerkung: Wenn die erweiterten Trace-Einstellungen aktiviert sind, werden Sie auf der WBM-Startseite im Bereich **Benachrichtigungen** darüber informiert. Ein direkter Link zu den Trace-Einstellungen des Service-Centers ist ebenfalls verfügbar.

25.8.4.4 Wie Sie alle Trace-Profile anzeigen

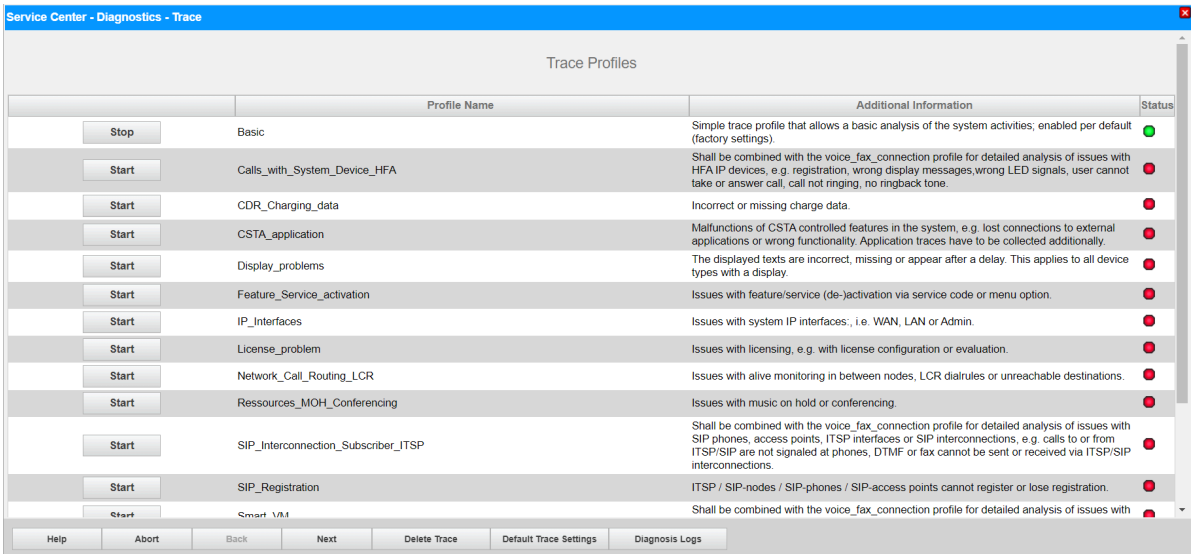
Mit dem Wizard **Trace** können Sie sich über den Status aller Trace-Profile informieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Trace**. Es wird Ihnen eine Liste aller Trace-Profile angezeigt und welche Trace-Profile gestartet sind und welche nicht gestartet sind.



3) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

25.8.4.5 Wie Sie ein Trace-Profil starten oder stoppen

Mit dem Wizard **Trace** können Sie Trace-Profile starten und stoppen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Trace**. Es wird Ihnen eine Liste aller Trace-Profile angezeigt. Ein roter Listenpunkt kennzeichnet die Trace-Profile, die gestartet werden können. Ein grüner Listenpunkt kennzeichnet die Trace-Profile, die gestoppt werden können.
3) Wählen Sie eine der folgenden Möglichkeiten:
   - Wie Sie ein Trace-Profil starten möchten, klicken Sie auf **Start**. Die Farbe des Listenpunkts, die den Status des zugehörigen Trace-Profils anzeigt, wechselt von rot nach grün.

     Anmerkung: Gestartete Trace-Profile wirken sich negativ auf die System-Performance aus. Stoppen Sie deshalb alle Trace-Profile nach Beendigung Ihrer Diagnosetätigkeiten mit Ausnahme des Trace-Profils **Default**. Das Trace-Profil **Default** muss aktiv bleiben.
   - Wie Sie ein Trace-Profil stoppen möchten, klicken Sie auf **Stop**. Die Farbe des Listenpunkts, die den Status des zugehörigen Trace-Profils anzeigt, wechselt von grün nach rot.
4) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

25.8.4.6 Wie Sie die Trace-Format-Konfiguration anzeigen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Eine Aufforderung des zuständigen Service-Supports zur Änderung der Trace-Format-Konfiguration liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Format-Konfiguration**. Es werden Ihnen die aktuellen Einstellungen der Trace-Format-Konfiguration angezeigt.
4) Ändern Sie bei Bedarf die gewünschten Einstellungen.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.4.7 Wie Sie die Trace-Ausgabe-Interfaces anzeigen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Eine Aufforderung des zuständigen Service-Supports zur Änderung der Trace-Ausgabe-Interfaces liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Ausgabe-Interfaces**. Das Simple Network Management Protocol (SNMP) ist ein Netzwerkprotokoll, über das Netzwerkkomponenten (zum Beispiel Router, Server, Switches, Drucker, Computer) von einer zentralen Station (Managementkonsole) aus überwacht und gesteuert werden können.
4) Ändern Sie bei Bedarf die gewünschten Einstellungen.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.4.8 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll anzeigen oder ändern

Mit dem Wizard **Event Viewer** können Sie die Ereignis-Anzeige (Kunden-Trace) starten und die Aktualisierungs-Einstellung ändern.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Event Viewer**.
3) Klicken Sie auf die Registerkarte **Anzeigen**.
4) Wählen Sie die gewünschte Einstellung aus:
   - Wenn das Protokoll automatisch aktualisiert werden soll, aktivieren Sie das Kontrollkästchen **Autom. Aktualisierung**.
   - Wenn das Protokoll nicht automatisch aktualisiert werden soll, deaktivieren Sie das Kontrollkästchen **Autom. Aktualisierung**.
5) Klicken Sie bei Bedarf auf **Aktualisieren**, um das Kunden-Trace-Protokoll manuell zu aktualisieren.
6) Klicken Sie auf **Beenden**.

25.8.4.9 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll herunterladen oder öffnen

Mit dem Wizard **Event Viewer** können Sie die Kunden-Trace-Protokolldatei auf einen PC übertragen oder öffnen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Event Viewer**.
3) Klicken Sie auf die Registerkarte **Laden über HTTP**.
4) Klicken Sie auf **Laden** und auf **OK**. Es erscheint das Dateidownload-Fenster.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Protokolldatei herunterladen möchten, klicken Sie auf **Speichern unter**. Speichern Sie die Datei im gewünschten Verzeichnis und schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.
   - Wenn Sie die Protokolldatei öffnen möchten, klicken Sie auf **Öffnen**. Anschließend wird der Inhalt der komprimierten Protokolldatei angezeigt.
6) Klicken Sie auf **Beenden**.

25.8.4.10 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll löschen

Mit dem Wizard **Event Viewer** können Sie die Kunden-Trace-Protokolldatei löschen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Event Viewer**.
3) Klicken Sie auf die Registerkarte **Event-Viewer-Protokoll löschen**.
4) Klicken Sie auf **Protokoll löschen** und anschließend auf **OK**.
5) Klicken Sie auf **Beenden**.

25.8.4.11 Wie Sie M5T-Trace-Komponenten anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **M5T-Trace-Komponenten**. Es wird Ihnen eine Liste aller M5T-Trace-Komponenten mit den aktuellen Einstellungen angezeigt. Darüber hinaus werden Ihnen im Menübaum die Namen aller M5T-Trace-Komponenten angezeigt. Ein farbiger Listenpunkt kennzeichnet den Status jeder einzelnen M5T-Trace-Komponente.

25.8.4.12 Wie Sie eine M5T-Trace-Komponente starten oder stoppen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Eine Aufforderung des zuständigen Service-Supports zum Starten oder Stoppen einer M5T-Trace-Komponente liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **M5T-Trace-Komponenten**. Im Menübaum werden Ihnen die Namen aller M5T-Trace-Komponenten angezeigt. Ein roter Listenpunkt kennzeichnet die M5T-Trace-Komponenten, die gestartet werden können. Ein grüner Listenpunkt kennzeichnet die M5T-Trace-Komponenten, die gestoppt werden können.
4) Klicken Sie im Menübaum auf die gewünschte M5T-Trace-Komponente.
5) Klicken Sie auf die Registerkarte **Trace-Komponente starten/stoppen**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie eine M5T-Trace-Komponente starten möchten, klicken Sie auf **Start** und anschließend auf **OK**.
   - Wenn Sie eine M5T-Trace-Komponente stoppen möchten, klicken Sie auf **Stop** und anschließend auf **OK**.

25.8.4.13 Wie Sie M5T-Trace-Komponenten ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Eine Aufforderung des zuständigen Service-Supports zur Änderung der M5T-Trace-Komponenten liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **M5T-Trace-Komponenten**. Es wird Ihnen eine Liste aller M5T-Trace-Komponenten mit den aktuellen Einstellungen angezeigt.
4) Ändern Sie die gewünschten Einstellungen.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.4.14 Wie Sie den Secure Trace starten oder stoppen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Secure Trace**.
4) Klicken Sie auf die Registerkarte **Secure Trace starten/beenden**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den Secure Trace starten möchten, gehen Sie folgendermaßen vor:

     Geben Sie im Feld **Secure Trace Aktivierungs-Passphrase** das Passwort für den Secure Trace ein.

     Geben Sie im Feld **Dauer des Secure Trace (Min.)** die Zeit in Minuten ein, die der Secure Trace aktiv sein soll.) Schlüsselsden öffentlichen Schlüssel aus.

     Aktivieren Sie die Kontrollkästchen der Protokolle für die der Secure Trace erstellt werden soll. Deaktivieren Sie die Kontrollkästchen der Protokolle für die der Secure Trace nicht erstellt werden soll.

     Klicken Sie auf **Secure Trace einschalten** und anschließend auf **OK**.
   - Wenn Sie den Secure Trace stoppen möchten, klicken Sie auf **Secure Trace beenden** und anschließend auf **OK**.

25.8.4.15 Wie Sie den Status des Secure Trace abfragen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Secure Trace**.
4) Klicken Sie auf die Registerkarte **Secure Trace Status**. Anschließend wird der aktuelle Status des Secure Trace angezeigt.

25.8.4.16 Wie Sie das Passwort für den Secure Trace ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Secure Trace**.
4) Klicken Sie auf die Registerkarte **Secure Trace Passphrase ändern**.
5) Geben Sie im Feld **Aktuelle Passphrase** das derzeitige Passwort für den Secure Trace ein.
6) Geben Sie in die Felder **Neue Passphrase** und **Neue Passphrase wiederholen** das neue, mindestens fünf- und maximal zwölfstellige Passwort für den Secure Trace ein.

7) Klicken Sie auf **Übernehmen**.

25.8.4.17 Wie Sie das Zertifikat für den Secure Trace aus einer X.509-Datei importieren

Voraussetzungen

Eine X.509-Datei im PEM- oder Binärformat liegt vor.

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Secure Trace**.
4) Klicken Sie auf die Registerkarte **X.509 Datei für Secure Trace importieren**.
5) Klicken Sie auf **Durchsuchen**, um die gewünschte X.509-Datei auszuwählen.
6) Klicken Sie auf **Öffnen**.
7) Klicken Sie auf **Zertifikat aus Datei importieren**.

25.8.4.18 Wie Sie die H.323-Stack-Trace-Konfiguration anzeigen oder ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Eine Aufforderung des zuständigen Service-Supports zur Änderung der H.323-Stack-Trace-Konfiguration liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **H.323-Stack-Trace**.
4) Klicken Sie auf die Registerkarte **H.323-Stack-Trace-Konfiguration ändern**. Es werden Ihnen die aktuellen Einstellungen der H.323-Stack-Trace-Konfiguration angezeigt.
5) Ändern Sie bei Bedarf die gewünschten Einstellungen.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.4.19 Wie Sie H.323-Module ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Eine Aufforderung des zuständigen Service-Supports zur Änderung der H.323-Module liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **H.323-Stack-Trace**.
4) Klicken Sie auf die Registerkarte **Alle H.323-Module ändern**.
5) Wählen Sie die gewünschte Einstellung für **Trace an** aus:
   - Wenn Sie den Trace für bestimmte H.323-Module aktivieren möchten, aktivieren Sie die Kontrollkästchen der gewünschten H.323-Module. Deaktivieren Sie die Kontrollkästchen der H.323-Module, für die der Trace deaktiviert werden soll.
   - Wenn Sie den Trace für alle H.323-Module deaktivieren möchten, klicken Sie auf **Keine**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.4.20 Wie Sie das H.323-Stack-Trace-Protokoll herunterladen oder öffnen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **H.323-Stack-Trace**.
4) Klicken Sie auf die Registerkarte **H.323-Stack-Trace-Protokoll über HTTP laden**.
5) Klicken Sie auf **Laden** und auf **OK**. Es erscheint das Dateidownload-Fenster.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die H.323-Stack-Trace-Protokolldatei speichern möchten, klicken Sie auf **Speichern unter**. Speichern Sie die Datei im gewünschten Verzeichnis und schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.
   - Wenn Sie die H.323-Stack-Trace-Protokolldatei öffnen möchten, klicken Sie auf **Öffnen**. Die Datei wird anschließend im Texteditor angezeigt.

25.8.4.21 Wie Sie das H.323-Stack-Trace-Protokoll löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **H.323-Stack-Trace**.
4) Klicken Sie auf die Registerkarte **H.323-Stack-Trace-Protokoll löschen**.
5) Klicken Sie auf **Protokoll löschen** und anschließend auf **OK**.

25.8.4.22 Wie Sie den Lizenz-Komponenten-Trace ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Eine Aufforderung des zuständigen Service-Supports zur Änderung des Lizenz-Komponenten-Trace liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Lizenz-Komponente** > **CLA**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den Lizenz-Komponenten-Trace stoppen möchten, wählen Sie in der Aufklappliste **Trace-Level** den Eintrag **Aus** aus.
   - Wenn Sie eine niedrige Detailtiefe für die Trace-Aufzeichnung möchten, wählen Sie in der Aufklappliste **Trace-Level** den Eintrag **Niedrig** aus.
   - Wenn Sie eine mittlere Detailtiefe für die Trace-Aufzeichnung möchten, wählen Sie in der Aufklappliste **Trace-Level** den Eintrag **Standard** aus.
   - Wenn Sie eine große Detailtiefe für die Trace-Aufzeichnung möchten, wählen Sie in der Aufklappliste **Trace-Level** den Eintrag **Alles** aus.
5) Klicken Sie auf **Übernehmen**.

25.8.4.23 Wie Sie Details eines Trace-Profils anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Profile**. Es wird Ihnen eine Liste aller Trace-Profile angezeigt. Darüber hinaus werden Ihnen im Menübaum die Namen aller Trace-Profile angezeigt. Ein farbiger Listenpunkt kennzeichnet den Status jedes einzelnen Trace-Profils.
4) Klicken Sie im Menübaum auf den Namen des gewünschten Trace-Profils. Es werden Ihnen die Detaildaten dieses Trace-Profils angezeigt.

25.8.4.24 Wie Sie alle Trace-Profile stoppen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Profile**.

4) Klicken Sie auf die Registerkarte **Alle Trace-Profile stoppen**.
5) Klicken Sie auf **Alle stoppen** und anschließend auf **OK**.

25.8.4.25 Wie Sie ein Trace-Profil hinzufügen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Profile**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein leeres Trace-Profil hinzuzufügen möchten, klicken Sie auf die Registerkarte **Trace-Profil hinzufügen (leeres Profil)**.
   - Wenn Sie ein Trace-Profil hinzuzufügen möchten, das die Trace-Komponenten aller aktuell gestarteten Trace-Profile enthält, klicken Sie auf die Registerkarte **Trace-Profil hinzufügen (mit aktuellen Trace-Einstellungen)**. Wählen Sie aus, welche der angezeigten Trace-Komponenten mit welchem Level in dem neuen Trace-Profil enthalten sein sollen.
5) Geben Sie im Feld **Profilname** den Namen des neuen Trace-Profils ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.4.26 Wie Sie Trace-Komponenten anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Komponenten**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Liste aller Trace-Komponenten angezeigt werden soll, klicken Sie auf die Registerkarte **Alle Trace-Komponenten anzeigen**.
   - Wenn die Liste aller gestarteten Trace-Komponenten angezeigt werden soll, klicken Sie auf die Registerkarte **Gestartete Trace-Komponenten anzeigen**.
   - Wenn die Liste aller gestoppten Trace-Komponenten angezeigt werden soll, klicken Sie auf die Registerkarte **Gestoppte Trace-Komponenten anzeigen**.

25.8.4.27 Wie Sie Details einer Trace-Komponente anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Komponenten**. Es wird Ihnen eine Liste aller Trace-Komponenten angezeigt. Darüber hinaus werden Ihnen im Menübaum die Namen aller Trace-Komponenten angezeigt. Ein farbiger Listenpunkt kennzeichnet den Status jeder einzelnen Trace-Komponente.
4) Klicken Sie im Menübaum auf den Namen der gewünschten Trace-Komponente. Es werden Ihnen die Detaildaten dieser Trace-Komponente angezeigt.

25.8.4.28 Wie Sie eine Trace-Komponente starten oder stoppen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Komponenten**. Im Menübaum werden Ihnen die Namen aller Trace-Komponenten angezeigt. Ein roter Listenpunkt kennzeichnet die Trace-Komponenten, die gestartet werden können. Ein grüner Listenpunkt kennzeichnet die Trace-Komponenten, die gestoppt werden können.
4) Klicken Sie im Menübaum auf die gewünschte Trace-Komponente.
5) Klicken Sie auf die Registerkarte **Trace-Komponente starten/stoppen**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie eine Trace-Komponente starten möchten, klicken Sie auf **Start** und anschließend auf **OK**.
   - Wenn Sie eine Trace-Komponente stoppen möchten, klicken Sie auf **Stop** und anschließend auf **OK**.

25.8.4.29 Wie Sie alle Trace-Komponenten stoppen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.

3) Klicken Sie im Menübaum auf **Traces** > **Trace-Komponenten**.
4) Klicken Sie auf die Registerkarte **Alle Trace-Komponenten stoppen**.
5) Klicken Sie auf **Alle stoppen** und anschließend auf **OK**.

25.8.4.30 Trace-Einstellungen auf Standardwerte festlegen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Komponenten**.
4) Klicken Sie auf die Registerkarte **Standard-Trace-Einstellungen**.
5) Klicken Sie auf die Schaltfläche **Standard-Trace-Einstellungen** und anschließend in der nächsten Popup-Meldung, die Sie darüber informiert, dass die Aktion erfolgreich abgeschlossen wurde, auf **OK**.

Anmerkung: Erweitertes Tracen erhöht die allgemeine Systemauslastung und sollte nicht dauerhaft aktiviert sein. Die Trace-Einstellungen sollten auf den Standardwert zurückgesetzt werden, indem Sie auf die Schaltfläche **Standard-Trace-Einstellungen** klicken, sobald die erforderlichen Traces erfolgreich erstellt **wurden.**

Anmerkung: Wenn die erweiterten Trace-Einstellungen aktiviert sind, werden Sie auf der WBM-Startseite im Bereich **Benachrichtigungen darüber informiert. Ein direkter Link zu den Trace-Einstellungen ist ebenfalls verfügbar.**

25.8.4.31 Wie Sie Trace-Komponenten ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie im Menübaum auf **Traces** > **Trace-Komponenten**.
4) Klicken Sie auf die Registerkarte **Trace-Komponenten ändern**. Es wird Ihnen eine Liste aller Trace-Komponenten mit den aktuellen Einstellungen angezeigt.
5) Ändern Sie die gewünschten Einstellungen.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.8.4.32 Automatische Weiterleitung von Systemprotokolldateien

Sie können die Option zur automatischen Weiterleitung von Systemprotokolldateien an ein externes Managementsystem bzw. einen Syslog-Server weiterzuleiten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces > Syslog-Weiterleitung**.
3) Geben Sie die **IP-Adresse** und den **Port** des Managementsystems ein, an das die Syslog-Datei weitergeleitet wird.
4) Klicken Sie auf **Start**, um die Konfigurationsänderungen zu speichern und den Vorgang zu starten.

   Wenn die Verbindung mit dem Managementportal/Syslog-Server erfolgreich war, wird der **Verbindungsstatus** mit einem grünen Kreis angezeigt.

   Wenn die Verbindung mit dem Managementportal/Syslog-Server nicht erfolgreich war, wird der **Verbindungsstatus** mit einem roten Kreis angezeigt.
5) Klicken Sie auf **Stopp**, um den Vorgang zu deaktivieren.

   Der **Verbindungsstatus** wird deaktiviert und mit einem grauen Kreis angezeigt.
6) Wenn Sie die Konfigurationseinstellungen ändern, klicken Sie auf **Übernehmen**, damit die Änderungen wirksam werden.

25.8.4.33 Kernel Crash-Datendienst starten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Ihr Kommunikationssystem verfügt über ein V3 OCC Mainboard (OCCLA, OCCMA(R), OCCMB(R)).
Vergewissern Sie sich, dass auf der Speicherplatte genügend freier Speicherplatz vorhanden ist, damit der Dienst ordnungsgemäß ausgeführt werden kann. Der Dienst erfordert einen Speicherplatz von 200 MB. Die betroffenen Festplatten sind:

- SATA SSD 16GB (wenn keine NVMe SSD eingebaut ist)
- NVMe SSD

Es wird empfohlen, die Traces vor dem Start des Dienstes zu löschen, wenn Sie Speicherplatz freigeben möchten.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.

3) Klicken Sie auf **Trace-Komponenten > Kernel Crash-Daten**.
4) Klicken Sie auf **Start**.

Der Kernel Crash-Daendienst wird gestartet und ein Neustart des Systems wird automatisch eingeleitet. Der Dienst behält seinen Status nach dem Neustart des Systems bei.

25.8.4.34 Kernel Crash-Datendienst anhalten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Ihr Kommunikationssystem verfügt über ein V3 OCC Mainboard (OCCLA, OCCMA(R), OCCMB(R)).

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie auf **Trace-Komponenten > Kernel Crash-Daten**.
4) Klicken Sie auf **Anhalten**.

Der Kernel Crash-Datendienst wird angehalten und ein Neustart des Systems wird automatisch eingeleitet. Der Dienst behält seinen Status nach dem Neustart des Systems bei.

25.8.4.35 Wie Sie den Medienserver-Trace starten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie auf **Medienserver-Trace**.
4) Wählen Sie eine Option aus der Aufklappliste **Trace-Level** aus, um den Detaillierungsgrad des Trace zu bestimmen.
5) Klicken Sie auf **Start**.

Anmerkung: Aktive Traces erhöhen die allgemeine Systemauslastung und können sich negativ auf die Systemleistung auswirken. Daher sollte der Medienserver-Trace deaktiviert werden, sobald Sie Ihre Diagnoseaktivitäten abgeschlossen haben.

25.8.4.36 Wie Sie den Medienserver-Trace anhalten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Traces**.
3) Klicken Sie auf **Medienserver-Trace**.
4) Klicken Sie auf **Anhalten**.

25.9 TCP-Dump

Ein TCP-Dump dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung.

Tipp: Das Aktivieren eines TCP-Dumps wirkt sich negativ auf die System-Performance aus und darf nur durch erfahrene Administratoren und nur in Absprache mit dem zuständigen Service-Support erfolgen.

TCP-Dump-Dateien werden im Kommunikationssystem gespeichert. Für die Diagnose der Dateien ist eine entsprechende Applikation erforderlich.

TCP-Dumps werden häufig eingesetzt, um

- für einen kurzen Zeitraum (zum Beispiel für ein reproduzierbares Fehlerbild) einen LAN-Trace zu erzeugen.
- Ermöglichen Sie autorisierten Servicetechnikern den Fernzugriff auf einen LAN-Trace.

Vorteile gegenüber RPCAP-Dämon: Fernzugriff möglich, Trace-Dateien müssen nicht per E-Mail verschickt werden

Nachteile gegenüber RPCAP-Dämon: Langzeit-Traces nicht sinnvoll, begrenzter Speicherplatz, keine Capture-Filter einstellbar, aufwendigere Handhabung bei vielen Einzel-Traces

25.9.1 Wie Sie einen TCP-Dump starten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Traces** > **TCP-Dump**.
3) Klicken Sie auf **TCP-Dump starten**.
4) Wählen Sie die gewünschten Einstellungen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.9.2 Wie Sie einen TCP-Dump stoppen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Traces** > **TCP-Dump**.
3) Klicken Sie auf **TCP-Dump beenden**.
4) Klicken Sie auf **OK**.

25.9.3 Wie Sie einen TCP-Dump löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Traces** > **TCP-Dump**.
3) Klicken Sie auf **TCP-Dump aufräumen**.
4) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.10 RPCAP-Dämon

Ein RPCAP (Remote Packet Capture)-Dämon dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung.

Tipp: Das Aktivieren eines RPCAP-Dämons wirkt sich negativ auf die System-Performance aus und darf nur durch erfahrene Administratoren und nur in Absprache mit dem zuständigen Service-Support erfolgen.

Über den RPCAP-Dämon wird ein Fernzugriff externer Applikationen auf die TCP/IP-Pakete der LAN-Schnittstellen des Kommunikationssystems ermöglicht.

Ein RPCAP-Dämon wird häufig für Langzeit-Traces eingesetzt, da die Trace-Dateien auf einem PC und nicht im Kommunikationssystem abgelegt werden.

Vorteile gegenüber TCP-Dump: Schnellere und einfachere Handhabung, Langzeit-Traces möglich, Anzahl und/oder Größe der Trace-Dateien frei wählbar, Trace des internen LAN möglich

Nachteile gegenüber TCP-Dump: Doppelter Datenverkehr im Netz und dadurch höhere Belastung der LAN-Schnittstellen des Kommunikationssystems, spezielle Portfreigabe nötig (Firewall)

25.10.1 Wie Sie den RPCAP-Dämon aktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Der RPCAP-Dämon wurde deaktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Traces** > **RPCAP Dämon**.
3) Wählen Sie die gewünschten Einstellungen.
4) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.10.2 Wie Sie den RPCAP-Dämon deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Der RPCAP-Dämon wurde aktiviert.

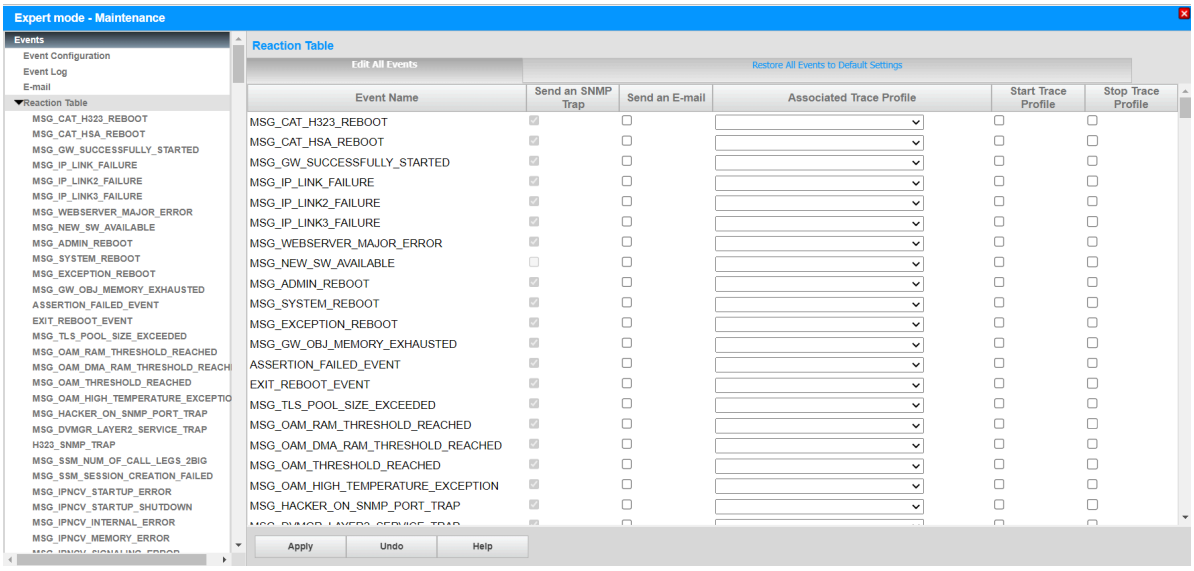
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Traces** > **RPCAP Dämon**.
3) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.11 Ereignisse

Events (Ereignisse) informieren über Mängel des Kommunikationssystems. Alle Events werden in eine Protokolldatei beschränkter Größe geschrieben. Ist die maximale Größe der Datei überschritten, wird eine neue Datei angelegt. Es können bis zu sieben Dateien entstehen.

Abhängig von der Einstellung in der Reaktionstabelle und der Problemklasse können Events einen SNMP-Trap erzeugen, eine E-Mail auslösen und/oder eine Trace-Überwachung starten/stoppen. Die Auswertung, Konfiguration und Speicherung des Event Logs (der Ereignisanzeige) ist über das WBM möglich.



Um die Event-Protokolldatei zu interpretieren, muss die Datei mit dem WBM heruntergeladen und extrahiert werden. Anschließend kann die Datei mit einem beliebigen Texteditor geöffnet und bearbeitet oder ausgedruckt werden. Nachdem die Event-Protokolldatei übertragen wurde, kann die Datei aus dem Speicher des Kommunikationssystems gelöscht werden.

Events, die Aktionen auslösen können, sind durch folgende Eigenschaften definiert:

- Event-Code:

  Kennzeichnet ein Event (Ereignis), wie zum Beispiel `MSG_ADMIN_LOGGED_OUT` = Information über das Logout eines Administrators.
- Event-Typ:

  Es gibt folgende verschiedene Typen:

  – Information: Reine Statusmeldung, keine Fehlermeldung.
  – Warning: Meldung über einen möglicherweise problematischen Vorgang oder Zustand, jedoch keine Fehlermeldung.
  – Minor: Fehlermeldung. Der Fehler hat keine problematischen Auswirkungen.
  – Major: Fehlermeldung. Der Fehler kann problematische Auswirkungen haben.
  – Kritisch: Fehlermeldung Der Fehler hat problematische Auswirkungen.
  – Cleared: Fehlermeldung. Der Fehler wurde vom Kommunikationssystem bereits behoben.
  – Indeterminate: Fehlermeldung. Die Fehlerursache ist nicht genau bestimmbar.

- Event-Text

  Einige Event-Texte enthalten variable Daten. Diese sind folgendermaßen gekennzeichnet:

  – %s: Zeichenkette
  – %u: Positive oder negative Dezimalzahl
  – %f: Fließkommazahl
  – %p: Zeiger (Speicheradresse)
  – %x: Hexadezimalzahl (mit Kleinbuchstaben)
  – %X: Hexadezimalzahl (mit Großbuchstaben)
  – %c: Einzelnes Zeichen
  – %d und %i: Positive Dezimalzahl

Reaktionstabelle

Anhand der Reaktionstabelle kann ein Administrator mit dem Profil **Expert** für jeden möglichen Event getrennt definieren, wie bei dessen Eintreten reagiert werden soll.

Eingestellt werden kann, ob ein SNMP-Trap versendet werden soll, ob das Kommunikationssystem neu gestartet werden soll, ob eine E-Mail versendet werden soll und ob ein Trace-Profil gestartet oder gestoppt werden soll. Ist dem Event ein Trace-Profil zugeordnet, wird dessen Name angezeigt.

E-Mail-Einstellungen

Anhand dieser Einstellungen kann ein Administrator mit dem Profil **Expert** Angaben für den E-Mailversand bei Eintreten eines Events vornehmen.

Diagnose-Protokolle

Das Kommunikationssystem protokolliert bestimmte Aktionen von Prozessen in Diagnose Logs. Diese Protokolldateien können für Diagnosezwecke durch einen Administrator mit dem Profil **Expert** ausgewertet werden.

Alarm-Signalisierung bei Temperaturüberschreitung

Im Kommunikationssystem sind zwei kritische Temperaturwerte gespeichert. Überschreitet die Temperatur des Systems den ersten Wert, erfolgt eine Warnmeldung per SNMP-Trap oder E-Mail, dass die Temperatur des Systems zu hoch ist. Zusätzlich kann diese Meldung auch im Display von bis zu 3 Systemtelefonen (UP0 & HFA) angezeigt werden, siehe Wie Sie die Ziele für die Alarm-Signalisierung festlegen. Wird der zweite Wert überschritten, werden die für die Überhitzung verantwortlichen Baugruppen kontrolliert heruntergefahren (z.B. OpenScape Business Booster Card) oder abgeschaltet (z.B. SLAV/SLAD). Um den Alarm zu löschen und die Baugruppen wieder in Betrieb zu nehmen, muss das System ausgeschaltet und wieder neu eingeschaltet werden.

Es kann eingestellt werden, welche 3 Ziele (Systemtelefone) bei einer Temperaturüberschreitung benachrichtigt werden sollen.

25.11.1 Wie Sie die Event-Protokollierung über LAN ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **Event-Konfiguration**.
4) Wählen Sie die gewünschte Einstellung aus:
   - Wenn die Event-Protokollierung über ein LAN übertragen werden soll, aktivieren Sie das Kontrollkästchen **Event-Protokollierung über LAN aktivieren**.
   - Wenn keine Event-Protokollierung über ein LAN übertragen werden soll, deaktivieren Sie das Kontrollkästchen **Event-Protokollierung über LAN aktivieren**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.11.2 Wie Sie eine Event-Protokolldatei herunterladen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **Event-Protokoll**.
4) Klicken Sie auf die Registerkarte **Laden über HTTP**.
5) Klicken Sie auf **Laden** und auf **OK**. Es erscheint das Dateidownload-Fenster.
6) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.

25.11.3 Wie Sie eine Event-Protokolldatei löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **Event-Protokoll**.
4) Klicken Sie auf die Registerkarte **Event-Viewer-Protokoll löschen**.
5) Klicken Sie auf **Protokoll löschen** und anschließend auf **OK**.

25.11.4 Wie Sie E-Mail-Einstellungen für Events ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Die **E-Mail-Weiterleitung** muss so konfiguriert sein, dass alle Systeme die Option **Empfänger von Notfallbenachrichtigungen** verwenden. Weitere Informationen siehe E-Mail-Versand konfigurieren auf Seite 205

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **E-Mail**.
4) Geben Sie als **Betreff** ein, was in den E-Mails im Feld Betreff angezeigt werden soll.

   Tipp: Der Betreff sollte eindeutig darauf hinweisen, dass es sich um eine E-Mail aufgrund eines Events handelt.

5) Geben Sie die E-Mail-Adressen, an welche die E-Mail gesendet werden soll, in die Felder **Empfänger 1** bis **Empfänger 5** ein.
6) Geben Sie im Feld **Empfänger für Notfälle** die E-Mail-Adresse eines Sicherheitsbeauftragten vor Ort ein, an den eine E-Mail gesendet wird, wenn eine Notrufnummer gewählt wird.

   Der Betreff der E-Mail lautet „Neuer Notruf“. Wenn dies konfiguriert wurde, sind die Rufnummer und der Name des Anrufers, die aus der Datenbank des Systems abgerufen werden, in der E-Mail enthalten.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.11.5 Wie Sie die Event-Reaktionstabelle anzeigen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **Reaktionstabelle**. Es wird Ihnen die Reaktionstabelle mit allen möglichen Events und deren Einstellungen angezeigt.

25.11.6 Wie Sie Reaktionseinstellungen eines Events ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **Reaktionstabelle**. Es wird Ihnen die Reaktionstabelle mit allen möglichen Events und deren Einstellungen

angezeigt. Darüber hinaus werden Ihnen im Menübaum die Namen aller möglichen Events angezeigt.

4) Klicken Sie im Menübaum auf den Namen des gewünschten Events.

5) Klicken Sie auf die Registerkarte **Event bearbeiten**. Es werden Ihnen die Reaktionseinstellungen des gewünschten Events angezeigt.

> **Tipp:** Die Reaktionseinstellungen **Gateway neu starten** und **OpenScape benachrichtigen** können Sie nicht ändern. Eine Änderung der Einstellung **SNMP-Trap senden** ist nicht bei allen Events möglich.

6) Falls möglich, wählen Sie die Einstellung für **SNMP-Trap senden**:

- Wenn bei Eintreten des Events ein SNMP-Trap gesendet werden soll, aktivieren Sie das Kontrollkästchen **SNMP-Trap senden**.
- Wenn bei Eintreten des Events kein SNMP-Trap gesendet werden soll, deaktivieren Sie das Kontrollkästchen **SNMP-Trap senden**.

7) Wählen Sie die Einstellung für **E-Mail versenden**:

- Wenn bei Eintreten des Events eine E-Mail gesendet werden soll, aktivieren Sie das Kontrollkästchen **E-Mail versenden**.
- Wenn bei Eintreten des Events keine E-Mail gesendet werden soll, deaktivieren Sie das Kontrollkästchen **E-Mail versenden**.

8) Wählen Sie in der Aufklappliste **Zugeordnetes Trace-Profil** das gewünschte Trace-Profil aus.

9) Wählen Sie die Einstellung für den Start oder Stopp des Trace-Profils:

- Wenn bei Eintreten des Events das ausgewählte Trace-Profil gestartet werden soll, aktivieren Sie das Kontrollkästchen **Trace-Profil starten**.
- Wenn bei Eintreten des Events das ausgewählte Trace-Profil gestoppt werden soll, aktivieren Sie das Kontrollkästchen **Trace-Profil stoppen**.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.11.7 Wie Sie Reaktionseinstellungen mehrerer Events ändern

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.

3) Klicken Sie im Menübaum auf **Events** > **Reaktionstabelle**. Es wird Ihnen die Reaktionstabelle mit allen möglichen Events und deren Reaktionseinstellungen angezeigt.

> **Tipp:** Die Reaktionseinstellungen **Gateway neu starten** und **OpenScape benachrichtigen** können Sie nicht ändern. Eine Änderung der Einstellung **SNMP-Trap senden** ist nicht bei allen Events möglich.

4) Ändern Sie die Reaktionseinstellungen der gewünschten Events in der Reaktionstabelle:
   - Falls möglich, wählen Sie die Einstellung für **SNMP-Trap senden**:

     Wenn bei Eintreten des Events ein SNMP-Trap gesendet werden soll, aktivieren Sie das Kontrollkästchen **SNMP-Trap senden**.

     Wenn bei Eintreten des Events kein SNMP-Trap gesendet werden soll, deaktivieren Sie das Kontrollkästchen **SNMP-Trap senden**.
   - Wählen Sie die Einstellung für **E-Mail versenden**:

     Wenn bei Eintreten des Events eine E-Mail gesendet werden soll, aktivieren Sie das Kontrollkästchen **E-Mail versenden**.

     Wenn bei Eintreten des Events keine E-Mail gesendet werden soll, deaktivieren Sie das Kontrollkästchen **E-Mail versenden**.
   - Wählen Sie in der Aufklappliste **Zugeordnetes Trace-Profil** das gewünschte Trace-Profil aus.
   - Wählen Sie die Einstellung für den Start oder Stopp des Trace-Profils:

     Wenn bei Eintreten des Events das ausgewählte Trace-Profil gestartet werden soll, aktivieren Sie das Kontrollkästchen **Trace-Profil starten**.

     Wenn bei Eintreten des Events das ausgewählte Trace-Profil gestoppt werden soll, aktivieren Sie das Kontrollkästchen **Trace-Profil stoppen**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.11.8 Wie Sie Diagnose Logs herunterladen oder öffnen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **Diagnose Logs**.
4) Klicken Sie auf die Registerkarte **Diagnose Logs holen**. Es wird Ihnen eine Liste aller verfügbaren Logs mit dem jeweiligen Dateinamen, der Dateigröße in Bytes, dem Zeitpunkt der letzten Änderung und den Dateiattributen angezeigt.
5) Klicken Sie unter **Dateiname** auf den Namen des gewünschten Diagnose Logs. Es erscheint das Dateidownload-Fenster.
6) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.

25.11.9 Wie Sie Diagnose Logs löschen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **Diagnose Logs**. Es wird Ihnen eine Liste aller verfügbaren Logs mit dem jeweiligen Dateinamen, der Dateigröße in Bytes, dem Zeitpunkt der letzten Änderung und den Dateiattributen angezeigt.
4) Klicken Sie auf die Registerkarte **Diagnose Logs löschen**.
5) Klicken Sie auf **Protokoll löschen** und anschließend auf **OK**.

25.11.10 Wie Sie die Ziele für die Alarm-Signalisierung festlegen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Events**.
3) Klicken Sie im Menübaum auf **Events** > **Alarm-Signalisierung**.
4) Wählen Sie in den Aufklapplisten **Teilnehmer 1-3** die drei Ziele (Systemtelefone mit Display, UP0 & HFA) aus, die im Display benachrichtigt werden sollen, wenn die Temperatur des Systems einen fest eingestellten kritischen Wert übersteigt.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

25.12 Konfigurationsdaten für die Diagnose

Für Diagnosezwecke können "kleinere" Backup-Sets erzeugt werden, die Daten für die Fehlersuche durch den Service-Support enthalten. Im Gegensatz zu den normalen Backup-Sets werden wesentlich kleinere Datenmengen erzeugt und damit zum Beispiel ein einfaches Versenden per E-Mail ermöglicht.

Diagnose-Backup-Sets enthalten unter anderem die Konfigurationsdaten des Kommunikationssystems und der UC Applikation (UC Smart oder UC Suite). Sprachnachrichten, Faxnachrichten und Ansagen sind nicht enthalten.

Für die Sicherung von Diagnose-Backup-Sets können folgende Medien verwendet werden:

- **USB-Device**

  Die Daten können zum Beispiel auf eine angeschlossene USB-Festplatte oder einen angeschlossenen USB-Stick gesichert werden.

  Anmerkung: Soll eine USB-Festplatte, die Partition einer USB-Festplatte oder ein USB-Stick für die Sicherung verwendet werden, muss diese(r) mit FAT-32 formatiert sein. Vom einem NTFS formatierten USB-Medium kann nur gelesen werden. Sind mehrere Partitionen vorhanden, ist eine Sicherung nur auf der ersten Partition möglich.

  Wird auf ein bootfähiges USB-Medium gespeichert, ist dieses USB-Medium nach der Sicherung zu entfernen.

- **HTTPS**

  Die Daten können über HTTPS auf der Festplatte des Client-PC gesichert werden.
- **Hard Disk** (nur für OpenScape Business X3/X5/X8 mit UC Booster Card (Application Board OCAB))

  Die Daten können auf der Festplatte des Application Boards OCAB gesichert werden.

Tipp: Eine Sicherung auf der Festplatte des Kommunikationssystems ist nicht möglich.

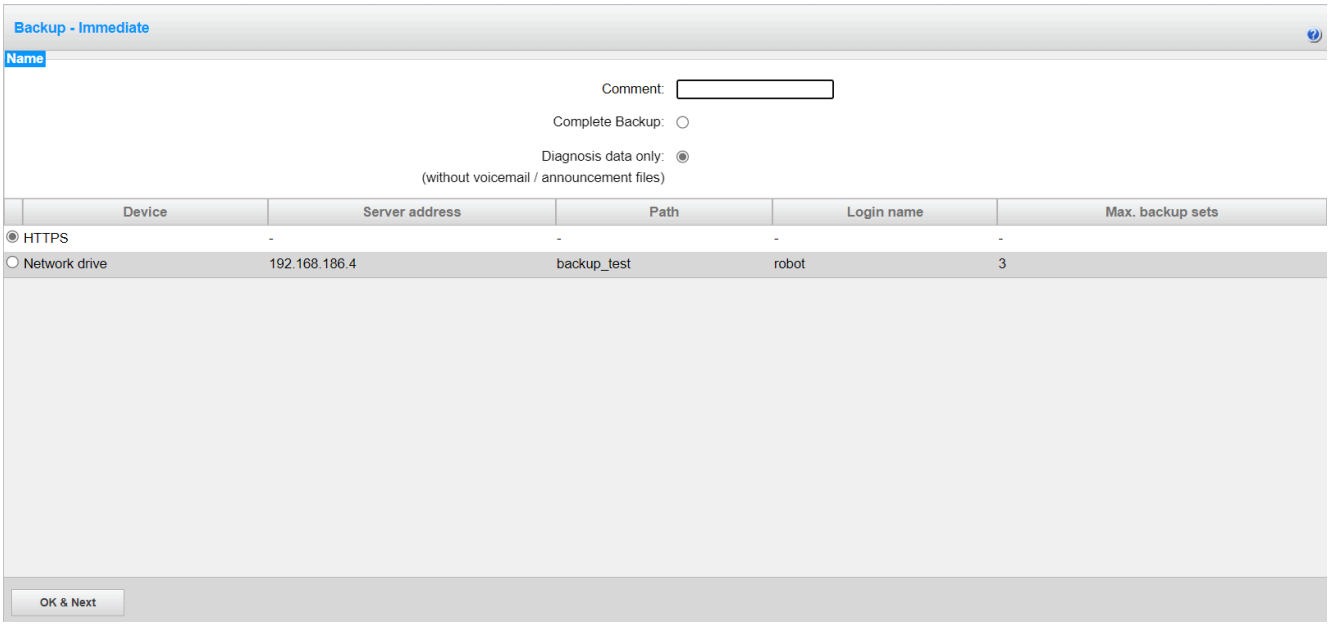
25.12.1 Wie Sie Konfigurationsdaten für die Diagnose erzeugen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Datensicherung** > **Backup - Sofort**.



3) Aktivieren Sie das Kontrollkästchen **Diagnose**.

4) Wählen Sie das Gerät aus, auf dem das Diagnose-Backup-Set gesichert werden soll. Es bestehen folgende Möglichkeiten:
   - Wenn Sie die Daten auf einer angeschlossenen USB-Festplatte oder einem angeschlossenen USB-Stick sichern möchten, aktivieren Sie das Optionsfeld **USB-Device**.
   - Wenn Sie die Daten über HTTPS auf der Festplatte des Client-PC sichern möchten, aktivieren Sie das Optionsfeld **HTTPS**.
   - Nur für OpenScape Business X3/X5/X8 mit UC Booster Card (Application Board OCAB): Wenn Sie die Daten auf der Festplatte des Application Board OCAB speichern möchten, wählen Sie das Optionsfeld **Festplatte**.
5) Geben Sie bei Bedarf im Feld **Kommentar** einen Kommentar zu Ihrem Diagnose-Backup-Set ein. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.
6) Klicken Sie auf **OK & Weiter**. Der Fortschritt des Backup-Vorgangs wird in einem separaten Fenster angezeigt.
7) Die Sicherung war erfolgreich, wenn die Meldung `Sicherung erfolgreich ausgeführt!` erscheint.
8) Wenn Sie als Backup-Medium **HTTPS** ausgewählt haben, müssen Sie das Diagnose-Backup-Set und die dazugehörige Text-Datei an einem Speicherort Ihrer Wahl sichern. Bei den anderen Backup-Medien geschieht dies automatisch. Das Browser-Fenster muss solange geöffnet bleiben, bis der Speichervorgang für Diagnose-Backup-Set und Text-Datei abgeschlossen ist.

   Anmerkung: Wenn Sie als Backup-Medium **USB-Device** ausgewählt haben, warten Sie ab, bis die LED des USB-Mediums aufhört zu blinken. Erst dann ist das Diagnose-Backup-Set vollständig auf dem USB-Medium gespeichert. Entfernen Sie anschließend das USB-Medium.
9) Klicken Sie auf **Beenden**.

Nächste Schritte

Das Diagnose-Backup-Set kann jetzt beispielsweise für die Fehlersuche an den zuständigen Service-Support per E-Mail verschickt werden.

25.13 Card Manager

OpenScape Business wird mit bootfähigen Medien geliefert, die die Systemsoftware enthalten. Card Manager ist ein Tool für den Service-Support, um neue System-Software auf einer leeren SDHC-Karte, M.2 SATA SSD und UC Booster Card-Festplatte (HDD) zu erstellen. Dazu wird die Software des Kommunikationssystems als kompatible Image-Datei benötigt.

Die Software auf der SDHC-Karte, M.2 SATA SSD oder Festplatte ist eine Standard-System-Software ohne Kundendaten. Software-Updates oder das Sichern von Kundendaten sind damit nicht möglich. Es ist nur im Fall der SDHC-Karte möglich, eine Backup-Datei bei der Erstellung einzuschließen.

Card Manager kann als ISO-Image auf einer Linux-Boot-DVD und einem bootfähigen Linux-USB-Stick oder in einer virtuellen Umgebung gestartet werden.

Die Card Manager-Software ist über das Partner-Portal verfügbar.

Anwendungsfälle

- Vor Auslieferung des Systems soll die Software durch die aktuelle Software getauscht werden.
- Die Speichervorrichtung ist defekt und muss durch eine neue ersetzt werden, auf der noch keine Software gespeichert ist.
- Die genutzte Software ist defekt und muss neu aufgespielt werden. Dabei werden alle Kundendaten gelöscht.

  Ist zur Wiederherstellung der Kundendaten ein Backup-Set vorhanden, sollte die neu installierte Software mit der Software-Version übereinstimmen, mit der das Backup-Set erzeugt wurde, damit die im Backup-Set enthaltenen Einstellungen auch von der installierten Software unterstützt und verarbeitet werden können.

25.13.1 Wie Sie mit dem Card Manager die Kommunikationssoftware auf die M.2 SATA SSD schreiben

Sie können den Card Manager verwenden, um die Kommunikationssoftware von OpenScape Business V3 auf die M.2 SATA SSD zu schreiben.

Voraussetzungen

Der Arbeitsspeicher des PC sollte über mindestens 3 GB verfügen.

PC mit Betriebssystem Windows 10, DVD-Laufwerk und mindestens 2 Schnittstellen mit USB 2.0 oder höher ist verfügbar.

Card Manager Tool V3 oder höher ist auf einem PC voll funktionsfähig.

USB-SATA-SSD-Adapter ist verfügbar. Der Adapter muss Key M und Key unterstützen.

Eine qualifizierte M.2 SATA SSD ist verfügbar.

Ein System-SW-Image in der richtigen Version ist als TAR-Datei verfügbar. Die SW-Version muss der Version des Zielsystems entsprechen. Es muss genau die gleiche Version sein, die im aktuellen Speichergerät des Systems verwendet wird.

Card Manager-Anwendung als DVD-ISO-Datei.

Die ISO-Datei von Card Manager muss auf eine DVD gebrannt sein.

Schritt für Schritt

1) Speichern Sie die aktuelle Image-TAR-Datei auf einem USB-Stick und booten Sie die Card Manager-Anwendung von der DVD-ISO-Datei.

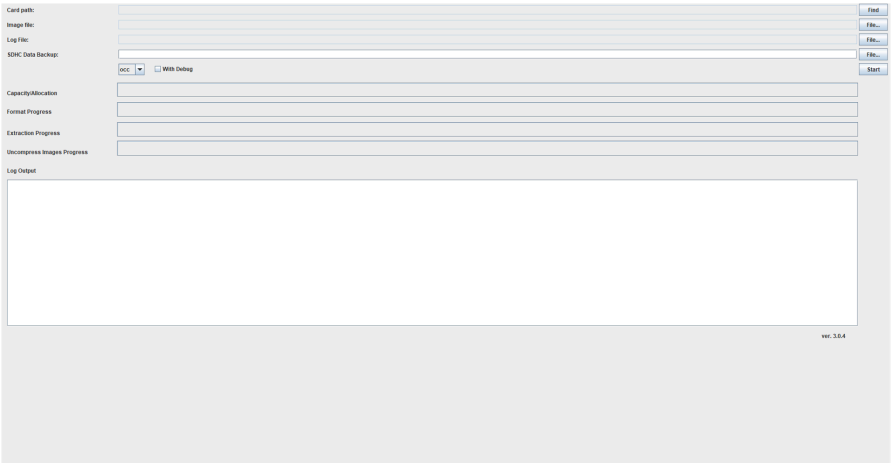
2) Schließen Sie den USB-SATA-SSD-Adapter an einen USB-Port am PC an.

3) Stecken Sie die M.2 SATA SSD in den Adapter ein und bestätigen Sie die Auswahl im Popup mit **OK**.

Alle Daten auf der eingesteckten SSD werden vom Card Manager gelöscht.

Stecken Sie keine weiteren USB-Geräte am PC ein, weil sie als OpenScape Business Speichermedien erkannt und alle Daten gelöscht werden.

4) Klicken Sie auf der Card Manager-Anwendung auf **Suchen** neben **Pfad der Karte**.



5) Stecken Sie den USB-Stick mit der Image-Datei ein und klicken Sie auf **Datei...** neben **Image-Datei** und wählen Sie die auf dem USB-Stick gespeicherte Image-TAR-Datei aus.

6) Wählen Sie **OCCe** aus dem Dropdownmenü, um die M.2 SATA SSD zu erstellen.

7) Optional können Sie auch eine Protokolldatei erstellen lassen, in der eventuell aufgetretene Programmfehler aufgezeichnet werden. Klicken Sie dazu auf **Datei...** neben **Protokolldatei** und navigieren Sie zum Ablageort der Protokolldatei. Geben Sie einen Namen für die Protokolldatei ein und klicken Sie auf **Speichern**.

8) Klicken Sie auf **Start**.

   Der Schreibvorgang wird gestartet und der Fortschritt jedes Schritts wird über eine Fortschrittsleiste angezeigt.

9) Klicken Sie nach Abschluss der Installation auf **OK** und entfernen Sie die M.2 SATA SSD aus dem Adapter.

10) Ziehen Sie den Adapter aus dem USB-Port.

11) Schalten Sie das Kommunikationssystem aus.

12) Stecken Sie die neue M.2 SATA SSD in das ausgeschaltete Kommunikationssystem.

13) Schalten Sie das Kommunikationssystem ein. Das System wird mit der neuen M.2 SATA SSD sowie mit derselben Softwareversion und Konfiguration gestartet und ist wieder betriebsbereit, wenn die grüne LED im 1-Hz-Takt blinkt (0,5 s ein, 0,5 s aus).

Anmerkung: Wenn die M.2 SATA SSD in ein OpenScape Business Kommunikationssystem eingesteckt wird, wird das System im Standardwerkszustand gestartet, darunter unter anderem mit der Standard-IP-Adresse `192.168.1.2`.

Stellen Sie eine Sicherung des Systems wieder her. Die Sicherung sollte die gleiche Nebenversion wie das installierte System haben.

25.13.2 Kommunikationssoftware mit dem Card Manager auf die SDHC-Karte schreiben

Sie können den Card Manager verwenden, um die Kommunikationssoftware von OpenScape Business V3 auf die SDHC-Karte zu schreiben.

Voraussetzungen

PC mit Betriebssystem Windows 10, DVD-Laufwerk und mindestens 2 USB-Schnittstellen 2.0 oder höher ist verfügbar.

Card Manager Tool V3 oder höher ist auf einem PC voll funktionsfähig.

USB SDHC Card Reader ist verfügbar.

Eine qualifizierte SDHC-Karte ist verfügbar.

Optional ist eine auf einem USB-Stick zusammen mit dem Image-System gespeicherte Datei für SDHC-Datensicherung (TAR-Datei) verfügbar.

Der Schreibschutz der SDHC-Karte ist deaktiviert.

Ein System-SW-Image in der richtigen Version ist als TAR-Datei verfügbar. Dies kann entweder die kleine (OCC) oder die große (OCAB) Image-Datei sein. Die SW-Version muss der Version des Zielsystems entsprechen. Es muss genau die gleiche Version sein, die in der aktuellen SDHC-Karte des Systems verwendet wird.

Card Manager-Anwendung als DVD-ISO-Datei.

Die ISO-Datei von Card Manager muss auf eine DVD gebrannt sein.

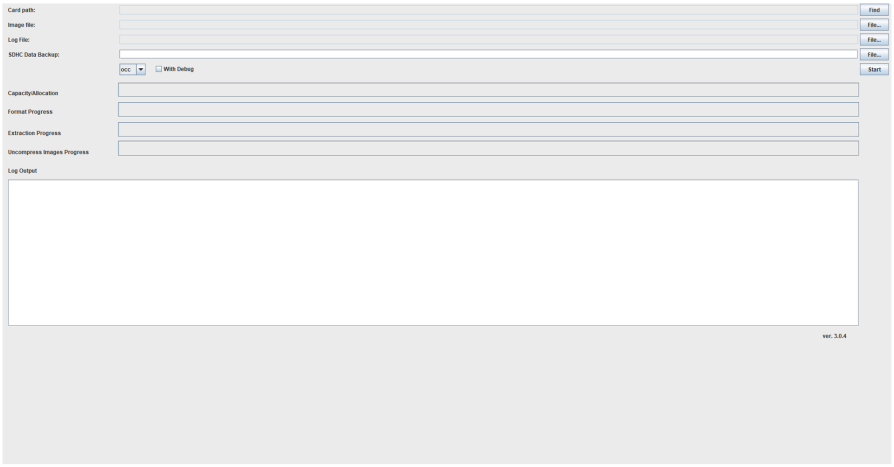
Schritt für Schritt

1) Speichern Sie die aktuelle Image-TAR-Datei auf einem USB-Stick und booten Sie die Card Manager-Anwendung von der DVD-ISO-Datei.
2) Schließen Sie den USB-SDHC-Kartenleser an einen USB-Port am PC an.
3) Ziehen Sie den Kartenleser ab, legen Sie die SDHC-Karte ein, stecken Sie den Kartenleser wieder ein und klicken Sie im Popupfenster zur Bestätigung auf **OK**. Unter **Pfad der Karte** wird der Pfad zur SDHC-Karte angezeigt.

   Alle Daten auf der eingesteckten SSD werden vom Card Manager gelöscht.

   Stecken Sie keine weiteren USB-Geräte am PC ein, weil sie als OpenScape Business Speichermedien erkannt und alle Daten gelöscht werden.

4) Klicken Sie auf der Card Manager-Anwendung auf **Suchen** neben **Pfad der Karte**.



5) Stecken Sie den USB-Stick mit der Image-Datei ein und klicken Sie auf **Datei...** neben **Image-Datei** und wählen Sie die auf dem USB-Stick gespeicherte Image-TAR-Datei aus.

6) Wählen Sie aus dem Dropdownmenü **OCC** aus, um die SDHC-Karte zu erstellen.

7) Optional können Sie auch eine Protokolldatei erstellen lassen, in der eventuell aufgetretene Programmfehler aufgezeichnet werden. Klicken Sie dazu unter **Protokolldatei** auf **Datei...** und navigieren Sie zum Ablageort der Protokolldatei. Vergeben Sie einen Namen für die Protokolldatei und bestätigen Sie mit **Speichern**.

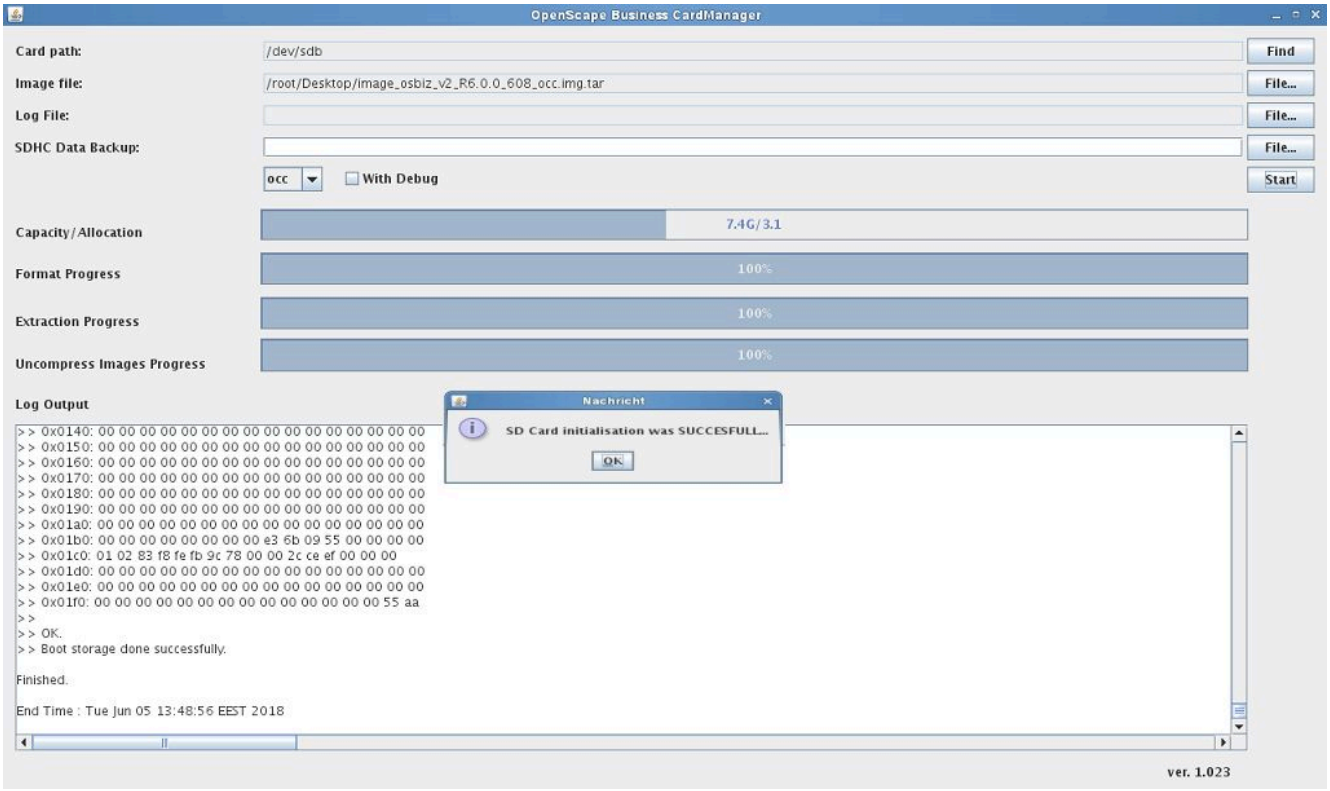
8) Klicken Sie optional unter **SDHC-Datensicherung** auf **Datei...** und wählen Sie die TAR-Datei aus, die eine kundenspezifische Backup-Datei für SDHC-Kartendaten enthält. Der Pfad zu der TAR-Datei wird unter **SDHC-Datensicherung** angezeigt.

9) Klicken Sie auf **Start**.

   Der Schreibvorgang wird gestartet und der Fortschritt jedes Schritts wird über eine Fortschrittsleiste angezeigt.

Anmerkung: Wenn das Textfeld (**SDHC-Datensicherung**) ausgefüllt ist, vergleicht Card Manager zunächst die Version der Backup-Datei mit den SDHC-Kartendaten mit der Version der System-SW-Image-Datei. Falls diese nicht übereinstimmen, wird eine Fehlermeldung angezeigt und der Vorgang abgebrochen. Im Falle einer Übereinstimmung schreibt der Card Manager das ausgewählte Image und extrahiert dann die angegebene TAR-Datei in die SDHC.

Wenn keine SDHC-Datensicherung verfügbar ist, lassen Sie das Textfeld leer.



10) Klicken Sie nach Abschluss der Installation auf **OK** und entfernen Sie die SDHC-Karte aus dem Kartenleser.
11) Ziehen Sie den Card Reader aus der USB-Schnittstelle.
12) Schalten Sie das Kommunikationssystem aus.
13) Stecken Sie die SDHC-Karte in den SD-Slot des ausgeschalteten Kommunikationssystems.
14) Schalten Sie das Kommunikationssystem ein. Das System wird mit der neuen SDHC-Karte sowie mit derselben Softwareversion und Konfiguration gestartet und ist wieder betriebsbereit, wenn die grüne LED im 1-Hz-Takt blinkt (0,5 s ein, 0,5 s aus).

Anmerkung: Wenn die SDHC-Karte in ein OpenScape Business Kommunikationssystem eingesteckt wird, wird das System im Standardwerkszustand gestartet, darunter unter anderem mit der Standard-IP-Adresse `192.168.1.2`.

25.13.3 Wie Sie mit dem Card Manager die Kommunikationssoftware auf die OCAB-Festplatte schreiben

Sie können den Card Manager verwenden, um die Kommunikationssoftware von OpenScape Business V3 mit OCAB auf die OCAB-Festplatte zu schreiben.

Voraussetzungen

PC mit Betriebssystem Windows 10, DVD-Laufwerk und mindestens 2 Schnittstellen mit USB 2.0 oder höher ist verfügbar.

Card Manager Tool V3 oder höher ist auf einem PC voll funktionsfähig.

Ein Adapter für die OCAB-Festplatte ist verfügbar. Der Adapter muss Key M und Key unterstützen.

Eine qualifizierte OCAB-Festplatte ist verfügbar.

Ein System-SW-Image (OCAB) in der richtigen Version ist als TAR-Datei verfügbar. Die SW-Version muss der Version des Zielsystems entsprechen. Es muss genau die gleiche Version sein, die im aktuellen Speichergerät des Systems verwendet wird.

Card Manager-Anwendung als ISO-Datei.

Die ISO-Datei von Card Manager muss auf eine DVD gebrannt sein.

Schritt für Schritt

1) Speichern Sie die aktuelle Image-TAR-Datei auf einem USB-Stick und booten Sie die Card Manager-Anwendung von der DVD-ISO-Datei.

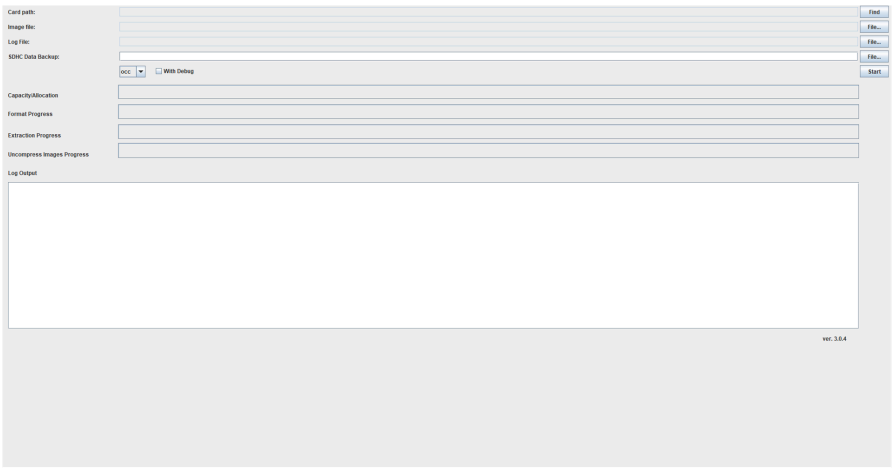
2) Schließen Sie den Adapter an einen USB-Port am PC an.

3) Stecken Sie die OCAB-Festplatte in den Adapter ein und bestätigen Sie die Auswahl im Popup mit **OK**.

Alle Daten auf der eingesteckten Festplatte werden vom Card Manager gelöscht.

Stecken Sie keine weiteren USB-Geräte am PC ein, weil sie als OpenScape Business Speichermedien erkannt und alle Daten gelöscht werden.

4) Klicken Sie auf der Card Manager-Anwendung auf **Suchen** neben **Pfad der Karte**.



5) Stecken Sie den USB-Stick mit der Image-Datei ein und klicken Sie auf **Datei...** neben **Image-Datei** und wählen Sie die auf dem USB-Stick gespeicherte Image-TAR-Datei aus.

6) Wählen Sie aus dem Dropdownmenü **OCAB** aus, um die OCAB- Festplatte zu erstellen.

7) Optional können Sie auch eine Protokolldatei erstellen lassen, in der eventuell aufgetretene Programmfehler aufgezeichnet werden. Klicken Sie

dazu auf **Datei...** neben **Protokolldatei** und navigieren Sie zum Ablageort der Protokolldatei. Geben Sie einen Namen für die Protokolldatei ein und klicken Sie auf **Speichern**.

8) Klicken Sie auf **Start**.

   Der Schreibvorgang wird gestartet und der Fortschritt jedes Schritts wird über eine Fortschrittsleiste angezeigt.

9) Klicken Sie nach Abschluss der Installation auf **OK** und entfernen Sie die OCAB-Festplatte aus dem Adapter.

10) Ziehen Sie den Adapter aus dem USB-Port.

11) Schalten Sie das Kommunikationssystem aus.

12) Legen Sie die neue OCAB-Festplatte in die UC Booster Card und dann in das ausgeschaltete Kommunikationssystem ein.

13) Schalten Sie das Kommunikationssystem ein. Das System wird mit der neuen OCAB-Festplatte sowie mit derselben Softwareversion und Konfiguration gestartet und ist wieder betriebsbereit, wenn die grüne LED im 1-Hz-Takt blinkt (0,5 s ein, 0,5 s aus).

Anmerkung:

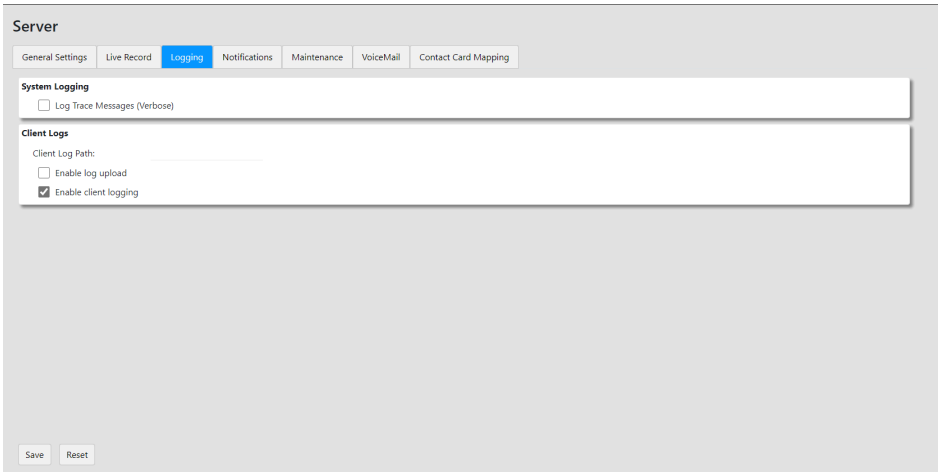
Alle Kundenmediendaten gehen verloren. Sie können eine Systemsicherung wiederherstellen, um diese Daten wiederherzustellen.

25.14 Überwachung und Wartung der UC Suite

Das WBM bietet einem Administrator mit dem Profil **Expert** verschiedene Funktionen zur Überwachung und Wartung der UC Suite.

25.14.1 Protokollierung

Der Programmablauf der UC Suite wird systemintern überwacht. Anhand der **Systemprotokolle** kann eingestellt werden, ob eine Aufzeichnung erfolgen soll. Darüber hinaus erfolgt eine Protokollierung der Aktivitäten der UC Suite (zum Beispiel der Start eines UC Suite Clients) in **Client Logs**.



Systemprotokolle

Folgendes Systemprotokoll kann aktiviert oder deaktiviert werden:

Systemprotokoll	Standardeinstellung
Trace-Meldungen protokollieren (ausführlich)	Nicht aktiviert

Die Ergebnisse des aktivierten Systemprotokolls werden täglich in eine Protokolldatei mit der Bezeichnung `vs-jjjj-mm-tt.log` (zum Beispiel `vs-2013-01-222.log`) eingetragen und im Kommunikationssystem unter `/var/system/trace_log/vsl/log` abgelegt.

Tipp: Die Auswertung der Protokolldateien ist ausschließlich durch die Entwicklung möglich.

Client-Logs:

Client-Logs sind die Protokolldateien der UC Suite. Für jeden UC Suite Client (myPortal for Desktop, myAttendant usw.) und jeden Teilnehmer (Anwender) wird ein eigenes Verzeichnis angelegt in das die jeweiligen Protokolldateien abgelegt werden. Protokolliert werden darin die Aktivitäten eines Teilnehmers, wie beispielsweise der Start des Clients, gehende und kommende Anrufe.

Tipp: Das Ablegen von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

Definiert werden kann der Pfad, in dem das Verzeichnis `CC-Logs` mit den Unterverzeichnissen der einzelnen UC Suite Clients abgelegt werden soll. Dabei kann gewählt werden, ob das Verzeichnis auf jedem Client-PC oder auf einem zentralen, im Netz befindlichen PC oder Server abgelegt werden soll.

Standardmäßig wird das Verzeichnis `CC-Logs` unter folgendem Pfad gespeichert: `<Drive>:\Documents and Settings/<PC User Name>/CC-Logs`

Die Aufbewahrungszeit für **Client-Logs** beträgt 5 Tage. Eine Änderung ist nicht möglich.

Standardmäßig ist die Protokollierung der UC Suite-Aktivitäten in **Client-Logs** aktiviert. Administratoren mit dem Profil **Advanced** können über den Wizard **Benutzerverzeichnis** die Protokollierung teilnehmerindividuell deaktivieren. Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** die Protokollierung systemweit deaktivieren.

In Abhängigkeit vom Szenario werden die Client-Logs standardmäßig auch auf der Festplatte der UC Booster Card (OCAB), des UC Booster Servers oder des Kommunikationssystems OpenScape Business S abgelegt. Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** das Speichern der Client-Logs auf der Festplatte deaktivieren.

Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Trace** die Client-Logs (Protokolldateien) der durch interne Teilnehmer genutzten UC Suite Clients (myPortal for Desktop, myAttendant usw.) herunterladen.

Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** die Client-Logs (Protokolldateien) der durch interne Teilnehmer genutzten UC Suite Clients (myPortal for Desktop, myAttendant usw.) herunterladen.

25.14.1.1 Aufzeichnung der Systemprotokolle aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Protokolle**.
4) Wählen Sie im Bereich **Systemprotokolle** eine der folgenden Möglichkeiten:
   - Wenn Trace-Meldungen täglich in einer Protokolldatei aufgezeichnet werden sollen, aktivieren Sie das Kontrollkästchen **Trace-Meldungen protokollieren (ausführlich)**.
   - Wenn Trace-Meldungen nicht in einer Protokolldatei aufgezeichnet werden sollen, deaktivieren Sie das Kontrollkästchen **Trace-Meldungen protokollieren (ausführlich)**.
5) Klicken Sie auf **Speichern**.

25.14.1.2 Aufzeichnung der Client-Logs systemweit aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Protokolle**.
4) Wählen Sie im Bereich **Systemprotokolle** eine der folgenden Möglichkeiten:
   - Wenn Client-Logs aufgezeichnet werden sollen, aktivieren Sie das Kontrollkästchen **Client-Protokollierung aktivieren**.
   - Wenn Client-Logs nicht aufgezeichnet werden sollen, deaktivieren Sie das Kontrollkästchen **Client-Protokollierung aktivieren**.

   Tipp: Die Aufzeichnung von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.
5) Klicken Sie auf **Speichern**.

25.14.1.3 Wie Sie die Aufzeichnung der Client-Logs teilnehmerindividuell aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards** > **UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten.
4) Markieren Sie den gewünschten Teilnehmer im Benutzerverzeichnis und klicken Sie auf **Bearbeiten**.
5) Klicken Sie im Menübaum auf **Meine Einstellungen** > **Verschiedenes**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Client-Logs für den gewünschten Teilnehmer aufgezeichnet werden sollen, aktivieren Sie das Kontrollkästchen **Debug-Meldungen protokollieren (ausführlich)**.
   - Wenn Client-Logs für den gewünschten Teilnehmer nicht aufgezeichnet werden sollen, deaktivieren Sie das Kontrollkästchen **Debug-Meldungen protokollieren (ausführlich)**.

   Tipp: Die Aufzeichnung von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.
7) Klicken Sie auf **Speichern**.
8) Wenn Sie für einen weiteren Teilnehmer die Aufzeichnung der Client-Logs aktivieren oder deaktivieren möchten, wiederholen Sie die Schritte 4 bis 7.

25.14.1.4 Ablagepfad für Client-Log-Dateien konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Protokolle**.
4) Geben Sie im Feld **Client-Log-Pfad:** im Bereich **Client-Logs** den Ablagepfad ein, in dem das Verzeichnis `CC-Logs` mit den Unterverzeichnissen der einzelnen UC Suite Clients und deren Client-Log-Dateien abgelegt werden soll. Wählen Sie eine der folgenden Optionen:
   - Wenn das Verzeichnis `CC-Logs` auf jedem Client-PC abgelegt werden soll, geben Sie Folgendes ein, beispielsweise: `<Drive>:\<Path>`.

- Wenn das Verzeichnis `CC-Logs` auf einem zentralen, im Netz befindlichen PC oder Server abgelegt werden soll, geben Sie Folgendes ein, beispielsweise: `\\<IP address>\<Drive>\<Path>`.

  Tipp: Das Ablegen von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

5) Klicken Sie auf **Speichern**.

25.14.1.5 Zentrales Speichern der Client-Logs auf der Festplatte aktivieren oder deaktivieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Protokolle**.
4) Wählen Sie im Bereich **Client-Logs** eine der folgenden Möglichkeiten:
   - Wenn Client-Logs auf der Festplatte der UC Booster Card (OCAB), des UC Booster Servers oder des Kommunikationssystems OpenScape Business S abgelegt werden sollen, aktivieren Sie das Kontrollkästchen **Protokoll-Upload aktivieren**.
   - Wenn Client-Logs nicht auf der Festplatte der UC Booster Card (OCAB), des UC Booster Servers oder des Kommunikationssystems OpenScape Business S abgelegt werden sollen, deaktivieren Sie das Kontrollkästchen **Protokoll-Upload aktivieren**.

     Tipp: Die Aufzeichnung von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

5) Klicken Sie auf **Speichern**.

25.14.1.6 Wie Sie Client Logs aller internen Teilnehmer herunterladen

Mit dem Wizard **Trace** können Sie Client Logs (Protokolldateien) der durch interne Teilnehmer genutzten UC Suite Clients (myPortal for Desktop, myAttendant usw.) herunterladen. Client Logs werden ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

Voraussetzungen

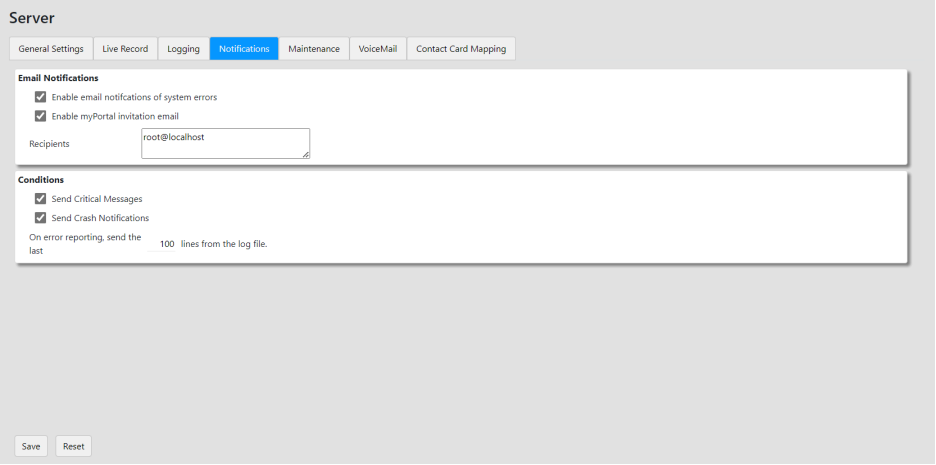
Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose** > **Trace**.
3) Klicken Sie auf **Diagnosedaten**.
4) Klicken Sie auf **Kein Protokoll**, um die Kontrollkästchen aller Protokolle zu deaktivieren.
5) Aktivieren Sie das Kontrollkästchen **Applikationsprotokolle**.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie das gesamte vorhandene Protokoll herunterladen möchten, wählen Sie in der Aufklappliste **Gesamtes Protokoll** aus.
   - Wenn Sie das Protokoll des heutigen Tages herunterladen möchten, wählen Sie in der Aufklappliste **Protokoll von heute** aus.
   - Wenn Sie das Protokoll eines bestimmten Zeitraums herunterladen möchten, wählen Sie in der Aufklappliste **Eigene Auswahl** aus. Wählen Sie in der Aufklappliste **Von:** den Anfang und in der Aufklappliste **Bis:** das Ende des gewünschten Zeitraums aus.
7) Klicken Sie auf **Laden** und auf **OK**. Es erscheint das Dateidownload-Fenster.
8) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.
9) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

25.14.2 Benachrichtigung

Durch die **E-Mail-Benachrichtigung** können E-Mails verschickt werden, um den oder die eingetragenen **Empfänger** zum Beispiel vor einem kritischem Füllstand der Festplatte zu warnen oder über Fehler zu informieren.



Das Verschicken von E-Mails kann an folgende **Bedingungen** geknüpft werden:

Bedingungen	Standardeinstellung
Wichtige Benachrichtigungen senden	Aktiviert
Benachrichtigungen über Systemabsturz senden	Aktiviert

Wichtige Benachrichtigungen und Benachrichtigungen über Systemabstürze sollten aktiviert und damit versendet werden. Diese warnen den oder die eingetragenen Empfänger über ein mögliches Problem, das an den zuständigen Service-Support gemeldet werden muss.

Zusätzlich kann definiert werden, wieviele der letzten Zeilen einer Protokolldatei mit der E-Mail verschickt werden sollen. Gemeldet werden können folgende Systemfehler (ausschließlich Englisch):

Systemfehler
NULL monitor
Could not notify CallHandler
Terminate call failed
Unable to load VM Structure from file
Alsa stuck
Alsa cancel failed
MEN CallID 0
NULL alsa handle
Database connection failed
Rules engine logic failure
Config schema format failure
90% Disk usage mark
Main: Could not connect to the database!
Main: Could not load the configuration from the database!
Main: Could not open configuration file!
Main: Could not read the settings from the configuration file!
A segmentation fault was detected.
Database logic error
Database schema error
ConnectionServer failed to start
MultisiteSync failed to start
Multisite failed to start
TransferManager failed to start
IPC failed to start
ConferenceManager failed to start
CallManager failed to start
MediaProcessing failed to start
Queues failed to start
Import failed to start
DataClient failed to start

Systemfehler
DirectoryClient failed to start
DirectoryServer failed to start
FV failed to start
IM failed to start
Switch failed to start
No Switches
Exchange Integration failed to start
Outbound Fax failed to start
SQL connection pool failed to start
Task scheduler failed to start
Trunks failed to start
Unknown switch type
Users failed to start
MEB has been disconnected
MEB ACK timeout
Switch Hearbeat timeout

25.14.2.1 So konfigurieren Sie E-Mail-Benachrichtigungen über Systemfehler

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Anwendungen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** gefolgt von **Benachrichtigungen**.
4) Wählen Sie im Bereich **E-Mail-Benachrichtigungen** die gewünschte Einstellung für die E-Mail-Benachrichtigung aus:
   - Wenn Sie E-Mail-Benachrichtigungen wünschen, aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen über Systemfehler aktivieren**.
   - Wenn Sie keine E-Mail-Benachrichtigungen wünschen, deaktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen über Systemfehler aktivieren**.
5) Geben Sie im Feld **Empfänger** die E-Mail-Adressen der Personen, an die E-Mail-Benachrichtigungen gesendet werden sollen, ein. Unterschiedliche E-Mail-Adressen müssen durch ein Komma "," gefolgt von Leerzeichen " "getrennt werden.

6) Wählen Sie die gewünschte Einstellung für kritische Nachrichten aus
   - Wenn Sie E-Mail-Benachrichtigungen für kritische Nachrichten erhalten möchten, aktivieren Sie das Kontrollkästchen **Kritische Nachrichten senden**.
   - Wenn Sie keine E-Mail-Benachrichtigungen für kritische Nachrichten erhalten möchten, deaktivieren Sie das Kontrollkästchen **Kritische Nachrichten senden**.
7) Wählen Sie die gewünschte Einstellung für Absturzbenachrichtigungen aus
   - Wenn Sie E-Mail-Benachrichtigungen für Systemabstürze erhalten möchten, aktivieren Sie das Kontrollkästchen **Absturzbenachrichtigungen senden**.
   - Wenn Sie keine E-Mail-Benachrichtigungen für Systemabstürze erhalten möchten, deaktivieren Sie das Kontrollkästchen **Absturzbenachrichtigungen senden**.
8) Geben Sie im Feld **Zeilen der Protokolldatei senden** die Anzahl der Protokolldatei-Zeilen, die mit einer E-Mail versendet werden sollen, ein.
9) Klicken Sie auf **Speichern**.

25.14.3 Wartung

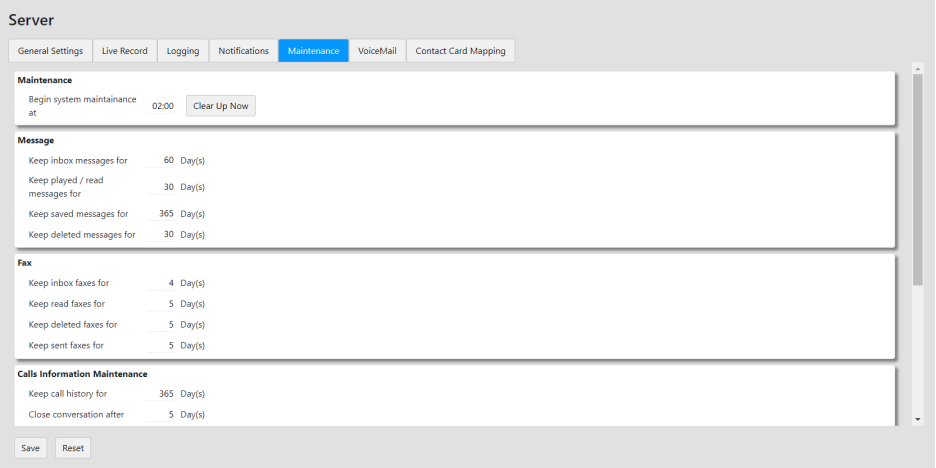
Über die Wartung können Aufbewahrungszeiten für Nachrichten, für Anrufinformationen im Anrufjournal, für die mit myAgent aufgezeichneten Anrufe, für die empfangenen und gesendeten Faxe und E-Mails für das Contact Center und für Protokolldateien definiert werden.

Ebenfalls kann eingestellt werden, zu welcher täglichen Uhrzeit das Löschen folgender Daten erfolgt, die die jeweils eingestellten Aufbewahrungszeiten überschritten haben:

- Meldungen
- Anrufinformationen im Anrufjournal (Anrufhistorie)
- Mit myAgent aufgezeichnete Anrufe (Contact Center)
- Empfangene und gesendete Faxe und E-Mails für das Contact Center
- Log-Dateien

Die Standardeinstellung ist 2:00 Uhr.

Darüber hinaus besteht die Möglichkeit, die Systemwartung sofort zu starten und damit das sofortige Löschen der genannten Daten zu veranlassen, die die jeweils eingestellten Aufbewahrungszeiten überschritten haben. Dies kann beispielsweise notwendig sein, wenn die Festplatte des Kommunikationssystems einen kritischem Füllstand erreicht hat.



Für weitere Informationen zur **Wartung der Nachrichten** siehe Sprachbox.

Für weitere Informationen zur **Wartung der Faxnachrichten** siehe Faxbox.

Für weitere Informationen zur **Wartung der Anrufinformationen**: Anrufhistorie, siehe Journal.

Bei der **Wartung der Anrufinformationen**: **Contact Center** werden die mit myAgent aufgezeichnete Anrufe und die empfangenen und gesendeten Faxe und E-Mails für das Contact Center gelöscht, die die eingestellte Aufbewahrungszeit überschritten haben. Die Standardeinstellung für die Aufbewahrungszeit der Contact-Center-Daten ist 60 Tage.

Tipp: Die Aufbewahrungszeiten für die Wartung der Anrufinformationen sind unabhängig voneinander.

Contact-Center-Berichte basieren auf der Anrufhistorie. Wurde für die Anrufhistorie eine kürzere Aufbewahrungszeit als für die Contact-Center-Daten eingestellt, stehen einige Berichte eventuell nicht mehr zur Verfügung.

Bei der **Wartung der Protokolldateien** werden die Protokolldateien gelöscht, die die eingestellte Aufbewahrungszeit überschritten haben. Die Standardeinstellung für die Aufbewahrungszeit der Protokolldateien ist 10 Tage.

25.14.3.1 Tageszeit für die Wartung konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Wartung**.
4) Geben Sie im Feld **Systemwartung beginnen um** im Bereich **Wartung** die Uhrzeit ein, zu der die tägliche Wartung durchgeführt werden soll. Zu der hier eingestellten Uhrzeit beginnt das Löschen der Nachrichten,

Anrufinformationen im Anrufjournal und Protokolldateien, die die jeweils eingestellten Aufbewahrungszeiten überschritten haben.

5) Klicken Sie auf **Speichern**.

25.14.3.2 Aufbewahrungszeit für Protokolldateien konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Wartung**.
4) Geben Sie im Feld **Protokollinformationen aufbewahren für** im Bereich **Wartung der Protokolldateien** die Aufbewahrungszeit in Tagen ein. Protokolldateien werden gelöscht, wenn diese die hier eingestellte Aufbewahrungszeit überschritten haben.
5) Klicken Sie auf **Speichern**.

25.14.3.3 Sofortige Systemwartung durchführen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Wartung**.
4) Klicken Sie unter dem Bereich **Wartung** auf **Jetzt leeren**.

Tipp: Gelöscht werden die Nachrichten, die Anrufinformationen im Anrufjournal, die mit myAgent aufgezeichneten Anrufe, die empfangenen und gesendeten Faxe und E-Mails für das Contact Center und die Protokolldateien, die die eingestellten Aufbewahrungszeiten überschritten haben.

---

5) Klicken Sie auf **OK**, um das Löschen zu bestätigen.

25.14.3.4 Aufbewahrungszeit für Contact-Center-Daten konfigurieren

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Wartung**.
4) Geben Sie die Aufbewahrungszeit in Tagen in das Feld **Contact Center** unter dem Bereich **Wartung der Anrufinformationen** ein. Die mit myAgent aufgezeichneten Anrufe und die empfangenen und gesendeten Faxe und E-Mails für das Contact Center werden gelöscht, wenn diese die hier eingestellte Aufbewahrungszeit überschritten haben.
5) Klicken Sie auf **Speichern**.

25.15 Überwachung der UC Smart

Den aktuellen Status der UC Smart kann ein Administrator mit dem Profil **Expert** über das WBM abrufen.

25.15.1 Wie Sie den aktuellen Status der UC Smart abrufen

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

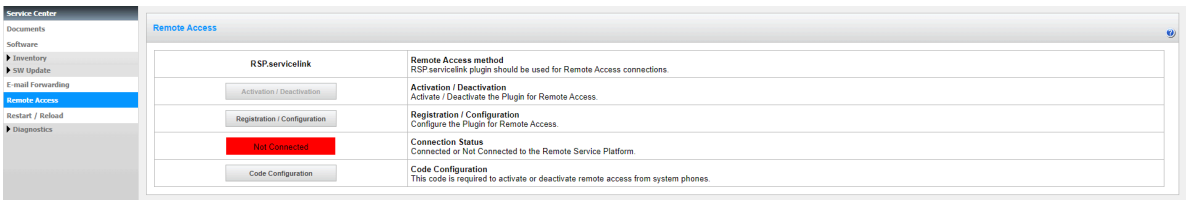
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen** > **UC Smart**.
3) Klicken Sie auf **Status**.

   Angezeigt wird der aktuelle Status des Applikationsservers und die Anzahl der aktiven Verbindungen der einzelnen UC Clients.

25.16 Remote Services

Durch verschiedene Remote Services wird ein Fernzugriff auf das Kommunikationssystem und auf angeschlossene Komponenten durch autorisierte Servicetechniker ermöglicht. Dadurch können Wartungstätigkeiten kostengünstig durchgeführt und Anwender vor Ort bei der Lösung von Problemen unterstützt werden.



Aufgrund dem Höchstmaß an Sicherheit ist der Remote Service über RSP.servicelink zu bevorzugen. Weitere Informationen siehe RSP.servicelink.

25.16.1 RSP.servicelink

Remotezugang mit der RSP.servicelink-Anschlussmöglichkeit (**R**emote **S**ervice **P**latform) bietet autorisierten Servicetechniker eines Remote Service Partners die Möglichkeit, das Kommunikationssystem inkl. der UC Booster Applikationen bequem und sicher aus der Ferne zu administrieren. Um RSP.servicelink zu konfigurieren, sind nur ein Internet-Anschluss, ein Webbrowser, die Partner ID und das Partner-Passwort des Remote Service Partners nötig. RSP.servicelink gewährleistet eine Breitbandverbindung mit hoher Sicherheit.

RSP.servicelink basiert auf der OpenVPN-Technologie. Es verwendet SSL/TSL-Protokoll und -Verschlüsselung und bietet mit einem zusätzlichen Client-Zertifikat die höchste Sicherheitsstufe. Der Begriff RSP.servicelink wird in der Dokumentation mit RSP abgekürzt.

Anmerkung: RSP verwendet den Bereich 100.64.0.1 - 100.127.255.254 für die tun0-Schnittstelle, wenn RSP aktiv ist. Das bedeutet, dass, wenn auf eine externe IP innerhalb dieses Bereichs zugegriffen werden muss, eine statische Route im Open Scape Business-System hinzugefügt werden sollte, um den Datenverkehr über die gewünschte Schnittstelle zu leiten.

In Verbindung mit OpenScape Business bietet RSP folgende wesentlichen Vorteile:

- Hohe Sicherheit durch gehende Internetverbindung

  Der komplette Remote-Verbindungsaufbau wird immer durch das Kommunikationssystem initiiert. Das bedeutet, die Firewall des Kundennetzes muss lediglich eine HTTPS-Verbindung zu einer einzigen Adresse im Remote Service Center zulassen (Port 443). Im Normalfall ist keine Änderung der Sicherheitsrichtlinie (Security Policy) des Kunden bzw. seiner Firewall erforderlich, da dieser Port in der Firewall des Kunden in der Regel für gehende Internet-Anrufe schon geöffnet ist. Damit ist eine hohe Sicherheit für das Kundennetz garantiert.

  Mit RSP behält der Administrator des Kommunikationssystems die Kontrolle über die Remote-Verbindung durch einfaches Ein- und Ausschalten des Zugangs. Bei RSP.servicelink wird automatisch auch ein Client-Zertifikat installiert.
- Hohe Bandbreite

  Durch die breitbandige Internetverbindung können im Fehlerfall Diagnosedaten schneller übertragen und damit die Servicequalität gesteigert werden.
- Einfache und kostengünstige Einrichtung

  Die Software des Kommunikationssystems beinhaltet bereits einen sogenannten RSP.servicelink. Bei der Aktivierung des Service Plugin müssen die Partner ID des Remote Service Partners und das Partner-Passwort eingegeben werden.

  Jeder Remote Service Partner, der RSP.servicelink nutzt, hat eine eigene Partner ID.

  Das RSP.servicelink-Plugin sollte deaktiviert und dann wieder aktiviert werden, wenn ein Software-Update durchgeführt wird.

- Zukunftssicherheit

  RSP ist die Basis für zukünftige Services ("value-added" Services), wie zum Beispiel Automatisierung von Backups, Reporting und Monitoring.

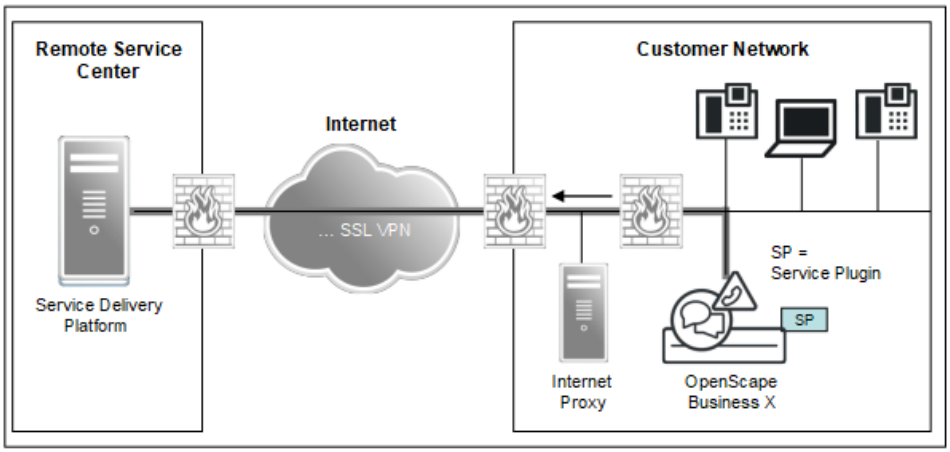


Abbildung 17: RSP - Übersicht für OpenScape Business X

RSP unterstützt die Web Services Standards, inklusive Hypertext Transfer Protocol Secure (HTTPS), Simple Object Access Protocol (SOAP) und Extensible Markup Language (XML).

Die Kommunikation zwischen Kundenseite und Remote Service Center wird für RSP.servicelink immer mit einer AES-256-CBC-Verschlüsselung abgesichert.

Service-Plugins

Das RSP.servicelink-Plugin kann separat aktiviert oder deaktiviert werden.

Ein Zurücksetzen des RSP.servicelink-Plugins ist zum Beispiel nach dem Austausch des Mainboards erforderlich. Durch das Zurücksetzen des Service-Plugin wird die gesamte RSP-Konfiguration gelöscht und das Plugin deaktiviert.

Anmerkung: Wenn das System sich nicht im DTAG-Modus befindet und das RSP.servicelink-Plugin aktiviert ist, können die Proxykonfigurationseinstellungen nicht geändert werden. Die Schaltfläche **Registrierung / Konfiguration ist deaktiviert.**

Wenn im DTAG-Modus das RSP.servicelink-Plugin aktiviert ist, wird bei einem Klick auf die Schaltfläche Registrierung / Konfiguration direkt die Seite Proxy-Einstellungen mit den Schaltflächen Abbrechen/Beenden aufgerufen. Dies ist auch vom Remote-Server aus möglich.

Geräteverwaltung (Managed Device)

In Kommunikationssystemen ohne UC Booster kann der Fernzugriff auf weitere Geräte im Kunden-LAN durch Konfiguration auf der SIRA-Seite ermöglicht werden. IP-Telefone können auf SIRA-Seite mit der Funktion "Verwaltete Geräte" konfiguriert werden.

Tipp: Der Fernzugriff auf andere im Kunden-LAN befindliche Kommunikationssysteme OpenScape Business ist nicht

möglich. Jede OpenScape Business muss für den Fernzugriff konfiguriert werden.

Aktivierung/Deaktivierung

Es bestehen folgende Möglichkeiten zur Aktivierung/Deaktivierung der Service-Plugins:

- über Wizard **Aktivierung / Deaktivierung**

  Für die RSP Service-Plugins gibt es jeweils einen eigenen Wizard für die Aktivierung/Deaktivierung.
- über Kennzahleingabe am Systemtelefon (Standard: Aktivierung über *996, Deaktivierung über #996)

  Aus Sicherheitsgründen ist bei der Aktivierung und Deaktivierung über ein Systemtelefon zusätzlich zur Kennzahl eine 4-stellige PIN einzugeben. Die Konfiguration dieser PIN erfolgt im WBM des Kommunikationssystems mit dem Profil **Advanced**.

Sicherung und Wiederherstellung

Die RSP-Anmeldeinformationen werden im Backup-Set des Systems gespeichert.

Wenn ein neues OpenScape Business System durch Klonen oder durch Datenwiederherstellung (Migration) eingerichtet wird und auf dem ursprünglichen System ein RSP-Zugriff konfiguriert war, muss sichergestellt werden, dass auf dem geklonten oder wiederhergestellten System eine andere RSP-Konfiguration aktiv ist.

Sie müssen das RSP deaktivieren oder deinstallieren, bevor Sie das ursprüngliche System klonen oder sichern.

Wenn ein Zertifikat für die Verbindung zu RSP in mehr als einem System verwendet wird, wird das Zertifikat widerrufen und keines der OpenScape-Systeme kann eine Verbindung zum RSP-Dienst herstellen.

Voraussetzungen

- Internetzugang für das Kommunikationssystem oder den HTTP-Proxy im Kunden-LAN.
- Eventuell Firewall im Kunden-LAN freischalten für Registrar:
  - https://188.64.18.51
  - https://188.64.17.51
- Eventuell Firewall im Kunden-LAN freischalten für VPN:
  - https://188.64.18.50
  - https://188.64.17.50
- Bei der Internet-Konfiguration muss ein Default-Router angegeben werden.

Anmerkung: Wenn das System sich während des Systemstarts im DTAG-Modus befindet und ohne installiertes und konfiguriertes RSP.serviceplugin Zugang zum Internet hat, wird das RSP.serviceplugin mittels Skript automatisch mit der Partner-ID und dem Kennwort für DTAG (Gerätename entspricht der MAC-Adresse des Systems) installiert, konfiguriert und aktiviert. Außerdem wird das Skript regelmäßig alle 10 Minuten

aufgerufen (z.B. für den Fall, dass nach der anfänglichen Systeminstallation kein Internetzugang verfügbar ist). Falls der Benutzer das Skript manuell deaktiviert hat, wird es vom RSP.serviceplugin nicht automatisch aktiviert.

25.16.1.1 Wie Sie das RSP.servicelink-Plugin installieren, konfigurieren und registrieren

Mit dem Wizard **Registrierung / Konfiguration** können Sie das RSP.servicelink-Plugin für den Remote-Zugriff auf das Kommunikationssystem über RSP installieren, konfigurieren und registrieren.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Klicken Sie auf **Registrierung / Konfiguration**.
4) Wenn das RSP.servicelink-Plugin noch nicht installiert ist, klicken Sie auf **Installieren** und anschließend auf **OK & Weiter**.
5) Wenn das RSP.servicelink-Plugin bereits installiert ist, klicken Sie auf **OK & Weiter**.
6) Wenn im Kundennetz kein Proxy-Server genutzt wird, klicken Sie auf **OK & Weiter**, da eine Konfiguration der **Proxy-Parameter** nicht erforderlich ist. Überspringen Sie die nächsten beiden Schritte.
7) Wenn im Kundennetz ein Proxy-Server genutzt wird, müssen Sie die Einstellung der **Proxy-Parameter** abhängig vom Kundennetz auswählen:
   - Wenn im Kundennetz ein Proxy mit HTTP-Protokoll vorliegt, aktivieren Sie das Kontrollkästchen **HTTP Proxy verwenden**. Geben Sie im Feld **HTTP Proxy Host** den Hostnamen und im Feld **HTTP Proxy Port** die Portnummer des Proxy-Servers ein. Falls erforderlich, geben Sie im Feld **Benutzername** den Benutzernamen und im Feld **Passwort** das Passwort für die Authentifizierung am Proxy-Server ein.
   - Wenn im Kundennetz ein Proxy mit SOCKS-Protokoll vorliegt, aktivieren Sie das Kontrollkästchen **SOCKS Proxy verwenden**. Geben Sie im Feld **SOCKS Proxy Host** den Hostnamen und im Feld **SOCKS Proxy Port** die Portnummer des Proxy-Servers ein. Falls erforderlich, geben Sie im Feld **Benutzername** den Benutzernamen und im Feld **Passwort** das Passwort für die Authentifizierung am Proxy-Server ein.

   Tipp: Ob eine Authentifizierung erforderlich ist oder nicht, hängt vom Typ und von der Konfiguration des Proxy-Servers ab.
8) Klicken Sie auf **OK & Weiter**.
9) Ändern Sie nur bei Bedarf im Feld **Partner ID** die vorbelegte Partner ID.
10) Geben Sie im Feld **Passwort** Ihr Passwort ein.

11) Geben Sie den Gerätenamen ein. Sie finden das Gerät unter seinem Gerätenamen im SIRA Equipment Explorer (EqE). Standardmäßig wird die MAC-Adresse der OpenScape Business angezeigt.
12) Klicken Sie auf **Beenden.**

In der Spalte **RSP.servicelink** wird Ihnen in der Zeile **Connection Status** angezeigt, ob die Registrierung erfolgreich war. Im Falle einer nicht erfolgreichen Registrierung können folgende Fehlermeldungen angezeigt werden:

- MAC bereits registriert:

  Lösung: Gerät (= OpenScape Business Kommunikationssystem) auf dem SIRA Equipment Explorer löschen und mit dem Wizard **Registrierung / Konfiguration** neu registrieren.

  Anmerkung: Sie finden das Gerät im SIRA Equipment Explorer über den Gerätenamen oder die MAC-Adresse. Der Gerätename oder die MAC-Adresse des OpenScape Business Kommunikationssystems finden Sie im **Service-Center** unter **Remote-Zugang**.

- Konfigurationsfehler:

  Lösung: Im Wizard **Registrierung / Konfiguration** Partner-ID und Passwort neu eingeben und den Wizard korrekt beenden.
- Falsche Anmeldeinformationen:

  Lösung: Im Wizard **Registrierung / Konfiguration** Partner-ID und Passwort neu eingeben und den Wizard korrekt beenden.

25.16.1.2 Wie Sie das RSP.servicelink-Plugin aktivieren

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie das RSP.servicelink-Plugin für den Remote-Zugriff auf das Kommunikationssystem über RSP aktivieren.

Voraussetzungen

Eine funktionierende DNS-Konfiguration liegt vor.

Ein Default-Router für den Internet-Zugang oder alternativ ein Proxy-Server im Kundennetz ist vorhanden.

Das RSP.servicelink-Plugin ist deaktiviert.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Klicken Sie in der Spalte **RSP.servicelink** auf **Aktivierung / Deaktivierung**.
4) Klicken Sie auf **Aktivieren**.

25.16.1.3 Wie Sie das RSP.servicelink-Plugin deaktivieren

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie das RSP.servicelink-Plugin für den Remote-Zugriff auf das Kommunikationssystem aktivieren.

Voraussetzungen

Das RSP.servicelink-Plugin ist aktiviert.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Klicken Sie auf **Aktivierung / Deaktivierung** in der Spalte **RSP.servicelink**.
4) Klicken Sie auf **Deaktivieren**.

25.16.1.4 Wie Sie das RSP Service-Plugin zurücksetzen

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie das RSP Service-Plugin zurücksetzen. Damit wird die gesamte RSP-Konfiguration gelöscht und das RSP Service-Plugin deaktiviert.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Klicken Sie in der Spalte **RSP.servicelink** auf **Aktivierung / Deaktivierung**.
4) Klicken Sie auf **Auf Standard zurücksetzen** und anschließend auf **OK**.
5) Klicken Sie in der Spalte **RSP.servicelink** auf **Aktivierung / Deaktivierung**.
6) Klicken Sie auf **Deaktivieren**.
7) Löschen Sie auf dem SIRA-Server das Gerät (= OpenScape Business Kommunikationssystem).

Anmerkung: Über die MAC-Adresse finden Sie das Gerät auf dem SIRA-Server. Die MAC-Adresse des OpenScape Business Kommunikationssystems finden Sie im **Service-Center** unter **Inventory**.

25.16.1.5 Wie Sie eine PIN für die Aktivierung und Deaktivierung des RSP.servicelink-Plugin konfigurieren

Die PIN gilt für die Aktivierung und die Deaktivierung des RSP.servicelink-Plugin über ein Systemtelefon.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Geben Sie im Feld **PIN** die gewünschte vierstellige PIN ein.
4) Klicken Sie auf **Sichern** und anschließend auf **OK**.

Nächste Schritte

Die Aktivierung des primären Service-Plugins über ein Systemtelefon erfolgt durch Eingabe der entsprechenden Kennzahl (Standardkennzahl = *996) und anschließender Eingabe der vierstelligen PIN.

Die Deaktivierung der Service-Plugins über ein Systemtelefon erfolgt durch Eingabe der entsprechenden Kennzahl (Standardkennzahl = #996) und anschließender Eingabe der vierstelligen PIN.

25.16.2 Remote-Zugang

Durch den Remote-Zugang kann autorisierten Servicetechnikern über eine Internet-Verbindung der Fernzugriff auf die Kommunikationssysteme OpenScape Business X ermöglicht werden. Damit ist zum Beispiel die Unterstützung bei der Lösung von Administrationsaufgaben oder bei der Fehlersuche möglich.

Um den Fernzugriff auf das Kommunikationssystem zu ermöglichen, muss der Remote-Zugang eingeschaltet werden. Es besteht folgende Zugriffsmöglichkeit:

Remote-Zugang über Internet-Verbindung

Tipp: Beim Remote-Zugang über eine Internet-Verbindung besteht ein erhöhtes Sicherheitsrisiko.

Zur Einwahl über Internet benötigt der Servicetechniker einen speziellen Port (**Port-Nummer**) zum Zugriff auf das Kommunikationssystem. Standardmäßig ist die Port-Nummer 10099 eingetragen. Bei Verwendung eines externen Routers muss im externen Router eine Port-Weiterleitung für diese Port-Nummer eingerichtet werden.

Die Port-Nummer darf nicht durch eine eventuell vorhandene Firewall auf dem PC des Servicetechnikers gesperrt sein. Die Auswahl der Port-Nummer ist deshalb mit dem Servicetechniker abzustimmen.

Die UC Booster Applikationen (wie z.B. UC Suite, OpenDirectory Service, Gate View) können über diesen Remote-Zugang nicht administriert werden.

Um den Fernzugriff auf das Kommunikationssystem zu deaktivieren, muss der Remote-Zugang ausgeschaltet werden.

Anmerkung: Um nicht autorisierte Zugriffe auf das Kommunikationssystem zu vermeiden, ist der Remote-Zugang nach Beendigung der Fernadministration wieder auszuschalten.

25.16.2.1 Wie Sie den Remote-Zugang über ISDN einschalten

Mit dem Wizard **Remote-Zugang** können Sie autorisierten Servicetechnikern über eine ISDN-Verbindung den Zugriff auf das Kommunikationssystem ermöglichen.

Voraussetzungen

OpenScape Business X verfügt über eine ISDN-Amtsverbindung.

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Klicken Sie auf **Remote-Zugang**, um den Wizard **Remote-Zugang** zu starten.
4) Aktivieren Sie das Optionsfeld **Remote-Zugang: ein**, um den Remote-Zugang einzuschalten.
5) Aktivieren Sie das Optionsfeld **Remote-Zugang über: ISDN**, um den Remote-Zugang über ISDN einzuschalten.
6) Geben Sie im Feld **Rufnummer** die interne Rufnummer ein, über die der Remote-Zugang erfolgen soll.
7) Geben Sie im Feld **Einwahlnummer** die Durchwahlnummer ein, über die der Remote-Zugang erfolgen soll.
8) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

25.16.2.2 Wie Sie einen PC mit Microsoft Windows Vista für Remote-Zugang über ISDN konfigurieren

Voraussetzungen

Der PC ist mit einer ISDN-Karte ausgestattet und verfügt über eine ISDN-Amtsverbindung.

Der Zugriff soll auf ein Kommunikationssystem OpenScape Business X3/X5/X8 mit Anlagenanschluss erfolgen. Ortsnetzkennzahl und Anlagenrufnummer des Kommunikationssystems liegen vor.

Der Remote-Zugang über ISDN wurde eingeschaltet. Die Einwahlnummer für den Remote-Zugang des Kommunikationssystems liegt vor.

Benutzername und Kennwort für den Zugriff auf das Kommunikationssystem liegen vor.

Tipp: Die folgende Beschreibung bezieht sich auf einen PC mit dem Betriebssystem Microsoft Windows Vista. Ein ähnlicher Ablauf ergibt sich für das Betriebssystem Microsoft Windows XP.

Schritt für Schritt

1) Klicken Sie im **Startmenü** von Windows Vista auf **Verbindung herstellen**. Das Fenster **Verbindung mit einem Netzwerk herstellen** erscheint.
2) Klicken Sie auf **Eine Verbindung oder ein Netzwerk einrichten**.
3) Klicken Sie auf die Verbindungsoption **Verbindung mit dem Arbeitsplatz herstellen** und anschließend auf **Weiter**.
4) Klicken Sie auf **Direkt wählen**.
5) Geben Sie im Feld **Rufnummer** die Amtskennziffer (zum Beispiel `0`), die Ortsnetzkennzahl (zum Beispiel `089`), die Anlagenrufnummer (zum Beispiel `12345678`) und die Einwahlnummer (zum Beispiel `666`) ein.

   Der Gesamteintrag für die genannten Beispiele lautet: `008912345678666`
6) Geben Sie im Feld **Zielname** eine Bezeichnung für diese Verbindung ein.
7) Aktivieren Sie das Kontrollkästchen **Jetzt nicht verbinden, nur für spätere Verwendung einrichten**.
8) Klicken Sie auf **Weiter**.
9) Geben Sie im Feld **Benutzername** den Benutzernamen für den Zugriff auf das Kommunikationssystem ein.
10) Geben Sie im Feld **Kennwort** das Kennwort für den Zugriff auf das Kommunikationssystem ein.

    Anmerkung: Als Standarddaten für den Zugriff auf das Kommunikationssystem werden der Standard-Benutzername und das Standard-Kennwort für den Systemzugriff mittels Servicetool Manager E verwendet.
11) Klicken Sie auf an **Erstellen**.
12) Klicken Sie auf **Verbindung jetzt herstellen**.

Damit ist der Fernzugriff auf das Kommunikationssystem möglich.

Tipp: Um die Verbindung zu deaktivieren, klicken Sie auf **Start** > **Verbindung herstellen**. Klicken Sie auf die im Schritt 6 definierte Bezeichnung der Verbindung (**Zielname**) und anschließend auf **Trennen**.

Das Aktivieren der Verbindung ist durch Klicken auf die im Schritt 6 definierte Bezeichnung (**Zielname**) und anschließendes Klicken auf **Verbinden** möglich.

25.16.2.3 Wie Sie einen PC mit Microsoft Windows 7 für Remote-Zugang über ISDN konfigurieren

Voraussetzungen

Der PC ist mit einer ISDN-Karte ausgestattet und verfügt über eine ISDN-Amtsverbindung.

Der Zugriff soll auf ein Kommunikationssystem OpenScape Business X3/X5/X8 mit Anlagenanschluss erfolgen. Ortsnetzkennzahl und Anlagenrufnummer des Kommunikationssystems liegen vor.

Der Remote-Zugang über ISDN wurde eingeschaltet. Die Einwahlnummer für den Remote-Zugang des Kommunikationssystems liegt vor.

Benutzername und Kennwort für den Zugriff auf das Kommunikationssystem liegen vor.

Tipp: Die folgende Beschreibung bezieht sich auf einen PC mit dem Betriebssystem Microsoft Windows 7.

Schritt für Schritt

1) Klicken Sie im **Startmenü** von Windows 7 auf **Systemsteuerung**.
2) Klicken Sie auf **Netzwerk und Internet**.
3) Klicken Sie auf **Netzwerk- und Freigabecenter**.
4) Klicken Sie auf **Eine Verbindung oder ein Netzwerk einrichten**.
5) Klicken Sie auf die Verbindungsoption **Verbindung mit dem Arbeitsplatz herstellen** und anschließend auf **Weiter**.
6) Klicken Sie auf **Direkt wählen**.
7) Geben Sie im Feld **Rufnummer** die Amtskennziffer (zum Beispiel `0`), die Ortsnetzkennzahl (zum Beispiel `089`), die Anlagenrufnummer (zum Beispiel `12345678`) und die Einwahlnummer (zum Beispiel `666`) ein.

   Der Gesamteintrag für die genannten Beispiele lautet: `008912345678666`
8) Geben Sie im Feld **Zielname** eine Bezeichnung für diese Verbindung ein.
9) Aktivieren Sie das Kontrollkästchen **Jetzt nicht verbinden, nur für spätere Verwendung einrichten**.
10) Klicken Sie auf **Weiter**.
11) Geben Sie im Feld **Benutzername** den Benutzernamen für den Zugriff auf das Kommunikationssystem ein.
12) Geben Sie im Feld **Kennwort** das Kennwort für den Zugriff auf das Kommunikationssystem ein.

    Anmerkung: Als Standarddaten für den Zugriff auf das Kommunikationssystem werden der Standard-Benutzername und das Standard-Kennwort für den Systemzugriff mittels Servicetool Manager E verwendet.

    ---
13) Klicken Sie auf an **Erstellen**.
14) Klicken Sie auf **Verbindung jetzt herstellen**. Anschließend erscheint die Meldung `Verbindung wurde hergestellt`.
15) Klicken Sie auf **Schließen**.

Damit ist der Fernzugriff auf das Kommunikationssystem möglich.

Tipp: Um die Verbindung zu deaktivieren, klicken Sie in der Symbolleiste auf das Symbol **Netzwerk**. Klicken Sie auf die im Schritt 8 definierte Bezeichnung der Verbindung (**Zielname**) und anschließend auf **Trennen**.

Das Aktivieren der Verbindung ist durch Klicken auf die im Schritt 8 definierte Bezeichnung (**Zielname**) und anschließendes Klicken auf **Verbinden** möglich.

25.16.2.4 Wie Sie den Remote-Zugang über Internet-Zugang mit fester IP-Adresse einschalten

Mit dem Wizard **Remote-Zugang** können Sie autorisierten Servicetechnikern über eine Internet-Verbindung den Zugriff auf das Kommunikationssystem ermöglichen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Ihnen liegt eine Port-Nummer vor, über die der Internet-Zugriff des Servicetechnikers auf das Kommunikationssystem möglich ist. Diese Port-Nummer darf nicht durch eine eventuell vorhandene Firewall auf dem PC des Servicetechnikers gesperrt sein.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Klicken Sie auf **Remote-Zugang**, um den Wizard **Remote-Zugang** zu starten.
4) Aktivieren Sie das Optionsfeld **Remote-Zugang: ein**, um den Remote-Zugang einzuschalten.
5) Aktivieren Sie das Optionsfeld **Remote-Zugang über: Internet**, um den Remote-Zugang über Internet einzuschalten.
6) Geben Sie im Feld **Port-Nummer** die Port-Nummer ein, über die der Remote-Zugang erfolgen soll.

   Standardmäßig ist die Port-Nummer 10099 eingetragen.
7) Klicken Sie auf **OK & Weiter**. Die Meldung `Der Remote-Zugang wurde aktiviert ...` wird angezeigt. Diese Meldung enthält die URL, über die der Fernzugriff auf das Kommunikationssystem per Webbrowser möglich ist.
8) Klicken Sie auf **Beenden**.

25.16.2.5 Wie Sie den Remote-Zugang über Internet-Zugang ohne feste IP-Adresse einschalten

Mit dem Wizard **Remote-Zugang** können Sie autorisierten Servicetechnikern über eine Internet-Verbindung den Zugriff auf das Kommunikationssystem ermöglichen.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Ihnen liegt eine Port-Nummer vor, über die der Internet-Zugriff des Servicetechnikers auf das Kommunikationssystem möglich ist. Diese Port-Nummer darf nicht durch eine eventuell vorhandene Firewall auf dem PC des Servicetechnikers gesperrt sein.

Ein DynDNS-Account liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Klicken Sie auf **Remote-Zugang**, um den Wizard **Remote-Zugang** zu starten.
4) Aktivieren Sie das Optionsfeld **Remote-Zugang: ein**, um den Remote-Zugang einzuschalten.
5) Aktivieren Sie das Optionsfeld **Remote-Zugang über: Internet**, um den Remote-Zugang über Internet einzuschalten.
6) Geben Sie im Feld **Port-Nummer** die Port-Nummer ein, über die der Remote-Zugang erfolgen soll.

   Standardmäßig ist die Port-Nummer 10099 eingetragen.
7) Klicken Sie auf **OK & Weiter**, um die Eingaben zu übernehmen. Das Fenster **DynDNS-Account einrichten** erscheint.
8) Geben Sie im Feld **Benutzername** den Benutzernamen für Ihren DynDNS-Account beim DynDNS-Anbieter ein, falls dieser nicht bereits angezeigt wird.
9) Geben Sie im Feld **Passwort** und im Feld **Passwort wiederholen** das Passwort Ihres DynDNS-Accounts beim DynDNS-Anbieter ein, falls dieses nicht bereits angezeigt wird.
10) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein (zum Beispiel `myhost`), falls dieser nicht bereits angezeigt wird.
11) Wählen Sie in der Aufklappliste **Domainname** Ihren DynDNS-Anbieter aus (zum Beispiel `dyndns.org`), falls dieser nicht bereits angezeigt wird. Ihr vollständiger Domänenname lautet dann beispielsweise `myhost.dyndns.org`.
12) Klicken Sie auf **Verbindung testen**. Es erscheint das Fenster **DynDNS-Zugang testen**.
13) Klicken Sie auf **OK**. Die DynDNS-Zugangsdaten werden nun zum Provider übermittelt. Das dauert ca. 10 Sekunden.
14) Wenn der Test erfolgreich war, wird die Meldung `Der Remote-Zugang wurde aktiviert ...` angezeigt. Diese Meldung enthält die URL,

über die der Fernzugriff auf das Kommunikationssystem per Webbrowser möglich ist. Klicken Sie auf **Beenden**.

15) Wenn der Test nicht erfogreich war, klicken Sie auf **OK**. Im anschließend erscheinenden Fenster **DynDNS-Zugang** erhalten Sie Hinweise zu den möglichen Fehlerursachen. Klicken Sie auf **OK**. Das Fenster **DynDNS-Account einrichten** erscheint. Überprüfen und korrigieren Sie gegebenenfalls hier die von Ihnen eingegebenen Zugangsdaten (Schritte 8 bis 11). Fahren Sie wie unter Schritt 12 beschrieben fort.

25.16.2.6 Wie Sie den Remote-Zugang ausschalten

Mit dem Wizard **Remote-Zugang** können Sie den Remote-Zugang ausschalten.

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.
3) Klicken Sie auf **Remote-Zugang**, um den Wizard **Remote-Zugang** zu starten. Angezeigt wird, ob der Remote-Zugang über Internet oder/und ISDN eingeschaltet ist.
4) Aktivieren Sie das Optionsfeld **Remote-Zugang: aus**, um einen Remote-Zugang auszuschalten.
5) Wählen Sie aus, welche Option des Remote-Zugangs Sie ausschalten möchten:
   - Wenn Sie den Remote-Zugang über Internet ausschalten möchten, aktivieren Sie das Optionsfeld **Remote-Zugang über: Internet**.
   - Wenn Sie den Remote-Zugang über ISDN ausschalten möchten, aktivieren Sie das Optionsfeld **Remote-Zugang über: ISDN**.
6) Klicken Sie auf **OK & Weiter**.
7) Wenn Sie auch die zweite Option des Remote-Zugangs ausschalten wollen, klicken Sie auf **Zurück**. Wiederholen Sie die Schritte 4 bis 6.
8) Klicken Sie auf **Beenden**.

25.16.3 Online-Benutzer

Der Online-Benutzer ermöglicht die Fernsteuerung, -prüfung und -überwachung von OpenStage-Telefonen über einen Windows-PC. Das Verhalten eines OpenStage-Telefons wird über den Online-Benutzer am PC nachgebildet.

Voraussetzung für die Kommunikation mit einem OpenStage-Telefon ist, dass die Telefon-Software über einen sogenannten Dongle-Key verfügt.

Für den Zugriff auf ein OpenStage-Telefon sind folgende Eingaben über den Online-Benutzer erforderlich:

- OpenStage-Telefon-Typ
- IP-Adresse des OpenStage-Telefons

- Administrator-Passwort des OpenStage-Telefons

Informationen über die Verwendung des Online-Benutzers können folgender Dokumentation entnommen werden: *OpenStage HUSIM Phone Tester User Guide*. Der Zugriff ist möglich über das Intranet-Portal für technische Produktdokumentation unter `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

Auch das Servicetool Manager E bietet Online-Benutzer für die Fernsteuerung, -prüfung und -überwachung von OpenStage-Telefonen.

Anmerkung: Die vom Online-Benutzer genannte Gateway-IP-Adresse ist dieselbe wie die System-IP-Adresse. Die Gateway-IP-Adresse ist nicht die IP-Adresse der Standard-Route.

25.16.3.1 Wie Sie Online-Benutzer starten

Voraussetzungen

Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung** > **Online-Benutzer**. Das Anmeldefenster des Online-Benutzers wird angezeigt.
3) Wählen Sie in der Aufklappliste **Model** das Modell des gewünschten OpenStage-Telefons aus.
4) Geben Sie im Feld **Phone IP** die IP-Adresse des gewünschten OpenStage-Telefons ein.
5) Geben Sie im Feld **Password** das Administrator-Passwort des gewünschten OpenStage-Telefons ein. Standardmäßig ist das Administrator-Passwort `123456`.
6) Wählen Sie in der Aufklappliste **Protocol** das gewünschte Transportprotokoll aus.
7) Wählen Sie eine der folgenden Möglichkeiten für die Internet Protocol Version IPv:
   - Wenn Sie die Internet Protocol Version 4 verwenden möchten, aktivieren Sie die Option **IPv4**.
   - Wenn Sie die Internet Protocol Version 6 verwenden möchten, aktivieren Sie die Option **IPv6**.
8) Wählen Sie in der Aufklappliste **Number of Key modules** die Anzahl der Beistellgeräte aus.
9) Klicken Sie auf **OK**, um den Zugriff auf das gewünschte OpenStage-Telefon zu starten.

Tipp: Informationen über die Bedienung des Online-Benutzers können Sie dem *OpenStage HUSIM Phone Tester User Guide* entnehmen, das über `http://apps.g-dms.com:8081/techdoc/search_en.htm` aufgerufen werden kann.

---

26 Migration

OpenScape Business V1, V2 Systeme und HiPath 3000 Systeme können auf OpenScape Business V3 migriert/aktualisiert werden.

Die folgenden Migrations-/Aktualisierungsszenarien werden von der OpenScape Business V3 Software unterstützt.

Anmerkung: Es ist wichtig, aktive Unify Phone-Benutzer z. B. vor Systemmigrationen zu löschen, um kritische Diskrepanzen zwischen der OpenScape Business-Datenbank und der Cloud-Datenbank zu vermeiden. Weitere Informationen finden Sie im Unify Experts Wiki Unify Phone Whitepaper.

Anmerkung: Siehe auch Wie entfernen oder löschen Sie Unify Phone-Benutzer auf Seite 1211.

OpenScape Business X System inklusive UC Booster Card oder Booster Server

- Software-Aktualisierung von OpenScape Business X V2 auf V3 mit „V2-Mainboard“
- Hardware-/Software-Migration von OpenScape Business X V2 auf V3 mit „V3-Mainboard“
- Hardware-/Software-Migration von OpenScape Business X V1 auf V3 mit „V3-Mainboard“
- Hardware-/Software-Migration von OpenScape Business X V3 mit „V2-Mainboard“ auf V3 mit „V3-Mainboard“

OpenScape Business S System

- Software-Aktualisierung von OpenScape Business S V2 auf V3

OpenScape Business Netzwerk

- Software-Aktualisierung von OpenScape Business Netzwerk von V2 auf V3

HiPath 3000 inklusive OpenScape Office HX

- Hardware-Migration HiPath 3000 inklusive OpenScape Office HX

HiPath 500

- Hardware-Migration HiPath 500 auf OpenScape Business X1 V3

Je nach Quellsystem können vorhandene Lizenzen ganz oder teilweise übertragen werden. Gleiches gilt für die weitere Verwendung von Peripheriemodulen und angeschlossenen Endgeräten.

Der bestehende Software-Support für OpenScape Business Systeme bleibt auch nach der Migration unverändert.

Sie können den Migrations-/Aktualisierungsaufwand für die weitere Nutzung vorhandener Lizenzen im Vergleich zu einer „Offline“-Lizenzübertragung verringern, wenn Sie das OpenScape Business System mit dem zentralen Unify-Lizenzserver verbinden und die Funktion **CLS Connect** nutzen.

In diesem Abschnitt werden die folgenden Begriffe verwendet:

Migration	bei Hardware- und Softwareänderungen
Upgrade	bei reinen Softwareänderungen
V2-Mainboard	Bezeichnung für die mit OpenScape Business eingeführte Mainboard-Familie.
V3-Mainboard	Bezeichnung für die mit der Software V3 eingeführte Mainboard-Familie.

Anmerkung: Eine Voraussetzung für alle Migrationsszenarien, um von einem V2-Mainboard- auf ein V3-Mainboard-System aufzurüsten, ist, dass der Administrator das Backup-Set über das HTTPS-Gerät hochladen muss. Andere Geräte wie Festplatten-, FTP- oder Netzlaufwerke werden nicht unterstützt und führen zum Scheitern des Migrationsprozesses.

Anmerkung: Abhängig von der Softwareversion des OSBiz-Systems gibt es zwei gültige Migrationspfade. Verwenden Sie entweder ein Backup-Set von einem V2-Hardware-System auf dem neuesten V2R7-Bind oder verwenden Sie denselben V3-Software-Bind sowohl auf dem V2-Hauptplatinensystem als auch auf dem V3-Hauptplatinensystem, um die Konsistenz der Datenbank zu gewährleisten.

Anmerkung: Wenn ein OpenScape Office V3 MX/LX-System durch ein OpenScape Business-System ersetzt werden soll, muss letzteres als neues System bestellt werden.

26.1 Software-Aktualisierung für OpenScape Business X Systeme

Die Software-Aktualisierung von OpenScape Business X Systemen beinhaltet im Wesentlichen den Ersatz einiger SW-Komponenten.

Vor der Aktualisierung eines OpenScape Business X Systems müssen Sie die aktuelle Systemkonfiguration und ggf. die zu ersetzenden Hardware-/Software- und Lizenzkomponenten bestimmen.

Tabelle 31: OpenScape Business X Software-Aktualisierung - Hardware-/ Software-Checkliste

Komponenten	Ersetzt durch
Hardwarekomponenten	
Softwarekomponenten	
V2 System-Software auf SDHC-Karte	V3 System-Software (Image vom Software Download Server)
VPN auf WAN im System beendet	VPN in externem Router beendet
XMPP	Keine Follow-on-Lösung

Komponenten	Ersetzt durch
myPortal Smart	myPortal @work
Lizenzkomponenten	
Lizenzen in Lizenzdatei	Übertragung der Lizenzen in eine neue Lizenzdatei

26.1.1 Software-Aktualisierung von OpenScape Business X V2 auf OpenScape Business X V3

Wenn Sie eine SW-Aktualisierung des OpenScape Business X-Modells von Softwareversion V2 auf V3 vornehmen, wird nur die Systemsoftware ersetzt - das V2-Mainboard und alle vorhandenen UC Booster Cards oder Booster Server bleiben erhalten. Bestehende Lizenzen und die Kundenkonfiguration bleiben erhalten. Der bestehende Software-Support wird nach der Migration unverändert fortgeführt.

Falls dieser nicht bereits vorhanden ist, müssen Sie vor der Software-Aktualisierung von Version V2 auf V3 im System einen permanenten Zugang zum Unify-Lizenzserver einrichten (über das Internet) und die Funktion **CLS Connect** aktivieren. Das vereinfacht die Lizenzübertragung und verkürzt erheblich die Migrationszeit.

Voraussetzungen

Für die SW-Aktualisierung und die Übertragung der bestehenden Kundenkonfiguration muss das System mit der vor der Aktualisierung zuletzt veröffentlichten SW-Version V2R7 betrieben werden. Aktualisieren Sie ggf. das System auf die neueste SW-Version. Dazu muss das System über einen gültigen Software-Support-Status verfügen.

Für die System-SW-Aktualisierung von V2 auf V3 ist je nachdem, ob CLS Connect verwendet wird oder nicht, Folgendes erforderlich:

- OpenScape Business V3 SW Upgrade-Lizenz (nur wenn **CLS Connect** nicht verwendet wird)

Bedingungen und Einschränkungen für funktionale Grenzen

Sie können im Verlauf der Migration bestehende Lizenzen vom vorhandenen V2-Mainboard vollständig auf das V3 Mainboard übertragen. Die Lizenzübertragung ohne Aktivierung der Funktion CLS Connect erfordert die Lizenz „SW Upgrade“ und eine viel komplexere Handhabung und mehr Zeitaufwand als die Verwendung der Funktion CLS Connect.

Die Kundenkonfiguration und die Kundendaten werden beim SW-Aktualisierungsprozess von SW-Version V2 auf V3 automatisch übertragen.

Die wichtigsten technischen Schritte der SW-Aktualisierung werden in den folgenden Kapiteln beschrieben. Um die bestehenden Lizenzen beizubehalten, wird folgende Unterscheidung in der Handhabung gemacht:

- SW-Aktualisierung für permanente Lizenzierung mit und ohne CLS Connect
- SW-Aktualisierung mit PayGo-Lizenzierung

26.1.1.1 SW-Aktualisierung von permanent lizenzierten Systemen mit CLS Connect

Führen Sie folgende Aktualisierungsschritte der Reihe nach durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor
   a) Aktualisieren Sie das vorhandene System auf Softwareversion V2R7.
   b) Richten Sie im System einen Zugang zum zentralen Unify-Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung.
   c) Aktivieren Sie **CLS Connect** im System.

2) Führen Sie die Softwareaktualisierung durch
   a) Führen Sie die Softwareaktualisierung auf V3 über OpenScape Business Assistant durch.
   b) Die Systemkonfiguration wird automatisch auf V3 übertragen.
   c) Bestehende Lizenzen werden nach V3 übernommen.

3) Die Lizenzdatei wird automatisch vom zentralen Lizenzserver generiert.

   Nach dem Neustart des Systems überträgt das System die Information, dass die bestehenden Lizenzen mit Softwareversion 3 betrieben werden, an den CLS.

26.1.1.2 SW-Aktualisierung von permanent lizenzierten Systemen ohne CLS Connect

Führen Sie folgende Aktualisierungsschritte der Reihe nach durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor.
   a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7.

2) Erstellen Sie auf dem zentralen Lizenzserver (CLS) „Upgrade-Lizenzdatei“ für das V2-System
   a) Aktivieren Sie die „SW-Upgrade-Lizenz“ für das vorhandene System.
   b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse des V2-Mainboards
   c) Laden Sie die Lizenzdatei vom CLS herunter

3) Importieren Sie die Lizenzdatei in das OpenScape Business V2-System und aktivieren Sie sie.

4) Führen Sie die SW-Aktualisierung durch.
   a) Führen Sie die SW-Aktualisierung auf V3 über OpenScape Business Assistant durch.
   b) Die Systemkonfiguration wird automatisch auf V3 übertragen.
   c) Im System vorhandene Lizenzen werden auf V3 übertragen

5) Starten Sie das System nach der SW-Aktualisierung neu.

26.1.1.3 SW-Aktualisierung auf PayGo-lizenzierte Systeme

Führen Sie folgende Aktualisierungsschritte der Reihe nach durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor
   a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7.
2) Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS) neu
   a) Generieren Sie erneut eine neue Lizenzdatei für die MAC-Adresse des V2-Mainboards.
   b) Laden Sie die Lizenzdatei vom CLS herunter.
3) Importieren Sie die neue Lizenzdatei in das OpenScape Business V2-System und aktivieren Sie sie.
4) SW-Aktualisierung OpenScape Business SW
   a) Führen Sie die SW-Aktualisierung auf V3 über OpenScape Business Assistant durch.
   b) Die Systemkonfiguration wird automatisch auf V3 übertragen.
   c) Das System ist nach einem Neustart betriebsbereit.

26.2 Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3

Die SW-Aktualisierung von einem UC Booster Server V2 auf V3 kann in einem Schritt durchgeführt werden.

Eine SW-Aktualisierung von einem UC Booster Server V1 auf Version V3 muss in zwei Schritten erfolgen. Aktualisieren Sie zuerst von V1 auf V2R7, dann von V2R7 auf V3.

26.2.1 So aktualisieren Sie UC Business Booster Server V2 auf V3

Das SW-Upgrade des UC Booster Servers von V2 auf V3 ist nur für OpenScape Business X-Systeme mit einem V2-Hauptplatine erforderlich. OpenScape Business X-Systeme mit V3-Hauptplatinen erfordern keinen UC Booster Server mehr. In diesem Fall ist SW-Version V2.7 auf dem UC Booster Server erforderlich, um Kundenkonfigurationen und Lizenzen auf die V3-Hauptplatine zu migrieren.

Voraussetzungen

- Linux-Betriebssystem muss geprüft und gegebenenfalls aktualisiert werden (siehe *technische Versionshinweise für OpenScape Business V3-System SW*)
- UC Booster Server wird vor dem Upgrade mit der zuletzt freigegebenen SW-Version V2R7 betrieben. Aktualisieren Sie das System gegebenenfalls auf die neueste SW-Version.
- Aktualisieren Sie zuerst das OpenScape Business X-System, mit dem der UC Booster Server verbunden ist, auf SW-Version V3, einschließlich Lizenzierung gemäß Beschreibung in Software-Aktualisierung von OpenScape Business X V2 auf OpenScape Business X V3 auf Seite 1391
- UC Booster Server SW-Image V3

Ermitteln Sie vor einem UC Booster Server SW-Upgrade die aktuelle Systemkonfiguration sowie die HW/SW und Lizenzkomponenten, die möglicherweise ersetzt werden müssen.

Tabelle 32: OpenScape Business S-Migration - HW/SW-Checkliste

Komponenten	Ersetzt durch
Hardwarekomponenten	
Server-PC	Wiederverwendung ist möglich. HW-Anforderungen müssen für OpenScape Business S-Erweiterungen geprüft werden.[9]
Softwarekomponenten	
SLES 12 oder SLES 15 Betriebssystem	Wiederverwendung ist möglich. Eventuell ist ein Upgrade auf das neueste Servicepack erforderlich [10]
XMPP	Keine Follow-on-Lösung
myPortal Smart	myPortal @work
Lizenzkomponenten	
Lizenzen in Lizenzdatei (ist Teil der OpenScape Business X-Lizenzdatei)	Übertragung der Lizenzen in eine neue Lizenzdatei
CSTA-Anwendung (über UC Booster Card / Server)	CSTA-Lizenz zur Anbindung externer Lösungen (nicht erforderlich für UC Suite, TAPI 170 und TAPI 120)

Im Folgenden wird das OpenScape Business SW-Upgrade unter Beibehaltung des SLES-Betriebssystems beschrieben.

Schritt für Schritt

1) Aktualisieren Sie OpenScape Business X-System auf V3.

Siehe Software-Aktualisierung von OpenScape Business X V2 auf OpenScape Business X V3 auf Seite 1391 für details.

9 Die vorhandene Server-PC-HW kann verwendet werden, wenn die Konfiguration des UC Booster Server Systems nach dem SW-Upgrade unverändert bleibt. Wenn Erweiterungen nach dem SW-Upgrade geplant sind, müssen möglicherweise die Hardwareanforderungen gemäß den Spezifikationen im *OpenScape Business S-Installationshandbuch, Kapitel Voraussetzungen* angepasst werden.

10 Das auf dem Server-PC installierte SLES-Betriebssystem kann im Falle eines UC Booster Server SW-Upgrades übernommen werden. Es sollte jedoch vor dem SW-Upgrade auf das zuletzt freigegebene Servicepack aktualisiert werden.

Wenn Novell den SW-Support für die verwendete SLES-Version eingestellt hat, muss der Kunde informiert und gegebenenfalls ein SLES-Upgrade vermarktet werden.

Das SLES-Upgrade muss möglicherweise in mehreren Schritten durchgeführt werden, um bestehende OpenScape Business S Installationen einschließlich der Kundenkonfiguration und Kundendaten zu übernehmen. Ein vorhandener SLES-Update-Schlüssel bleibt bei einem SLES-Upgrade gültig. Möglicherweise muss es jedoch vor dem SLES-Upgrade bei Novell abgemeldet und dann für das neue System neu registriert werden.

2) Upgrade der UC Booster Server SW auf V3

Verwenden Sie die Upgrade-Funktion im OpenScape Business Assistant des UC Booster Servers, um die V2R7 SW auf die Version V3 zu aktualisieren (siehe Update des Kommunikationssystems auf Seite 1263).

3) Führen Sie nach dem SW-Upgrade eine Datensicherung durch

Sichern Sie Ihre V3 Daten (siehe Sofortiges Sichern auf Seite 1256)

26.3 Hardware/Software-Migration von OpenScape Business X Systemen auf V3

Bei der Migration von OpenScape Business X Systemen werden HW-, SW- und Lizenzkomponenten ausgetauscht.

Bestimmen Sie vor der Migration eines Business X Systems die aktuelle Systemkonfiguration und die zu ersetzenden HW-, SW- Lizenzkomponenten.

Anmerkung: Die OCCLA-Platine mit V3-System kann bis zu 60 (+16) MEB-Kanäle aufnehmen. Bei der Migration auf die neue Platine wird die bestehende OCC-Konfiguration wiederhergestellt. Wenn Sie die Vorteile der zusätzlichen MEB-Kanäle nutzen möchten, sollten Sie Ihr System mit Hilfe der entsprechenden Assistenten/WBM-Seiten neu konfigurieren.

Module, die in Steckplatz 10 von OpenScape Business X5 Wandsystemen vorhanden sind, können nicht in Verbindung mit V3-Mainboards betrieben werden. Diese Module müssen durch Nachfolgemodule/-lösungen ersetzt werden.

Tabelle 33: Migration von OpenScape Business X - HW-/SW-Checkliste

Komponente	Ersetzt durch
Hardwarekomponenten	
Vorhandenes „V2-Mainboard“	V3-Mainboard (einfache oder erweitert, je nach Konfiguration)
UC Booster Card / Server (mit UC Suite)	Zusätzliche M.2 SSD
CMA-Modul	CMAe-Modul
EXMR-Modul für externe Ansagegeräte	V3-Mainboard (Audio-In-Buchse auf der Vorderseite)
S0-Schnittstellena auf dem V2-Mainboard	S0-Anschluss der S0-Peripheriekarte
X5W-Karten für Steckplatz 10 • SLCN16 • SLA16N • SLA24N	Ersetzt durch: • Schnurlose Direktverbindung • SLAV16 • SLAV16 + SLAV8
Optipoint 500 Telefone	OpenScape Deskphone CP Telefone

Komponente	Ersetzt durch
Optipoint 400 Telefone	
Softwarekomponenten	
V2 System-SW auf SDHC-Karte	V3 System-SW (Image vom Software Download Server)
VPN auf WAN im System beendet	VPN in externem Router beendet
XMPP	Keine Follow-on-Lösung
myPortal Smart	myPortal @work
Lizenzkomponenten	
Lizenzen in Lizenzdatei	Übertragung der Lizenzen in eine neue Lizenzdatei
Externe CSTA-Anwendungen (bisher lizenzfrei, da an UC Booster-Karte / Server HW angeschlossen)	Separate CSTA-Lizenz für den Anschluss externer Lösungen (nicht erforderlich für UC Suite, TAPI 170 und TAPI 120)

26.3.1 Migration von OpenScape Business X V2 zu OpenScape Business X V3

Bei der Migration eines OpenScape Business X-Modells von V2 zu V3 werden das Mainboard und die Systemsoftware ausgetauscht. Bestehende Lizenzen und die Kundenkonfiguration können übertragen werden. Der bestehende Software-Support wird nach der Migration unverändert fortgesetzt.

Bitte konfigurieren Sie vor der Migration, sofern noch nicht vorhanden, einen permanenten Zugriff auf den Unify Linzenz Server (über das Internet) im System und aktivieren Sie die Funktion „CLS Connect“. Dies vereinfacht die Lizenzübertragung und verkürzt die Migrationszeit erheblich. Der Kunde muss über den erforderlichen Zugriff vom OpenScape Business System auf den CLS informiert werden.

Voraussetzungen

Das System wird mit der letzten vor dem Upgrade veröffentlichten SW-Version V2R7 betrieben. Führen Sie bei Bedarf ein Upgrade des Systems auf die neueste SW-Version durch. Dazu muss das System über einen gültigen Software-Support-Status verfügen.

Für die Migration von V2 auf V3 sind je nachdem, ob CLS Connect, UC Suite oder externe CSTA-Anwendungen verwendet werden, die folgenden Komponenten erforderlich:

- V3-Mainboard
- V3 SW auf M.2 SATA SSD Datenspeicher
- M.2 SSD 256 GB Massendatenspeicher (optional mit UC Suite Anwendung)
- OpenScape Business V3 HW Migrationslizenz (falls CLS Connect nicht verwendet wird)
- OpenScape Business CSTA-Lizenz (optional)

Bedingungen und Einschränkungen für funktionale Grenzen

Bestehende Lizenzen können während der Migration vollständig vom bestehenden V2-Mainboard auf das V3-Mainboard übertragen werden. Die Lizenzübertragung ohne Aktivierung der CLS Connect Funktion erfordert die Lizenz „HW Migration“ und ist wesentlich aufwändiger und zeitintensiver als die Verwendung der CLS Connect Funktion.

Die Kundenkonfiguration und Kundendaten werden über einen Backup-/Restore-Prozess von der SW-Version V2 auf V3 migriert.

Die wichtigsten technischen Schritte der Migration werden in den folgenden Themen beschrieben. Um die bestehenden Lizenzen beizubehalten, wird hinsichtlich der Handhabung unterschieden zwischen:

- SW-Upgrade für permanente Lizenzierung mit und ohne CLS Connect
- SW-Upgrade mit PayGo-Lizenzierung

Anmerkung: Während der Migration vom V2-Mainboard zum V3-Mainboard werden die zusätzlichen EVM-Ports nicht zusätzlich in die SmartVM-Hunt-Gruppe aufgenommen. Dies erfordert eine manuelle Konfiguration, in deren Verlauf auch die COS-Einschränkung vorgenommen werden sollte.

Anmerkung: Bei einer Hardware-Migration von V2-Hardware, die mit einer nicht standardmäßigen DSP-IP-Adresse konfiguriert ist, auf ein V3-Hardwaresystem wird die DSP-IP-Adresse auf den Standardwert zurückgesetzt. Nach der Migration muss der Administrator die DSP-IP-Adresse und auch die FPGA-IP-Adresse entsprechend den spezifischen Kundenanforderungen manuell neu konfigurieren.

26.3.1.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf V3 migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor
   a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7
   b) Richten Sie im System einen Zugang zum zentralen Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung
   c) Aktivieren Sie CLS Connect im System

2) Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS)
   a) Übertragen Sie die bestehenden Lizenzen von der MAC-Adresse des V2-Mainboards mithilfe der Funktion **Neu generieren** auf die MAC-Adresse des V3-Mainboards
   b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse auf dem V3-Mainboard

3) Sichern Sie die V2-Systemkonfiguration und die Kundendaten.

4) Tauschen Sie die Mainboards

a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus

b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard

c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.

d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard

e) Schalten Sie die Versorgungsspannungen wieder ein

Das System startet automatisch.

5) Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein

a) Stellen Sie Systemdatum und -uhrzeit ein

b) Stellen Sie das Anwendungspaket ein

UC Smart für System ohne UC oder mit UC Smart

UC Suite für Systeme mit UC Suite

6) Stellen Sie die Systemkonfiguration wieder her

a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her

b) Importieren Sie die neu erstellte Lizenzdatei

26.3.1.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf V3 migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor

a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7

2) Erstellen Sie auf dem zentralen Lizenzserver (CLS) die „Migrations-Lizenzdatei“ für das V2-System

a) Aktivieren Sie die „HW-Migrationslizenz“ für das vorhandene System

b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse des V2-Mainboards.

Geben Sie dazu die MAC-Adresse des V3-Mainboards ein.

c) Laden Sie die Lizenzdatei vom CLS herunter

3) Importieren Sie die Lizenzdatei in das OpenScape Business V2-System

4) Notieren Sie den **Bestätigungscode**, der im OpenScape Business Assistant angezeigt wird

5) Generieren Sie auf dem zentralen Lizenzserver (CLS) einen neue Lizenzdatei für das V3-Mainboard

a) Erstellen Sie auf dem CLS eine neue Lizenzdatei für die MAC-Adresse des V3-Mainboards, indem Sie die MAC-Adresse des V2-Mainboards mit dem zuvor notierten Bestätigungscode erneut generieren

b) Suchen Sie auf dem CLS das OpenScape Business System mit der MAC-Adresse der V3-Mainboards.

c) Entsperren Sie das OpenScape Business System, indem Sie den Bestätigungscode eingeben und aktivieren

d) Generieren Sie die Lizenzdatei erneut

e) Laden Sie die neu generierte Lizenz vom CLS herunter

6) Sichern Sie die V2-Systemkonfiguration und die Kundendaten.

7) Tauschen Sie die Mainboards

a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus

a) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard

b) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.

c) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard

b) Schalten Sie die Versorgungsspannungen wieder ein

Das System startet automatisch.

8) Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein

a) Stellen Sie Systemdatum und -uhrzeit ein

b) Stellen Sie das Anwendungspaket ein

UC Smart für System ohne UC oder mit UC Smart

UC Suite für Systeme mit UC Suite

9) Stellen Sie die Systemkonfiguration wieder her

a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her

10) Importieren Sie nach dem Hochfahren des Systems manuell die neue Lizenzdatei in das V3-System

26.3.1.3 Wie Sie PayGo-lizenzierte Systeme auf V3 migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor

a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7

2) Sichern Sie die V2-Systemkonfiguration und die Kundendaten.

3) Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS) neu
   a) Generieren Sie erneut eine neue Lizenzdatei für die MAC-Adresse auf dem V3-Mainboard

      Übertragen Sie die bestehenden Lizenzen von der MAC-Adresse des V2-Mainboards auf die MAC-Adresse des V3-Mainboards.
   b) Laden Sie die neue Lizenzdatei vom CLS herunter

4) Tauschen Sie die Mainboards
   a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus
   b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard
   c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.
   d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard
   e) Schalten Sie die Versorgungsspannungen wieder ein

      Das System startet automatisch.

5) Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein
   a) Stellen Sie Systemdatum und -uhrzeit ein
   b) Stellen Sie das Anwendungspaket ein

      UC Smart für System ohne UC oder mit UC Smart

      UC Suite für Systeme mit UC Suite

6) Stellen Sie die Systemkonfiguration wieder her
   a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her

7) Importieren Sie manuell die neue Lizenzdatei in das V3-System und aktivieren Sie die Lizenzdatei

26.4 OpenScape Business X V3 System von einem V2-Mainboard auf ein V3-Mainboard migrieren

In diesem Szenario wird das bestehende V2-Mainborard des OpenScape Business Systems und möglicherweise vorhandene UC Booster HW mit einem V3-Mainboard ersetzt. Das System wurde zuvor auf die SW-Version V3 aktualisiert, z. B. im Zuge des SW-Supports.

Bestehende Lizenzen und die Kundenkonfiguration können übertragen werden. Der bestehende Software-Support wird nach der Migration unverändert fortgeführt.

Eine möglicherweise vorhandene UC Booster Card oder ein UC Booster Server sind in Verbindung mit dem V3-Mainboard nicht mehr notwendig. Zu diesem Zweck wird auf dem V3-Mainboard ein zusätzlicher Massenspeicher verwendet.

In Tabelle 33: Migration von OpenScape Business X - HW-/SW-Checkliste auf Seite 1395 finden Sie Informationen, welche Komponenten durch die Verwendung des V3-Mainboards ersetzt oder ersatzlos gestrichen wurden. Eine CSTA-Lizenz ist für eine bestehende Verbindung zu externen CSTA-Applikationen erforderlich. Das gilt nicht für die Verbindung zu OpenScape TAPI 170 oder TAPI 120.

Voraussetzungen

Das System wird vor der Aktualisierung mit der zuletzt veröffentlichten SW-Version V2R7 betrieben. Aktualisieren Sie ggf. das System auf die neueste SW-Version. Dazu muss das System über einen gültigen Software-Support-Status verfügen.

Für die Migration ist Folgendes erforderlich, je nachdem, ob CLS Connect, UC Suite oder externe CSTA-Applikationen verwendet werden:

- V3-Mainboard
- V3 SW auf M.2 SATA SSD-Datenspeicher
- M2 SSD 256 GB Massenspeicher (optional mit Applikation UC Suite)
- OpenScape Business V3 HW-Migrationslizenz (optional)
- OpenScape Business CSTA-Lizenz (optional)

Bedingungen und Einschränkungen für funktionale Grenzen

Im Verlauf der Migration können bestehende Lizenzen vom vorhandenen V2-Mainboard vollständig auf das V3 Mainboard übertragen werden. Die Lizenzübertragung ohne Aktivierung der Funktion CLS Connect erfordert die Lizenz „HW-Migration“ und eine viel komplexere Handhabung und mehr Zeitaufwand als die Verwendung der Funktion CLS Connect.

Die Kundenkonfiguration und die Kundendaten werden über den Sicherungs-/Wiederherstellungsprozess übertragen.

Die wichtigsten technischen Schritte der Migration werden in den folgenden Abschnitten beschrieben. Um die bestehenden Lizenzen beizubehalten, wird folgende Unterscheidung in der Handhabung gemacht:

- SW-Aktualisierung für permanente Lizenzierung mit und ohne CLS Connect
- SW-Aktualisierung mit PayGo-Lizenzierung

Anmerkung: Bei der Migration von V2 Mainboard auf V3 Mainboard werden die zusätzlichen EVM-Ports nicht zusätzlich in den SmartVM-Sammelanschluss aufgenommen. Dies erfordert eine manuelle Konfiguration, in deren Verlauf man auch die COS-Einschränkung vornehmen sollte.

Die Konvertierung eines KDS in derselben Softwareversion in einen anderen Systemtyp wird von Manager E nicht unterstützt. Wenn Sie nur die KDS-Daten verwenden möchten, können Sie die folgenden Schritte versuchen:

- Führen Sie eine vollständige Migration von einem V2-Mainboard zu einem V3-Mainboard-System durch.
- Laden Sie das V3-Mainboard-System KDS mit Manager E herunter und speichern Sie es lokal.
- Laden Sie das V3-Mainboard-System neu.
- Laden Sie das zuvor gespeicherte V3-Mainboard-KDS in Ihr V3-Mainboard-System hoch.

Das V3-Mainboard-System verwendet die KDS-Datenbankkonfiguration und Sie können mit der manuellen UC-Konfiguration fortfahren.

Anmerkung: Die Migration des KDS des V2-Mainboard-Systems auf das V3-Mainboard-System wird nicht unterstützt,

da die Datenbank des V2-Mainboards nicht mit der Datenbank des V3-Mainboards kompatibel ist.

26.4.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf ein V3-Mainboard migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor
   a) Richten Sie im System einen Zugang zum zentralen Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung
   b) Aktivieren Sie CLS Connect im System

2) Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS)
   a) Übertragen Sie die bestehenden Lizenzen von der MAC-Adresse des V2-Mainboards mithilfe der Funktion **Neu generieren** auf die MAC-Adresse des V3-Mainboards
   b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse auf dem V3-Mainboard

3) Sichern Sie die V3-Systemkonfiguration und die Kundendaten.

4) Erstellen Sie ggf. eine Sicherung der Booster Server-Konfiguration.

5) Tauschen Sie die Mainboards
   a) Fahren Sie das System herunter und schalten Sie alle Stromversorgungen aus
   b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard
   c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.
   d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard
   e) Schalten Sie die Versorgungsspannungen wieder ein

   Das System startet automatisch.

6) Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein
   a) Stellen Sie Systemdatum und -uhrzeit ein
   b) Stellen Sie das Anwendungspaket ein

   UC Smart für System ohne UC oder mit UC Smart

   UC Suite für Systeme mit UC Suite

7) Stellen Sie die Systemkonfiguration wieder her
   a) Importieren Sie die neu erstellte Lizenzdatei
   b) Stellen Sie mithilfe der Wiederherstellungsfunktion die Systemsicherung und ggf. die Booster Server-Sicherung wieder her

26.4.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf ein V3-Mainboard migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1) Erstellen Sie auf dem zentralen Lizenzserver (CLS) die „Migrations-Lizenzdatei“ für das vorhandene V2-Mainboard

a) Aktivieren Sie die „HW-Migrationslizenz“ für das vorhandene System

b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse des V2-Mainboards

Dazu muss die MAC-Adresse des V3-Mainboards eingegeben werden.

c) Laden Sie die Lizenzdatei vom CLS herunter

2) Importieren Sie die Lizenzdatei in das OpenScape Business System mit V2-Mainboard.

3) Notieren Sie den **Bestätigungscode**, der im OpenScape Business Assistant angezeigt wird

4) Generieren Sie auf dem zentralen Lizenzserver (CLS) einen neue Lizenzdatei für das V3-Mainboard

a) Erstellen Sie auf dem CLS eine neue Lizenzdatei für die MAC-Adresse des V3-Mainboards, indem Sie die MAC-Adresse des V2-Mainboards mit dem zuvor notierten Bestätigungscode erneut generieren.

a) Suchen Sie auf dem CLS das OpenScape Business System mit der MAC-Adresse der V3-Mainboards.

b) Entsperren Sie das OpenScape Business System, indem Sie den Bestätigungscode eingeben und aktivieren

c) Generieren Sie die Lizenzdatei erneut

b) Laden Sie die neu generierte Lizenz vom CLS herunter.

5) Sichern Sie die Systemkonfiguration und die Kundendaten.

6) Tauschen Sie die Mainboards

a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus

b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard

c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.

d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard

e) Schalten Sie die Versorgungsspannungen wieder ein

Das System startet automatisch.

7) Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein

a) Stellen Sie Systemdatum und -uhrzeit ein

b) Stellen Sie das Anwendungspaket ein

UC Smart für System ohne UC oder mit UC Smart

UC Suite für Systeme mit UC Suite

8) Stellen Sie nach dem Hochfahren des Systems die Systemkonfiguration wieder her

a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her

9) Importieren Sie nach dem Hochfahren des Systems manuell die neue Lizenzdatei in das V3-System

26.4.3 Wie Sie PayGo-lizenzierte Systeme auf ein V3-Mainboard migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1) Sichern Sie die Systemkonfiguration und die Kundendaten.

2) Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS) neu

a) Generieren Sie erneut eine neue Lizenzdatei für die MAC-Adresse auf dem V3-Mainboard

Übertragen Sie die bestehenden Lizenzen von der MAC-Adresse des V2-Mainboards auf die MAC-Adresse des V3-Mainboards.

b) Laden Sie die neue Lizenzdatei vom CLS herunter

3) Tauschen Sie die Mainboards

a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus

b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard

c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.

d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard

e) Schalten Sie die Versorgungsspannungen wieder ein

Das System startet automatisch.

4) Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein

a) Stellen Sie Systemdatum und -uhrzeit ein

b) Stellen Sie das Anwendungspaket ein

UC Smart für System ohne UC oder mit UC Smart

UC Suite für Systeme mit UC Suite

5) Stellen Sie nach dem Hochfahren des Systems die Systemkonfiguration wieder her

a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her

6) Importieren Sie manuell die neue Lizenzdatei in das V3-System und aktivieren Sie die Lizenzdatei

26.5 Software-Aktualisierung von OpenScape Business S

Bestimmen Sie vor der Aktualisierung der OpenScape Business S System-Software die aktuelle Systemkonfiguration und ggf. die zu ersetzenden HW-/SW- und Lizenzkomponenten.

Tabelle 34: Migration von OpenScape Business S - HW-/SW-Checkliste

Komponenten	Ersetzt durch
Hardwarekomponenten	

Komponenten	Ersetzt durch
Server-PC	Wiederverwendung ist möglich. Die HW-Anforderungen müssen für OpenScape Business S-Erweiterungen geprüft werden.[11]
Optipoint 400 Telefone	OpenScape Deskphone CP Telefone
Softwarekomponenten	
Betriebssystem SLES12	Wiederverwendung ist möglich. Schließlich ist eine Aktualisierung auf das neueste Service Pack erforderlich[12]
V2 System-SW auf SDHC-Karte	V3 System-SW (Image vom Software Download Server)
XMPP	Keine Follow-on-Lösung
myPortal Smart	myPortal @work
Lizenzkomponenten	
Lizenzen in Lizenzdatei	Übertragung der Lizenzen in eine neue Lizenzdatei
CSTA-Applikation (über UC Booster Card / Server)	CSTA-Applikation (über UC Booster Card / Server)

26.5.1 Software-Aktualisierung von OpenScape Business S V2 auf OpenScape Business S V3

Bei der Aktualisierung eines OpenScape Business S-Modells von SW-Version V2 auf V3 wird nur die System-SW ausgetauscht.

Bestehende Lizenzen und die Kundenkonfiguration werden übernommen. Der bestehende Software-Support wird nach der Migration unverändert fortgeführt.

---

11 Die bestehende PC-HW kann verwendet werden, wenn das UC Booster Server System nach der SW-Aktualisierung unverändert bleibt. Wenn nach der SW-Aktualisierung Erweiterungen geplant sind, müssen die Hardwareanforderungen ggf. gemäß den Spezifikationen in *OpenScape Business S Installationsanleitung, Kapitel Voraussetzungen* angepasst werden.

12 Das auf dem Server-PC installierte SLES-Betriebssystem kann im Fall einer SW-Aktualisierung von OpenScape Business S/UC Booster Server angepasst werden. Allerdings sollte vor der SW-Aktualisierung auf das letzte veröffentlichte Service Pack aktualisiert werden.

Wenn Novell den SW-Support für die verwendete SLES-Version eingestellt hat, muss der Kunde informiert und ggf. eine SLES-Aktualisierung verkauft werden.

Die SLES-Aktualisierung muss möglicherweise in mehreren Schritten durchgeführt werden, um bestehende Installationen von OpenScape Business S gemeinsam mit der Kundenkonfiguration und den Kundendaten zu übernehmen. Ein vorhandener SLES Update Key bleibt mit einer SLES-Aktualisierung gültig. Seine Registrierung bei Novell muss jedoch ggf. vor der SLES-Aktualisierung aufgehoben werden, bevor er für das neue System erneut registriert wird.

Im Folgenden wird die SW-Aktualisierung von OpenScape Business unter Beibehaltung des SLES-Betriebssystems beschrieben.

In diesem Fall sind keine separaten Bestellpositionen für die System-SW-Aktualisierung von V2 auf V3 erforderlich.

Beachten Sie, dass die SW-Version V3 bestimmte Funktionen und Hardwarekomponenten nicht mehr unterstützt. In Tabelle 34: Migration von OpenScape Business S - HW-/SW-Checkliste auf Seite 1404 finden Sie Informationen darüber, welche Komponenten in Version V3 ersetzt werden und welche Komponenten ohne Ersatz entfallen. Das hängt von der Ausbaustufe des Kundensystems ab.

Voraussetzungen

Das System wird vor der Aktualisierung mit der zuletzt veröffentlichten SW-Version V2R7 betrieben. Aktualisieren Sie ggf. das System auf die neueste SW-Version. Dazu muss das System über einen gültigen Software-Support-Status verfügen.

Vor der Software-Aktualisierung von Version V2 auf V3 müssen Sie im System einen permanenten Zugang zum Unify-Lizenzserver einrichten (über das Internet) und die Funktion **CLS Connect** aktivieren.

Bedingungen und Einschränkungen für funktionale Grenzen

Bestehende Lizenzen können im Verlauf der SW-Aktualisierung nur übernommen werden, wenn die Funktion CLS Connect aktiviert ist.

Die Kundenkonfiguration und die Kundendaten werden beim SW-Aktualisierungsprozess von SW-Version V2 auf V3 automatisch übertragen.

Die wichtigsten technischen Schritte der Migration werden in den folgenden Kapiteln beschrieben. Um die bestehenden Lizenzen beizubehalten, wird folgende Unterscheidung in der Handhabung gemacht:

- SW-Aktualisierung für permanente Lizenzierung mit und ohne CLS Connect
- SW-Aktualisierung mit PayGo-Lizenzierung

Technische Abwicklung der Aktualisierung

Die wichtigsten technischen Schritte der Aktualisierung werden nachfolgend beschrieben. Es wird unterschieden zwischen

- Aktualisierung für permanente Lizenzierung mit CLS Connect
- Aktualisierung mit PayGo-Lizenzierung

26.5.1.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf V3 aktualisieren

Führen Sie folgende Migrationsschritte durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business V2 System vor
   a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7
   b) Richten Sie im System einen Zugang zum zentralen Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung
   c) Aktivieren Sie CLS Connect im V2-System

2) Bereiten Sie das SLES-Betriebssystem vor

Aktualisieren Sie das Betriebssystem von der in Verbindung mit OpenScape Business S verwendeten SLES-Version auf das zuletzt veröffentlichte Service Pack.

3) Aktualisieren Sie die OpenScape Business-Software

a) Führen Sie die Softwareaktualisierung auf V3 über OpenScape Business Assistant durch.

b) Die Systemkonfiguration wird automatisch auf V3 übertragen.

c) Bestehende Lizenzen werden auf V3 übertragen.

4) Die Lizenzdatei wird automatisch vom zentralen Lizenzserver (CLS) generiert

a) Nach dem Neustart des Systems überträgt das System die Information, dass die bestehenden Lizenzen mit Softwareversion 3 betrieben werden.

b) Der Lizenzserver generiert automatisch eine neue Lizenzdatei mit den V3-Informationen und überträgt sie zurück an das System.

26.5.1.2 Wie Sie PayGo-lizenzierte Systeme auf V3 aktualisieren

Führen Sie folgende Migrationsschritte durch:

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor

a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7

2) Bereiten Sie das SLES-Betriebssystem vor

Aktualisieren Sie das Betriebssystem von der in Verbindung mit OpenScape Business S verwendeten SLES-Version auf das zuletzt veröffentlichte Service Pack.

3) Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS) neu

a) Generieren Sie erneut eine neue Lizenzdatei für das V2-System

b) Laden Sie die neue Lizenzdatei vom CLS herunter

4) Importieren Sie die neue Lizenzdatei in das OpenScape Business V2-System und aktivieren Sie sie.

5) Aktualisieren Sie die OpenScape Business-Software

a) Führen Sie die Softwareaktualisierung auf V3 über OpenScape Business Assistant durch.

b) Die Systemkonfiguration wird automatisch auf V3 übertragen.

c) Das System ist nach einem Neustart betriebsbereit.

26.5.2 Software-Aktualisierung von OpenScape Business S V2 auf OpenScape Business S V3

Um ein OpenScape Business S V1 System auf ein OpenScape Business S V2 System zu aktualisieren, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

Voraussetzungen

Vor der Migration ist zu prüfen, ob die Hard- und Softwareeigenschaften des Linux-Servers für OpenScape Business S V2 ausreichend sind. Ggf. reicht eine Aktualisierung des Linux Servers aus (z. B. mehr verfügbarer Arbeitsspeicher). Das für OpenScape Business V2 veröffentlichte SLES 64-Bit-Linux-Betriebssystem ist eine Voraussetzung. Für den Aktualisierungsschritt auf OpenScape Business SW-Version V3 ist die für V3 veröffentlichte SLES 64-Bit-Version erforderlich.

Wird ein neuer Linux Server benötigt, ist nach der Linux-Installation die OpenScape Business V1 S Kommunikationssoftware zu installieren. Eine V1-Datensicherung kann übernommen werden und Sie können anschließend mit der Migration Schritt 1 fortfahren.

Bedingungen und Einschränkungen für funktionale Grenzen

Wenn das System von OpenScape Business V1 auf OpenScape Business V2 aktualisiert wird, ist eine ITSP-Aktivierung/Deaktivierung im Internet-Telefonie-Wizard erst dann möglich, wenn ein LCR-Reset durchgeführt wurde. Bereits in OpenScape Business V1 konfigurierte ITSPs funktionieren weiterhin in OpenScape Business V3 ohne LCR-Reset. Der bereits aktivierte ITSP kann bearbeitet jedoch nicht deaktiviert werden. Um im Wizard eine Änderung an der Aktivierung/Deaktivierung vorzunehmen, ist ein LCR-Reset erforderlich. Dies soll die nötigen Änderungen für die Erhöhung der ITSPs von 4 auf 8 widerspiegeln. Gehen Sie für das LCR-Reset zu **Experten-Modus** > **LCR** > **LCR-Flags** und klicken Sie auf das Flag **LCR-Daten zurücksetzen**.

Aktualisierungsvorgang

Führen Sie folgende Aktualisierungsschritte durch:

1) **OpenScape Business V1 Software aktualisieren**

   Aktualisieren Sie mithilfe des WBM die OpenScape Business V1 Software auf die Version V1 R3.3 oder höher (siehe Update des Kommunikationssystems auf Seite 1263).
2) **OpenScape Business V2 Lizenzdatei laden**

   Laden Sie die OpenScape Business V2 Lizenzdatei in das OpenScape Business V1 System und aktivieren Sie die Lizenzen (siehe Lizenzaktivierung (Standalone) auf Seite 314).

   Die Lizenz für die kostenfreien SLES Upgrades kann weiterhin genutzt werden.
3) **Aktuelle OS Biz V2 Software laden**

   Laden Sie mit Hilfe des WBM die aktuelle OpenScape Business V2 Software in das Kommunikationssystem. Die V1-Daten werden dabei automatisch in V3-Daten konvertiert (siehe Update des Kommunikationssystems auf Seite 1263).
4) **Datensicherung durchführen**

   Sichern Sie Ihre V2-Daten (siehe Sofortiges Sichern auf Seite 1256).

26.6 OpenScape Business V2 Netzwerk-Migration/-Aktualisierung auf V3

Bei der Migration oder Aktualisierung eines OpenScape Business Netzwerks auf V3 müssen alle Knoten im Netzwerk auf die SW-Version V3 aktualisiert

werden. Für die Netzwerkfunktionen ist es unerheblich, ob die SW-Version V3 auf einem OpenScape Business X System im Netzwerk mit einem V2-Mainboard oder einem V3-Mainboard betrieben wird.

Aktualisieren Sie jeden OpenScape Business Knoten im Netzwerk getrennt. Die für eine Aktualisierung erforderlichen Komponenten werden pro Knoten je nach den einzelnen Knoten gemäß den Beschreibungen in den Kapiteln Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390, Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393, Hardware/Software-Migration von OpenScape Business X Systemen auf V3 auf Seite 1395 oder OpenScape Business X V3 System von einem V2-Mainboard auf ein V3-Mainboard migrieren auf Seite 1400 bestimmt.

Die Lizenzen für die Knoten im V2-Netzwerk können über den zentralen Lizenzserver auf die V3-Systeme übertragen werden. Es gibt verschiedene Verfahren für Systeme mit der oder ohne die Funktion **CLS Connect**. Das Verfahren für die „Pay as yo go“-Lizenzierung wird im OpenScape Business Netzwerk nicht unterstützt.

Der erforderliche Aufwand für die Übertragung von Lizenzen mit **CLS Connect** ist in einem Netzwerk erheblich geringer als ohne die Funktion CLS Connect.

Wichtig: Aktualisieren Sie die Knoten in einem Netzwerk in der für jedes Szenario beschriebenen Reihenfolge. Es ist wichtig, dass alle Slave-Knoten mit der Softwareversion V3 betrieben werden, bevor der Master-Knoten auf die Softwareversion V3 migriert oder aktualisiert werden kann.

Während der Netzwerkaktualisierung kommt es zu einem heterogenen Netzwerk, auf dem vorübergehend die Software V2 und V3 läuft. Während dieser Zeit kann die volle Funktionalität des Leistungsspektrums im Netzwerk nicht garantiert werden. In einigen Szenarien arbeiten die aktualisierten/migrierten Systeme nur im Notbetrieb bis die Lizenzdatei vom Master-Knoten aktualisiert wird.

OpenScape Business Netzwerke können in verschiedenen Kombinationen in Bezug auf die Verwendung von OpenScape Business X und S Systemen und die Lizenzierung der Systeme im Netzwerk realisiert werden. Die wichtigsten Schritte für die Migration oder Aktualisierung eines OpenScape Business Netzwerks und ihre Reihenfolge werden anhand von typischen Kombinationen gezeigt.

Die Beschreibung geht immer davon aus, dass eine Netzwerklizenzdatei für das Netzwerk auf dem zentralen Lizenzserver vorhanden ist, durch die der Master-Knoten alle Slave-Knoten mit Lizenzinformationen versorgt.

- **Netzwerk nur bestehend aus OpenScape Business X Systemen**
  - Szenario 1: HW-Migration nur auf dem Master-Knoten, SW-Aktualisierung auf allen Slave-Knoten
  - Szenario 2: SW-Aktualisierung für alle OpenScape Business X Knoten im Netzwerk

- **Netzwerk bestehend aus OpenScape Business S und OpenScape Business X Systemen**
  - Szenario 3: OpenScape Business S ist Master-Knoten und OpenScape Business X Systeme sind Slave-Knoten
    - Szenario 3a: SW-Aktualisierung für alle OpenScape Business Knoten im Netzwerk
    - Szenario 3b: SW-Aktualisierung auf dem OpenScape Business S Master-Knoten, Migration der Slave-Knoten

26.6.1 Szenario 1: Hardware-Migration von Master-Knoten, Software-Aktualisierung von Slave-Knoten

Bei der Migration des Netzwerks muss unterschieden werden zwischen der Funktion **CLS Connect** und dem Lizenzübertragungsverfahren.

26.6.1.1 Migration/Aktualisierung mit CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Die Funktion **CLS Connect** ist auf dem Master-Knoten aktiviert. CLS Connect muss auf den Slave-Knoten nicht eingeschaltet werden.

Schritt für Schritt

1) Aktualisieren Sie alle Slave-Knoten auf die Softwareversion V3 (Details siehe Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 oder Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393)

a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.

b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.

Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.

2) Generieren Sie eine neue Netzwerklizenzdatei auf dem Lizenzserver.

a) Generieren Sie erneut die Netzwerklizenzdatei für die MAC-Adresse des V3-Mainboards

b) Laden Sie die neue Netzwerklizenzdatei vom CLS herunter

3) Migrieren Sie den Master-Knoten auf das V3-Mainboard (Details siehe Hardware/Software-Migration von OpenScape Business X Systemen auf V3 auf Seite 1395)

a) Sichern Sie die Systemkonfiguration über WBM

b) Tauschen Sie das Mainboard aus

c) Stellen Sie Datum/Uhrzeit und Anwendungspaket über WBM ein

d) Importieren und aktivieren Sie die neue Netzwerklizenzdatei über WBM.

e) Stellen Sie die Systemkonfiguration über WBM wieder her

Die Lizenzdatei wird in diesem Fall nicht überschrieben.

4) Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

26.6.1.2 Migration/Aktualisierung ohne CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Hardware-Migrationslizenz-für Master-Knoten ist verfügbar
- Software-Upgrade-Lizenzen sind für jeden Slave-Knoten verfügbar

Schritt für Schritt

1) Generieren Sie die neue Netzwerklizenzdatei auf dem Lizenzserver
   a) Unterteilen Sie die Netzwerkdatei auf dem CLS in einzelne Lizenzdateien
   b) Generieren Sie eine Lizenzdatei für den Master-Knoten
      Aktivieren Sie die Hardware-Migrationslizenz für den Master-Knoten
   c) Generieren Sie die Lizenzdatei für die Slave-Knoten
      Aktivieren Sie die Software-Upgrade-Lizenz für jeden einzelnen Slave-Knoten
   d) Führen Sie die einzelnen Knotenlizenzdateien zu einer neuen Netzwerklizenzdatei zusammen
   e) Laden Sie die neue Netzwerklizenzdatei vom CLS herunter
2) Aktualisieren Sie die Slave-Knoten auf V3 (Details siehe Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 oder Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393)
   a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
   b) Die Konfiguration und die Lizenzinformationen werden automatisch übertragen.

   Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.
3) Migrieren Sie den Master-Knoten nach V3 (Details siehe Hardware/Software-Migration von OpenScape Business X Systemen auf V3 auf Seite 1395)
   a) Sichern Sie die Systemkonfiguration über WBM
   b) Wechseln Sie das Mainboard
   c) Stellen Sie Datum/Uhrzeit und Anwendungspaket über WBM ein
   d) Importieren und aktivieren Sie die neue Netzwerklizenzdatei über WBM.
   e) Stellen Sie die Systemkonfiguration über WBM wieder her (die Lizenzdatei wird in diesem Fall nicht überschrieben)

4) Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

26.6.2 Szenario 2: Software-Aktualisierung aller Systeme im Netzwerk auf V3

Bei der Aktualisierung der Netzwerksoftware definiert die Verwendung der Funktion **CLS Connect** oder nicht das zu befolgende Verfahren für die Übertragung der Lizenz.

26.6.2.1 Software-Aktualisierung mit CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Die Funktion **CLS Connect** ist auf dem Master-Knoten aktiviert. CLS Connect muss auf den Slave-Knoten nicht eingeschaltet werden.

Schritt für Schritt

1) Migrieren Sie alle Slave-Knoten auf die Softwareversion V3 (Details siehe Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 oder Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393)
   a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
   b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.

   Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.
2) Aktualisieren Sie den Master-Knoten auf V3 (Details siehe Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 oder Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393
   a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
   b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
   c) Sie das System neu.

3) Die folgenden Schritte werden automatisch durchgeführt (kein manueller Eingriff erforderlich)
   a) Der Master-Knoten meldet sich nach dem Start am CLS mit der Softwareversion 3.
   b) Der CLS generiert eine neue Netzwerklizenzdatei.
   c) Der CLS überträgt die neue Netzwerklizenzdatei an den Master-Knoten.
   d) Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

26.6.2.2 Software-Aktualisierung ohne CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Software-Upgrade-Lizenzen sind für jeden Knoten verfügbar

Schritt für Schritt

1) Generieren Sie neue Netzwerklizenzdateien auf dem Lizenzserver
   a) Unterteilen Sie die Netzwerkdatei auf dem CLS in einzelne Lizenzdateien
   b) Generieren Sie eine Lizenzdatei für den Master-Knoten

      Aktivieren Sie die Software-Upgrade-Lizenz für den Master-Knoten
   c) Generieren Sie die Lizenzdatei für die Slave-Knoten

      Aktivieren Sie die Software-Upgrade-Lizenz für jeden einzelnen Slave-Knoten
   d) Führen Sie die einzelnen Knotenlizenzdateien zu einer neuen Netzwerklizenzdatei zusammen
   e) Laden Sie die neue Netzwerklizenzdatei vom CLS herunter
2) Migrieren Sie alle Slave-Knoten auf V3 (Details siehe Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 oder Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393)
   a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
   b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
   c) Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.

   Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.
3) Aktualisieren Sie den Master-Knoten auf V3 (Details siehe Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 oder Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393
   a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.

b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
c) Importieren Sie die Netzwerklizenzdatei in den Master-Knoten und aktivieren Sie die Lizenzdatei

4) Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

26.6.3 Szenario 3a: Software-Aktualisierung aller Knoten

In diesem Szenario ist der Master-Knoten ein OpenScape Business S System und die Slave-Knoten sind OpenScape Business X Systeme.

Dieses Szenario ist identisch mit Szenario 2: Software-Aktualisierung aller Systeme im Netzwerk auf V3 auf Seite 1412

26.6.4 Szenario 3b: Software-Aktualisierung auf dem Master-Knoten, Hardware-Migration auf den Slave-Knoten

In diesem Szenario werden die Slave-Knoten durch einen HW-/SW-Austausch auf das V3-Mainboard und die SW-Version 3 migriert. Im OpenScape Business S Master-System wird die SW von V2 auf V3 aktualisiert. Für die HW-/SW-Aktualisierung des Netzwerks definiert die Verwendung der Funktion CLS Connect das Lizenzübertragungsverfahren.

26.6.4.1 Migration/Aktualisierung mit CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Die Funktion **CLS Connect** ist auf dem Master-Knoten aktiviert. CLS Connect muss auf den Slave-Knoten nicht eingeschaltet werden.
- Die V3-Mainboards einschließlich der V3-Software sind verfügbar.

Schritt für Schritt

1) Migrieren Sie alle Slave-Knoten auf das V3-Mainboard (Details siehe Hardware/Software-Migration von OpenScape Business X Systemen auf V3 auf Seite 1395)
a) Sichern Sie die Systemkonfiguration über WBM
b) Ersetzen Sie die Mainboards
c) Stellen Sie Datum/Uhrzeit und Anwendungspaket über WBM ein
d) Stellen Sie die Systemkonfiguration über WBM wieder her

Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.

2) Aktualisieren Sie den Master-Knoten auf V3 (Details siehe Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 oder Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393
   a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
   b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
   c) Sie das System neu.
3) Die folgenden Schritte werden automatisch durchgeführt (kein manueller Eingriff erforderlich)
   a) Der Master-Knoten meldet sich nach dem Start am CLS mit der Softwareversion 3.
   b) Der CLS generiert eine neue Netzwerklizenzdatei.
   c) Der CLS überträgt die neue Netzwerklizenzdatei an den Master-Knoten.
   d) Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

26.6.4.2 Migration/Aktualisierung ohne CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Die Software-Upgrade-Lizenz für den Master-Knoten ist verfügbar
- Hardware-Migrationslizenzen sind für jeden Slave-Knoten verfügbar
- Die V3-Mainboards einschließlich der V3-Software sind verfügbar.

Schritt für Schritt

1) Generieren Sie eine neue Netzwerklizenzdatei auf dem Lizenzserver
   a) Unterteilen Sie die Netzwerkdatei auf dem CLS in einzelne Lizenzdateien
   b) Generieren Sie eine Lizenzdatei für den Master-Knoten
      Aktivieren Sie die Software-Upgrade-Lizenz für den Master-Knoten
   c) Generieren Sie die Lizenzdatei für die Slave-Knoten
      Aktivieren Sie die Hardware-Migrationslizenz für jeden Slave-Knoten
   d) Führen Sie die einzelnen Knotenlizenzdateien zu einer neuen Netzwerklizenzdatei zusammen
   e) Laden Sie die neue Netzwerklizenzdatei vom CLS herunter

2) Migrieren Sie alle Slave-Knoten auf das V3-Mainboard (Details siehe Hardware/Software-Migration von OpenScape Business X Systemen auf V3 auf Seite 1395)

a) Sichern Sie die Systemkonfiguration über WBM
b) Ersetzen Sie die Mainboards
c) Stellen Sie Datum/Uhrzeit und Anwendungspaket über WBM ein
d) Stellen Sie die Systemkonfiguration über WBM wieder her

Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.

3) Aktualisieren Sie den Master-Knoten auf V3 (Details siehe Software-Aktualisierung für OpenScape Business X Systeme auf Seite 1390 oder Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3 auf Seite 1393

a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
c) Importieren Sie die Netzwerklizenzdatei in den Master-Knoten und aktivieren Sie die Lizenzdatei

4) Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

26.7 Migration von HiPath 3000 auf OpenScape Business V3

Beschrieben wird die technische Migration von HiPath 3000 / 500 V9 Standalone-Systemen und HiPath 3000 Netzverbunden auf OpenScape Business V3 mit V3-Mainboards.

Bei der Migration von HiPath 3000 Systemen nach OpenScape Business X V3 mit V3-Mainboards kann je nach Hardwarekonfiguration ein Teil der Hardwareausstattung des Systems und der angeschlossenen Terminals/Clients übertragen werden.

Vor der Migration von HiPath 3000 müssen die aktuelle Systemkonfiguration sowie ggf. die zu ersetzenden HW-/SW- und Lizenzkomponenten durch wiederholte Prüfungen bestimmt werden.

Allgemeine Prüfungen

- **Funktions-Kompatibilitätscheck**

  Bitte informieren Sie sich, welche Funktionen gegenüber HiPath 3000 V9 nicht mehr unterstützt werden oder sich geändert haben. Kapitel Geänderte/gestrichene Leistungsmerkmale und Schnittstellen von HiPath 3000 auf Seite 1440 listet die Funktionen von HiPath 3000 auf, die in OpenScape Business nicht mehr unterstützt werden oder durch neuere Funktionen ersetzt wurden.

- **Prüfung der Softwareversion**

  Das System muss vor der Migration unter SW-Version V9 betrieben werden. Systeme mit einer SW-Version vor V9 müssen vor der Migration auf SW-Version V9 aktualisiert und in Betrieb genommen werden.

- **Prüfung der Schutzerdung**

  Für alle OpenScape Business X Kommunikationssysteme ist eine Schutzerdung über einen zusätzlichen Schutzleiter zwingend erforderlich!

Hardware-Kompatibilitätscheck

Einige Module und Endgeräte können aus technischen Gründen nicht in den OpenScape Business X Systemen eingesetzt werden. Bei der Migration von HiPath 3000 V9 auf OpenScape Business V3 müssen diese Module und Terminals entfernt werden. Verwenden Sie bei Bedarf stattdessen die jeweiligen Nachfolgetypen. Die Liste der nicht mehr unterstützten Module und deren Nachfolger finden Sie in der *OpenScape Business X3/X5/X8 Servicedokumentation* im Abschnitt *Nicht unterstützte HW-Komponenten*.

- **Netzteil**

  OpenScape Business 33xx / 35xx kann mit UPSC-D/DR- oder OCPSM-Netzteil betrieben werden. Verbleibende PSU-Netzteile müssen mit OCPSM ersetzt werden. Geeignete PSU-Upgrade-Kits sind erhältlich.
- **Peripheriekomponenten**

  Bitte überprüfen Sie, ob die vorhandene Hardware weiterhin verwendet werden kann. Nicht mehr unterstützte Module und Endgeräte müssen entfernt oder ggf. durch Nachfolger ersetzt werden.
- **Backplane-Prüfung**

  In HiPath 3550 Systemen wird Steckplatz 10 der Backplane nicht mehr vom V3-Mainboard angesprochen. Vorhandene Peripheriemodule, die diesen Steckplatz nutzen, können in OpenScape Business nicht betrieben werden.
- **Prüfung der Telefongeräte**

  OpenScape Business V3 Systeme mit V3-Mainboards unterstützen analoge, ISDN-, SIP- und OpenStage oder OpenScape Deskphone IP-/CP-Geräte. Vorhandene Optiset E-, Optipoint 4xx- und Optipoint 5xx-Geräte müssen ersetzt werden.
- **Gehäuseprüfung**

  Bei migrierten HiPath 33xx/35xx Systemen müssen gegebenenfalls die Gehäusedeckel ausgetauscht und Lüftereinheiten installiert werden.

  Entsprechende Lieferpositionen sind erhältlich.

Sonstige Prüfungen

- **Rufnummernplan für vernetzte Systeme**

  Bei reiner Sprachvernetzung ist die offene und die geschlossene Nummerierung möglich. Bei Nutzung von UC Suite ist eine geschlossene Nummerierung im Netzwerk erforderlich (netzweite UC-Funktionalität).

26.7.1 Migration von HiPath 33xx, 35xx, 3800 nach OpenScape Business X3/X5/X8 V3

Bei der Migration eines HiPath 33xx, 35xx oder 3800 Systems nach OpenScape Business X V3 werden das Mainboard, die ermittelten Peripheriegruppen und Endgeräte sowie die System-SW ersetzt. Vorhandene Lizenzen können mit einer Upgrade-Lizenz migriert werden. Die

Systemkonfiguration kann übertragen werden. Nach der Migration hat das OpenScape Business V3 System 3 Jahre lang Software-Support.

Für die Migration von HiPath 3000 V9 nach OpenScape Business V3 sind grundsätzlich folgende Punkte erforderlich:

- V3-Mainboard
- V3 SW auf SSD-Datenspeicher
- M2 SSD 256 GB Massendatenspeicher (optional mit UC Suite-Anwendung)
- OpenScape Business Upgrade HiPath 3000 V9 (Lizenzmigration) oder
- OpenScape Business Upgrade HiPath 3000 V8 (Lizenzmigration) oder
- OpenScape Business Upgrade HiPath 3000 V7 (Lizenzmigration)
- OpenScape Business CSTA-Lizenz (optional)

Bei Bedarf müssen zusätzliche Hardwarekomponenten und Lizenzen bestellt werden. Das hängt von der Konfiguration des Kundensystems ab.

In der *OpenScape Business X3/X5/X8 Servicedokumentation* im Abschnitt *Nicht unterstützte HW-Komponenten* finden Sie Informationen darüber, welche Komponenten in der Version V3 ersetzt werden oder ersatzlos entfallen. Bitte beachten Sie, dass eine CSTA-Lizenz für eine bestehende Verbindung zu externen CSTA-Applikationen erforderlich ist. Das gilt nicht für die Verbindung zu OpenScape Business TAPI 170 oder TAPI 120.

Voraussetzungen

Alle HW-/SW-Komponenten wurden auf Wiederverwendbarkeit geprüft.

Alle neuen HW-/SW-Komponenten sind verfügbar

Eine Upgrade-Lizenz für die Aktualisierung von HiPath 3000 V7, V8 oder V9 auf OpenScape Business V3 wurde bestellt und der LAC der Upgrade-Lizenz ist vorhanden, um die neue Lizenz vom Lizenzserver abzurufen.

Das System wurde für die technische SW-Migration der Kundenkonfiguration auf die neueste SW-Version V9 aktualisiert.

Die neueste Version des Manager E wird verwendet

OpenScape Business Lizenzen während der Migration bestimmen

Die vorhandenen Lizenzen in HiPath 3000 können durch Aktivierung der Lizenz „OpenScape Business Upgrade HiPath 3000 (V7, V8 oder V9)“ auf dem zentralen Lizenzserver auf das OpenScape Business V3 System übertragen werden. Während der Lizenzübertragung wird eine neue Lizenzdatei für das OpenScape Business V3 System mit den folgenden Lizenzen erstellt:

Tabelle 35: HiPath 3000 Lizenzmigration

HP 3000 Lizenz	OpenScape Business Lizenz	Hinweise
	Basislizenz	Neu erstellt inkl. 3 Jahre SW-Support
	OpenDirectory Basislizenz	Neu erstellt
	Web Collaboration Connector Lizenz	Neu erstellt

HP 3000 Lizenz	OpenScape Business Lizenz	Hinweise
	TDM Benutzerlizenz	Anzahl berechnet aus der Systemkonfiguration[13]
IP-Teilnehmer (ComScendo)	IP Benutzerlizenz	1:1-Übertragung von HP 3000 Lizenzdatei
	TDM Benutzerlizenzierung	berechnet aus der Systemkonfiguration[13]
S2M-Kanäle	IP/S2M/TI Trunk-Leitungslizenzen	1:1-Übertragung von HP 3000 Lizenzdatei
Mobility Entry	Mobility Benutzerlizenzen	1:1-Übertragung von HP 3000 Lizenzdatei

Bestimmung der TDM Benutzerlizenzen innerhalb der Lizenzdatei

Während der technischen Konvertierung der HiPath 3000 Systemkonfiguration wird die Anzahl der aktiven TDM-Teilnehmer vom Tool Manager E bestimmt und in eine „Inventardatei (XML)“ geschrieben.

Die Anzahl der TDM User Lizenzen wird nach folgenden Regeln ermittelt:

- 1x TDM User Lizenz pro aktivem UP0-Port - Telefon (Master/Slave) bereit, Rufnummer verfügbar
- 1x TDM User Lizenz pro registriertem DECT-Telefon - Rufnummer verfügbar
- 1x TDM User Lizenz pro aktivem a/b-Port (Rufnummer) für gesteckte Baugruppen
- 1x TDM User Lizenz pro aktivem S0-Port (Rufnummer) für aktive Baugruppen

Die Migration der TDM Benutzerlizenz selbst wird offline am CLS über die XML-Inventardatei ausgeführt.

Der zentrale Lizenzserver prüft, ob eine Lizenzdatei für die MAC-Adresse des HiPath 3000 Mainboards vorhanden ist.

Wenn eine Lizenzdatei vorhanden ist, wird die Lizenzmigration auf Basis dieser Lizenzdatei und der Informationen in der „Inventardatei“ durchgeführt.

Wenn keine Lizenzdatei vorhanden ist, wird die Aktualisierung von OpenScape Business auf Basis der XML-„Inventardatei“ durchgeführt.

Je nach vorhandener Upgrade-Lizenz (V7, V8 oder V9) wird der folgende Prozentsatz der ermittelten TDM-Benutzer in OpenScape Business übernommen.

- Aktualisierung von HiPath 3000 V4 oder älter auf OpenScape Business V3:

  TDM-Nutzer werden nicht für günstigere / kostenlose OpenScape Business-Upgrade-Lizenzen berechnet

[13] Ermittelt im Zuge der technischen Umstellungsbeschreibung siehe unten.

- Aktualisierung von HiPath 3000 V5, V6 oder V7 auf OpenScape Business V3:

  70% der TDM-Benutzer werden für günstigere/kostenlose OpenScape Business Upgrade-Lizenzen berechnet
- Aktualisierung von HiPath 3000 V8 auf OpenScape Business V3:

  80% der TDM-Benutzer werden für günstigere/kostenlose OpenScape Business Upgrade-Lizenzen berechnet
- Aktualisierung von HiPath 3000 V9 OpenScape Business V3:

  100% der TDM-Benutzer werden für günstigere/kostenlose OpenScape Business Upgrade-Lizenzen berechnet.

Bedingungen und Einschränkungen für funktionale Grenzen

- Die Lizenzmigration kann nur auf V3 erfolgen. Eine Lizenzmigration auf V2 wird vom Manager E nicht unterstützt.
- Die Lizenzmigration eines HiPath 3000 Systems (Mainboard) kann nur einmal durchgeführt werden und das Mainboard ist für weitere Aktionen nach der Migration am CLS gesperrt.
- Um S2M-Leitungen und ComScendo-Teilnehmer zu migrieren, muss eine HiPath 3000 Lizenzdatei auf dem zentralen Lizenzserver verfügbar sein.
- Die während der Migration generierten TDM-Benutzerlizenzen können nicht auf andere Systeme oder auf ein CLS-Konto übertragen werden.
- Benutzerlizenzen und UC benutzerbezogene Lizenzen werden Benutzern in OpenScape Business permanent zugewiesen. Bitte beachten Sie, dass für Benutzer von myAgent und myAttendant eine ausreichende Anzahl an Lizenzen zur Verfügung steht. In OpenScape Business sind Änderungen im Präsenzstatus anderer Benutzer durch Benutzer von myAgent an die myAttendant Lizenz gebunden. Diese sind separat zu bestellen.
- Das Leistungsmerkmal Deskshare User (IP-Moblity) ist in OpenScape Business lizenzpflichtig im Gegensatz zur HiPath 3000. Zusätzliche IP-Benutzerlizenzen müssen im OpenScape Business Assistant Lizenzierungsdialogfeld für die „Deskshare User“ vorhanden und diesen zugewiesen sein.

- Für folgende Produkte und Funktionen wird keine Lizenzmigration durchgeführt:
  - HG1500 B-Kanäle: Baugruppe entfällt, die Funktionalität ist auf dem neuen Mainboard integriert.
  - optiClient Attendant V8: läuft nicht an OpenScape Business.

    Nachfolgeprodukt: OpenScape Business Attendant
  - optiClient BLF V1/V2: läuft nicht an OpenScape Business.

    Nachfolgeprodukt: OpenScape Business BLF
  - HiPath TAPI 120/170 V2: läuft nicht an OpenScape Business.

    Nachfolgeprodukt: OpenScape Business TAPI 120/170
  - Entry VoiceMail: Modul entfällt, die Funktionalität ist auf dem neuen Mainboard integriert.

    Nachfolgeprodukt: Smart Voicemail
  - myPortal entry Web Services Communications Clients auf dem Plug PC.
  - Basisstationen: Lizenzen für Basisstationen werden nicht mehr benötigt.
  - ITSP-Amtszugang: für die Nutzung von ITSP-Kanälen für die Internet-Telefonie sind in OpenScape Business Lizenzen zu kaufen.
  - Für S0-Amt, Analog-Amt und CAS-Amt werden weiterhin keine Lizenzen benötigt.
  - Für Vernetzungen und Anbindung von Fremdsystemen über Querleitungen ist pro Knoten in OpenScape Business eine Networking-Lizenz zu kaufen.

Technische Abwicklung

Führen Sie folgende Migrationschritte der Reihe nach durch:

1) HiPath 3000 Kundendatenbank (KDS) aus dem System herunterladen

Laden Sie mit Hilfe der neuesten Version von Manager E den aktuellen HiPath 3000 KDS aus dem HiPath 3000 System herunter.

2) HG1500 Einstellungen notieren (optional)

Sind eine oder mehrere HG1500 Baugruppen gesteckt, müssen Sie sich die HG1500-Einstellungen, die in Bezug auf die Standard-Einstellungen geändert wurden, mit Hilfe des HG1500-WBM notieren:

- IP-Routing
- PSTN-Routing
- IP-Firewall
- MAC-Firewall
- Application Firewall
- IP-Accounting
- IP-Mapping
- SNMP

3) HiPath 3000 KDS konvertieren

Konvertieren Sie mit Hilfe der neuesten Version von Manager E den aktuellen HiPath 3000 KDS in den OpenScape Business V3 KDS.

4) Hardware austauschen

Tauschen Sie das HiPath 3000 Mainboard gegen das neue OpenScape Business V3-Mainboard aus. Entfernen Sie auch alle HG1500 Baugruppen und alle nicht mehr unterstützten Unterbaugruppen. Alle OpenScape

Business Kommunikationssysteme sind mit einem zusätzlichen Schutzleiter zu erden.

5) **Erstinstallation durchführen**

   Konfigurieren Sie das Kommunikationssystem über das WBM mit dem Wizard **Erstinstallation**. Berücksichtigen Sie dabei auch die HG1500 Einstellungen, die Sie sich vorher notiert haben.

6) **Konvertierten KDS laden**

   Laden Sie den konvertierten KDS mit Hilfe der neuesten Version von Manager E in das OpenScape Business V2 System. Anschließend startet das OpenScape Business System automatisch neu.

7) **Neue Lizenzdatei am CLS generieren**

   Generieren Sie am CLS eine neue Lizenzdatei mit dem LAC der Upgrade-Lizenz, der Konfigurationsdatei (XML-Datei) und der Locking-ID von OpenScape Business.

8) **Lizenzen aktivieren und zuordnen**

   Lizenzieren Sie das OpenScape Business Kommunikationssystem innerhalb von 30 Tagen mit Hilfe der Lizenzdatei.

9) **LCR-Einträge zurücksetzen**

   Bei Bedarf können Sie die im HiPath 3000 System konfigurierten LCR-Einträge (z. B. Wahlpläne, Wegetabellen, Wahlregeln) auf die Standardeinträge von OpenScape Business zurücksetzen. Diese Einstellung finden Sie im WBM im Wizard **Basisinstallation**.

26.7.1.1 Wie Sie den KDS aus HiPath 3000 laden

Voraussetzungen

Ein HiPath 3000 Kommunikationssystem (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 oder HiPath 3800) ist vorhanden.

Alle Telefone sind angeschlossen und aktiv.

Der neueste Manager E ist auf dem Admin-PC installiert.

Der Admin-PC ist mit dem HiPath 3000 Kommunikationssystem verbunden.

Schritt für Schritt

1) Melden Sie sich auf dem Admin-PC am Manager E an.
2) Klicken Sie in der Menüleiste auf **Datei** > **Übertragen**.
3) Klicken Sie auf die Registerkarte **Kommunikation**.
4) Aktivieren Sie im Bereich **Zugang** die entsprechende Option, je nach Verbindungsart des Admin-PC zum System.
5) Aktivieren Sie das Optionsfeld **KDS lesen/schreiben** und klicken Sie auf **Anlage** > **PC**.
6) Klicken Sie auf **OK**. Der KDS wird von HiPath 3000 zum Manager E übertragen.
7) Klicken Sie nach erfolgreicher Übertragung auf **OK** und anschließend auf **Schließen**.
8) Klicken Sie in der Menüleiste auf **Datei** > **KDS speichern unter** und speichern Sie den KDS auf dem Admin-PC in einem Ordner Ihrer Wahl.

Nächste Schritte

Wie Sie die HG1500 Einstellungen auslesen auf Seite 1423

26.7.1.2 Wie Sie die HG1500 Einstellungen auslesen

Voraussetzungen

Eine oder mehrere HG1500 Baugruppen sind gesteckt.

Sie sind am Manager E angemeldet.

Schritt für Schritt

1) Klicken Sie im Manager E in der Anlagenansicht auf den Eintrag der HG1500. Das WBM der HG1500 öffnet sich.
2) Notieren Sie sich die Einstellungen, die gegenüber den Standard-Einstellungen geändert wurden. Die HG1500 Einstellungen werden bei der Konvertierung des KDS nicht übernommen und müssen bei der Erstinbetriebnahme der OpenScape Business im WBM nochmals konfiguriert werden.

Nächste Schritte

Wie Sie den HiPath 3000 KDS konvertieren auf Seite 1423

26.7.1.3 Wie Sie den HiPath 3000 KDS konvertieren

Voraussetzungen

Ein HiPath 3000 Kommunikationssystem (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 oder HiPath 3800) ist vorhanden.

Der Admin-PC ist mit dem HiPath 3000 Kommunikationssystem verbunden.

Schritt für Schritt

1) Klicken Sie in der Menüleiste auf **Datei** > **KDS konvertieren**.
2) Wählen Sie den zuvor auf dem Admin-PC abgespeicherten KDS aus und klicken Sie auf **OK**.
3) Geben Sie als Kundendaten **Name** und Ihre **Vertragsnummer** ein und klicken Sie auf **Weiter**.
4) Wählen Sie als **Version OpenScape Business V2** aus und klicken Sie auf **Weiter**.
5) Bestätigen Sie die Hinweise auf nicht mehr unterstützte Baugruppen mit **OK**.
6) Klicken Sie auf **Ja**, um das Infofenster mit der Anzahl der zu migrierenden TDM-Benutzer zu bestätigen und fahren Sie mit der Migration fort.

   Die Anzahl der zu migrierenden TDM-Benutzer wird automatisch berechnet.
7) Bestätigen Sie die Anzeige der gesteckten Baugruppen mit **Weiter**.
8) Klicken Sie in der Menüleiste auf **Datei** > **KDS speichern** und speichern Sie den KDS unter einem anderen Namen auf dem Admin-PC in einem Ordner Ihrer Wahl.
9) Schließen Sie den Manager E.

Nächste Schritte

Wie Sie die Hardware bei HiPath 3300/3500 austauschen auf Seite 1424 oder

Wie Sie die Hardware bei HiPath 3350/3550 austauschen auf Seite 1425 oder

Wie Sie die Hardware bei HiPath 3800 austauschen auf Seite 1427

26.7.1.4 Wie Sie die Hardware bei HiPath 3300/3500 austauschen

Voraussetzungen

Laufendes HiPath 3000 Kommunikationssystem für den Rackbetrieb (HiPath 3300 oder HiPath 3500).

OpenScape Business V3-Mainboard (OCCMRA oder OCCMRB).

Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Stellen Sie sicher, dass für das Kommunikationssystem ein zusätzlicher Schutzleiter mit dem geforderten Mindest-Leiterquerschnitt vorhanden ist (siehe Servicedokumentation, Montage der Hardware).

Schritt für Schritt

1) Schalten Sie die HiPath 3000 aus und ziehen Sie anschließend den Netzstecker.
2) Entfernen Sie alle Stecker vom Mainboard, wie z.B. analoge Teilnehmer, ISDN-Leitungen, usw.
3) Lösen Sie die beiden Feststellschrauben in der Frontblende des Mainboards.
4) Lösen Sie mit zwei Baugruppenschlüssel (C39165-A7027-C26) das Mainboard von der Backplane.
5) Ziehen Sie vorsichtig mit beiden Händen das HiPath 3000 Mainboard waagrecht aus dem Baugruppenrahmen und legen Sie es auf einer flachen, geerdeten und leitfähigen Unterlage ab.
6) Entfernen Sie evtl. vorhandene HG1500 Baugruppen aus dem Gehäuse. Die frei gewordenen HG1500-Steckplätze können für zusätzliche Baugruppen verwendet werden.
7) Ziehen Sie falls vorhanden alle nicht mehr unterstützten Baugruppen aus dem Gehäuse. Die frei gewordenen Steckplätze können für zusätzliche Baugruppen verwendet werden.
8) Entfernen Sie alle auf dem HiPath 3000 Mainboard gesteckten Submodule und stecken Sie diese (falls noch benötigt und unterstützt) auf das OpenScape Business V3-Mainboard.
9) Stecken Sie die M.2 SATA SSD mit System-SW und optional eine M.2 NVMe SDD auf das V3-Mainboard.
10) Stecken Sie optionale Module wie OCCBH oder OCCBL ein
11) Schieben Sie vorsichtig mit beiden Händen das OCCMRA- oder OCCMRB-Mainboard waagerecht in den Steckplatz des Baugruppenrahmens, wo vorher das HiPath 3000 Mainboard steckte.
12) Schließen Sie optionale Module wie STRBR an das V3-Mainboard an.

13) Stecken Sie wieder alle Stecker in das Mainboard, wie z.B. analoge Teilnehmer, ISDN-Leitungen, usw.

Anmerkung: Bei Verwendung von mehr als 2 analogen a/b-Ports in HiPath 3300 oder 3500 sind in OpenScape Business 1 bzw. 2 Y-Adapterkabel erforderlich. Es müssen bis zu 4 a/b-Ports über die 2 physikalischen RJ11-Buchsen herausgeführt werden. Das neue Mainboard hat aus Platzgründen lediglich 2 RJ11-Buchsen, über die 4 a/b-Teilnehmer anzubinden sind.

14) Verbinden Sie Ihr Kommunikationssystem ordnungsgemäß mit dem Schutzleiter.

15) Stecken Sie den Netzstecker wieder ein und fahren Sie das System hoch.

Nächste Schritte

Wie Sie die Erstinstallation durchführen auf Seite 1427

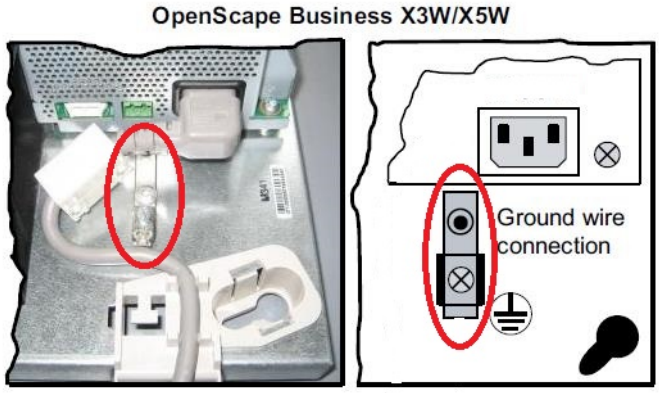
26.7.1.5 Wie Sie die Hardware bei HiPath 3350/3550 austauschen

Voraussetzungen

Laufendes HiPath 3000 Kommunikationssystem für den Wandbetrieb (HiPath 3350 oder HiPath 3550).

OpenScape Business Mainboard (OCCMA oder OCCMB).

Bei Migration von HiPath 3350/3550 zu OpenScape Business X3W/X5W muss die Schutzerdungsklemme installiert werden wie in der Abbildung unten gezeigt. Danach muss das Schutzerdungskabel wie in der Installationsanleitung beschreiben innerhalb von OpenScape Business V2 bzw. OpenScape Business X3/X5/X8 angeschlossen werden.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Stellen Sie sicher, dass für das Kommunikationssystem ein zusätzlicher Schutzleiter mit dem geforderten Mindest-Leiterquerschnitt vorhanden ist (siehe Servicedokumentation, Montage der Hardware).

Schritt für Schritt

1) Schalten Sie die HiPath 3000 aus und ziehen Sie anschließend den Netzstecker.
2) Lösen Sie die Verriegelung des Gehäuses und entfernen Sie das Gehäuse.
3) Entfernen Sie die Abdeckung.
4) Entfernen Sie alle Steckverbinder (Edge-Connectoren) vom Mainboard, wie z.B. analoge Teilnehmer, ISDN-Leitungen, usw.
5) Entfernen Sie den Baugruppenriegel.
6) Entfernen Sie vorsichtig das HiPath Mainboard aus dem Baugruppenrahmen und legen Sie es auf einer flachen, geerdeten und leitfähigen Unterlage ab.
7) Entfernen Sie evtl. vorhandene HG1500 Baugruppen aus dem Gehäuse. Die frei gewordenen HG1500-Steckplätze können für zusätzliche Baugruppen verwendet werden.
8) Ziehen Sie falls vorhanden alle nicht mehr unterstützten Baugruppen aus dem Gehäuse. Die frei gewordenen Steckplätze können für zusätzliche Baugruppen verwendet werden.
9) Entfernen Sie alle auf dem HiPath 3000 Mainboard gesteckten Submodule und stecken Sie diese (falls noch benötigt und unterstützt) auf das OpenScape Business Mainboard.
10) Stecken Sie die M.2 SATA SSD mit System-SW und optional eine M.2 NVMe SSD auf das V3-Mainboard.
11) Stecken Sie optionale Module wie OCCBH oder OCCBL ein.
12) Stecken Sie vorsichtig das OpenScape Business OCCMA- oder OCCMB-Mainboard in den gleichen Slot, wo vorher das HiPath 3000 Mainboard steckte.
13) Schließen Sie optionale Module wie STRBR an das V3-Mainboard an.
14) Stecken Sie wieder alle Steckverbinder (Edge-Connectoren) in das Mainboard, wie z.B. analoge Teilnehmer, ISDN-Leitungen, usw. Beachten Sie, dass die Stecker für die ISDN-Leitungen zuerst durch das Loch des neuen Baugruppenriegels geführt werden müssen.
15) Bringen Sie den neuen Baugruppenriegel an.
16) Verbinden Sie Ihr Kommunikationssystem ordnungsgemäß mit dem Schutzleiter.
17) Setzen Sie das Gehäuse auf und verriegeln Sie es.
18) Stecken Sie den Netzstecker wieder ein und fahren Sie das System hoch.

Nächste Schritte

Wie Sie die Erstinstallation durchführen auf Seite 1427

26.7.1.6 Wie Sie die Hardware bei HiPath 3800 austauschen

Voraussetzungen

Laufendes HiPath 3800 Kommunikationssystem.

OpenScape Business Mainboard OCCLA.

Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Stellen Sie sicher, dass für das Kommunikationssystem ein zusätzlicher Schutzleiter mit dem geforderten Mindest-Leiterquerschnitt vorhanden ist (siehe Servicedokumentation, Montage der Hardware).

Schritt für Schritt

1) Schalten Sie die HiPath 3000 aus und ziehen Sie anschließend den Netzstecker.
2) Entfernen Sie alle Stecker vom Mainboard.
3) Ziehen Sie vorsichtig das HiPath 3000 Mainboard aus dem Baugruppenrahmen und legen Sie es auf einer flachen, geerdeten und leitfähigen Unterlage ab.
4) Ziehen Sie evtl. vorhandene HG1500 Baugruppen aus dem aus dem Baugruppenrahmen. Die frei gewordenen HG1500-Steckplätze können für zusätzliche Baugruppen verwendet werden.
5) Ziehen Sie falls vorhanden alle nicht mehr unterstützten Baugruppen aus dem aus dem Baugruppenrahmen. Die frei gewordenen Steckplätze können für zusätzliche Baugruppen verwendet werden.
6) Entfernen Sie alle auf dem HiPath 3000 Mainboard gesteckten Submodule und stecken Sie diese (falls noch benötigt und unterstützt) auf das OpenScape Business Mainboard.
7) Stecken Sie die M.2 SATA SSD mit System-SW und optional eine M.2 NVMe SDD auf das V3-Mainboard.
8) Stecken Sie optionale Module wie OCCBH oder OCCBL ein.
9) Stecken Sie vorsichtig das OpenScape Business OCCLA-Mainboard in den gleichen Slot, wo vorher das HiPath 3000 Mainboard steckte.
10) Stecken Sie wieder alle Stecker in das Mainboard.
11) Verbinden Sie Ihr Kommunikationssystem ordnungsgemäß mit dem Schutzleiter.
12) Stecken Sie den Netzstecker wieder ein und fahren Sie das System hoch.

Nächste Schritte

Wie Sie die Erstinstallation durchführen auf Seite 1427

26.7.1.7 Wie Sie die Erstinstallation durchführen

Die Erstinstallation des Kommunikationssystems wird in Integration ins Kunden-LAN beschrieben.

Die Erstinstallation umfasst die Konfiguration der IP-Adresse des Systems, die DHCP-Einstellungen sowie Länder- und Zeiteinstellungen.

Hatte das HiPath 3000 System zusätzlich eine HG 1500 installiert, so sollte bei der Erstinstallation für die IP-Adresse des OpenScape Business Systems die IP-Adresse der HG 1500 verwendet werden.

Nach erfolgreicher Erstinstallation führt das Kommunikationssystem einen Neustart durch.

Nächste Schritte

Wie Sie den konvertierten KDS in das neue System laden auf Seite 1428

26.7.1.8 Wie Sie den konvertierten KDS in das neue System laden

Voraussetzungen

Die Hardware wurde ausgetauscht.

Der Admin-PC ist mit dem OpenScape Business Kommunikationssystem verbunden (über die LAN-Schnittstelle).

Der Admin-PC ist so konfiguriert, dass er IP-Adresse und Netzmaske vom DHCP-Server von OpenScape Business empfangen kann.

Schritt für Schritt

1) Melden Sie sich auf dem Admin-PC am Manager E an.
2) Klicken Sie in der Menüleiste auf **Datei** > **KDS öffnen**.
3) Navigieren Sie zum Ablageort des konvertierten OpenScape Business KDS und klicken Sie auf **OK**.
4) Bestätigen Sie die Meldung mit **OK**.
5) Klicken Sie in der Menüleiste auf **Datei** > **Übertragen**.
6) Klicken Sie auf die Registerkarte **Kommunikation**.
7) Aktivieren Sie die Option **IP - HiPath** im Bereich **Zugang** und geben Sie im Feld IP-Adresse die IP-Adresse des OpenScape Business Kommunikationssystem sein. Standard: `192.168.1.2`.
8) Aktivieren das Optionsfeld **Sicherheit**.
9) Klicken Sie auf **Kennwort ändern**.
10) Geben Sie altes und neues Kennwort ein und bestätigen Sie mit **OK**.
11) Aktivieren Sie das Optionsfeld **KDS lesen/schreiben**.
12) Aktivieren Sie die Kontrollkästchen **Gebühren** und **Hardware** und klicken Sie auf **PC** > **Anlage**.
13) Klicken Sie auf **OK**. Der KDS wird vom Manager E zum System übertragen.
14) Klicken Sie nach erfolgreicher Übertragung des KDS auf **OK** und anschließend auf **Schließen**.
15) Beenden Sie den Manager E. Das System führt automatisch einen Neustart durch.

Nächste Schritte

Wie Sie eine neue Lizenzdatei generieren auf Seite 1429

26.7.1.9 Wie Sie eine neue Lizenzdatei generieren

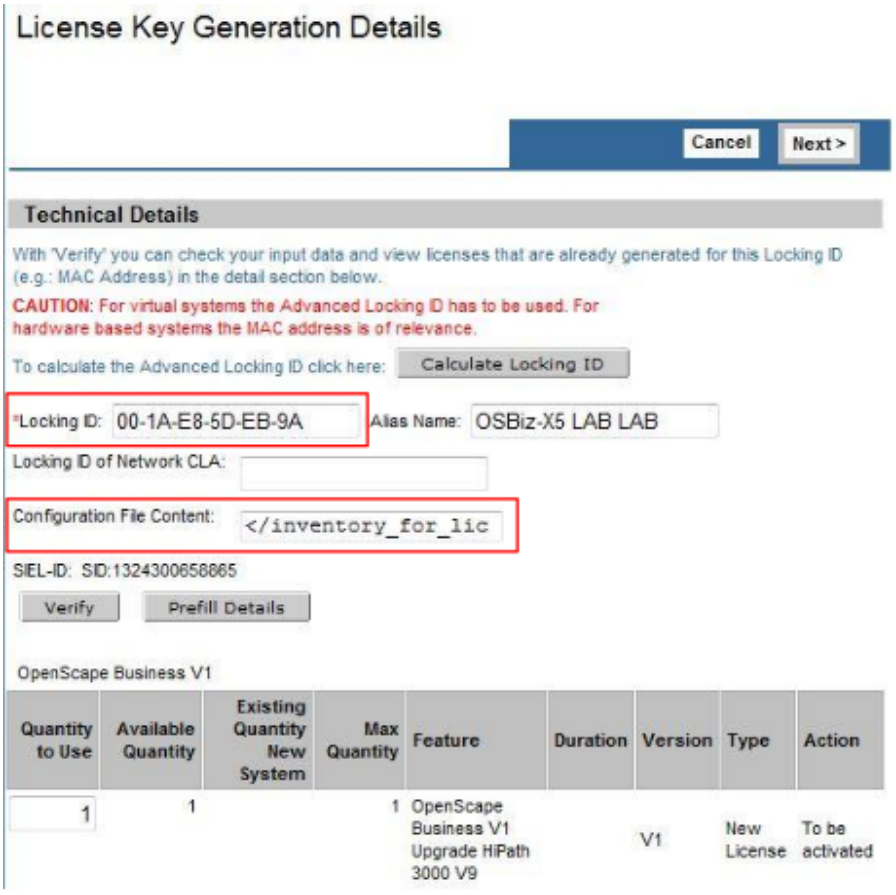
Voraussetzungen

Der LAC der Upgrade-Lizenz ist vorhanden.

Die Registrierungsdaten des Kunden liegen vor.

Schritt für Schritt

1) Melden Sie sich am WBM mit dem Profil **Advanced** an.
2) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
3) Notieren Sie sich die Locking ID von OpenScape Business, die oberhalb der Tabelle angezeigt wird.
4) Klicken Sie im Navigationsbaum auf **Registrierung**.
5) Geben Sie Ihre Daten ein und klicken Sie auf **OK & Weiter**.
6) Klicken Sie auf **Daten exportieren**. Es wird eine Konfigurationsdatei (XML-Datei) generiert mit den Registrierungsdaten und den Inventory-Informationen inklusive der Anzahl der angeschlossenen TDM-Teilnehmer.
7) Speichern Sie die Konfigurationsdatei in einem Verzeichnis Ihrer Wahl.
8) Melden Sie sich am CLS mit Benutzernamen und Kennwort an.
9) Klicken Sie im Menübaum auf **License** > **Generate License Key**.
10) Geben Sie unter **LAC** den LAC der Upgrade-Lizenz ein und klicken Sie auf **Generate Key**.
11) Markieren Sie das Leistungsmerkmal **OpenScape Business V2 Update HiPath 3000** und klicken Sie erneut auf **Generate Key**.



12) Geben Sie im Feld **Locking ID** die Locking-ID von OpenScape Business ein.
13) Öffnen Sie die Konfigurationsdatei mit einem Text-Editor (z. B. Notepad) und kopieren Sie den kompletten Inhalt aus der Konfigurationsdatei in das Feld **Configuration File Content**.
14) Klicken Sie auf **Next** und folgen Sie den Anweisungen, um eine neue Lizenzdatei zu generieren.

Anmerkung: Die Prozedur der Lizenzmigration am CLS ist nur einmal möglich. Achten Sie daher bitte auf korrekte Angaben!

15) Speichern Sie die neue Lizenzdatei in einem Verzeichnis Ihrer Wahl.

Nächste Schritte

Wie Sie die Lizenzdatei offline aktivieren auf Seite 1430

26.7.1.10 Wie Sie die Lizenzdatei offline aktivieren

Die Offline-Lizenzaktivierung wird im Kapitel Wie Sie Lizenzen offline aktivieren (Standalone) beschrieben.

Nächste Schritte

Wie Sie Lizenzen zuordnen auf Seite 1430

26.7.1.11 Wie Sie Lizenzen zuordnen

Die Lizenzzuordnung wird in Lizenzzuordnung (Standalone) auf Seite 317 beschrieben.

26.7.1.12 Wie Sie die LCR-Einträge zurücksetzen

Die Grundinstallation des Kommunikationssystems wird in Basiskonfiguration auf Seite 156 beschrieben).

Die Basisinstallation umfasst die Konfiguration der Systemrufnummer, der Teilnehmer sowie den Zugang zum Internet und die Internet-Telefonie.

Im Wizard **Grundinstallation** finden Sie im Fenster **Zentrale Teilnehmerfunktionen** ein zusätzliches Optionsfeld **Konfigurierte LCR-Daten löschen und mit LCR-Standarddaten initialisieren**. Dieses Optionsfeld erscheint nur, wenn zuvor ein konvertierter KDS in das System geladen wurde. Wird dieses Optionsfeld aktiviert, werden die im HiPath 3000 System konfigurierten LCR-Einträge gelöscht und durch die Standard-Einträge des OpenScape Business Systems ersetzt.

Zugehörige Konzepte

Teilnehmerdaten auf Seite 160

26.7.2 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit V3-Mainboard

Bei der Migration von HiPath 3000 Systemen mit einem angeschlossenen OpenScape Office HX Server ist der externe Server nicht erforderlich. Seine Funktion wird vom entsprechenden V3-Mainboard des OpenScape Business X Systems übernommen.

Das HiPath 3000 System wird migriert wie in Migration von HiPath 33xx, 35xx, 3800 nach OpenScape Business X3/X5/X8 V3 auf Seite 1417 beschrieben.

OpenScape Office HX Lizenzen sind Teil der HiPath 3000 Lizenzdatei. Daher werden sie im Verlauf der HiPath 3000 Lizenzmigration auch auf die OpenScape Business Lizenzen übertragen.

Anforderungen

Um OpenScape Business HX Lizenzen zu migrieren, muss eine HiPath 3000 Lizenzdatei auf dem zentralen Lizenzserver verfügbar sein.

Für die HiPath 3000 Lizenzen wird die Lizenzmigration durchgeführt wie in Tabelle 35: HiPath 3000 Lizenzmigration auf Seite 1418 gezeigt. Das Folgende gilt für die OpenScape Office HX Lizenzmigration:

Tabelle 36: OpenScape Office HX Lizenzmigration

OpenScape Office HX Lizenz	OpenScape Business Lizenz	Hinweise
Pro Basislizenz	1x AutoAttendant Lizenz	
Pro OpenScape Office Standardbenutzer:	1x UC Benutzer 1x Voicemail Benutzer 1x Fax Benutzer	Gilt für alle Standardbenutzerlizenzen in den HX Basislizenzen 5/10 sowie für Single-User-Lizenzen
OpenScape Office HX Voicemail Lizenz	500 x Voicemail Benutzer	
myPortal for Outlook	Groupware User	Anzahl laut Lizenzdatei
myAttendant	myAttendant	Anzahl laut Lizenzdatei
myAgent	myAgent Benutzer	Anzahl laut Lizenzdatei
Contact Center Fax	Contact Center Fax Benutzer	Anzahl laut Lizenzdatei
Contact Center E-Mail	Contact Center E-Mail Benutzer	Anzahl laut Lizenzdatei
myReports	myReports	Anzahl laut Lizenzdatei
Application Launcher	Application Launcher	Anzahl laut Lizenzdatei
OpenDirectory Connector	OpenDirectory Connector	Anzahl laut Lizenzdatei

Bedingungen und Einschränkungen für funktionale Grenzen

Die Lizenzmigration kann nur auf V3 erfolgen. Eine Lizenzmigration auf V2 wird vom Manager E nicht unterstützt.

Die der Lizenzmigration ist nur einmal möglich.

Benutzerlizenzen und UC benutzerbezogene Lizenzen werden Benutzern in OpenScape Business permanent zugewiesen. Bitte beachten Sie, dass für Benutzer von myAgent und myAttendant eine ausreichende Anzahl an Lizenzen zur Verfügung steht.

In OpenScape Business sind Änderungen im Präsenzstatus anderer Benutzer durch Benutzer von myAgent an die myAttendant Lizenz gebunden. Diese sind separat zu bestellen.

Es ist nicht möglich, Ansagen, Bilder, Voicemails, Fax, Journal, Contact Center-Daten, Teilnehmerkonfiguration, Profile, externes Verzeichnis, Termine von OpenScape Office HX auf OpenScape Business V3 mit V3-Mainboard zu übertragen.

26.7.3 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit UC Booster Server

Die Migration muss in zwei Schritten erfolgen. In einem ersten Schritt werden die Systeme auf V2 migriert. In einem weiteren Schritt werden die Systeme auf V3 migriert.

Dieses Migrationsszenario sollte nur durchgeführt werden, wenn Kundendaten innerhalb des OpenScape Office HX-Servers beibehalten werden müssen. Die Migration ist zeitaufwändig und es muss ein neuer UC Booster Server eingerichtet werden. Die Migration endet mit einem OpenScape Business X V3 System mit V2-Mainboard und angeschlossenem UC Booster Server V3.

Eine Migration wie in Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit V3-Mainboard auf Seite 1431 sollte alternativ in Betracht gezogen werden, wenn die Kundendaten auf dem HX-Server nicht beibehalten werden müssen.

Schritt 1 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V2

Bei diesem Schritt wird HiPath 3000 nach OpenScape Business V2 migriert und die UC-Funktionalität des OpenScape Office V3 HX wird auf einen OpenScape Business UC Booster Server V2 gemappt.

Der UC Booster Server muss auf einer neuen HW- und SW-Basis vollkommen neu aufgesetzt werden. Die Lizenzen und Kundendaten können von OpenScape Office V3 HX auf den UC Booster Server übertragen werden, wenn der UC Booster Server zuerst mit der OpenScape Business SW-Version 1R2.2 eingerichtet wird. Nur in diesem Fall werden die folgende UC-Konfiguration sowie die Benutzerdaten übertragen:

- Ansagen
- Bilder
- Voicemail
- Faxe
- Journal
- Contact Center Daten
- Benutzerkonfiguration
- Benutzer-Profile

- Externes Verzeichnis
- Zeitpläne

Folgende UC-Konfigurations- und Benutzerdaten werden **nicht** übernommen und müssen im UC Booster Server neu konfiguriert werden:

- Web-Services (z. B. XMpp, Web Collaboration, Mobility)
- Open Directory Service

Nach der Übertragung der Lizenzen und Kundendaten muss die UC Booster Server SW auf die SW-Version V1R3.3 und anschließend wieder auf die neueste SW-Version V2R7 aktualisiert werden.

Führen Sie für die Migration/Aktualisierung die folgenden Schritte der Reihe nach durch:

1) **Agenten-IDs notieren** (nur bei Nutzung des Contact Centers)

   Notieren Sie sich die Zuordnung der Agenten-IDs zu den Teilnehmern der UC Suite, da diese Zuordnung nicht migriert wird. Die Zuordnung muss mit dem Wizard **Anrufverteilung** im WBM des OpenScape Business Kommunikationssystems neu konfiguriert werden.
2) **OpenScape Office V3 HX aktualisieren**

   Rüsten Sie falls noch nicht geschehen die OpenScape Office V3 HX auf die Software V3 R3FR6 hoch.
3) **OpenScape Office V3 HX Backup-Set erstellen**

   Erstellen Sie über das WBM von OpenScape Office V3 HX ein Backup-Set auf ein externes Medium.

   Genauere Informationen finden Sie in der Online-Hilfe des OpenScape Office Assistant.
4) **HiPath 3000 aktualisieren**

   Führen Sie die Aktualisierung von HiPath 3000 auf OpenScape Business V1 wie in der Migrationsprozedur für ein Standalone-System beschrieben durch (siehe Migration von HiPath 33xx, 35xx, 3800 nach OpenScape Business X3/X5/X8 V3 auf Seite 1417). Die Lizenzen der OpenScape Office V3 HX werden bei der Lizenzmigration am Lizenzserver nach OpenScape Business übernommen. Die Lizenzdatei enthält sowohl Lizenzdaten der OpenScape Business X3/X5/X8 als auch der UC-Suite.
5) **UC Booster Server einrichten und in das Kunden-LAN integrieren**

   Das Linux-Betriebssystem SLES 64-Bit muss auf dem neuen Server-PC (Linux-Server) installiert werden, gefolgt von der Kommunikationssoftware (Version V1 R2.2). Details siehe *OpenScape Business Linux-Server Installationsanleitung*.
6) **UC Booster aktivieren**

   Aktivieren Sie die UC Booster-Funktionalität im WBM des OpenScape Business Kommunikationssystems (**Grundinstallation** > **Erstinstallation** > **Paket mit UC Suite auf OpenScape Business UC Booster Server**) und geben Sie die IP-Adresse des neuen Server-PCs ein (mit der gleichen IP-Adresse wie der alte Server-PC, wenn möglich). Stellen Sie sicher, dass die UC Suite auf dem UC Booster Server aktiv ist.

   Genauere Informationen finden Sie im Kapitel „Erstinstallation OpenScape Business X3/X5/X8“ unter Wie Sie die UC-Lösung festlegen auf Seite 154.

7) **UC Booster konfigurieren**

   Im WBM des UC Booster Servers muss die IP-Adresse des Kommunikationssystems angegeben werden.

   Genauere Informationen finden Sie im Kapitel „Erstinstallation OpenScape Business UC Booster“ unter IP-Adresse des Kommunikationssystems bekannt geben auf Seite 288.

8) **OpenScape Office V3 HX Backup-Set konvertieren**

   Das auf dem externen Medium gesicherte OpenScape Office V3 HX Backup-Set muss über ein Linux-Script in ein OpenScape Business V1 Backup-Set konvertiert werden. Dafür benötigen Sie Linux-Kenntnisse. Anschließend ist das konvertierte Backup-Set über das WBM in den UC Booster Server zu laden. Danach stehen die o.g. UC-Konfigurations- und Benutzerdaten zur Verfügung.

   Weitere Information dazu finden Sie in diesem Kapitel unter Wie Sie ein OpenScape Office V3 HX Backup-Set konvertieren auf Seite 1434.

9) **Aktualisierung der UC Booster Server Software auf V2**

   Aktualisieren Sie den UC Booster Server zuerst auf die Version V1 R3.3 und anschließend auf die neueste OpenScape Business V2 Software.

26.7.3.1 Wie Sie ein OpenScape Office V3 HX Backup-Set konvertieren

Voraussetzungen

Der OpenScape Business UC Booster Server ist betriebsbereit.

Das OpenScape Office V3 HX Backup-Set liegt auf dem externen Medium vor.

Schritt für Schritt

1) Kopieren Sie das OpenScape Office V3 HX Backup-Set von dem externen Medium auf den Server-PC (Linux-Server) in folgendes Verzeichnis:

   ```
   /mnt/persistent/apollo/
   ```

2) Öffnen sie ein Terminal auf dem Server-PC oder verbinden sie sich mit einer SSH-Shell mit dem Server-PC. Sie benötigen root-Rechte.

3) Wechseln Sie zum Backup-Verzeichnis mit folgendem Kommando:

   ```
   cd /mnt/persistent/backup/
   ```

4) Rufen Sie das Konvertierungsscript auf wie folgt:

   ```
   /opt/symappl/services/backup/script/migrate.sh /mnt/
   persistent/apollo/<Name des Backup-Sets>
   ```

   ```
   /opt/symappl/services/backup/script/migrate.sh /mnt/
   persistent/apollo/BackupSet_130913-0400007.tar
   ```

5) Nachdem das Konvertierungsscript durchlaufen ist, kann das konvertierte Backup-Set für den Restore verwendet werden.

26.7.4 Migration von HiPath 3000 Netzwerk auf OpenScape Business Netzwerk

Um ein HiPath 3000 Netzwerk auf ein OpenScape Business Netzwerk zu aktualisieren, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

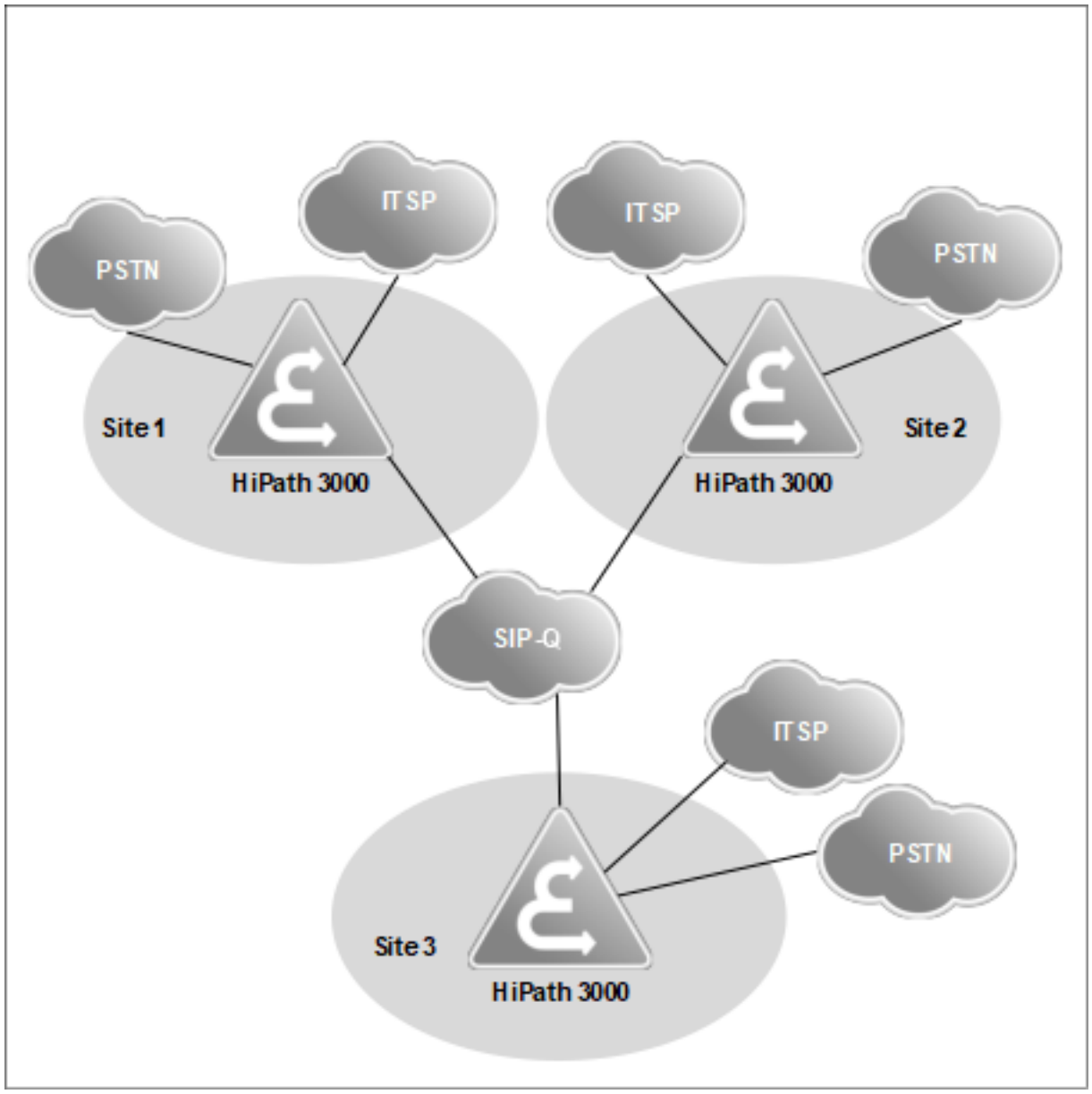


Abbildung 18: HiPath 3000 V9 Netzverbund

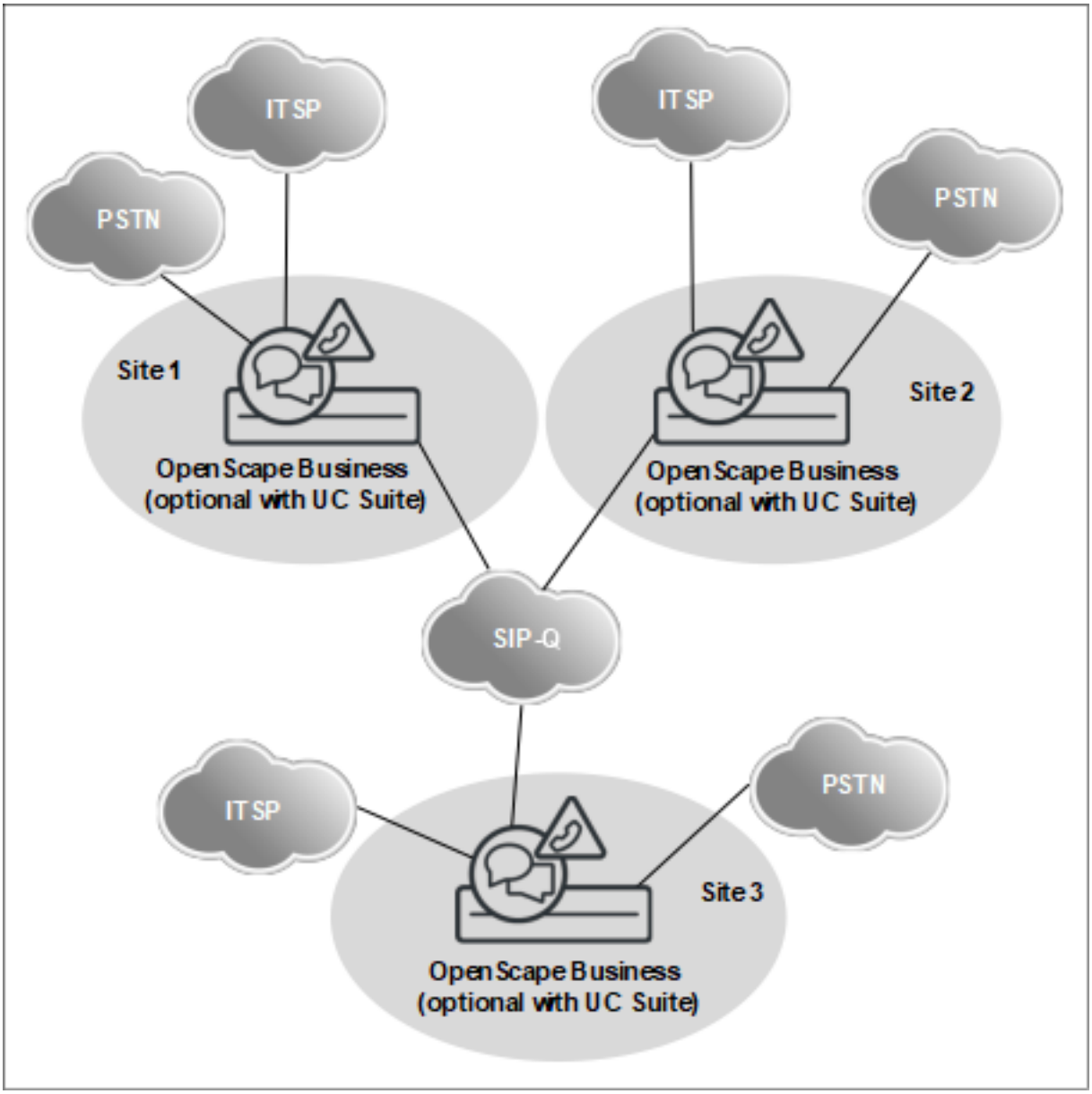


Abbildung 19: OpenScape Business Netzverbund

Migrationsschritte

Führen Sie folgende Schritte der Reihe nach durch:

1) HiPath 3000 aktualisieren

Alle HiPath 3000 Systeme des Netzverbunds sind separat gemäß der Migrationsbeschreibung eines Standalone-Systems zu aktualisieren (siehe 1.7.1).

2) **Konfiguration anpassen**

   Folgende Konfigurationsparameter sind nachträglich über den WBM-Experten-Modus anzupassen:

   - LCR-Einträge
   - Voicemail-System (Sammelanschluss, Kennzahl zur Anwahl der Voicemail)
   - Ansagen

3) **Lizenzierung durchführen.**

   Nachdem alle Systeme hochgerüstet sind, erfolgt die Zusammenfassung der einzelnen Lizenz-Dateien zu einer netzweiten Lizenz am CLS.

26.7.5 Migration eines HiPath 3000 V9 Netzverbunds mit HiPath 5000 RSM

Ein HiPath 3000/5000 Netzwerk mit einer gemeinsamen Netzwerklizenzdatei kann über den zentralen Lizenzserver (CLS) in Standalone-Systeme mit einzelnen Lizenzdateien unterteilt werden. Jedes Standalone-System wird dann auf OpenScape Business migriert und separat lizenziert.

Bei Bedarf können die OpenScape Business Systeme nach der Migration am CLS wieder zu einer Netzwerkgruppe mit einer einzigen Netzwerklizenzdatei zusammengeführt werden.

Der Leistungsumfang von HiPath 5000 RSM wurde in OpenScape Business integriert, somit wird HiPath 5000 RSM selbst im OpenScape Business Netzverbund nicht mehr benötigt.

Für die Vernetzung der OpenScape Business Systeme sind zusätzlich OpenScape Business Networking-Lizenzen pro Knoten verfügbar.

Für Internettelefonie und T1-Leitungen sind zusätzliche Leitungslizenzen erforderlich.

Die folgenden Migrationsschritte müssen wie unten beschrieben ausgeführt werden.

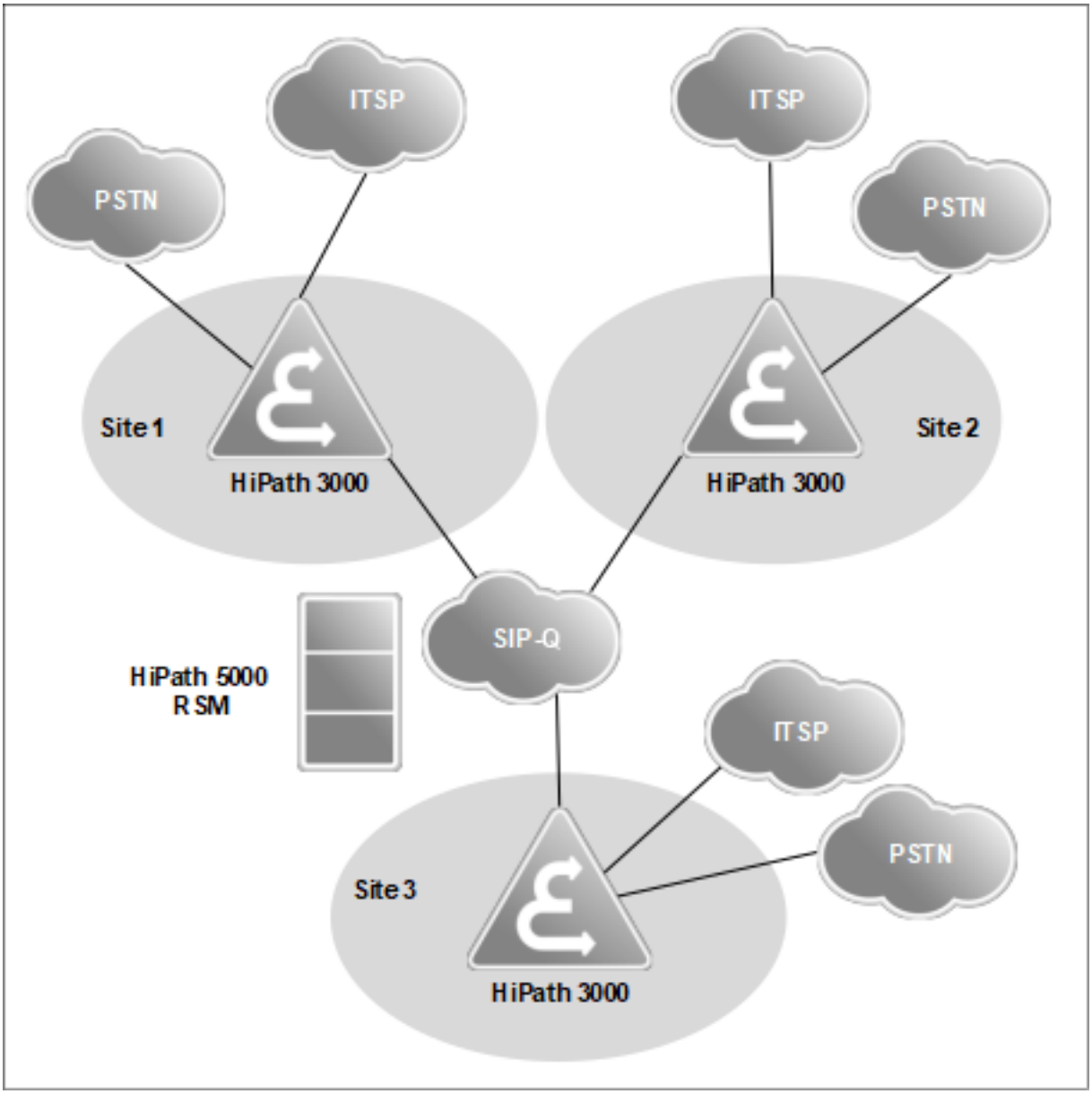


Abbildung 20: HiPath 3000 V9 Netzverbund

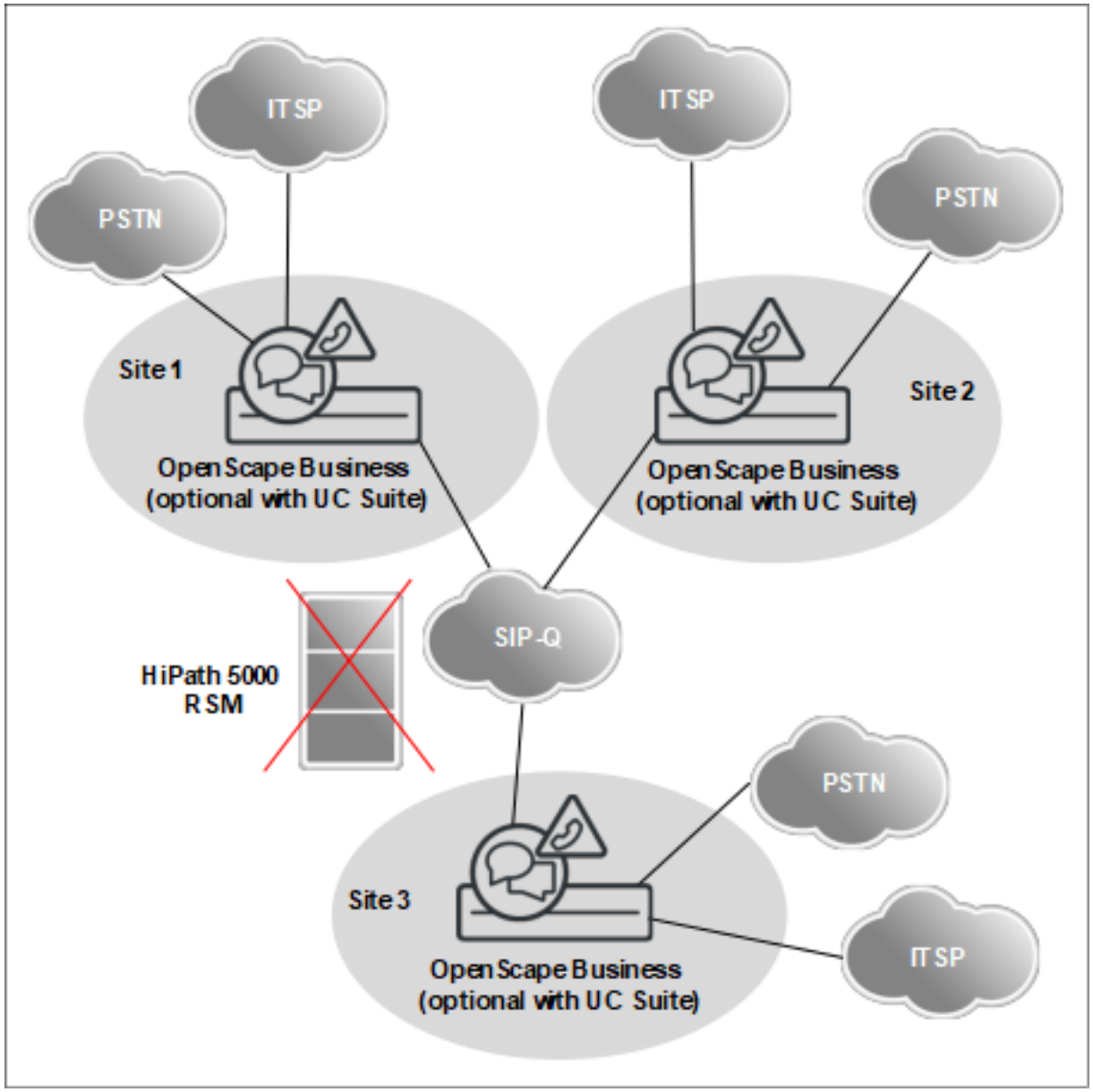


Abbildung 21: OpenScape Business Netzverbund

Migrationsschritte

Führen Sie folgende Schritte der Reihe nach durch:

1) Netzweite Lizenzierung auflösen

Ein HiPath 3000 Netzverbund mit HiPath 5000 RSM nutzt die netzweite Lizenzierung. Die Netzwerklizenzdatei ist am CLS zunächst in einzelne Lizenzdateien aufzulösen und den Locking-IDs (MAC-Adressen) der HiPath 3000 V9 Systeme zuzuordnen, bevor die eigentliche Migration nach OpenScape Business beginnen kann.

- Ordnen Sie zunächst die Lizenzen des HiPath 5000 RSM Netzverbundes den jeweiligen Locking-IDs der HiPath 3000 Knoten zu. Empfehlung: Erstellen Sie eine Excel-Liste mit entsprechender Zuordnung der jeweiligen Lizenzen zu den Locking-IDs der HiPath 3000 Systeme.

- Kontaktieren Sie die Lizenz-Hotline, um die Aufteilung der Lizenzen gemäß Exel-Liste ausführen zu lassen.
- Laden Sie die Einzellizenzen der HiPath 3000 Systeme zur Kontrolle vom CLS. Eine Aktivierung der Lizenzen, d.h. die Lizenz-Übertragung in die HiPath 3000 Systeme ist nicht erforderlich.

2) HiPath 5000 RSM entfernen

Vor der Hochrüstung der HiPath 3000 Systeme wird HiPath 5000 RSM abgeschaltet.

3) HiPath 3000 aktualisieren

Alle HiPath 3000 Systeme des Netzverbunds sind separat gemäß der Migrationsbeschreibung eines Standalone-Systems hochzurüsten. Siehe 1.7.1

4) Konfiguration anpassen

Folgende Konfigurationsparameter sind nachträglich innerhalb von OpenScape Business über den WBM-Experten-Modus anzupassen:

- LCR-Einträge
- Voicemail-System (Sammelanschluss, Kennzahl zur Anwahl der Voicemail)
- Ansagen

5) Lizenzierung durchführen.

Nachdem alle Systeme aktualisiert sind, erfolgt die Zusammenfassung der einzelnen Lizenz-Dateien von OpenScape Business zu einer netzweiten Lizenz am CLS.

Anmerkung: Bei erweiterter netzweiter UC-Funktionalität ist eine Umstellung von offener auf verdeckte (geschlossene) Nummerierung erforderlich, um die internen Rufnummern anzupassen. Hierzu muss die offene Nummerierung deaktiviert werden, um anschließend die Knotennummer zu löschen und als Präfix neu hinzuzufügen (beispielsweise als erweiterte Internrufnummer 87100 statt 100 und 88100 statt 100).

Unterschiede:

- Die Auswahl der Teilnehmer auf ihrem eigenen Knoten erfolgt über die erweiterte Internrufnummer.

- Die interne und die DuWa-Rufnummer dürfen voneinander abweichen, die Durchwahlnummern dürfen jedoch nicht geändert werden.

26.7.6 Geänderte/gestrichene Leistungsmerkmale und Schnittstellen von HiPath 3000

Einige HiPath 3000 Leistungsmerkmale und Schnittstellen sind für OpenScape Business in ihrer Funktion angepasst und erweitert worden.

Tausch der MMC-Karte

Der Austausch der SDHC-/M.2 SATA SSD-Karte bei eingeschaltetem System (bei HiPath 3000 als Speed-Update bekannt) ist aus technischen Gründen nicht möglich. Ferner kann die SDHC-/M.2 SATA SSD-Karte eines lizenzierten Systems A nicht für ein anderes System B verwendet werden, da die Lizenzierung an die Locking-ID des Mainboards A gebunden ist. Wenn die SDHC-/M.2 SATA SSD-Karte im System B verwendet werden soll, muss sie zunächst mit neuer Software initialisiert werden – mit Hilfe des Card Manager.

HG1500 DSP-Kanäle/B-Kanäle

Das HG1500-Modul wird nicht mehr benötigt. Die DSP-Funktionalität ist in OpenScape Business auf dem V3 Motherboard und über die optionalen Voice Channel Booster Cards integriert.

Bitte ermitteln Sie die Anzahl der benötigten DSP-Kanäle. DSP-Kanäle werden benötigt, um Netzübergänge von TDM-Telefonie auf VoIP zu realisieren. OpenScape Business hat auf dem V3-Mainboard 8 DSP-Kanäle integriert. Zur Erweiterung von DSP-Kanälen kann das DSP-Modul OCCB1/OCCBL (bis zu 40 Kanäle) oder das DSP-Modul OCCB3/OCCBH (bis zu 120 Kanäle) eingesetzt werden.

entry Web Services

Die entry Web Services werden nicht mehr unterstützt. Der Nachfolger von myPortal entry nennt sich myPortal @work und bietet einen erweiterten Funktionsumfang. myPortal for Mobile wird durch myPortal to go (Web Edition) ersetzt. Für den Einsatz von myPortal to go (Web Edition) ist der Plug PC nicht mehr nötig.

Entry Voicemail

Das Modul Entry Voicemail wird in OpenScape Business gestrichen. Die Funktion ist als Smart Voicemail in das OpenScape Business-Mainboard integriert. Smart Voicemail-Benutzer müssen lizenziert werden.

Externe Voicemail

Wird bei HiPath 3000 eine externe Voicemail-Lösung wie z. B. Xpressions verwendet, müssen nach der KDS-Konvertierung die 10 EVM-Ports im Manager E von **Phonemail** auf **Standard** gesetzt werden.

Erweiterung der SIP-Funktionalität

Folgende SIP-Leistungsmerkmale sind gegenüber HiPath 3000 V9 zusätzlich implementiert:

- Call completed elsewhere
- Message Waiting Indication for Voicemail
- Calling Name Presentation (CNIP)
- Distinctive Ringing (internal/external calls)
- 3rd Party Call Control
- Call Forwarding busy/no reply/unconditional (handset controlled)

SIP-Trunking

Zur Anbindung externer SIP-Server (z.B. OpenScape Alarm Server, HiPath 4000, OpenScape Voice oder UC-Suite) stehen in OpenScape Business zusätzliche native SIP-Q-Richtungen zur Verfügung (bei HiPath 3000 nur eine

SIP-Q-Richtung). Damit sind zusätzlich zu den klassischen Richtungen für Amt, Vernetzung und ITSP, native SIP/SIP-Q-Trunk-Schnittstellen für zertifizierte SIP-Applikationen vorgesehen (SIP-Interconnection genannt).

Siehe Vernetzung von OpenScape Business

LCR

Die Wegetabellen 1 bis 15 sind für Default-Einträge bzw. für eine Konfiguration über Wizards vorgesehen. Bei einer Migration werden die in HiPath 3000 vorhandenen Einträge in diese Wegetabellen nicht übernommen. Eine manuelle Nachbearbeitung der Wegetabellen ist erforderlich.

Automatische Leitungsbelegung

Es kann entweder die Funktion "LCR" oder die Funktion "Automatische Leitungsbelegung (Vereinfachte Wahl)" aktiviert sein. Deshalb wird bei der Migration automatisch "LCR" aktiviert und "Automatische Leitungsbelegung (Vereinfachte Wahl)" deaktiviert. Soll aber "LCR" deaktiviert und "Automatische Leitungsbelegung (Vereinfachte Wahl)" aktiviert werden, muss zuerst der Wizard "Basisinstallation" durchlaufen werden und anschließend können die Flags mit dem Manager E entsprechend gesetzt werden (nicht für OpenScape Business X1, da hier keine Administration über den Manager E möglich ist).

Anmerkung: Vereinfachtes Wählen wird in CSTA-Anwendungen nicht unterstützt.

VoIP over PPP via ISDN

Geroutete Sprachverbindungen über Leitungen mit geringer Bandbreite werden nicht mehr unterstützt

G.723-Unterstützung

G.723-Codecs werden nicht mehr unterstützt.

Raumüberwachung (Babyphone)

Das Leistungsmerkmal "Babyphone (Raumüberwachung)" wird nicht mehr unterstützt. Da die Funktion "CSTA-Monitoring" immer aktiv ist (ein Systemtelefon kann von einer Applikation - z. B. myAgent, myPortal - überwacht werden), kann die Funktion "Raumüberwachung" für dieses Systemtelefon nicht mehr aktiviert werden. Während der KDS-Konvertierung mit dem Manager E wird die Kennzahl für die Aktivierung der Raumüberwachung gelöscht.

Anzahl der Basisstationen und DECT-Telefone an OpenScape Business X3

Die Anzahl der Basisstationen an OpenScape Business X3 wurde gegenüber HiPath 33xx von 3 auf 7 erhöht. Die Anzahl der DECT-Telefone an OpenScape Business X3 wurde gegenüber HiPath 33xx von 16 auf 32 erhöht.

HiPath 3000 BS4

Lizenzen für Basisstationen werden in OpenScape Business nicht mehr benötigt.

SSDP auf Basis des Plug PC

SSDP ist in OpenScape Business integriert. Der Plug PC ist nicht mehr nötig.

Accounting-Schnittstelle

Die Schnittstellen der Accounting-Daten sind gegenüber HiPath 3000 geändert.

V24-Applikationen

V24-Applikationen werden nicht mehr unterstützt.

CSTA-Applikationen

Innerhalb von OpenScape Business V3 ist entweder ein V3-Mainboard oder UC Booster Card / Server in Kombination mit einem V2-Mainboard für die Verbindung von CSTA-Applikationen erforderlich. In einem Netzverbund dürfen V3-Mainboard / UC Booster Card / Server nur auf dem Master-Knoten vorhanden sein. Die Applikationen müssen CSTAv3-Protokoll unterstützen. Im Vergleich zu HiPath 3000 wurden Änderungen am CSTA-Protokoll implementiert. Daher sind CSTA-Applikationen am HiPath 3000 V9 ggf. nicht kompatibel einsetzbar bei OpenScape Business. Das CSTAv2-Protokoll wird nicht mehr unterstützt.

In SW-Version 3 ist eine CSTA-Lizenz für die Verwendung der CSTA-Schnittstelle mit folgenden Ausnahmen erforderlich:

- UC Booster Card CSTA-Verbindungen im Allgemeinen
- OpenScape Business TAPI 120 oder TAPI 170 CSTA-Verbindungen im Allgemeinen

Für die OpenScape Business CSTA-Schnittstelle gelten im Vergleich zur HiPath 3000 CSTA-Schnittstelle die nachfolgend beschriebenen Änderungen.

- Die Anschaltung an die CSTA-Schnittstelle ist für einzelne und vernetzte OpenScape Business Slave-Knoten identisch. CSTA auf dem Master-Knoten in einem Netzwerk bietet erweiterte Funktionen. Sie erfolgt ausschliesslich über LAN. RS232 (V.24) und S0 Schnittstellen werden nicht mehr unterstützt.
- Hard- und Software-Zusatzkomponenten wie CSTA Service Provider (CSP), HG 1500 Baugruppe oder HiPath 5000 RSM System werden bei OpenScape Business nicht mehr benötigt. Stattdessen werden UC Booster HW oder V3-Mainboards benötigt.
- Die CSTA-Schnittstelle ist mit Ausnahme von UC Booster Card- und TAPI 120/170-Verbindungen lizenziert.
- Maximal 4 CSTA-Links können zur Anschaltung externer Applikationen verwendet werden. Im Auslieferungszustand sind 3 der 4 CSTA Schnittstellen zur Verwendung von internen Applikationen von OpenScape Business vorkonfiguriert. Diese können optional auch zur Anschaltung externer Applikationen eingesetzt werden.
- Die Absicherung der CSTA Schnittstellen gegen Missbrauch wurde verbessert. Der Zugangsmechanismus wurde überarbeitet.
- MULAP-Monitoring über CSTA ist nur möglich, wenn ein Monitorpunkt auf die MULAP-Nummer gesetzt wird. Einzelne MULAP-Mitglieder können nicht überwacht werden. Möchte eine CSTA-Applikation dennoch einzelne MULAP-Mitglieder überwachen, werden von OpenScape Business keine CSTA-Events an die Applikation übertragen. Das gilt auch für MULAP-Mitglieder, die Teil eines Sammelanschlusses sind.
- Die zur Verfügung gestellten CSTA-Funktionen wurde erweitert. Details sind im OpenScape Business CSTA Interface Manual beschrieben.
- Die CSTA Phase II Protokollversion wird nicht mehr unterstützt.

- CSTA-Applikationen, die an OpenScape Business betrieben werden, sollten in Verbindung mit OpenScape Business getestet und freigeben sein.

HiPath TAPI 120/170 V2-Anwendungen

Für HiPath TAPI 120/170 V2 können die bestehenden Lizenzen nicht übernommen werden. Es müssen neue Lizenzen gekauft werden. HiPath TAPI 120/170 V2 muss deinstalliert und dafür OpenScape Business TAPI 120/170 V1 neu installiert und konfiguriert werden.

TAPI-Lizenzen sind in OpenScape Business userbezogen einrichtbar, daher entfällt die TAPI-Lizenzierung innerhalb der TAPI-Einrichtung. Die Lizenzierung ist ab dem ersten TAPI-Benutzer erforderlich (damit ist auch TAPI120 für die ersten 6 Benutzer nicht mehr lizenzfrei). Der CMD (CSTA Message Dispatcher) ist in OpenScape Business integriert. Ein separater Windows-Server für den CMD ist daher nicht mehr erforderlich. Die Anbindung an externe TAPI-Anwendungen ist für OpenScape Business und OpenScape Business S möglich. OpenScape Business erfordert ein V3-Mainboard oder UC Booster Card / Server. In einem Netzverbund muss entweder OpenScape Business S vorhanden sein oder ein V3-Mainboard, eine UC Booster Card oder ein UC Booster Server muss zumindest auf dem Master-Knoten vorhanden sein.

Für OpenScape Business TAPI 120/170 V2 V1 gelten im Vergleich zu HiPath TAPI 120/170 V2 die nachfolgend beschriebenen Änderungen.

- Der Zugang zum System erfolgt ausschließlich über Ethernet-LAN. RS-232- und S0-Schnittstellen werden nicht mehr unterstützt.
- Neue gemeinsame TAPI-Lizenz auf "pro Benutzer"-Basis für TAPI 120 TSP und TAPI 170 TSP.
- Die Lizenzen sind an die Locking-ID von OpenScape Business gebunden.
- Bestehende HiPath TAPI 120 TSP oder HiPath TAPI 170 TSP Benutzerlizenzen werden von dem neuen Lizenzierungsmechanismus nicht unterstützt.
- Keine Abwärtskompatibilität mit HiPath 3000 V8 oder V9
- Für TAPI 170 TSP gilt:
  - Der Zugang zum System erfolgt standardmäßig über den Port 8800.
  - Die Konfiguration der CSTA-Anmeldeinformationen im Setup-Dialog ist obligatorisch.
  - Multi-Node-Unterstützung im Netzwerk über den CSP des zentralen Master-Knotens.
- Für TAPI 120 TSP gilt:
  - Der Zugang zum System erfolgt standardmäßig über den Port 8900.
  - Single-Node-Unterstützung, auch bei Anbindung an den Master-Knoten eines Netzwerks.

Weitere externe Applikationen

Nachrangige Anwendungen, die extern an HiPath 3000 angebunden sind, können auf OpenScape Business nicht mehr betrieben werden.

HiPath 3000 Application	Nachfolgeanwendung für OpenScape Business	Hinweise
optiClient Attendant	OpenScape Business Attendant	Neue Anwendung Keine Lizenzübertragung möglich
optiClient BLF V1/V2	OpenScape Business Attendant (OpenScape Business BLF)	Neue Anwendung Keine Lizenzübertragung möglich
HiPath TAPI 120/170	OpenScape Business TAPI 120/170	Neue Anwendung Keine Lizenzübertragung möglich
Communication Clients der Entry WEB Services auf Plug PC	Integrierte UC-Lösung	Neue Anwendung Keine Lizenzübertragung möglich
myPortal for Mobile/ Tablet	myPortal to go	Neue Anwendung Keine Lizenzübertragung möglich

Geänderte/gestrichene Leistungsmerkmale von HiPath 5000 RSM

HiPath 5000 RSM wird nicht mehr unterstützt. Die Funktionalität von HiPath 5000 RSM wurde in OpenScape Business integriert. Das bedeutet, dass kein separater Server mehr benötigt wird.

Tabelle 37: Unterschiede zwischen HiPath 5000 RSM und OpenScape Business V3

Leistungsmerkmal	HiPath 5000 RSM	OpenScape Business
netzweite Lizenzierung, Zuordnung der Lizenzen zu den einzelnen Knoten	Alle System-Lizenzen des Netzes sind am CLS zu einer netzweiten Lizenz zusammengefasst.	Alle System-Lizenzen des Netzes sind am CLS zu einer netzweiten Lizenz zusammengefasst.
netzweite Administration	DB-Feature Server: Per Manager E werden alle Knoten des Netzes zu einem Netz-KDS zusammengefasst. Das Nummerierungsschema wird über das Netzwerk synchronisiert.	Über OpenScape Business Assistant (WBM) werden alle Knoten des Netzes mit einem Netzwerk-Wizard erfasst. Der Rufnummernhaushalt wird netzweit synchronisiert (geschlossene Nummerierung).

Leistungsmerkmal	HiPath 5000 RSM	OpenScape Business
Anbindung an Fremd-Knoten bzw. Fremd-Applikationen	SIP-Q-Anbindung von bis zu 4 Fremd-Knoten	Bis zu 10 SIP-Interconnection-Richtungen mit bis zu 2 SIP-Q bzw. 10 Native SIP oder bis zu 8 ITSP
Resilience / Survivability	User-Survivability für HFA-Telefone bei geschlossener Nummerierung	User-Survivability für HFA-Telefone mit geschlossener Nummerierung (Wechsel von OpenScape Business S <-> OpenScape Business X3 / X5 / X8)
Backup / Restore	Netzweit	Lokal
Inventory-Funktion	Netzweit	Lokal
Presence Manager	netzweite Funktion mit der Bereitstellung von 5000 RSM	Netzwerkweite Funktion durch Bereitstellung eines Multi-Node CSP basierend auf der OpenScape Business UC Booster Card, dem OpenScape Business UC Booster Server oder OpenScape Business S. Voraussetzung: geschlossene Nummerierung.
TAPI 170 am Standalone-System	TAPI 170 am Standalone-System läuft auf einem Windows-PC mit eigener Lizenzierung (separate Lizenzdatei für den TAPI 170).	TAPI 170 am Standalone-System läuft auf einem Windows-PC. Die Lizenzabfrage und Versorgung der TAPI 170 Database erfolgen aus der SQL-DB von OpenScape Business. Die Anbindung des TAPI 170 erfolgt über den CSP des Systems (OpenScape Business UC Booster Card, OpenScape Business UC Server Booster oder OpenScape Business S).

Leistungsmerkmal	HiPath 5000 RSM	OpenScape Business
TAPI 170 im Netzverbund	TAPI 170 läuft auf 5000 RSM mit eigener Lizenzierung (separate Lizenzdatei für den TAPI 170). Die TAPI 170 Database wird aus dem DB-Feature Server von 5000 RSM bezogen.	Wie am Standalone-System, jedoch erfolgt die Anbindung des TAPI 170 am Multinode-CSP des Master-Knotens (d.h. netzweit). Voraussetzung: geschlossene Nummerierung

Gemischte Netze

Ein gemischter Netzverbund aus OpenScape Business und OpenScape Office wird nicht unterstützt.

26.8 Migration innerhalb von OpenScape Business V3

Beschrieben werden die verschiedenen Migrationsmöglichkeiten innerhalb von OpenScape Business X V3 Systemen mit V2-Mainboards.

Anmerkung: Diese Szenarien sind für OpenScape Business X V3 Systeme mit V3-Mainboards überholt (nicht gültig)!

Erhöhung der Anzahl von UC Smart Benutzern

Es gibt folgende Möglichkeiten:

- Migration von **OpenScape Business X** (UC Smart) auf **OpenScape Business X** mit **UC Booster Card** (UC Smart)

  Sinnvoll für 50 - 150 UC Smart Benutzer. Alle Konfiguration- und Benutzerdaten werden übernommen. Bei Downgrades findet keine Datenübertragung statt. Für die neuen UC-Smart-Benutzer sind zusätzliche UC-Benutzerlizenzen erforderlich. OpenScape Business X1 ist nicht mit der UC Booster Card erweiterbar.
- Migration von **OpenScape Business X** (UC Smart) auf **OpenScape Business X** mit **UC Booster Server** (UC Smart)

  Sinnvoll für 50 - 500 UC Smart Benutzer. Alle Konfiguration- und Benutzerdaten werden übernommen. Bei Downgrades findet keine Datenübertragung statt. Für die neuen UC-Smart-Benutzer sind zusätzliche UC-Benutzerlizenzen erforderlich.
- Migration von **OpenScape Business X** mit **UC Booster Card** (UC Smart) auf **OpenScape Business X** mit **UC Booster Server** (UC Smart)

  Sinnvoll für 150 - 500 UC Smart Benutzer. Alle Konfiguration- und Benutzerdaten werden übernommen. Bei Downgrades findet keine Datenübertragung statt. Für die neuen UC-Smart-Benutzer sind zusätzliche UC-Benutzerlizenzen erforderlich.

Upgrade von UC Smart auf UC Suite

Es gibt folgende Möglichkeiten:

- Migration von **OpenScape Business X** (UC Smart) auf **OpenScape Business X** mit **UC Booster Card** (UC Suite)

  Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.
- Migration von **OpenScape Business X** (UC Smart) auf **OpenScape Business X** mit **UC Booster Server** (UC Suite)

  Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.
- Migration von **OpenScape Business X** mit **UC Booster Card** (UC Smart) auf **OpenScape Business X** mit **UC Booster Server** (UC Suite)

  Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.
- Migration innerhalb **OpenScape Business S** von UC Smart auf UC Suite

  Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.
- Migration innerhalb **OpenScape Business UC Booster Server** von UC Smart auf UC Suite

  Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.

Erhöhung der Anzahl von UC Suite Benutzern

Es gibt folgende Möglichkeiten:

- Migration von **OpenScape Business X** mit **UC Booster Card** (UC Suite) auf **OpenScape Business X** mit **UC Booster Server** (UC Suite)

  Sinnvoll für 150 - 500 UC Suite Benutzer. Alle Konfiguration- und Benutzerdaten werden übernommen. Bei Downgrades findet keine Datenübertragung statt. Für die neuen UC Suite-Benutzer sind zusätzliche UC-Benutzer- oder Groupware-Benutzerlizenzen erforderlich.

26.9 Migration von HW-Baugruppen

Die folgenden Aktionen zur Hardware-Migration sind für ein OpenScape Business X8-System möglich:

- Ersetzen von SLMO24N durch SLMU
- Ersetzen von SLMO8N durch SLMU
- Ersetzen von SLCN durch SLMUC (SLMU + CMAe)

26.9.1 Ersetzen von SLMO24N durch SLMU

Ein einfacher Kartenaustausch wird unterstützt. Die SLMO24N kann aus dem System entfernt und die neue SLMU eingesteckt werden. Alle konfigurierten Ports bleiben unverändert. Das Ausschalten des Systems ist nicht erforderlich.

26.9.2 Ersetzen von SLM8N durch SLMU

Da die SLMU-Karte mehr Ports als die SLMO8 besitzt, muss diese über die Administration entfernt werden. Um die Karte aus dem System zu entfernen, sollte der Online-Benutzer mit folgendem Dialog verwendet werden:

```
Systemadministration 29- 4 - 1
```

und ändern Sie den Kartentyp zu SLMUC.

Anmerkung:

Wenn die Benutzer für UC Suite konfiguriert sind, werden sie mit den Standardeinstellungen erstellt. Alle vorherigen Daten (z. B. Sprachbox, Fax, Benutzereinstellungen) gehen verloren.

Anmerkung:

Wenn die SLMO8- durch die SLMU-Karte ersetzt wird, ohne die Karte anhand der beschriebenen Schritte zu entfernen, könnten die zusätzlichen 16 Ports der SLMU-Karte nicht funktionsfähig sein, da sie nicht konfiguriert werden konnten. Dies geschieht, wenn bereits eine andere Karte den Port-Bereich dieser 16 Ports verwendet. Wenn nur eine SLMO8 im System vorhanden ist, sind bei einem Austausch durch die SLMU-Karte alle Ports verfügbar.

26.9.3 Ersetzen von SLCN durch SLMUC (SLMU + CMAe)

Da die SLMU-Karte mehr Ports als die SLCN besitzt, muss diese über die Administration entfernt werden, bevor die SLMUC an diesem Steckplatz eingesetzt wird. Die Schritte zur Entfernung der Karte sind folgende:

1) **Aufheben der Registrierung aller CMI-Mobilteile an ihrer Basisstation**
2) **Entfernen Sie die Karte aus dem System.**
3) **Entfernen Sie die SLCN-Karte über den Online-Benutzer mit dem Dialog:**

   ```
   Systemadministration 29- 4 - 1
   ```

   und ändern Sie den Kartentyp zu SLMUC.
4) **Installation der SLMUC-Karte**
5) **Konfigurieren des verwendeten Mobilteils**
6) **Registrieren der CMI-Mobilteile**

   Alle Benutzer der betroffenen DECT-Telefone (maximal 128) müssen diese zur Neuregistrierung abgeben.

Anmerkung:

Beim Ersetzen einer SLCN-Karte durch eine SLMUC ist auch eine Blindblende statt der für die SLCN verwendeten Kunststoffblende erforderlich.

Anmerkung:

Wenn die Benutzer für UC Suite konfiguriert sind, werden sie mit den Standardeinstellungen erstellt. Alle vorherigen Daten (z. B. Sprachbox, Fax, Benutzereinstellungen) gehen verloren.

26.10 Migration von OpenScape Business X1 V2 auf OpenScape Business X1W V3

Bei der Migration eines OpenScape Business X1-Modells muss das gesamte System ausgetauscht werden.

Bestehende Lizenzen können übernommen werden. Die Kundenkonfiguration kann nicht übernommen werden und muss nach der Migration manuell wiederhergestellt werden. Der bestehende Software-Support wird nach der Migration unverändert weitergeführt oder es wird ein neues Software-Support-Datum für das V3-Mainboard übernommen, wenn dieses über den 31.12.2026 hinaus gültig ist.

Vor der Migration sollte im System ein permanenter Zugang zum Unify-Lizenzserver (über das Internet) eingerichtet werden, falls nicht bereits vorhanden, und die Funktion „CLS Connect“ sollte aktiviert werden. Das vereinfacht die Lizenzübertragung und verkürzt erheblich die Migrationszeit. Der Kunde muss über den erforderlichen Zugang vom OpenScape Business System zum CLS informiert werden.

Erforderliche Bestellpositionen

Für die Migration des Modells X1 auf X1W mit V3-Mainboard ist Folgendes erforderlich, je nachdem, ob CLS Connect, UC Suite oder externe CSTA-Applikationen verwendet werden:

- X1W-System
- V3 SW auf M.2 SATA SSD-Datenspeicher
- M2 SSD 256 GB Massenspeicher (optional mit Applikation UC Suite)
- OpenScape Business Upgrade für OS Biz X1-Lizenz (wird immer benötigt)
- OpenScape Business CSTA-Lizenz (optional)

Bedingungen für funktionale Grenzen

Im Verlauf der Migration können bestehende Lizenzen vom vorhandenen X1-System vollständig auf das X1W-System mit V3 Mainboard übertragen werden. Die Lizenzübertragung ohne Aktivierung der Funktion CLS Connect erfordert die Lizenz „Migration“ und eine viel komplexere Handhabung und mehr Zeitaufwand als die Verwendung der Funktion CLS Connect.

X1-Systeme mit aktivem CLS Connect können nicht über die Funktion „Regeneration“ zu X1W-Systemen mit V3-Mainboard aufgerüstet werden. Die Lizenz „OpenScape Business Upgrade für OS Biz X1“ muss immer aktiviert

werden, aber es muss kein Bestätigungscode während des Upgrade-Prozesses eingegeben werden.

Ein Upgrade von OpenScape Business X1 PAYGO-Systemen auf OpenScape Business X1W PAYGO-Systeme wird nicht unterstützt.

Für den Fall, dass OpenScape Personal Edition-Clients auf dem System betrieben werden und entsprechende Lizenzen vorhanden sind, müssen diese immer manuell am zentralen Lizenzserver für die neue Locking-ID (MAC-Adresse) des V3-Mainboards neu generiert werden, unabhängig davon, ob CLS Connect verwendet wird oder nicht.

Die Kundenkonfiguration kann nicht übernommen werden und muss nach der Migration manuell wiederhergestellt werden.

Technische Abwicklung der Migration

Die wichtigsten technischen Schritte der Migration werden nachfolgend beschrieben. Es wird unterschieden zwischen

- Migration mit permanenter Lizenzierung
  - Migration mit aktivierter CLS Connect-Funktion und Anbindung an den zentralen Lizenzserver
  - Migration ohne CLS Connect-Funktion und ohne Anbindung an den zentralen Lizenzserver

Weitere Details zur technischen Abwicklung der Migration finden Sie im Handbuch OpenScape Business Administrations.

26.10.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf X1W V3 migrieren

Schritt für Schritt

1) Generieren Sie die Lizenzdateien auf dem zentralen Lizenzserver (CLS).
   a) Aktivieren Sie die Lizenz „OpenScape Business Upgrade für OS Biz X1“ auf dem X1-System mit V2-Mainboard. Geben Sie während des Aktivierungsvorgangs die MAC-Adresse des V3-Mainboards an.
   b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse auf dem X1W-System mit V3-Mainboard. Diese Lizenzdatei enthält die erweiterte SW-Unterstützung.
   c) Übertragung eventuell vorhandener Personal Edition-Lizenzen von der MAC-Adresse des V2-Mainboards auf die MAC-Adresse des V3-Mainboards mittels der Funktion „Regenerieren“ und Generierung einer neuen Lizenzdatei für die Personal Edition-Lizenzen.

2) Bereiten Sie das OpenScape Business System vor.
   a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7.
   b) Richten Sie im System einen Zugang zum zentralen Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung.
   c) Aktivieren Sie CLS Connect im System. Falls noch nicht geschehen, wird der SW-Support erneut um 3 Monate verlängert.

3) X1-Systemwechsel

a) Fahren Sie das X1-System herunter und schalten Sie alle Versorgungsspannungen aus.

b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem X1W-System.

c) Entfernen Sie die CAMe- und/oder die OCCB Voice Channel Booster-Karte vom V2-Mainboard und stecken Sie sie in das X1W V3-Mainboard ein.

d) Ersetzen Sie das X1-System durch das X1W-System.

e) Schließen Sie das Erdungskabel an das X1W-System an.

f) Schließen Sie die Telefon-, Amtsleitungs-, LAN- und ggf. USB-Kabel an das X1W-System an.

g) Versorgungsspannungen wieder einschalten, System bootet automatisch.

4) Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein.

a) Stellen Sie Systemdatum und -uhrzeit ein.

b) Stellen Sie das Applikationspaket ein.

- UC Smart für Systeme ohne UC oder mit UC Smart
- UC Suite für Systeme mit UC Suite

c) Stellen Sie die Systemkonfiguration wieder her.

- Manuelle Konfiguration des X1W.
- Importieren Sie die neu erstellte Lizenzdatei.

26.10.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf X1W V3 migrieren

Schritt für Schritt

1) Bereiten Sie das OpenScape Business System vor.

a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7.

2) Erstellen Sie auf dem zentralen Lizenzserver (CLS) eine Migrationslizenzdatei für das X1 mit V2-Mainboard.

a) Aktivieren Sie die „X1-Migrationslizenz“ für das vorhandene System.

b) Generieren Sie die neue Lizenzdatei für die MAC-Adresse des V2-Mainboards. Dazu muss die MAC-Adresse des X1W-Systems auf dem CLS eingegeben werden.

c) Laden Sie die Lizenzdatei vom CLS herunter. Diese Lizenzdatei enthält die erweiterte SW-Unterstützung.

3) Importieren Sie die Lizenzdatei in das OpenScape Business X1-System mit V2-Mainboard.

4) Notieren Sie den Bestätigungscode, der im OpenScape Business Assistant angezeigt wird.

5) Generieren Sie auf dem zentralen Lizenzserver (CLS) eine neue Lizenzdatei für das X1W-System mit V3-Mainboard.

a) Erstellen Sie auf dem CLS eine neue Lizenzdatei für die MAC-Adresse des X1W-Systems mit V3-Mainboard, indem Sie die MAC-Adresse des

X1 mit V2-Mainboard mit dem zuvor notierten Bestätigungscode erneut generieren.

- Suchen Sie auf dem CLS das OpenScape Business System mit der MAC-Adresse des X1W-Systems mit V3-Mainboard.
- Entsperren Sie das OpenScape Business System, indem Sie den Bestätigungscode eingeben und aktivieren.
- Generieren Sie die Lizenzdatei erneut.

b) Laden Sie die neu generierte Lizenz vom CLS herunter.

6) Austausch des Mainboards

a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus.
b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem X1W-System mit V3-Mainboard.
c) Entfernen Sie die CAMe- und/oder die OCCB Voice Channel Booster-Karte vom V2-Mainboard und stecken Sie sie in das X1W-System mit V3-Mainboard ein.
d) Ersetzen Sie das X1-System mit V2-Mainboard durch das X1W-System mit V3-Mainboard.
e) Schließen Sie das Erdungskabel an das X1W-System an.
f) Schließen Sie die Telefon-, Amtsleitungs-, LAN- und ggf. USB-Kabel an das X1W-System an.
g) Schalten Sie die Stromversorgung wieder ein und das System startet automatisch.

7) Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein.

a) Stellen Sie Systemdatum und -uhrzeit ein.
b) Stellen Sie das Applikationspaket ein.

- UC Smart für Systeme ohne UC oder mit UC Smart
- UC Suite für Systeme mit UC Suite

c) Stellen Sie die Systemkonfiguration wieder her.

- Manuelle Konfiguration des X1W

d) Importieren Sie nach dem Hochfahren des Systems manuell die neue Lizenzdatei in das V3-System.

27 Ausbaugrenzen und Kapazitäten

Die Ausbaugrenzen und Kapazitäten basieren auf systembedingten Maximalwerten für ein Einzelsystem. Die Maximalwerte eines Systems in einem Netzwerk können unterschiedlich sein.

27.1 Maximalwerte für Teilnehmer

- Daten für Systeme mit V2 OCC Mainboards finden Sie in Tabelle 38: Ausbaustufe Teilnehmer/Benutzer mit OCCx Mainboards auf Seite 1454
- Daten für Systeme mit V3 OCC Mainboards finden Sie in Tabelle 39: Stationen/Benutzer der Erweiterungsebene mit OCCSB/R, OCCMA/B oder OCCLA Hauptplatinen auf Seite 1455
- Daten für OpenScape Business S Server-Systemen finden Sie in Tabelle 40: Ausbaustufe Teilnehmer/Benutzer mit OpenScape Business S auf Seite 1456

Tabelle 38: Ausbaustufe Teilnehmer/Benutzer mit OCCx Mainboards

Teilnehmer	X1	X3W/R	X5W/R	X8
Teilnehmermaximum				
Max. Anzahl Teilnehmer[15]	30	500	500	500
IP-Teilnehmer				
IP-Teilnehmersystem (HFA)	20[16]	500	500	500
IP-Teilnehmer (SIP)	20[16]	500	500	500
TDM-Teilnehmer				
Max. Anzahl der TDM-Teilnehmer[17] [21]	30	384	384	384
Analoge Teilnehmer (TDM)	4	20	68	384
U_{P0}-Master-Teilnehmer (TDM)[21]	8	24	56	384
U_{P0}-Slave-Teilnehmer (TDM) (inkl. a/b- und S0-Adapter)	8	24	56	116
S0-ISDN-Teilnehmer (TDM)	2	36	52	128
DECT-CMI-Teilnehmer (TDM)	16	64	64	250
Mobility-Benutzer				
Max. Anzahl der Mobility-Teilnehmer[18]	30	150	150	150
Mobility Entry-Teilnehmer	20	150	150	150
myPortal to go-Benutzer[19]	30	150	150	150
Skype for Business-Teilnehmer	30	150	150	150

Teilnehmer	X1	X3W/R	X5W/R	X8
Andere Teilnehmer				
RAS-Teilnehmer	2	500	500	500
Virtuelle Teilnehmer frei konfigurierbar	30	250	250	250

Anmerkung: Für jede Systemkonfiguration muss geprüft werden, ob die Nennleistungsabgabe der systemeigenen Stromversorgung ausreicht oder ob eine externe Zusatzspeisung erforderlich ist (siehe *OpenScape Business Servicedokumentation - Leistungsbedarf eines Kommunikationssystems*).

Tabelle 39: Stationen/Benutzer der Erweiterungsebene mit OCCSB/R, OCCMA/B oder OCCLA Hauptplatinen

Teilnehmer	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Teilnehmer maximal								
Max. Anzahl Teilnehmer[15]	30	30	500	500	500	500	500	500
IP-Teilnehmer								
IP-Teilnehmersystem (HFA)	500	500	500	500	500	500	500	500
IP-Teilnehmer (SIP)	500	500	500	500	500	500	500	500
TDM-Teilnehmer								
Max. Anzahl der TDM-Teilnehmer[17] [21]	384	384	384	384	384	384	384	384

14 Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

15 Summe von: Teilnehmer IP (HFA), IP (SIP), Analog, UP0 Master/Slave, DECT (CMI), ISDN S0, Mobility und Deskshare

16 Summe von IP-Benutzern und Desk Share-Benutzern (Beschränkung durch Konfiguration)

17 Summe von: Teilnehmer Analog, UP0, DECT (CMI) und ISDN S0

18 Summe von: Mobility Entry, myPortal to go- Skype for Business-Teilnehmer

19 Die Anzahl der gleichzeitigen VoIP-Verbindungen des Abonnenten ist abhängig:

1) den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

2) den im System verfügbaren internen RTP-Proxykanälen für VoIP-Anrufe über das Internet.

20 der Anzahl der gleichzeitigen Verbindung je nach den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

21 Abhängig von den Telefontypen und dem Gesamtleistungsbedarf des Kommunikationssystems

Teilnehmer	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Analoge Teilnehmer (TDM)	4	4	20	20	68	68	384	384
U_{P0} Master/Slave-Teilnehmer (TDM)[21]	8	8	24	24	56	56	384 Master 116 Slave	384 Master 116 Slave
S0-ISDN-Teilnehmer (TDM)	0	0	32	32	48	48	128	128
DECT-CMI-Teilnehmer (TDM)	16	16	64	64	64	64	250	250
Mobility-Benutzer								
Max. Anzahl der Mobility-Teilnehmer[18]	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500 [22]	150/ 500[22]	500	500
Mobility Entry-Teilnehmer	150	20	150	150	150	150	150	150
myPortal to go-Teilnehmer[19]	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500
myPortal for Teams-Benutzer[19]	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500
Skype for Business-Teilnehmer	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500

Tabelle 40: Ausbaustufe Teilnehmer/Benutzer mit OpenScape Business S

Teilnehmer	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Teilnehmermaximum			
Max. Anzahl Teilnehmer	50	500	1500
IP-Teilnehmer			
IP-Teilnehmersystem (HFA)	50	500	1500
IP-Teilnehmer (SIP)	50	500	500
Mobility-Benutzer			
Max. Anzahl der Mobility-Teilnehmer	50	250	500
Mobility Entry-Teilnehmer	50	150	150
myPortal to go-Teilnehmer	50	250	500

22 Werte sind gestaffelt nach Board-Version: Basic/Advanced

Teilnehmer	Basic Server (S)	Standard Server (S)	Advanced Server (S)
myPortal for Teams-Benutzer	50	250	500
Skype for Business-Teilnehmer	50	250	500

27.2 Maximalwerte für Leitungen

- Kanäle für alle Arten von Leitungen (Amts-, Quer-, Verbindungsleitungen usw.) in V2 OCC Mainboards finden Sie in Tabelle 41: Ausbaustufe Leitungskanäle mit OCCx Mainboards auf Seite 1457.
- Kanäle für alle Arten von Leitungen (Amts-, Quer-, Verbindungsleitungen usw.) in V3 OCC Mainboards finden Sie in Tabelle 42: Leitungskanäle der Expansionsstufe mit OCCSB/R, OCCMA/B oder OCCLA Hauptplatinen auf Seite 1458
- Kanäle für alle Arten von Leitungen (Amts-, Quer-, Verbindungsleitungen usw.) in OpenScape Business S finden Sie in Tabelle 43: Ausbaustufe Leitungskanäle mit OpenScape Business S auf Seite 1458

Tabelle 41: Ausbaustufe Leitungskanäle mit OCCx Mainboards

	X1	X3W/R	X5W/R	X8
Maximale Leitungskanäle				
Max. Anzahl von Leitungskanälen[23]	250	250	250	250
Leitungskanäle für die Verbindung von Telefoniedienstanbieter, Vernetzung, externem Computer				
SIP-Leitungskanäle (ITSP)	30	60[24]	60[24]	60[24]
SIPQ-Kanäle (Vernetzung)	100	100	100	100
ISDN S_0 - Kanäle (BRI)	4	20	52	128
ISDN S_{2M} - Kanäle (PRI)	-	30	30	80
ISDN CAS - Kanäle (PRI)	-	30	30	180
Analoge (a/b) Kanäle	-	X3R: 8 X3W: 16	X5R: 24 X5W: 48	120
Leitungskanäle für interne Zwecke				
MEB-Kanäle für interne Ansagen[25]	0	16	16	16
MEB-Leitungskanäle für UC Suite[26]	0	60 / 30 / 0[27]	60 / 30 / 0[27]	60 / 30 / 0[27]

23 Summe von: SIP-Leitung, ITSP, SIPQ, TDM-Leitungskanäle und MEB-Leitungskanäle ohne (MEB-Ansagekanäle).

24 Bei Vernetzung mit OpenScape Business S als ITSP-Gateway sind auch mehr als 60 Kanäle möglich

25 Die MEB-Kanäle werden vom System für systeminterne Ansagen dynamisch belegt. Sie sind immer in der maximalen Anzahl von Leitungskanälen enthalten.

26 Für Systeme mit UC Suite werden die MEB-Kanäle dynamisch generiert für: Voicemail, AutoAttendant, Fax, Call-Me-Verbindungen, Ansagen und Konferenzrufe. Sie gelten nur als Teil der maximalen Anzahl von Leitungskanälen in UC Suite-Systemen.

Tabelle 42: Leitungskanäle der Expansionsstufe mit OCCSB/R, OCCMA/B oder OCCLA Hauptplatinen

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Maximale Leitungskanäle								
Max. Anzahl von Leitungskanälen[23]	250	250	250	250	250	250	250	250
Leitungskanäle für die Verbindung von Telefoniedienstanbieter, Vernetzung, externem Computer								
SIP-Leitungskanäle (ITSP)	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	120	120
SIPQ-Kanäle (Vernetzung)	100	100	100	100	100	100	100	100
ISDN S_0 - Kanäle (BRI)	-	-	16	16	48	48	128	128
ISDN S_{2M} - Kanäle (PRI)	-	-	30	30	30	30	180	120
ISDN CAS - Kanäle (PRI)	-	-	30	30	30	30	180	120
Analoge (a/b) Kanäle	-	-	X3R: 8 X3W: 16	X3R: 8 X3W: 16	X5R: 24 X5W: 48	X5R: 24 X5W: 48	120	120
Leitungskanäle für interne Zwecke								
MEB-Kanäle für interne Ansagen[25]	16	16	16	16	16	16	16	16
MEB-Leitungskanäle für UC Suite[26]	0	30/60[28]	0	30/60[28]	0	30/60[28]	0	60

Tabelle 43: Ausbaustufe Leitungskanäle mit OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Maximale Leitungskanäle			
Max. Anzahl von Leitungskanälen[23]	250	250	250
Leitungskanäle für die Verbindung von Telefoniedienstanbieter, Vernetzung, externem Computer			
SIP-Leitungskanäle	180	180	180
SIPQ-Kanäle (Vernetzung)	100	100	100
Leitungskanäle für interne Zwecke			
MEB-Kanäle für interne Ansagen[25]	16	16	16

27 Die Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

28 Werte sind gestaffelt nach Board-Version: Basic/Advanced

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
MEB-Leitungskanäle für UC Suite[26]	60	60	60

27.3 Maximalwerte der Ressourcen

Tabelle 44: Ausbaustufen weitere Funktionen/Ressourcen

	X1		X3		X5		X8	Server (S)
	Rack	Wand	Rack	Wand	Rack	Wand	OCCL / OCCLA	
Systemressourcen								
DSP-Kanäle								
DSP G.711 ohne Verschlüsselung	8	8	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	n/a
DSP G.711 + G.729 ohne Verschlüsselung	8	8	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	n/a
DSP G.711 mit Verschlüsselung	6	6	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	n/a
DSP G.711 + G.729 mit Verschlüsselung	6	6	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	n/a
DSP Fax T.38 (für ISDN-Gateway)[32]	3	3	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	n/a
DSP Fax T.38 (für UC Suite Fax)[33]	-	-	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	n/a
RTP-Proxykanäle								
RTP-Proxykanäle	30	30	60	60	60	60	60	180
MEB-Leitungskanäle								
MEB-Leitungskanäle gesamt	**0**	**0**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76**
MEB-Leitungskanäle für Ansagen	0	0	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16

	X1		X3		X5		X8	Server (S)
	Rack	Wand	Rack	Wand	Rack	Wand	OCCL / OCCLA	
MEB-Leitungskanäle für UC Suite	-	-	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60
Warteschleifenmusik und PPP								
MOH-Quellen [29] (G.711a, G.711u, G.729ab, G.729a)	4	4	4	4	4	4	4	32
PPP-Kanäle	8	8	8	8	8	8	8	n/a
Ansagen								
Anzahl der Ansagegeräte pro System	16	16	16	16	16	16	16	16
Ansagegeräte über a/b	4	4	16	16	16	16	16	n/a
Ansagen über Smart VM	6	6	6	6	6	6	6	6
Ansage über UC-Suite	16	16	16	16	16	16	16	16
Ansage vor Beantwortung (System, nicht UC-Suite)								
Anzahl der Anrufer, für die eine Ansage gleichzeitig wiedergegeben werden kann	24	24	24	24	24	24	24	24
DTMF-Empfänger								
DTMF-Empfänger	16	16	16	16	16	16	16	Pro Gespräch via ITSP

29 Max. Anzahl von 16 gleichzeitigen Verbindungen pro MOH-Quelle

30 Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

31 Der Wert ist abhängig von UC Suite: System mit UC Suite / System ohne UC Suite

32 Werte gelten für OpenScape Business als ISDN-Gateway. G.711 zu T38 oder umgekehrt ohne UC Suite Fax

33 UC Suite kann generell bis zu 8 gleichzeitige Faxverbindungen verarbeiten. OpenScape Business X3/ X5/X8 als ISDN-Gateway kann abhängig vom DSP-Modul 3 bis 12 Faxe gleichzeitig verarbeiten. Beide Parameter in Kombination bestimmen die Anzahl der gleichzeitigen T.38- oder G.711-Faxverbindungen.

34 Die Werte sind gestaffelt nach Voice Channel Booster-Konfiguration: mit OCCBH oder OCCB3 / mit OCCBL oder OCCB1 / nur Mainboard

27.3.1 Details zur Verwendung von DSP-Kanälen

Innerhalb von OpenScape Business werden "DSP-Kanäle" für die Konvertierung (Transcodierung) von Datenströmen verwendet. Dies ist grundsätzlich erforderlich, wenn ein IP-zu-TDM- oder TDM-zu-IP-Übergang für die Sprachdaten besteht oder wenn eine Verschlüsselung der Sprachdaten erforderlich ist. Im Einzelnen:

- Sprachverbindung zwischen IP-Telefon und ISDN oder analoger (Stamm-)Leitung.
- Sprachverbindung über IP SIP/ITSP-Leitung und interne UP0/E, a/b oder ISDN-Telefone.
- Sprachverbindung von IP-Leitung oder IP-Abonnenten zu einer internen Konferenz. Hier ist ein Gateway-Kanal erforderlich für jede/jeden an einer Konferenz beteiligten Leitung/IP-Client.
- Verbindungen von UP0/E, A/B oder ISDN Telefonen oder ISDN/ Analogleitungen zu UC Suite-Ankündigungen, Voicemail, Fax oder Konferenzen.
- Verschlüsselte Sprachverbindungen zwischen Terminals und verschlüsselte Sprachverbindungen über ITSP-Leitungen. Dies ist nicht der Fall für die V3-Hauptplatine-Familie, ab OpenScape Business V3R4.
- Verbindungen zu interner Wartemusik erfordern einen DSP-Kanal pro konfiguriertem MoH-Codec.

Für die folgenden Verbindungen wird kein DSP-Kanal benötigt:

- Verbindung zwischen internen IP-Benutzern ohne Verschlüsselung (direkte Nutzlast).
- Verbindung zwischen ITSP und IP-Abonnenten ohne Verschlüsselung.

Die DSP-Kanäle werden durch einen Signalprozessor, der in den Modellen X1, X3, X5 und X8 auf der jeweiligen OCCL- oder OCCLA-Platine integriert ist, realisiert.

Je nach Art der Transcodierung kann ein Signalprozessor mehr oder weniger DSP-Kanäle gleichzeitig verarbeiten. Folgende Codierungen (Codecs) werden unterstützt:

- **Für Sprachverbindungen**
  - Konvertierung von IP (G.711) auf TDM mit G.711 oder umgekehrt.
  - Konvertierung von IP (G.711) auf TDM mit G.711 oder umgekehrt mit Verschlüsselung (SPE).
  - Konvertierung von IP (G.729) auf TDM mit G.711 oder umgekehrt.
  - Konvertierung von IP (G.729) auf TDM mit G.711 oder umgekehrt mit Verschlüsselung (SPE).
- **Für Faxverbindungen**
  - Konvertierung von T.38 auf G.711 bei Verwendung von OpenScape Business als ISDN-Gateway.
  - Konvertierung von G.711 Fax auf T.38 Fax oder umgekehrt, wenn Sie das UC-Suite Fax-Merkmal verwenden.

Reicht die Kapazität des auf der Hauptplatine integrierten Signalprozessors nicht aus, um die erforderliche Anzahl an DSP-Kanälen zu realisieren, können diese mit den optional erhältlichen "Sprachkanal-Booster"-Karten OCCBL oder OCCBH erweitert werden.

Die maximale Anzahl verfügbarer DSP-Kanäle in Abhängigkeit von der Codierung ist in Tabelle 11 angegeben. Bitte beachten Sie, dass jede Zeile die maximale Anzahl ähnlicher DSP-Kanäle darstellt, diese aber während des Betriebs vom System dynamisch zugewiesen werden. Die Anzahl der aktuell im Betrieb belegten DSP-Kanäle kann über den OpenScape Business Assistant (WBM) ermittelt werden. Weitere Hinweise zur Ermittlung der erforderlichen Anzahl DSP-Kanäle finden Sie im Administrationshandbuch.

27.3.2 Details zur Verwendung von RTP-Proxykanälen

OpenScape Business verwendet einen internen „RTP-Proxy“ für alle VoIP-Verbindungen über das Internet. Der Proxy bietet einen Pool von RTP-Kanälen, die den VoIP-Verbindungen über das Internet wie folgt zugeordnet sind:

- 1 RTP-Proxykanal pro ITSP-Anruf
- 1 RTP-Proxy-Kanal pro Unify Phone-Anruf
- 1 RTP-Proxykanal pro System Device @Home in einem Anruf
- 1 RTP-Proxykanal pro SIP Device @Home in einem Anruf
- 1 RTP-Proxykanal pro myPortal to go VoIP @Home in einem Anruf
- 1 RTP-Proxykanal pro myPortal @work VoIP @Home in einem Anruf

In den verschiedenen OpenScape Business-Modellen ist eine verschiedene Anzahl von RTP-Proxykanälen verfügbar. Siehe Tabelle 44: Ausbaustufen weitere Funktionen/Ressourcen auf Seite 1459.

Beispiele

- Ein externer abgehender Sprachanruf von einem internen IP-Systemteilnehmer über eine ISTP-Leitung erfordert einen RTP-Proxykanal.
- Ein externer Sprachanruf vom myPortal to go VoIP Client über internes WLAN (Campus) zu einem Teilnehmer im öffentlichen Netz über eine ITSP-Leitung erfordert einen RTP-Proxykanal. Dieser wird für die Verbindung über ITSP zum angerufenen Teilnehmer im öffentlichen Netz verwendet.
- Ein externer Sprachanruf vom myPortal to go VoIP-Client über öffentliches WLAN zu einem Teilnehmer im öffentlichen Netz über eine ITSP-Leitung erfordert zwei RTP-Proxykanäle. Ein RTP-Proxykanal ist für die Verbindung des VoIP-Clients zu OpenScape Business und ein anderer RTP-Proxykanal für die Verbindung über ITSP zum angerufenen Teilnehmer im öffentlichen Netz erforderlich.
- Ein externer Anruf, der über ITSP bei einem myPortal @work VoIP-Client im Homeoffice ankommt, erfordert zwei RTP-Proxykanäle. Ein RTP-Proxykanal ist für die Verbindung von ITSP zum OpenScape Business System und ein anderer für die Verbindung von OpenScape Business über das Internet zum myPortal @work VoIP-Client im Homeoffice erforderlich.

27.4 Maximalwerte für Leistungsmerkmale

Bei den hier beschriebenen Maximalwerten handelt es sich hauptsächlich um die Software-Kapazitäten von OpenScape Business.

27.4.1 Anbindung an Service-Provider

	X1W/R		X3W/R		X5W/R		X8W/R		Server (S)
	V2	V3	V2	V3	V2	V3	V2	V3	
ITSP (Internet-Telefonie-Service-Provider)-Anbindung									
SIP-Leitungskanäle	30	120	60	120	60	120	60	120	180
Gleichzeitig aktivierter ITSP	8	8	8	8	8	8	8	8	8
Richtungen									
Richtungen	16	16	16	16	16	16	16	16	16
Überlaufrichtungen pro Richtung	1	1	1	1	1	1	1	1	1

27.4.2 Teilnehmer

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Teilnehmerrufnummer/Durchwahlnummer					
Ziffern pro Teilnehmerrufnummer/ Durchwahlnummer	16 (Standard = 3)	16 (Standard = 3)	16 (Standard = 3)	16 (Standard = 3)	16 (Standard = 3)

27.4.3 UC Smart-Ausbaustufen

- Ausbaustufen mit V2 OCC Mainboards finden Sie in Tabelle 45: Ausbaustufe UC SMART mit OCCx Mainboards auf Seite 1463
- Ausbaustufen mit V3 OCC Mainboards finden Sie in Tabelle 46: Ausbaustufe UC Smart mit OCCSB/R, OCCMA/B oder OCCLA Mainboards auf Seite 1465
- Ausbaustufen mit OpenScape Business S Server-Systemen finden Sie in Tabelle 47: Ausbaustufe UC Smart mit OpenScape Business S auf Seite 1466

Tabelle 45: Ausbaustufe UC SMART mit OCCx Mainboards

	X1	X3W/R	X5W/R	X8
UC Smart Benutzer maximal				
Max. Anzahl von UC Smart-Benutzern (Konten)	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
UC Smart Clients				
Anzahl der gleichzeitig aktiven UC-Clients.[36]	30	500/ 300/ 150[35]	500/ 300/ 150[35]	500/ 300/ 150[35]

	X1	X3W/R	X5W/R	X8
myPortal @work	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern[37]	20	30	30	30
myPortal to go[37]	30	150/ 150/ 50[35]	150/ 150/ 50[35]	150/ 150/ 50[35]
Deskphone CP 400/600/600E/ 700/700X/710 (UC-Modus)	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
OpenScape Business Attendant	8	8	8	8
Anwesenheitsstatus				
Status pro Benutzer	9	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1	1
Favoriten				
Favoriten pro Benutzer	100	100	100	100
Favoritengruppen pro Benutzer	10	10	10	10
Anrufjournal				
Anrufjournaleinträge pro Benutzer	100	100	100	100
UC Smart Verwaltete Konferenz (über UC Client)				
Anzahl der verwalteten Konferenzen	5	5	5	5
Anzahl der Benutzer pro verwalteter Konferenz	16	16	16	16
Kanäle für verwaltete Konferenzen	30	30	30	30

35 Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

36 Summe von: myPortal @work, myPortal to go, CP 400/600/600E/700/700X/710 UC-Modus, Application Launcher, Business Attendant, TAPI 120 (WSI), Drittanbieter-WSI-Clients (Hintergrund: Mehrere Clients mit dem gleichen UC Smart-Konto können sich am System anmelden)

37 Die Anzahl der gleichzeitigen VoIP-Verbindungen des Teilnehmers hängt ab von:

1) den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

2) den im System verfügbaren internen RTP-Proxykanälen für VoIP-Anrufe über das Internet.

38 der Anzahl der gleichzeitigen Verbindung je nach den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

Tabelle 46: Ausbaustufe UC Smart mit OCCSB/R, OCCMA/B oder OCCLA Mainboards

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
UC Smart Benutzer maximal								
Max. Anzahl von UC Smart-Benutzern (Konten)	150	150	150/ 500[39]	150/ 500[39]	150/ 500[39]	150/ 500[39]	500	500
UC Smart Clients								
Anzahl der gleichzeitig aktiven UC-Clients.[36]	150	150	150/ 500[39]	300 / 1000	150/ 500[39]	300/ 1000[39]	1000	1000
myPortal @work	150	150	150/ 250[39]	150/ 250[39]	150/ 250[39]	150/ 250[39]	250	250
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern[37]	150	150	30/ 70[39]	30/ 70[39]	30/ 70[39]	30/ 70[39]	70	70
myPortal to go[37]	150	150	150/ 500[39]	150/ 500[39]	150/ 500[39]	150/ 500[39]	500	500
myPortal for Teams	150	150	150/ 500[39]	150/ 500[39]	150/ 500[39]	150/ 500[39]	500	500
Deskphone CP 400/600/600E/ 700/700X/710 (UC-Modus)	150	150	150/ 500[39]	150/ 500[39]	150/ 500[39]	150/ 500[39]	500	500
OpenScape Business Attendant	8	8	8	8	8	8	8	8
Anwesenheitsstatus								
Status pro Benutzer	9	9	9	9	9	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1	1	1	1	1	1
Favoriten								
Favoriten pro Benutzer	100	100	100	100	100	100	100	100
Favoritengruppen pro Benutzer	10	10	10	10	10	10	10	10
Anrufjournal								
Anrufjournaleinträge pro Benutzer	100	100	100	100	100	100	100	100

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
UC Smart Verwaltete Konferenz (über UC Client)								
Anzahl der verwalteten Konferenzen	5	5	5	5	5	5	5	5
Anzahl der Benutzer pro verwalteter Konferenz	16	16	16	16	16	16	16	16
Kanäle für verwaltete Konferenzen	30	30	30	30	30	30	30	30

Tabelle 47: Ausbaustufe UC Smart mit OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
UC Smart Benutzer maximal			
Max. Anzahl von UC Smart-Benutzern (Konten)	50	500	1500
UC Smart Clients			
Anzahl der gleichzeitig aktiven UC-Clients.[36]	50	500	1500
myPortal @work	50	250	500
myPortal to go[37]	50	250	500
myPortal for Teams	50	250	500
Deskphone CP 400/600/600E/ 700/700X/710 (UC-Modus)	50	250	500
OpenScape Business Attendant	8	8	8
Anwesenheitsstatus			
Status pro Benutzer	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1
Favoriten			
Favoriten pro Benutzer	100	100	100
Favoritengruppen pro Benutzer	10	10	10
Anrufjournal			

39 Werte sind gestaffelt nach Board-Version: Basic/Erweitert

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Anrufjournaleinträge pro Benutzer	100	100	100
UC Smart Verwaltete Konferenz (über UC Client)			
Anzahl der verwalteten Konferenzen	10	10	10
Anzahl der Benutzer pro verwalteter Konferenz	16	16	16
Kanäle für verwaltete Konferenzen	30	30	30

27.4.4 Smart Voicemail Ausbaustufen

- Ausbaustufen mit V2 OCC Mainboards finden Sie in Tabelle 48: Ausbaustufe Smart Voicemail mit OCCx Mainboards auf Seite 1467
- Ausbaustufen mit V3 OCC Mainboards finden Sie in Tabelle 49: Ausbaustufe Smart Voicemail mit OCCSB/R, OCCMA/B oder OCCLA Mainboards auf Seite 1467
- Ausbaustufen mit OpenScape Business S Server-Systemen finden Sie in Tabelle 50: Ausbaustufe Smart Voicemail mit OpenScape Business S auf Seite 1468

Tabelle 48: Ausbaustufe Smart Voicemail mit OCCx Mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
Smart Voicemail					
Smart Voicemail-Boxen	30	320	320	320	1500
Nachrichten pro Voicemail-Box	100	100	100	100	100
Aufzeichnungszeit pro Anruf (Minuten)	2	2	2	2	2
Gesamtaufnahmekapazität in Stunden	32	32	32	32	32
Gleichzeitige Voicemail-Verbindungen (Kanäle)	10	10	10	10	60
Ansagen	16	16	16	16	16
Company/AutoAttendants	100	100	100	100	100
Company/AutoAttendants (gleichzeitig aktiv)	6	6	6	6	6

Tabelle 49: Ausbaustufe Smart Voicemail mit OCCSB/R, OCCMA/B oder OCCLA Mainboards

	X1W/R		X3W/R	X5W/R		X8		
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Smart Voicemail								

	X1W/R		X3W/R	X5W/R		X8		
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Smart Voicemail-Boxen	320	320	320/ 500[40]	320/ 500[40]	320/ 500[40]	320/ 500[40]	500	500
Nachrichten pro Voicemail-Box	100	100	100	100	100	100	100	100
Aufzeichnungszeit pro Anruf (Minuten)	2	4	4	4	4	4	4	4
Gesamtaufnahmekapazität in Stunden	32	64	32	64	32	64	32	64
Gleichzeitige Voicemail-Verbindungen (Kanäle)	30	30	30	30	30	30	30	30
Ansagen	16	16	16	16	16	16	16	16
Company/ AutoAttendants	100	100	100	100	100	100	100	100
Company/ AutoAttendants (gleichzeitig aktiv)	6	6	6	6	6	6	6	6

Tabelle 50: Ausbaustufe Smart Voicemail mit OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Smart Voicemail			
Smart Voicemail-Boxen	1500	1500	1500
Nachrichten pro Voicemail-Box	100	100	100
Aufzeichnungszeit pro Anruf (Minuten)	4	4	4
Gesamtaufnahmekapazität in Stunden	64	64	64
Gleichzeitige Voicemail-Verbindungen (Kanäle)	60	60	60
Ansagen	16	16	16
Company/AutoAttendants	100	100	100
Company/AutoAttendants (gleichzeitig aktiv)	6	6	6

40 Werte sind gestaffelt nach Board-Version: Basic/Erweitert

27.4.5 UC Suite-Ausbaustufen

- Ausbaustufen mit V2 OCC Mainboards finden Sie in Tabelle 51: Ausbaustufe UC Suite mit V2 Mainboards auf Seite 1469
- Ausbaustufen mit V3 OCC Mainboards finden Sie in Tabelle 52: Ausbaustufe UC Suite mit OCCSB, OCCMA/B oder OCCLA Mainboards auf Seite 1472
- Ausbaustufen mit OpenScape Business S Server-Systemen finden Sie in Tabelle 53: Ausbaustufe UC Suite mit OpenScape Business S auf Seite 1475

Tabelle 51: Ausbaustufe UC Suite mit V2 Mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
UC Suite Benutzer maximal					
Max. Anzahl von UC Suite-Benutzern (Konten)	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	1500
UC Suite Clients					
Anzahl der gleichzeitig aktiven UC-Clients.[42]	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myPortal for Desktop	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myPortal for Outlook	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myAgent (gleichzeitig aktiv)	-	64	64	64	64
myAgent (konfigurierbar)	-	192	192	192	192
myReports	-	1	1	1	1
myAttendant	-	20	20	20	20
myPortal @work	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	250
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern[44]	-	30	30	30	60
myPortal to go[44]	-	150/ 150/ 0[41]	150/ 150/ 0[41]	150/ 150/ 0[41]	250
Deskphone 400/600/600E/700/700X/710	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	250
OpenScape Business Attendant	-	8	8	8	8
Anwesenheitsstatus					
Status pro UC Suite Teilnehmer	-	9	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	-	1	1	1	1

	X1	X3W/R	X5W/R	X8	Server (S)
Anrufjournal (myPortal for Desktop/myPortal for Outlook)					
Archivierungsdauer in den UC Clients (Tage)	-	30 Standard = 30	30 Standard = 30	30 Standard = 30	30 Standard = 30
Archivierungsdauer im Kommunikationssystem	-	365 Standard = 30	365 Standard = 30	365 Standard = 30	365 Standard = 30
Anrufjournaleinträge[46]	-	Uneingeschränkt[46]	Uneingeschränkt[46]	Uneingeschränkt[46]	Uneingeschränkt[46]
Anrufjournaleinträge myPortal for Desktop modernes GUI	-	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb
UC Suite Voicemail					
VM-Boxen	-	500/ 500/ 0[45]	500/ 500/ 0[45]	500/ 500/ 0[45]	1500
VM-Gruppen	-	20/ 20/ 0	20/ 20/ 0	20/ 20/ 0	20
Nachrichten pro Sprachbox[46]	-	n/a	n/a	n/a	n/a
Aufzeichnungsdauer pro Anruf (Minuten)	-	15	15	15	15
Aufzeichnungsdauer zur Weiterleitung per E-Mail (Minuten)[47]	-	~10	~10	~10	~10
Gesamtaufnahmekapazität (Stunden)[46]	-	n/a	n/a	n/a	n/a
Gleichzeitige Verbindungen zu Voicemail (MEB-Kanäle)	-	30	30	30	60
UC Suite AutoAttendant					
Personal AutoAttendant	-	20/ 20/ 0[41]	20/ 20/ 0[41]	20/ 20/ 0[41]	20
Company AutoAttendant	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Multi-User-Chat (Instant Messaging)					
Interne Kommunikationspartner	-	unbeschränkt	unbeschränkt	unbeschränkt	unbeschränkt
Externe Kommunikationspartner (XMPP)	-	-	-	-	-
Ansagen pro UC Suite Benutzer					
Begrüßungsansagen	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Ansagen basierend auf Anwesenheitsstatus	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1

	X1	X3W/R	X5W/R	X8	Server (S)
Ansage Personal AutoAttendant	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
UC Suite Anrufaufzeichnung					
Aufzeichnungsdauer pro Anruf/Konferenz	-	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer
UC Suite Fax					
Faxboxen	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
Faxbox-Gruppen	-	60/ 60/ 0[41]	60/ 60/ 0[41]	60/ 60/ 0[41]	60
Teilnehmer pro Faxbox-Gruppe	-	10/ 10/ 0[41]	10/ 10/ 0[41]	10/ 10/ 0[41]	10
Faxlänge in Seiten	-	500/ 500/ 0[41]	500/ 500/ 0[41]	500/ 500/ 0[41]	500
Gleichzeitige T.38 Faxgeräte	-	8/ 3/ 0[41]	8/ 3/ 0[41]	8/ 3/ 0[41]	8
Serienfaxempfänger	-	unbeschränkt	unbeschränkt	unbeschränkt	unbeschränkt
UC Suite Konferenzen					
Gleichzeitige UC Suite Konferenzen	-	5/ 5/ 0[41]	5/ 5/ 0[41]	5/ 5/ 0[41]	10
Teilnehmer pro UC Suite Konferenz	-	16/ 16/ 0[41]	16/ 16/ 0[41]	16/ 16/ 0[41]	16
Externe Teilnehmer als Benutzer pro UC Suite Konferenz	-	15/ 15/ 0[41]	15/ 15/ 0[41]	15/ 15/ 0[41]	15
Max. Anzahl Kanäle für UC Suite Konferenzen	-	30/ 30/ 0[41]	30/ 30/ 0[41]	30/ 30/ 0[41]	60
Anzahl der reservierten Kanäle für UC Suite Ad-hoc- und Meet-Me-Konferenzen	-	20/ 20/ 0[41]	20/ 20/ 0[41]	20/ 20/ 0[41]	60
Externe Datenbankanbindung (LDAP)					
Externe Datenbankverbindungen von UC Server	-	10/ 10/ 0[41]	10/ 10/ 0[41]	10/ 10/ 0[41]	10

41 Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

42 Summe von: myPortal Desktop, myPortal for Outlook, myAttendant, myAgent, myReports, myPortal @work, myPortal to go, myPortal for Teams, CP 400/600/600E/700/700X/710 UC-Modus (Hintergrund: Mehrere Clients mit dem gleichen UC Suite-Konto können sich am System anmelden)

43 Der niedrigere Wert gilt für Systeme mit UC Suite Contact Center

44 Die Anzahl der gleichzeitigen VoIP-Verbindungen des Teilnehmers hängt ab von

1) den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

2) den im System verfügbaren internen RTP-Proxykanälen für VoIP-Anrufe über das Internet.

45 Die UC Booster Card unterstützt maximal 500 Voicemail-Boxen, unabhängig vom UC Suite Client-Limit (150 Benutzer).

Tabelle 52: Ausbaustufe UC Suite mit OCCSB, OCCMA/B oder OCCLA Mainboards

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
UC Suite Benutzer maximal						
Max. Anzahl von UC Suite-Benutzern (Konten)	-	50/ 500[48] 300 bei Contact Center	-	50/ 500[48]	-	500 300 bei Contact Center
UC Suite Clients						
Anzahl der gleichzeitig aktiven UC-Clients.[42]	-	100/ 1000[48] 600 bei Contact Center	-	100/ 1000[48] 600 bei Contact Center	-	1000 600 bei Contact Center
myPortal for Desktop	-	50/ 500[48] 300 bei Contact Center	-	50/ 500[48] 300 bei Contact Center	-	500 300 bei Contact Center
myPortal for Outlook	-	50/ 500[48] 300 bei Contact Center	-	50/ 500[48] 300 bei Contact Center	-	500 300 bei Contact Center
myAgent (gleichzeitig aktiv)	-	0/ 64[48]	-	0/ 64[48]	-	64
myAgent (konfigurierbar)	-	0/ 192[48]	-	0/ 192[48]	-	192
myReports	-	0/ 1[48]	-	0/ 1[48]	-	1
myAttendant	-	4/ 20[48]	-	4/ 20[48]	-	20
myPortal @work	-	50/ 250[48] 300 bei Contact Center	-	50/ 250[48] 300 bei Contact Center	-	250 300 bei Contact Center

46 Der Wert hängt von der verfügbaren HD-/SSD-Speicherkapazität der Festplatte ab. Eine teilnehmerbezogene Begrenzung ist nicht implementiert.

1) Voicemail / Aufzeichnungen: Eine Minute Aufnahmezeit benötigt ca. 1 MB Speicherplatz

2) Fax: Ein Normfax (2 DIN-A4-Seiten) entspricht ca. 48 KB Speicherbedarf

Beispiel: Das Speichervolumen der Partition für die Aufzeichnung von Sprachansagen, Sprachnachrichten, Sprachanrufe und Faxe beträgt 20 GB auf einer Festplatte mit 160 GB. Das entspricht einer Gesamtaufzeichnungsdauer von ca. 20.000 Minuten.

47 Bei längeren Aufzeichnungen wird die Aufnahme in mehrere Dateien aufgeteilt und gesendet.

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern[44]	-	30/ 70[48]	-	30/ 70[48]	-	70
myPortal to go[44]	-	50/ 500[48] 300 bei Contact Center	-	50/ 500[48] 300 bei Contact Center	-	500 300 bei Contact Center
myPortal for Teams	-	50/ 500[48] 300 bei Contact Center	-	50/ 500[48] 300 bei Contact Center	-	500 300 bei Contact Center
Deskphone CP 400/600/600E/ 700/700X/710	-	50/ 500[48] 300 bei Contact Center	-	50/ 500[48] 300 bei Contact Center	-	500 300 bei Contact Center
OpenScape Business Attendant	-	8	-	8	-	8
Anwesenheitsstatus						
Status pro UC Suite Teilnehmer	-	9	-	9	-	9
Sprachbox-Ansagen pro Anwesenheitsstatus	-	1	-	1	-	1
Anrufjournal (myPortal for Desktop/myPortal for Outlook)						
Archivierungsdauer in den UC Clients (Tage)	-	30 Standard = 30	-	30 Standard = 30	-	30 Standard = 30
Archivierungsdauer im Kommunikationssystem	-	365 Standard = 30	-	365 Standard = 30	-	365 Standard = 30
Anrufjournaleinträge[46]	-	Uneingeschränkt[46]		Uneingeschränkt[46]		Uneingeschränkt[46]
Anrufjournaleinträge myPortal for Desktop modernes GUI	-	100 nach Inbetriebnahme >100 im Betrieb	-	100 nach Inbetriebnahme >100 im Betrieb	-	100 nach Inbetriebnahme >100 im Betrieb
UC Suite Voicemail						
VM-Boxen	-	50/ 500[48]	-	50/ 500[48]	-	500
VM-Gruppen	-	32	-	32	-	32

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Nachrichten pro Sprachbox[46]	-	n/a	-	n/a	-	n/a
Aufzeichnungsdauer pro Anruf (Minuten)	-	15	-	15	-	15
Aufzeichnungsdauer zur Weiterleitung per E-Mail (Minuten)[47]	-	~10	-	~10	-	~10
Gesamtaufnahmekapazität (Stunden)[46]		n/a	-	n/a	-	n/a
Gleichzeitige Verbindungen zu Voicemail (MEB-Kanäle)	-	30/ 60[48]	-	30/ 60[48]	-	60
UC Suite AutoAttendant						
Personal AutoAttendant	-	20	-	20	-	20
Company AutoAttendant	-	1	-	1	-	1
Multi-User-Chat (Instant Messaging)						
Interne Kommunikationspartner	-	unbeschränkt	-	unbeschränkt	-	unbeschränkt
Ansagen pro UC Suite Benutzer						
Begrüßungsansagen	-	1	-	1	-	1
Ansagen basierend auf Anwesenheitsstatus	-	1	-	1	-	1
Ansage Personal AutoAttendant	-	1	-	1	-	1
UC Suite Anrufaufzeichnung						
Aufzeichnungsdauer pro Anruf/Konferenz	-	Begrenzt durch Anrufdauer	-	Begrenzt durch Anrufdauer	-	Begrenzt durch Anrufdauer
UC Suite Fax						
Faxboxen	-	50/ 500[48]	-	50/ 500[48]	-	500
Faxbox-Gruppen	-	60	-	60	-	60
Teilnehmer pro Faxbox-Gruppe	-	10	-	10	-	10
Faxlänge in Seiten	-	500	-	500	-	500
Gleichzeitige T.38 Faxgeräte	-	3/ 8[48]	-	3/ 8[48]	-	8
Serienfaxempfänger	-	unbeschränkt	-	unbeschränkt	-	unbeschränkt
UC Suite Konferenzen						

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Gleichzeitige UC Suite Konferenzen	-	5	-	5	-	5
Teilnehmer pro UC Suite Konferenz	-	16	-	16	-	16
Externe Teilnehmer als Benutzer pro UC Suite Konferenz	-	15	-	15	-	15
Max. Anzahl Kanäle für UC Suite Konferenzen	-	30	-	30	-	30
Anzahl der reservierten Kanäle für UC Suite Ad-hoc- und Meet-Me-Konferenzen	-	20	-	20	-	20
Externe Datenbankanbindung (LDAP)						
Externe Datenbankverbindungen von UC Server	-	10	-	10	-	10

Tabelle 53: Ausbaustufe UC Suite mit OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
UC Suite Benutzer maximal			
Max. Anzahl von UC Suite-Benutzern (Konten)	150	500	1500
UC Suite Clients			
Anzahl der gleichzeitig aktiven UC-Clients.[42]	150	500	1500
myPortal for Desktop	50	500	1500
myPortal for Outlook	50	500	1500
myAgent (gleichzeitig aktiv)	0	64	64
myAgent (konfigurierbar)	0	192	192
myReports	1	1	1
myAttendant	20	20	20
myPortal @work	50	250	500

48 Werte sind gestaffelt nach Board-Version: Basic/Advanced

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern[44]	30	60	60
myPortal to go[44]	50	250	500
myPortal for Teams	50	250	500
Deskphone CP 400/600/600E/ 700/700X/710	50	250	500
OpenScape Business Attendant	8	8	8
Anwesenheitsstatus			
Status pro UC Suite Teilnehmer	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1
Anrufjournal (myPortal for Desktop/myPortal for Outlook)			
Archivierungsdauer in den UC Clients (Tage)	30 Standard = 30	30 Standard = 30	30 Standard = 30
Archivierungsdauer im Kommunikationssystem	365 Standard = 30	365 Standard = 30	365 Standard = 30
Anrufjournaleinträge[46]	Uneingeschränkt[46]	Uneingeschränkt[46]	Uneingeschränkt[46]
Anrufjournaleinträge myPortal for Desktop modernes GUI	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb
UC Suite Voicemail			
VM-Boxen	150	500	1500
VM-Gruppen	32	32	32
Nachrichten pro Sprachbox[46]	n/a	n/a	n/a
Aufzeichnungsdauer pro Anruf (Minuten)	15	15	15
Aufzeichnungsdauer zur Weiterleitung per E-Mail (Minuten)[47]	~10	~10	~10
Gesamtaufnahmekapazität (Stunden)[46]	n/a	n/a	n/a
Gleichzeitige Verbindungen zu Voicemail (MEB-Kanäle)	60	60	60
UC Suite AutoAttendant			
Personal AutoAttendant	20	20	20
Company AutoAttendant	1	1	1

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Multi-User-Chat (Instant Messaging)			
Interne Kommunikationspartner	unbeschränkt	unbeschränkt	unbeschränkt
Ansagen pro UC Suite Benutzer			
Begrüßungsansagen	1	1	1
Ansagen basierend auf Anwesenheitsstatus	1	1	1
Ansage Personal AutoAttendant	1	1	1
UC Suite Anrufaufzeichnung			
Aufzeichnungsdauer pro Anruf/Konferenz	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer
UC Suite Fax			
Faxboxen	1500	1500	1500
Faxbox-Gruppen	60	60	60
Teilnehmer pro Faxbox-Gruppe	10	10	10
Faxlänge in Seiten	500	500	500
Gleichzeitige T.38 Faxgeräte	8	8	8
Serienfaxempfänger	unbeschränkt	unbeschränkt	unbeschränkt
UC Suite Konferenzen			
Gleichzeitige UC Suite Konferenzen	10	10	10
Teilnehmer pro UC Suite Konferenz	16	16	16
Externe Teilnehmer als Benutzer pro UC Suite Konferenz	15	15	15
Max. Anzahl Kanäle für UC Suite Konferenzen	60	60	60
Anzahl der reservierten Kanäle für UC Suite Ad-hoc- und Meet-Me-Konferenzen	60	60	60
Externe Datenbankanbindung (LDAP)			
Externe Datenbankverbindungen von UC Server	10	10	10

27.4.6 Funktionen am Telefon

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Anruferliste für Systemtelefone (HFA)					
Anruferlisten pro System	650	650	650	650	1300
Anruferlisten pro Teilnehmer im System	1	1	1	1	1
Einträge pro Anruferliste	10	10	10	10	10

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Gespeicherte Ziffern pro Eintrag plus Belegungskennzahl	25 + (6)	25 + (6)	25 + (6)	25 + (6)	25 + (6)
Direktruftasten (DSS-Tasten)					
Beistellgeräte pro Kommunikationssystem	250	250	250	250	250
Beistellgeräte pro Telefon	2	2	2	2	2
Tasten pro OpenStage Beistellgerät	12	12	12	12	12
Tasten pro OpenStage Beistellgerät 15	18	18	18	18	18
Besetztlampenfelder (BLF) pro Kommunikationssystem	12	25	25	25	25
Tasten pro Besetztlampenfeld	90	90	90	90	90
Kurzwahl individuell (KWI)					
Einträge im KWI-Pool pro Kommunikationssystem	2000	2000	2000	2000	2000
Einträge pro Teilnehmer	10	10	10	10	10
Ziffern pro Eintrag (plus Belegungskennzahl)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Kurzwahl zentral (KWZ)					
Einträge im KWI-Pool pro Kommunikationssystem	8000	8000	8000	8000	8000
Zeichenlänge des Namens	16	16	16	16	16
Ziffern pro Eintrag (plus Belegungskennzahl)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Wahlwiederholung					
Einträge pro OpenStage 20/ 20E/ 20G/ 40/ 40G	3	3	3	3	3
Einträge pro OpenStage 15	10	10	10	10	10
Einträge pro OpenStage 60/ 60G/ 80/ 80G	30	30	30	30	30
Einträge pro Telefon ohne Display	1	1	1	1	1
Gespeicherte Ziffern pro Eintrag	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Anklopfen/Rufeinblendung					
Wartende Anrufer pro Telefon	16				
Parken					

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Parkpositionen pro System	10				
Rückrufe					
Rückrufeinträge pro Telefon	5				
Abwesenheitstexte/Mitteilungstexte					
Abwesenheitstexte pro System	250	250	250	250	250
Mitteilungstexte pro System	150	150	150	150	150
Konfigurierbare Abwesenheitstexte + Mitteilungstexte pro System	10 + 10	10 + 10	10 + 10	10 + 10	10 + 10
Zeichenlänge eines konfigurierbaren Abwesenheitstextes/ Mitteilungstextes	24	24	24	24	24
Empfangene Abwesenheitstexte/ Mitteilungstexte pro Telefon mit Display	5	5	5	5	5
Empfangene Abwesenheitstexte/ Mitteilungstexte pro Telefon ohne Display	1	1	1	1	1
Rufzuschaltung					
Zugeschaltete Teilnehmer	5				
Anrufumleitung (AUL)					
AUL-Ziele pro Telefon	4	4	4	4	4
Zeichen pro externem AUL-Ziel (plus Belegungskennzahl)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Verkettete AUL-Ziele					5
Systemgesteuerte Konferenzen					
Gleichzeitige System-Konferenzen pro System	10	10	10	10	8
Teilnehmer pro Konferenz	8	8	8	8	8
Externe Teilnehmer pro Konferenz	7	7	7	7	7
Konferenzkanäle	32	32	32	32	20
Türsprechstelle/Türöffner					
Anschlüsse über a/b-Schnittstellen pro System	4	4	4	4	-
Ziffern pro Codeeintrag	5	5	5	5	-
Leitungsvormerken					

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Gleichzeitige Einträge pro System	32	32	32	32	-

Anmerkung: Für alle oben genannten Szenarien der Anrufumleitung kann der Benutzer nur ein Weiterschaltungsziel pro MSN eingeben. Die maximale Anzahl weiterschaltbarer MSN ist 10.

Falls ITSP oder ISDN mit der Durchwahl konfiguriert ist, lautet diese Nummer 249.

27.4.7 Arbeiten im Team (Gruppen)

- Informationen zu V2 OCC Mainboards finden Sie in Tabelle 54: Daten für V2 Mainboards auf Seite 1480
- Informationen zu V3 OCC Mainboards finden Sie in Tabelle 55: Daten für V3 Mainboards auf Seite 1481
- Informationen zu OpenScape Business S Server-Systemen finden Sie in Tabelle 56: Daten für OpenScape Business S auf Seite 1483

Tabelle 54: Daten für V2 Mainboards

	X1	X3W/R	X5W/R	X8
Anrufübernahmegruppen				
Anrufübernahmegruppen pro System	32	32	32	32
Teilnehmer pro Anrufübernahmegruppe	32	32	32	32
Rufzuschaltung (benutzerkonfigurierbare Gruppe)				
Anzahl der Nebenstellen in der Rufzuschaltungsgruppe	5	5	5	5
Gruppenruf, Sammelanschluss, Basic-MULAPs				
Summe der Gruppenrufe, Sammelanschlüsse, Basic-MULAPs, Chef-MULAPs und Sprachbox-Gruppen pro Kommunikationssystem	800	800	800	800
Länge des Gruppennamens	16	16	16	16
Anzahl der Gruppen, denen ein Benutzer zugewiesen werden kann	32	32	32	32
Teilnehmer pro Gruppenruf, Sammelanschluss, Basic-MULAP	20	20	20	20
Chef-MULAPs, Team-Gruppen, Top-Gruppen und Voicemail-Gruppen:				
Summe der Chef-MULAPs, Team- und Top-Gruppen pro	500	500	500	500

	X1	X3W/R	X5W/R	X8
Teilnehmer pro Chef-MULAP, Team-Gruppe, Top-Gruppe	10	10	10	10
MULAP-Tasten pro Telefon	10	10	10	10
Voicemail-Gruppen				
Anzahl der Voicemail-Gruppen	20	20	20	20
Teilnehmer pro Sprachbox-Gruppe	20	20	20	20
Durchsage an Gruppe (Sprachdurchsage)				
Gleichzeitige Durchsagen pro Kommunikationssystem	1	1	1	1
Empfänger der Durchsage	20	20	20	20
UCD-Gruppen				
UCD-Gruppen pro System	60	60	60	60
Ansagen pro UCD-Gruppe	7	7	7	7
Prioritätsebenen pro UCD-Gruppe	10	10	10	10
Wartende Anrufe pro UCD-Gruppe (letzte Gruppe max. 72)	30	30	30	30
UCD-Agenten				
UCD-Agenten-IDs pro Kommunikationssystem	330	330	330	330
Gleichzeitig aktive UCD-Agenten pro Kommunikationssystem	64	64	64	64
UCD-Ansagen				
Anrufer pro Kommunikationssystem, denen gleichzeitig eine Ansage eingespielt werden kann	8	8	8	8

Tabelle 55: Daten für V3 Mainboards

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Anrufübernahmegruppen								
Anrufübernahmegruppen pro System	64	64	64/128[49]	64/128[49]	64/128[49]	64/128[49]	128	128
Teilnehmer pro Anrufübernahmegruppe	32	32	32	32	32	32	32	32
Rufzuschaltung (benutzerkonfigurierbare Gruppe)								
Anzahl der Nebenstellen in der Rufzuschaltungsgruppe	5	5	5	5	5	5	5	5

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Gruppenruf, Sammelanschluss, Basic-MULAPs								
Summe der Gruppenrufe, Sammelanschlüsse, Basic-MULAPs, Chef-MULAPs und Sprachbox-Gruppen pro Kommunikationssystem	800	800	800	800	800	800	800	800
Länge des Gruppennamens	16	16	16	16	16	16	16	16
Anzahl der Gruppen, denen ein Benutzer zugewiesen werden kann	32	32	32	32	32	32	32	32
Teilnehmer pro Gruppenruf, Sammelanschluss, Basic-MULAP	20	20	20/32[49]	20/32[49]	20/32[49]	20/32[49]	32	32
Chef-MULAPs, Team-Gruppen, Top-Gruppen und Voicemail-Gruppen:								
Summe der Chef-MULAPs, Team- und Top-Gruppen pro	500	500	500	500	500	500	500	500
Teilnehmer pro Chef-MULAP, Team-Gruppe, Top-Gruppe	10	10	10	10	10	10	10	10
MULAP-Tasten pro Telefon	10	10	10	10	10	10	10	10
Voicemail-Gruppen								
Anzahl der Voicemail-Gruppen	20	20	20	20	20	20	20	20
Teilnehmer pro Sprachbox-Gruppe	20	20	20	20	20	20	20	20
Durchsage an Gruppe (Sprachdurchsage)								
Gleichzeitige Durchsagen pro Kommunikationssystem	1	1	1	1	1	1	1	1
Empfänger der Durchsage	20	20	20/32[49]	20/32[49]	20/32[49]	20/32[49]	32	32
UCD-Gruppen								
UCD-Gruppen pro System	60	60	60	60	60	60	60	60

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Ansagen pro UCD-Gruppe	7	7	7	7	7	7	7	7
Prioritätsebenen pro UCD-Gruppe	10	10	10	10	10	10	10	10
Wartende Anrufe pro UCD-Gruppe (letzte Gruppe max. 72)	30	30	30	30	30	30	30	30
UCD-Agenten								
UCD-Agenten-IDs pro Kommunikationssystem	330	330	330	330	330	330	330	330
Gleichzeitig aktive UCD-Agenten pro Kommunikationssystem	64	64	64	64	64	64	64	64
UCD-Ansagen								
Anrufer pro Kommunikationssystem, denen gleichzeitig eine Ansage eingespielt werden kann	8	8	8	8	8	8	8	8

Tabelle 56: Daten für OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Anrufübernahmegruppen			
Anrufübernahmegruppen pro System	32	64	128
Teilnehmer pro Anrufübernahmegruppe	32	32	32
Rufzuschaltung (benutzerkonfigurierbare Gruppe)			
Anzahl der Nebenstellen in der Rufzuschaltungsgruppe	5	5	5
Gruppenruf, Sammelanschluss, Basic-MULAPs			
Summe der Gruppenrufe, Sammelanschlüsse, Basic-MULAPs, Chef-MULAPs und Sprachbox-Gruppen pro Kommunikationssystem	800	800	800
Länge des Gruppennamens	16	16	16
Anzahl der Gruppen, denen ein Benutzer zugewiesen werden kann	32	32	32

[49] Werte sind gestaffelt nach Board-Version: Basic/Erweitert

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Teilnehmer pro Gruppenruf, Sammelanschluss, Basic-MULAP	32	32	32
Chef-MULAPs, Team-Gruppen, Top-Gruppen und Voicemail-Gruppen:			
Summe der Chef-MULAPs, Team- und Top-Gruppen pro	500	500	500
Teilnehmer pro Chef-MULAP, Team-Gruppe, Top-Gruppe	10	10	10
MULAP-Tasten pro Telefon	10	10	10
Voicemail-Gruppen			
Anzahl der Voicemail-Gruppen	20	20	20
Teilnehmer pro Sprachbox-Gruppe	20	20	20
Durchsage an Gruppe (Sprachdurchsage)			
Gleichzeitige Durchsagen pro Kommunikationssystem	1	1	1
Empfänger der Durchsage	20	20	20
UCD-Gruppen			
UCD-Gruppen pro System	60	60	60
Ansagen pro UCD-Gruppe	7	7	7
Prioritätsebenen pro UCD-Gruppe	10	10	10
Wartende Anrufe pro UCD-Gruppe (letzte Gruppe max. 72)	30	30	30
UCD-Agenten			
UCD-Agenten-IDs pro Kommunikationssystem	330	330	330
Gleichzeitig aktive UCD-Agenten pro Kommunikationssystem	64	64	64
UCD-Ansagen			
Anrufer pro Kommunikationssystem, denen gleichzeitig eine Ansage eingespielt werden kann	8	8	8

27.4.8 Anruf-Routing

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Leitweglenkung LCR					
Gewählte Ziffern	24	24	24	24	24
Geprüfte Ziffern	24	24	24	24	24

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Wahlpläne (max. 10 Felder pro Plan)	1000	1000	1000	1000	1000
Wegetabellen	254	254	254	254	254
Wege pro Wegetabelle	16	16	16	16	16
Wahlregeln pro Richtung	254	254	254	254	254
Anzahl der Zeitzonen pro Tag/ Woche	8	8	8	8	8
Ziffern pro Wahlregel	40	40	40	40	40
Nachtschaltung					
Berechtigte Teilnehmer pro System	5	5	5	5	5
Notrufdienst E911 (nur für USA)					
Ziffern pro LIN (Location Identification Number)	16	16	16	16	16
Röchelschaltung/Hotline					
Hotlineziele pro Kommunikationssystem	6	6	6	6	6
VBZ-Gruppen					
VBZ-Gruppen pro System	64	64	64	64	64

Attendants für V2 Mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
myAttendant					
myAttendant (UC Suite) pro System	-	20	20	20	20
AutoAttendant (UC Smart)					
Company Auto-Attendant	100	100	100	100	100
AutoAttendant (UC Suite)					
Automatischer Vermittlungsplatz (VPL)	-	20/ 20/ 0[50]	20/ 20/ 0[50]	20/ 20/ 0[50]	20
OpenScape Business Attendant					
OpenScape Business Attendants pro System	-	8	8	8	8

50 Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster. Für V3 Mainboards ist der höchste Wert gültig.

Attendants für V3 Mainboards

	X1W/R	X3W/R	X5W/R	X8	Server (S)
myAttendant					
myAttendant (UC Suite) pro System	4	4/20[51]	4/20[51]	20	20
AutoAttendant (UC Smart)					
Company Auto-Attendant	100	100	100	100	100
AutoAttendant (UC Suite)					
Automatischer Vermittlungsplatz (VPL)	20	20/ 20/[51]	20/ 20[51]	20/ 20[51]	20
OpenScape Business Attendant					
OpenScape Business Attendants pro System	8	8	8	8	8

27.4.9 Multimedia Contact Center

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Contact Center Warteschlangen					
Warteschlangen pro Kommunikationssystem	-	50	50	50	50
Nachbearbeitung					
Nachbearbeitungscodes	-	unbeschränkt	unbeschränkt	unbeschränkt	unbeschränkt
Agenten					
(Agenten gleichzeitig aktiv)	-	64	64	64	64
Agenten (konfigurierbar)	-	192	192	192	192
Historische Berichte					
myReports Clients gleichzeitig aktiv pro System	-	1	1	1	1

27.4.10 Mobility Ausbaugrenzen

Tabelle 57: Daten für V2 OCC Mainboards

	X1	X3W/R	X5W/R	X8
Teleworker-Arbeitsplätze:				
Teleworker-Arbeitsplätze über VPN pro Kommunikationssystem	10	10	10	10
Mobility Teilnehmer:				

[51] Werte sind gestaffelt nach Board-Version: Basic/Erweitert

	X1	X3W/R	X5W/R	X8
Mobility Entry-Teilnehmer pro System	30	150	150	150
myPortal to go (UC Smart): Teilnehmer pro System	30	150/ 150/ 50[52]	150/ 150/ 50[52]	150/ 150/ 50[52]
myPortal to go (UC Suite): Teilnehmer pro System	-	150/ 150/ 0[52]	150/ 150/ 0[52]	150/ 150/ 0[52]

Tabelle 58: Daten für V3 OCC Mainboards

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Teleworker-Arbeitsplätze:								
Teleworker-Arbeitsplätze über VPN pro Kommunikationssystem	10	10	10	10	10	10	10	10
Mobility Teilnehmer:								
Mobility Entry-Teilnehmer pro System	150/ 500[53]	150/ 500[53]	150	150/ 500[53]	150/ 500[53]	150/ 500[53]	500	500
myPortal to go (UC Smart): Teilnehmer pro System	150	150	150/ 500[53]	150/ 500[53]	150/ 500[53]	150/ 500[53]	500	500
myPortal to go (UC Suite): Teilnehmer pro System	-	50	-	50/ 500 300 bei Contact Center	-	50/ 500 300 bei Contact Center	-	500 300 bei Contact Center
myPortal for Teams (UC Smart): Teilnehmer pro System	150	150	150/ 500[53]	150/ 500[53]	150/ 500[53]	150/ 500[53]	500	500
myPortal for Teams (UC Suite): Teilnehmer pro System	-	50	-	50/ 500 300 bei Contact Center	-	50/ 500 300 bei Contact Center	-	500 300 bei Contact Center

52 Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

53 Werte sind gestaffelt nach Board-Version: Basic/Erweitert

Tabelle 59: Daten für OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Mobility Teilnehmer:			
Mobility Entry-Teilnehmer pro System	50	150	150
myPortal to go (UC Smart): Teilnehmer pro System	50	250	500
myPortal to go (UC Suite): Teilnehmer pro System	50	250	500
myPortal for Teams (UC Smart): Teilnehmer pro System	50	250	500
myPortal for Teams (UC Suite): Teilnehmer pro System	50	250	500

27.4.11 Sicherheit

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Individuelles Codeschloss					
Ziffern pro Telefonschlosscode	5	5	5	5	5
Zulässige Zeichen	0 - 9	0 – 9	0 – 9	0 – 9	0 – 9
Amtsberechtigung					
Anzahl der Erlaubnislisten	6	6	6	6	6
Anzahl der Verbotslisten	6	6	6	6	6
Erlaubnisliste kurz (10 Einträge mit jeweils 32 Stellen)	5	5	5	5	5
Erlaubnisliste lang (100 Einträge mit jeweils 32 Stellen)	1	1	1	1	1
Verbotsliste kurz (10 Einträge mit jeweils 32 Stellen)	5	5	5	5	5
Verbotsliste lang (50 Einträge mit jeweils 32 Stellen)	1	1	1	1	1
Berechtigungsklassen					
Berechtigungsklassen pro System	15	15	15	15	15
Matrixgröße – Tag und Nacht – Anzahl der Amtsleitungen	30	30	30	30	30

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Erlaubnis- und Verbotslisten	15	15	15	15	15
Geschlossene verwendete Gruppen (VBZ-Gruppen)					
VBZ-Gruppen) pro System	16	64	64	64	64
Matrixgröße – Tag und Nacht – Anzahl der Amtsleitungen	30	30	30	30	30
Erlaubnis- und Verbotslisten	15	15	15	15	15

27.4.12 Vernetzung von OpenScape Business

Vernetzung von OpenScape Business X1W/R, OpenScape Business X3R/X3W, OpenScape Business X5R/X5W, OpenScape Business X8, OpenScape Business S: Darüber hinausgehende Ausbaugrenzen für Vernetzungen können über projektspezifische Freigaben beantragt werden. Bitte beachten Sie die aktuelle Vertriebsfreigabe.

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Vernetzung von OpenScape Business					
Vernetzte Kommunikationssysteme (Knoten)	8/ 32[54]	8/ 32[54]	8/ 32[54]	8/ 32[54]	8/ 32[54]
Teilnehmer im Netz	1000	1000	1000	1000	1000

27.4.13 Application Connectivity

Tabelle 60: Daten für V2 OCC Mainboards

	X1	X3W/R	X5W/R	X8
CSTA-Schnittstelle				
CSTA-Links via CSP pro System	-	4/ 4/ 0[55]	4/ 4/ 0[55]	4/ 4/ 0[55]
Monitorpunkte für Amtsleitungen oder Teilnehmer	-	1500	1500	1500
TAPI 170 Middleware Server	-	4	4	4
TAPI 120 Clients (CSTA)	-	150/ 150/ 0[55]	150/ 150/ 0[55]	150/ 150/ 0[55]
Web Services Interface (WSI)				
WSI - gleichzeitig aktive Clients in Summe	30	500/ 300/ 150[55]	500/ 300/ 150[55]	500/ 300/ 150[55]
myPortal @work	30	250/ 150/ 50[55]	250/ 150/ 50[55]	250/ 150/ 50[55]
myPortal to go	30	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]

[54] Die Werte sind gestaffelt nach: Netzwerk mit UC Suite / Netzwerk ohne UC Suite

	X1	X3W/R	X5W/R	X8
DeskPhone CP 400/600/600E/ 700/700X/710 mit WSI	30	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]
OpenScape Business Attendant	0	8/ 8/ 8[55]	8/ 8/ 8[55]	8/ 8/ 8[55]
OpenScape Business BLF	0	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]
Application Launcher	30	250/ 150/ 50[55]	250/ 150/ 50[55]	250/ 150/ 50[55]
TAPI 120 (WSI-Modus)	30	0/ 0/ 30[55]	0/ 0/ 30[55]	0/ 0/ 30[55]
Anwendung von Drittanbietern	Rest	Rest	Rest	Rest

Tabelle 61: Daten für V3 OCC Mainboards

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
CSTA-Schnittstelle								
CSTA-Links via CSP pro System	-	-	4	4	4	4	4	4
Monitorpunkte für Amtsleitungen oder Teilnehmer	1650	1650	1650/ 3750[56]	1650/ 3750[56]	1650/ 3750[56]	1650/ 3750[56]	3750	3750
TAPI 170 Middleware Server	4	4	4	4	4	4	4	4
TAPI 120 Clients (CSTA)	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
Web Services Interface (WSI)								
WSI - gleichzeitig aktive Clients in Summe	150	300	150/ 500[56]	300/ 1000[56]	150/ 500[56]	300/ 1000[56]	1000	1000
myPortal @work	150	150	150/ 250[56]	150/ 250[56]	150/ 250[56]	150/ 250[56]	250	250
myPortal to go	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
myPortal for Teams	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
DeskPhone CP 400/600/600E/ 700/700X/710 mit WSI	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500

55 Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
OpenScape Business Attendant	8	8	8	8	8	8	8	8
OpenScape Business BLF	150	150	150	150	150	150	150	150
Application Launcher	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
TAPI 120 (WSI-Modus)	**Anmerkung:** Produktauslauf auf V3 OCC Mainboards. In V3 nur für V2 Mainboards unterstützt.							
Anwendung von Drittanbietern	Rest	Rest	Rest	Rest	Rest	Rest	Rest	Rest

Tabelle 62: Daten für OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
CSTA-Schnittstelle			
CSTA-Links via CSP pro System	4	4	4
Monitorpunkte für Amtsleitungen oder Teilnehmer	3750	3750	3750
TAPI 170 Middleware Server	4	4	4
TAPI 120 Clients (CSTA)	50	500	1500
Web Services Interface (WSI)			
WSI - gleichzeitig aktive Clients in Summe	150	500	1500
myPortal @work	50	250	500
myPortal to go	50	250	500
myPortal for Teams	50	250	500
DeskPhone CP 400/600/600E/ 700/700X/710 mit WSI	50	250	500
OpenScape Business Attendant	8	8	8
Application Launcher	50	250	500
TAPI 120 (WSI-Modus)	0	0	0
Anwendung von Drittanbietern	Rest	Rest	Rest

56 Werte sind gestaffelt nach Board-Version: Basic/Erweitert

27.4.14 Gebührenabrechnung

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Gesprächsdatenerfassung zentral					
Einträge im Gesprächsdatenpuffer pro System	20000	20000	20000	20000	20000
Projektkennzahl (PKZ):					
PKZ-Einträge pro Kommunikationssystem	1000	1000	1000	1000	1000
Prüfbare Ziffern pro PKZ	11	11	11	11	11
Zulässige Zeichen	0-9	0-9	0-9	0-9	0-9

28 Experten-Modus

Der **Experten-Modus** stellt Menüs mit Funktionen für die Konfiguration und Wartung des Systems zur Verfügung.

28.1 Darstellungskonventionen für Parameterbeschreibungen

Die Parameterbeschreibungen folgen der Struktur des Experten-Modus im WBM.

Menüeintrag	Jedem Menüeintrag des Experten-Modus ist ein Hilfe-Topic zugeordnet, das Sie direkt (kontext-sensitiv) aus dem WBM aufrufen können. Die Überschrift des Hilfe-Topics zeigt den Pfad des WBM-Fensters. Beispiel: **Grundeinstellungen** > **System** > **System Flags**
Registerkarte	Jeder Registerkarte ist eine eigene Parameter-Tabelle im Hilfe-Topic zugeordnet. Gleiche Parameter unterschiedlicher Registerkarten werden in der selben Parameter-Tabelle beschrieben. Über jeder Parameter-Tabelle finden Sie eine Auflistung für welche Registerkarte(n) die Parameter gelten. Beispiel: • **Statische IP Adresse hinzufügen** • **Statische IP Adresse ändern** • **Statische IP Adresse löschen**
Bereich	Wenn WBM-Fenster in Bereiche strukturiert sind, finden Sie diese Struktur auch in der Parameter-Tabelle wieder. Die Parameter-Tabelle enthält dann für jeden Bereich eine Zwischenüberschrift, gefolgt von den Parametern dieses Bereichs.
Parameter	Parameter werden in einer zweispaltigen Parameter-Tabelle beschrieben. Die linke Spalte nennt Parameter. Die rechte Spalte beschreibt Parameter. Selbsterklärende Parameter werden genannt aber nicht beschrieben. Wertebereich und Standardwert (Default) finden Sie am Ende der Beschreibung, sofern vorhanden.

Parameter (optional)	Parameter, die nicht ausgefüllt werden müssen, sind mit dem Schlüsselwort optional gekennzeichnet.
Eintrag in Aufklappliste	Nicht selbsterklärende Einträge in Aufklapplisten werden auch als Parameter in der linken Spalte der Parameter-Tabelle genannt. Der Eintrag wird durch einen Doppelpunkt vom Namen der Aufklappliste getrennt. Beispiel: **Verschlüsselungsalgorithmen: AES**
Kontrollkästchen/Optionsfeld/Flag	Die Beschreibung von Kontrollkästchen/Optionsfeldern/Flags bezieht sich immer auf den aktivierten Zustand.

28.2 Wartung

Die Funktionen zur Wartung des Kommunikationssystems, z. B. zum Hochladen von Musik in der Warteschleife oder Aktualisieren von Softwarebildern sind unter **Wartung**zusammengefasst.

28.2.1 Konfiguration

Unter **Konfiguration** sind Funktionen zusammengefasst, um z.B. Wartemusik (MoH) zu laden oder die Hardware-Konfiguration anzuzeigen.

28.2.1.1 Konfiguration > Wartemusik (MoH) > Laden zum Gateway

Parameterbeschreibung der Registerkarten:

- **Wartemusik-Dateien über HTTP hochladen**

Parameter	Beschreibung
Wartemusik-Dateien über HTTP hochladen	
Wartemusik-Datei Tag	Auswählen der MoH-Datei für Tag vom lokalen Dateisystem. Dateiformat: siehe Hinweis im WBM.
Wartemusik-Datei Nacht	Auswählen der MoH-Datei für Nacht vom lokalen Dateisystem. Dateiformat: siehe Hinweis im WBM.
Laden	Hochladen der gewählten MoH-Dateien in das System (erfordert Neustart). Aktivierung unter Einrichtung, Zentrale Telefonie > Wartemusik/Ansagen.

Parameterbeschreibung der Registerkarten:

- **Laden der Audio-Dateien via HTTP**

Parameter	Beschreibung
Laden der Audio-Dateien via HTTP	
Ansagedatei	Auswählen der WAV-Datei mit der Ansage vom lokalen Dateisystem auswählen. Dateiformat: siehe Hinweis im WBM.
Bereits geladene Audio-Dateien	
WAV-Datei	Anzeige der im Kommunikationssystem geladenen Ansagedateien
Löschen	Löschen der Ansagedatei
Laden	Hochladen der gewählten Ansagedatei in das System. Aktivierung unter Einrichtung, Zentrale Telefonie > Wartemusik/Ansagen.

28.2.1.2 Konfiguration > Ansagen > Auf Gateway laden

Parameterbeschreibung der Registerkarten:

- **Audiodateien über HTTP laden**

Parameter	Beschreibung
Audiodateien über HTTP laden	
Ansagedatei	Wählen Sie die WAV-Datei mit der Ansage aus dem lokalen Dateisystem aus. Dateiformat: siehe Hinweis in WBM.
Bereits hochgeladene Audiodateien	
Wave-Datei	Zeigt die im Kommunikationssystem geladenen Ansagedateien an.
Löschen	Löscht die Ansagedatei.
Laden	Lädt die ausgewählte Ansagedatei in das System. Aktivierung unter „Einrichtung“, „Zentrale Telefonie und Wartemusik/Ansagen“.

28.2.1.3 Konfiguration > Port-Konfiguration

Parameterbeschreibung der Registerkarte:

- **Konfiguration exportieren**

Parameter	Beschreibung
Konfiguration exportieren	
Dateiname	Name der exportierten Datei.

Parameter	Beschreibung
Maßnahme	Export einer gezippten XML-Datei (z.B. für Bearbeitung in Excel) mit folgenden Daten: Name, Rufnummer des Teilnehmers, Durchwahlnummer, Teilnehmertyp, Lizenzen, Gruppen/Sammelanschlüsse (nicht Team/Top), virtuelle Teilnehmer, Leitungen, Leitungsgruppen, Voicemail.

28.2.1.4 Konfiguration > SmartVM

Parameterbeschreibung der Registerkarten:

- **Übersicht**

Parameter	Beschreibung
Sprachen Anzeige aller Sprachen, in denen die Sprachbenutzerführung vorliegt. Es gilt die folgende Namenskonvention: aabb aa = zweistelliger Sprachcode bb = zweistelliger Ländercode Der Ländercode (bb) ist in der Regel mit dem Sprachcode (aa) identisch	
Mailbox-Informationen	
Rufnummer	Anzeige der Sprachbox-Rufnummer.
Name	Anzeige des Namens der Sprachbox.
Meldungen	Anzeige der Anzahl neuer Nachrichten / Anzahl aller Nachrichten.
Mailbox-Belegung gesamt	Anzeige des Speicherplatzverbrauchs in Prozent.

28.2.1.5 Konfiguration > SmartVM > Mailbox-Operationen

Parameterbeschreibung der Registerkarten:

- **Mailbox-Operationen ausführen**

Parameter	Beschreibung
Alle Mailbox-Konfigurationen zurücksetzen (alle Nachrichten und Begrüßungsansagen löschen)	Ist dieses Flag aktiviert, werden alle Begrüßungen und Nachrichten aller Sprachboxen auf SmartVM gelöscht. Standard: Deaktiviert.
Index	Anzeige des Index der Sprachbox.
Rufnr.	Anzeige der Sprachbox-Rufnummer.
Name	Anzeige des Namens der Sprachbox.

Parameter	Beschreibung
Kennwörter zurücksetzen	Ist dieses Flag aktiviert, wird das Passwort der Sprachbox auf das Standardpasswort `123456` zurückgesetzt. Der Benutzer muss das Kennwort bei der nächsten Benutzung der Sprachbox ändern. Standard: Deaktiviert.
Mailboxen initialisieren	Ist dieses Flag aktiviert, werden für die ausgewählte Sprachbox folgende Aktionen ausgeführt: Standard Mailboxen: – Passwort wird zurückgesetzt – Flag **Aufnahme** wird gesetzt – Nachrichten werden gelöscht – Begrüßungen werden gelöscht – Begrüßungskontrolle auf manuell – Aktive Begrüßung: Begrüßung 1 AutoAttendant Mailboxen: – Passwort wird zurückgesetzt – Flag **Abwurf nach Ansage** wird deaktiviert – Kurzwahlziele werden gelöscht – Begrüßungen werden gelöscht – Begrüßungskontrolle auf manuell – Aktive Begrüßung: Begrüßung 1 Standard: Deaktiviert.

28.2.1.6 Konfiguration > SmartVM > Dateioperationen

Parameterbeschreibung der Registerkarten:

- **Backup**

Parameter	Beschreibung
Backup	
Meldungen	Ist diese Flag aktiviert, werden zusätzlich zu den Begrüßungen auch die Nachrichten der ausgwählten Sprachboxen gesichert. Standard: Deaktiviert.
Verfügbare Mailboxen	Liste aller vorhandenen Sprachboxen. Es können einzelne oder auch alle Sprachboxen in die Liste der zu sichernden Sprachboxen aufgenommen werden.
Zu sichernde Mailboxen	Liste der zu sichernden Sprachboxen.
Schaltflächen	

Parameter	Beschreibung
Übernehmen	Die Begrüßungen (und die Nachrichten, wenn Flag **Messages** aktiviert) der zu sichernden Sprachboxen werden in eine Sicherungsdatei (`*.tar`) gesichert.

Parameterbeschreibung der Registerkarten:

- **Begrüßungen**

Parameter	Beschreibung
Begrüßungen	
Mailbox-Auswahl	Auswahl der Sprachbox.
Begrüßung 1 (Tag)	Anzeige der momentan verwendeten Begrüßung. **Standard** bedeutet: es ist keine individuelle Begrüßung für den Teilnehmer vorhanden.
Begrüßung 2 (Nacht)	Anzeige der momentan verwendeten Begrüßung. **Standard** bedeutet: es ist keine individuelle Begrüßung für den Teilnehmer vorhanden.
Begrüßung 3	Anzeige der momentan verwendeten Begrüßung. **Standard** bedeutet: es ist keine individuelle Begrüßung für den Teilnehmer vorhanden.
Begrüßung 4	Anzeige der momentan verwendeten Begrüßung. **Standard** bedeutet: es ist keine individuelle Begrüßung für den Teilnehmer vorhanden.
Schaltflächen	
Durchsuchen	Navigation zum Ablagepfad der Begrüßungsdatei.
Laden	Eine zuvor gespeicherte Begrüßung oder eine Wave-Datei wird in die SmartVM geladen. Die zu ladende Wave-Datei muss folgendes Format haben: PCM, 16 bit, 8khz, mono Beim Laden wird die ausgewählte Wave-Datei konvertiert. Je nach Größe der Wave-Datei kann dies einige Zeit in Anspruch nehmen.
Backup	Die momentan verwendete Begrüßung wird auf den PC gesichert. Die Begrüßung wird im Binär-Format auf dem PC gespeichert (vma-Datei) und kann deshalb nicht abgespielt oder geändert werden.
Löschen	Die momentan verwendete Begrüßung wird aus der SmartVM gelöscht.

Parameterbeschreibung der Registerkarten:

- **Wiederherstellen**

Parameter	Beschreibung
Wiederherstellen	
Meldungen	Überschreibt nicht nur die Begrüßungen der ausgewählten Sprachboxen, sondern auch die Nachrichten. Standard: Deaktiviert.

Parameter	Beschreibung
Aufschalten	Ist dieses Flag deaktiviert, werden nur die Begrüßungen der ausgewählten Sprachboxen überschrieben, die in den Sicherungsdaten vorhandenen sind. Ist zusätzlich das Flag **Nachrichten** aktiviert, werden auch die in den Sicherungsdaten enthaltenen Nachrichten hinzugefügt. Die bereits existierenden Nachrichten bleiben erhalten. Ist dieses Flag aktiviert, werden vor der Wiederherstellung alle Begrüßungen und Nachrichten der ausgewählten Sprachboxen in der SmartVM gelöscht. Sind Sprachboxen ausgewählt, die nicht in den Sicherungsdaten enthaltenen sind, werden diese auch gelöscht! Die in den Sicherungsdaten enthaltenen Begrüßungen werden übertragen. Ist zusätzlich das Flag **Nachrichten** aktiviert, werden auch die in den Sicherungsdaten enthaltenen Nachrichten übertragen. Standard: Deaktiviert.
Verfügbare Mailboxen	Liste aller in der Sicherungsdatei vorhandenen Sprachboxen. Es können einzelne oder auch alle Sprachboxen in die Liste der wiederherzustellenden Sprachboxen aufgenommen werden.
Zu sichernde Mailboxen	Liste der zu wiederherzustellenden Sprachboxen.
Schaltflächen	
Durchsuchen	Navigation zum Ablagepfad der Sicherungsdatei.
Laden	Die in der Sicherungsdatei enthaltenen Sprachboxen werden angezeigt. Ein erneutes Anklicken der Schaltfläche stellt die Begrüßungen und Nachrichten der ausgewählten Sprachboxen wieder her.

28.2.1.7 Konfiguration > Branding

Parameterbeschreibung der Registerkarte:

- **Branding**

Parameter	Beschreibung
Branding	Auswahl der Produktbezeichnung.

28.2.1.8 Konfiguration > IP-Gateway-Adresse

Parameterbeschreibung der Registerkarte:

- **IP-Gateway-Adresse ändern**

Parameter	Beschreibung
IP-Gateway-Adresse ändern	
Gateway-IP-Adresse	Eingabe der IP-Adresse des Kommunikationssystems, z.B. 192.168.1.2

28.2.2 Software-Image

Unter **Software-Image** sind die Funktionen für das Aktualisieren der Gateway-Software und der Telefon-Images zusammengefasst.

28.2.2.1 Software-Image > System-Software > Update via Internet

Parameterbeschreibung der Registerkarten:

- **Laden der Software-Images von einem Webserver**

Parameter	Beschreibung
Web-Server-Einstellungen	
Software-Image URL	Anzeige und Änderung des Links zum Software-Server inkl. Pfad zur Image-Datei.
Benutzername	Benutzername für die Anmeldung am Software-Server.
Kennwort	Passwort für die Anmeldung am Software-Server.
Software Update-Information	Aktivierung der Abfrage, ob am Software-Server eine neue Software-Version bereitgestellt ist.
Startzeit	Zeitpunkt der Abfrage. Wertebereich: 00,00 bis 24,00, Standardwert: 02,00
Proxy verwenden	Proxy-Aktivierung, falls ein Proxy verwendet wird.
HTTP-Proxy	
HTTP-Proxy	Eingabe des Links zum Proxy-Server.
HTTP-Proxy Port	Eingabe des Ports des Proxy-Servers. Standardwert: 80
Benutzername	Benutzername für die Anmeldung am Proxy-Server.
Kennwort	Passwort für die Anmeldung am Proxy-Server.
Eigene statische Route verwenden	Kunden mit einer WAN-Verbindung für SIP-Trunks ohne Internet-Datenvolumen können die Funktion **Eigene statische Route verwenden** nutzen, um ein OSBiz-Software-Update über eine alternative LAN-Schnittstelle durchzuführen. Die dynamische IP-Adresse des Update-Servers wird automatisch ermittelt und steht dann als Routing-Eintrag für diesen Vorgang zur Verfügung. Um diese Option zu verwenden: • Aktivieren Sie das Flag **Eigene statische Route verwenden**
Eigene statische Route für Software-Update über LAN-Schnittstelle	
Gateway-IP-Adresse der Route	Konfigurieren Sie die IP-Adresse des Standard-Gateways der LAN-Schnittstelle – über die eine Verbindung zum Internet möglich ist – als Gateway-IP-Adresse der Route.
Letzter Software Update	Anzeige, wann das letzte Software-Update durchgeführt wurde.

Parameter	Beschreibung
Schaltflächen	
Standard	Setzt die geänderten Werte wieder auf die Standardwerte zurück.

28.2.2.2 Software-Image > System-Software > Update via File Upload

Parameterbeschreibung der Registerkarten:

- **Laden der Software-Images über Datei-Upload**

Parameter	Beschreibung
Remote-Dateiname (PC-Dateisystem)	Navigation zum Ablageort der Image-Datei.
Speicherplatz vor der Übertragung freigeben	Wenn das Update mit diesem Flag durchgeführt wird, werden Protokolle, Traces, Telefon-Software-Images und TCP-Dumps gelöscht, um Speicherplatz freizugeben.
Software-Aktivierung	
Start der Aktion Sofort nach der Übertragung	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach zwei Neustarts ist die Software aktualisiert.
Start der Aktion in	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach Ablauf des angegebenen Zeitraums wird die Software aktiviert. Eingabe des Zeitraum in Tagen, Stunden und Minuten.
Start der Aktion am	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Zu dem angegebenen Zeitpunkt wird die Software aktiviert. Eingabe des Zeitpunkt als Datum und Uhrzeit.
Lokale Systemzeit	Anzeige von Datum und Uhrzeit des Systems.
Softwareversion des aktuell verwendeten System Software-Images	Anzeige der Softwareversion der aktuellen Image-Datei.

28.2.2.3 Software-Image > System-Software > Update via USB-Stick

Parameterbeschreibung der Registerkarten:

- **Laden der Software-Images vom USB-Stick**

Parameter	Beschreibung
Liste aller vorhandenen kompatiblen Image-Dateien	
Version	Anzeige der Versionsnummer der auf dem USB-Medium gefundenen Image-Dateien.
Laden	Markieren der auf dem USB-Medium gefundenen Image-Datei, die für die Software-Aktualisierung verwendet werden soll.

Parameter	Beschreibung
Dateiname	Anzeige der Dateinamen der auf dem USB-Medium gefundenen Image-Dateien.
Dateigröße (MB)	Anzeige der Dateigröße der auf dem USB-Medium gefundenen Image-Dateien.
Software-Aktivierung	
Start der Aktion Sofort nach der Übertragung	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen und aktiviert. Zur Aktivierung erfolgt eine vorübergehende Unterbrechung des Anlagenbetriebs.
Start der Aktion in	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach Ablauf des angegebenen Zeitraums wird die Software aktiviert. Eingabe des Zeitraum in Tagen, Stunden und Minuten.
Start der Aktion am	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Zu dem angegebenen Zeitpunkt wird die Software aktiviert. Eingabe des Zeitpunkts mit Datum und Uhrzeit.
Lokale Systemzeit	Anzeige von Datum und Uhrzeit des Systems.
Softwareversion des aktuell verwendeten System Software-Images	Anzeige der aktiven Softwareversion.

28.2.2.4 Software-Image > Telefon-Images > Laden

Parameterbeschreibung der Registerkarten:

- **Laden der Telefonsoftware**

Parameter	Beschreibung
Remote-Dateiname (PC-Dateisystem)	Auswahl der Telefonsoftware (Image-Datei)
Aktuell installierte Images	
Löschen	Die Telefon-Images werden zum Löschen markiert.
Dateiname	Anzeige des Dateinamens der Image-Datei.
Gerätetyp	Anzeige des Systemtelefontyps, der zur Image-Datei gehört.
Version	Anzeige der Version der Image-Datei.
Schaltflächen	
Laden	Das angegebene Telefon-Image wird in das Kommunikationssystem geladen.
Löschen	Die markierten Telefon-Images werden vom Kommunikationssystem gelöscht.

28.2.2.5 Software-Image > Telefon-Images > Verteilen

Parameterbeschreibung der Registerkarten:

- **Verteilen der Telefonsoftware**

Parameter	Beschreibung
Aktuell installierte Images	
Verteilen	Ist das Kontrollkästchen aktiviert, wird diese Telefonsoftware an alle angeschlossenen Systemtelefone des Telefontyps übertragen.
Dateiname	Anzeige des Dateinamens der Image-Datei.
Gerätetyp	Anzeige des Systemtelefontyps, der zur Image-Datei gehört.
Version	Anzeige der Version der Image-Datei.
Type	Typ des Systemtelefons.
Standard	Als Default markierte Telefonsoftware wird automatisch auf ein diesem Typ zugehöriges Systemtelefon übertragen, wenn es sich zum ersten Mal am System anmeldet.

28.2.2.6 Software-Image > Telefon-Images > Verteilen pro Endgerät

Parameterbeschreibung der Registerkarten:

- **Verteilen der Telefonsoftware pro Endgerät**

  Wenn der Benutzer ein Deskshare-Benutzer ist, ist das Kontrollkästchen ausgegraut, so dass Sie ein Gerät nicht für diesen Benutzer bereitstellen können.

Parameter	Beschreibung
Aktuell installierte Images	
Rufnr	Rufnummer des Systemtelefons.
Gerätetyp	Typ des Systemtelefons.
IP-Adresse	IP-Adresse des Systemtelefons; direkter Link zum WBM des Systemtelefons.
MAC-Adresse	MAC-Adresse des Systemtelefons.
Aktuelle SW-Version	Aktuelle Software-Version des Systemtelefons.
Verteilbare Software	Auswahl des Telefon-Images, das an das Systemtelefon übertragen werden soll.

28.2.2.7 Software-Image > Telefon-Logo-Images > Laden

Ein Bild (z.B. ein Firmen-Logo) kann auf das Display der Systemtelefone (OpenStage 40/60/80 bzw. Telekom-Varianten) geladen werden, Anzeige im Ruhezustand (on-hook). Spezifikation der Logo-Datei siehe Telefon-Logos.

Parameterbeschreibung der Registerkarten:

- **Laden des Telefon-Logos**

Parameter	Beschreibung
Remote-Dateiname (PC-Dateisystem)	Auswahl der Datei mit dem Telefon-Logo.
Aktuell installierte Logo-Images	
Löschen	Die Telefon-Logo-Dateien werden zum Löschen markiert.
Dateiname	Anzeige des Dateinamens der Telefon-Logo-Datei.
Schaltflächen	
Laden	Die angegebene Telefon-Logo-Datei wird in das Kommunikationssystem geladen.
Löschen	Die markierten Telefon-Logo-Dateien werden vom Kommunikationssystem gelöscht.

28.2.2.8 Software-Image > Telefon-Logo-Images > Verteilen

Ein Bild (z.B. ein Firmen-Logo) kann auf das Display der Systemtelefone (OpenStage 40/60/80 bzw. Telekom-Varianten) geladen werden, Anzeige im Ruhezustand (on-hook). Spezifikation der Logo-Datei siehe Telefon-Logos.

Parameterbeschreibung der Registerkarten:

- **Verteilen des Telefon-Logos**

Parameter	Beschreibung
Aktuell installierte Logo-Images	
Verteilen	Ist das Kontrollkästchen aktiviert, wird diese Telefon-Logo-Datei an die ausgewählten Systemtelefone übertragen.
Dateiname	Anzeige des Dateinamens der Telefon-Logo-Datei.
An Workpoints folgenden Typs verteilen	Auswahl, ob das Telefon-Logo an alle Systemtelefone oder nur an einen bestimmten Systemtelefontyp übertragen werden soll.

28.2.3 Cordless

Unter **Cordless** sind die Funktionen für alle konfigurierten Basisstationen zusammengefasst.

28.2.3.1 Cordless > Basisstationen

Parameterbeschreibung der Registerkarten:

- **Basisstation Status**

Parameter	Beschreibung
Basisstationsdaten	
BS-Frequenz	Zeigt die Frequenzen der ausgewählten Basistation an. Es können bis zu 10 verschiedene Frequenzkanäle gleichzeitig ausgewählt werden (siehe nachfolgende Tabelle).
Basistation	Nummer der Basisstation.
SW-Version	Software-Version der Basisstation.
HW Version	Hardware-Version der Basisstation.
Status	Zustand des zugehörigen Ports: Port aktiv Port nicht angeschlossen Port gesperrt Port angeschlossen, nicht aktiv Port angeschlossen, nicht aktiv 1. Zusatzport zu ... (Nr. des Mutterports) 2. Zusatzport zu ... (Nr. des Mutterports)
Overload	Anzahl der Overload-Situationen an der UP0/E -Schnittstelle.
Restart	Anzahl der Restarts der Basisstation.
L1/L2 Error	Anzahl der an der Basisstation aufgetretenen L1/L2-Fehler.
Abnormal Release	Anzahl der abgebrochenen Gespräche der Basisstation.
Calls per BS	Anzahl der Gespräche über die Basisstation (kommend und gehend gemeinsam).
Hopping Mode	Cordless Version 2 Systeme arbeiten immer im ”Fast Hopping Mode”, d.h. es können alle Frequenz-Zeitschlitzpaare benutzt werden. Es stehen also 120 Duplexkanäle zur Verfügung. Bei Slow Hopping BS kann nur jedes zweite Frequenz-Zeitschlitzpaar benutzt werden. Es stehen also nur 60 Duplexkanäle zur Verfügung. Alle Cordless Version 1 Systeme arbeiten im ”Slow Hopping Mode”.
BHO Count OK	Anzahl der erfolgreich durchgeführten Intracell Handovers (Bearer Handovers BHO), d.h. erfolgreiche Wechsel der Trägerfrequenz und/oder des Zeitschlitzes innerhalb einer Funkzelle. Nicht unterstützt durch Hicom cordless EM V2.1 und V2.2. Der Zähler wird zwar nicht unterstützt, aber das Leistungsmerkmal des Bearer Handover steht zur Verfügung.
BHO Count not OK	Anzahl der nicht erfolgreich durchgeführten Intracell Handovers (Bearer Handovers BHO). Nicht unterstützt durch Hicom cordless EM V2.1 und V2.2. Der Zähler wird zwar nicht unterstützt, aber das Leistungsmerkmal des Bearer Handover steht zur Verfügung.
Intra SLC Handover	Anzahl der Handover-Vorgänge innerhalb der Baugruppe SLC. Gezählt wird bei der neuen Basisstation.
Inter SLC Handover	Anzahl der Handover-Vorgänge zwischen SLC-Baugruppen. Gezählt wird bei der neuen Basisstation.
SLC-weit	

Parameter	Beschreibung
Lost Calls	Anzahl von Gesprächen, die aus Ressourcengründen nicht vermittelt werden konnten.
SLMUC Overload	Anzahl der Overload-Situationen auf der Baugruppe SLC. Die Anzahl der freien Poolelemente auf der SLC-Baugruppe unterschreitet einen Minimalwert. Alle kommenden Belegungen werden von der IWU der SLC abgewiesen, bis die Überlastsituation beendet ist.
LR Roam	LR Roam zählt jede Belegung eines Mobiltelefons mit einem Standard-PMID und geänderter Aufenthalts-SLC. Es handelt sich um die Anzahl der Locate-Request-Nachrichten, die Roaming berichteten (d.h. der aktuelle Aufenthaltsort des Mobiltelefons ist verändert). Das Mobiltelefon führt mit jedem Einschalten ein Locate Request durch. Wird das Mobiltelefon ausgeschaltet und in einer anderen Funkzelle eingeschaltet, zählt dieser Zähler nicht.
LR Async	LR Async zählt jede Belegung eines Mobiltelefons mit einem Standard- PMID bei gleichbleibender Aufenthalts-SLC. Es handelt sich um die Anzahl der Locate-Request-Nachrichten, die Asynchronität von Layern berichteten (d.h. der aktuelle Aufenthaltsort des Mobiltelefons ist unverändert). Die Zählung erfolgt jedoch immer auf der Heimat-SLC und zählt deshalb nur dann, wenn die Funkverbindung tatsächlich zustande kommt bzw. das CHO mit Standard-PMID unterstützt. Zusätzlich müssen bei den Belegungen die Kriterien für eine Aufenthaltsortaktualisierung erfüllt sein, d.h. ein LOCATE-Request empfangen oder die Sicherheitsmaßnahmen, Authentikation (und Ciphering), für den Link durchgeführt worden sein.
HDLC Error	Anzahl der nicht kritischen HDLC-Fehlermeldungen, die nicht an das Kommunikationssystem gemeldet wurden (Overflow, Underrun, CRC Error).
CMI Version	Hier wird die aktuelle Cordless-Version angezeigt.

Frequenz (Channel)	**DECT**	Europa 1880 – 1900 MHz	Latein-Amerika 1910 – 1930 MHz
10	9	1881,792 MHz	1911,16 MHz
9	8	1883,520 MHz	1912,896 MHz
8	7	1885,24 MHz	1914,624 MHz
7	6	1886,976 MHz	1916,352 MHz
6	5	1888,704 MHz	1918,080 MHz
5	4	1890,432 MHz	1919,80 MHz
4	3	1892,160 MHz	1921,536 MHz
3	2	1893,88 MHz	1923,264 MHz
2	1	1895,616 MHz	1924,992 MHz
1	0	1897,344 MHz	1926,720 MHz

28.2.4 Port/Baugruppen Zustand

Der Zustand aller Baugruppen kann angezeigt werden. Zusätzlich können die Baugruppen und ihre Ports freigegeben und gesperrt werden.

28.2.4.1 Port/Baugruppen Zustand > Baugruppen Zustand

Parameterbeschreibung der Registerkarten:

- **Baugruppenstatus**

Parameter	Beschreibung
Slot	Physikalische Slotnummer.
Baugruppe	Bezeichnung der Baugruppe.
Nicht gesteckt	Angekreuzt, wenn Baugruppe nicht gesteckt ist.
Defekt	Angekreuzt, wenn Baugruppe defekt (nicht geladen) ist. Es ist auch möglich, dass eine defekte oder nicht konfigurierte Baugruppe nicht angezeigt wird.
Gesperrt	Angekreuzt,wenn mindestens ein Port dieser Baugruppe gesperrt ist.
Frei	Angekreuzt,wenn alle Ports dieser Baugruppe frei sind.
Belegt	Angekreuzt,wenn mindestens ein Teilnehmer oder Leitung dieser Baugruppe abgehoben hat, gerufen wird oder im Gespräch ist.
Taktquelle	Angekreuzt, wenn die Baugruppe den Referenztakt liefert.
Schaltflächen	
Start	Aktualisierung der Anzeige wird gestartet. Der Zustand wird alle 3 Sekunden aktualisiert.
Anhalten	Aktualisierung der Anzeige wird gestoppt.

28.2.4.2 Port / Baugruppen Zustand > Out of Service

Parameterbeschreibung der Registerkarten:

- **Port außer Betrieb**
- **Baugruppe out of Service**

Parameter	Beschreibung
Zugang	Einbauplatz und Port, an dem der Teilnehmer bzw. die Leitung angeschlossen ist.
Ruf-Nr.	Die dem Port zugeordnete Rufnummer.
Name	Der zum Teilnehmer bzw. zur Leitung gehörende Name.
Status	Je nachdem, ob am Port ein zugelassenes Endgerät oder eine zugelassene Leitung angeschlossen ist oder nicht, können die Ports **aktiv** oder **inaktiv** sein. Ports können auch im Zustand **in Betrieb** (Standardeinstellung) oder **außer Betrieb durch Tool** sein, d.h. dass sie über **Baugruppe sperren** gesperrt wurden. Der Zustand in Betrieb ist nicht identisch mit aktiv. Der Port-Status kann beispielsweise aktiv, in Betrieb oder auch inaktiv, in Betrieb sein.
Schaltflächen	

Parameter	Beschreibung
Auswahl sperren	Die markierten Ports werden gesperrt. Bei der Sperrung von $U_{P0/E}$-Ports geht immer der zugehörige physikalische Port außer Betrieb. Dies hat zur Folge, dass bei Auswahl eines Master-Ports der zugehörige Slave-Port ebenfalls außer Betrieb geht.
Auswahl freigeben	Die markierten Ports werden freigegeben.
Baugruppe sperren	Die markierten Baugruppen und deren Ports werden gesperrt. Beim Sperren einzelner Mobiltelefone einer Cordless-Baugruppe wird immer die gesamte Baugruppe und somit auch alle Mobiltelefone gesperrt. Das Sperren einzelner Mobiltelefone wird durch Ändern der PIN der Mobiltelefone erreicht.
Baugruppe freigeben	Die markierten Baugruppen und deren Ports werden freigegeben.

28.2.5 Traces

Unter **Traces** sind die Funktionen zum Tracen zusammengefasst. Der Administrator kann Traces starten und stoppen und die Trace-Einstellungen ändern.

28.2.5.1 Traces > Trace-Format-Konfiguration

Über die Trace-Format-Konfiguration wird definiert, welche Header-Daten in der Trace-Ausgabe enthalten sein sollen und wie die Trace-Daten formatiert werden sollen.

Parameterbeschreibung der Registerkarten:

- **Trace-Konfiguration ändern**

Parameter	Beschreibung
In der Trace-Ausgabe enthaltene Header-Daten	
Globale Trace-Header Format-Einstellungen	Bei aktiviertem Flag können die Optionen für die nachfolgenden Header-Daten aktiviert oder deaktiviert werden. Standardwert: Aktiviert
Subsystem-ID	Bei aktiviertem Flag ist die Subsystem-ID in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Task-Name	Bei aktiviertem Flag ist der Task-Name in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Task-ID	Bei aktiviertem Flag ist die Task-ID in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Uhrzeit	Bei aktiviertem Flag ist die Zeitangabe in der Trace-Ausgabe enthalten. Standardwert: Aktiviert

Parameter	Beschreibung
Modulname	Bei aktiviertem Flag ist der Modul-Name in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Zeilennummer	Bei aktiviertem Flag ist die Zeilennummer in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Aufbereitung der Trace-Daten	
Volle Formatierung mit Parameterexpansion (Standard)	Standard Ausgabe-Modus: Alle Datentypen werden erweitert. Trace-Ausgabe: Normal (geeignet für den Normalbetrieb) Standardwert: Aktiviert
Eingeschränkt (Meldungstypen binär, speziell für Xtracer)	In diesem eingeschränkten Ausgabemodus werden die Datentypen im Binär-Format ausgegeben, das heißt so, wie sie zum Tracezeitpunkt vorliegen. Das Binär-Format ist für die Analyse mit dem X-Tracer-Tool bestimmt. Trace-Ausgabe: Schnell (geeignet für mittlere bis hohe Last) Standardwert: Deaktiviert
Eingeschränkt (nur Expansion elementarer Datentypen)	In diesem Ausgabemodus werden nur elementare Datentypen (zum Beispiel integer, short, long, string) expandiert. Trace-Ausgabe: Sehr schnell (geeignet für hohe Last) Standardwert: Deaktiviert
Performanceoptimierter Trace ohne Parameterexpansion	In diesem Ausgabemodus wird keine Datentyp-Expansion vorgenommen. Damit entsteht auch kein Aufwand für die Trace-Formatierung. Trace-Ausgabe: Extrem schnell (geeignet für sehr hohe Last) Standardwert: Deaktiviert

28.2.5.2 Traces > Trace-Ausgabe-Interfaces

Parameterbeschreibung der Registerkarten:

- **Ausgabe-Interfaces ändern**

Parameter	Beschreibung
Datei-Trace	
Datei-Trace aktivieren	Bei aktiviertem Flag werden Trace-Meldungen im Kommunikationssystem in eine Protokolldatei eingetragen. Standardwert: Aktiviert
Max. Trace-Quota (kByte)	Anzeige der maximalen Größe des Trace-Speichers in kByte
Strategie bei Erreichen der max. Quota	Auswahlmöglichkeit, was beim Erreichen der maximalen Trace-Quota passieren soll.

Parameter	Beschreibung
Strategie bei Erreichen der max. Quota: Wrap Around (Lösche älteste Datei)	Beim Erreichen der maximalen Trace-Quota wird die jeweils älteste Trace-Protokolldatei überschrieben. Standardwert: Aktiviert
Strategie bei Erreichen der max. Quota: Datei-Trace wird temporär gestoppt	Beim Erreichen der maximalen Trace-Quota wird die Datei-Trace-Ausgabe gestoppt. Standardwert: Deaktiviert
Zeit, nach der jeweils eine neue Trace-Datei angelegt wird (s)	Anzeige der Zeit in Sekunden, nach deren Ablauf eine neue Trace-Protokolldatei angelegt wird.
Zeitraum für den Trace-Dateien verfügbar sind	Anzeige des Zeitraums, für den Trace-Protokolldateien verfügbar sind.
Trace über LAN (XTracer)	
Trace über LAN (XTracer) aktivieren	Trace-Meldungen werden über die LAN-Schnittstelle übertragen. Standardwert: Deaktiviert
Timer-Wert (s)	Anzeige der Zeit in Sekunden, nach deren Ablauf Trace-Daten übertragen werden.

28.2.5.3 Traces > Trace-Protokoll

Parameterbeschreibung der Registerkarten:

- **Laden über HTTP**
- **Trace-Protokoll löschen**

Tipp: Das Löschen von Trace-Protokolldaten kann nicht rückgängig gemacht werden.

Parameter	Beschreibung
Trace-Protokoll	
Gesamtes Protokoll	Alle vorhandenen Trace-Protokolldateien werden heruntergeladen.
Protokoll von heute	Trace-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen.
Eigene Auswahl	Trace-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen.

28.2.5.4 Traces > Digitale Prüfschleife

Die Konfiguration von digitalen Prüfschleifen ist ausschließlich mit Manager E möglich.

Digitale Prüfschleifen werden zur Leitungsüberprüfung von B-Kanälen der S_0-, S_{2M}- und T1-Schnittstellen eventuell vorhandener Baugruppen eingesetzt.

Die Aktivierung digitaler Prüfschleifen sollte nur nach Aufforderung durch den Service-Provider erfolgen.

Parameterbeschreibung der Registerkarten:

- **Digital Loopback ändern**

28.2.5.5 Traces > Kunden-Trace-Protokoll

Mit dieser Funktion kann die Ereignis-Anzeige (Kunden-Trace) gestartet werden. Meldungstypen sind unter anderem System, SIP, STUN und LDAP.

Parameterbeschreibung der Registerkarten:

- **Anzeige**
- **Laden über HTTP**
- **Trace-Protokoll löschen**

Parameter	Beschreibung
Autom. Aktualisierung	Bei aktiviertem Flag erfolgt eine automatische Aktualisierung der Anzeige des Kunden-Trace-Protokolls. Standardwert: Aktiviert
Sekunden bis zur nächsten Aktualisierung	Zeit in Sekunden nach deren Ablauf eine Aktualisierung des Kunden-Trace-Protokolls erfolgt.

28.2.5.6 Traces > M5T-Trace-Komponenten

Diese Funktion dient zur Überwachung des SIP-Stacks.

Änderungen der Einstellungen sollten nur nach Aufforderung durch den zuständigen Service-Support erfolgen.

Parameterbeschreibung der Registerkarten:

- **M5T-Trace-Komponenten bearbeiten**
- **Trace-Komponenten starten/stoppen**

Parameter	Beschreibung
Paketname	Name der M5T-Trace-Komponente
Trace-Level	Detailtiefe der Aufzeichnung der M5T-Trace-Komponente (Trace-Level 0 = geringste Detailtiefe bis Trace-Level 9 = größte Detailtiefe) Standardwert: 0
Trace an	Bei aktiviertem Flag erfolgt eine Aufzeichnung der Daten der M5T-Trace-Komponente. Standardwert: Deaktiviert
Crotch	Schrittweite der Aktivierung

28.2.5.7 Traces > Secure Trace

Diese Funktion dient zur Aufzeichnung von verschlüsselten VoIP-Nutz- und Signalisierungsdatenströmen.

Die Aufzeichnung verschlüsselter Verbindungsdaten erfordert zwingend die Zustimmung des Kunden und darf nur in Abstimmung mit dem zuständigen Service-Support vorgenommen werden. Informationen zur Vorgehensweise siehe Traces (Secure Trace).

Anmerkung: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Strafttatbestand, falls die betroffenen Teilnehmer nicht darüber informiert wurden.

Parameterbeschreibung der Registerkarten:

- **Secure Trace Passphrase ändern**
- **X.509-Datei für Secure Trace importieren**

Parameter	Beschreibung
Ändern der Secure Trace Aktivierungs-Passphrase	
Aktuelle Passphrase	Aktuelles Passwort (Passphrase) für das Starten und Stoppen des Secure Trace
Neue Passphrase	Neues Passwort (Passphrase) für das Starten und Stoppen des Secure Trace Wertebereich: 5 bis 12 Zeichen
Neue Passphrase wiederholen	Identisches neues Passwort (Passphrase) für das Starten und Stoppen des Secure Trace Wertebereich: 5 bis 12 Zeichen
Datei mit dem Zertifikat (PEM oder Binär-Format)	Auswahl der X.509-Datei, die das in das Kommunikationssystem zu importierende Zertifikat beinhaltet. Nach Auswahl der X.509-Datei kann der Fingerabdruck des zu importierenden Zertifikats angezeigt und anschließend das Zertifikat in das Kommunikationssystem importiert werden. ***INFO:*** Das Importieren des Zertifikats sollte nach der Prüfung des Fingerabdrucks erflogen.

28.2.5.8 Traces > Secure Trace > Secure Trace-Zertifikat

Diese Funktion dient zur Anzeige des importierten Secure Trace-Zertifikats.

Parameterbeschreibung der Registerkarten:

- **Secure Trace-Zertifikat anzeigen**

28.2.5.9 Traces > Secure Trace > Secure Trace-Einstellungen

Diese Funktion dient zur Statusabfrage und zum Starten/Stoppen des Secure Trace.

Parameterbeschreibung der Registerkarten:

- **Secure Trace Status**
- **Secure Trace starten/beenden**

Parameter	Beschreibung
Aktueller Secure Trace Status	
Secure Trace aktiviert	Status des Secure Trace
Automatischer Deaktivierungszeitpunkt	Zeit zu der der Secure Trace automatisch deaktiviert wird.
Secure Trace für folgende Protokolle	Anzeige der Protokolle, für die der Secure Trace erstellt wird.
Start Parameter	
Secure Trace Aktivierungs-Passphrase	Passwort (Passphrase) für das Starten und Stoppen des Secure Trace
Dauer des Secure Trace (Min.)	Zeitraum in Minuten in dem der Secure Trace aktiv sein soll. ***INFO:*** Die Eingabe eines Wertes ist unbedingt erforderlich.
Secure Trace für folgende Protokolle	
TC (TLS)	Bei aktiviertem Flag berücksichtigt der Secure Trace das TC (TLS)-Protokoll. Standardwert: Deaktiviert
H.323 Core/HSA (TLS)	Bei aktiviertem Flag berücksichtigt der Secure Trace das H.323 Core/HSA (TLS)-Protokoll. Standardwert: Deaktiviert
MMX (PEP)	Bei aktiviertem Flag berücksichtigt der Secure Trace das MMX (PEP)-Protokoll. Standardwert: Deaktiviert
SIP Core/SSA (TLS)	Bei aktiviertem Flag berücksichtigt der Secure Trace das SIP Core/SSA (TLS)-Protokoll. Standardwert: Deaktiviert
MSC (SRTP)	Bei aktiviertem Flag berücksichtigt der Secure Trace das MSC (SRTP)-Protokoll. Standardwert: Deaktiviert

28.2.5.10 Traces > H.323-Stack-Trace

Diese Funktion dient zur Verfolgung von Problemen mit Komponenten, die das H.323-Protokoll nutzen.

Änderungen der Einstellungen sollten nur nach Aufforderung durch den zuständigen Service-Support erfolgen.

Parameterbeschreibung der Registerkarten:

- **H.323-Stack-Trace-Konfiguration ändern**
- **Alle H.323-Module ändern**
- **H.323-Stack-Trace-Protokoll über HTTP laden**
- **H.323 Stack-Trace-Protokoll löschen**

Parameter	Beschreibung
Allgemeines	
Trace-Level	Trace-Detailtiefe (Trace-Level 0 = niedrigste Detailtiefe bis Trace-Level 4 = höchste Detailtiefe) Standardwert: 2
Konsolen-Trace	
Konsolen-Trace aktivieren	Bei aktiviertem Flag werden H.323-Stack-Trace-Meldungen auf der Konsole ausgegeben. Standardwert: Deaktiviert
Datei-Trace	
Datei-Trace aktivieren	Bei aktiviertem Flag werden H.323-Stack-Trace-Meldungen in eine Protokolldatei eingetragen. Standardwert: Deaktiviert
Max. Größe des Trace-Buffers (Byte)	Maximale Größe des Trace-Buffers in Byte (Menge der Daten, die im Zwischenspeicher gehalten wird.)
Max. Größe der Trace-Datei (Byte)	Maximale Größe der Trace-Protokolldatei in Byte
Trace-Timer (s)	Zeit in Sekunden, nach deren Ablauf Trace-Daten in die Protokolldatei geschrieben werden.
Modulname	Name des H.323-Stack-Trace-Moduls
Trace an	Bei aktiviertem Flag ist das H.323-Stack-Trace-Modul aktiv.

28.2.5.11 Traces > Call Supervision

Mit dieser Funktion kann die Überwachung von Leitungs- und Teilnehmerschnittstellen gestartet und gestoppt werden.

Parameterbeschreibung der Registerkarten:

- **Protokoll starten/stoppen**
- **Anzeige**
- **Laden über HTTP**

Parameter	Beschreibung
Ausgewählter Port	Leitungs- oder Teilnehmerschnittstelle für die die Anrufüberwachung gestartet oder gestoppt werden soll.
Nr.	Fortlaufende Nummer.

Parameter	Beschreibung
Uhrzeit	Uhrzeit des Events (Ereignisses).
CallNumber/Access	Rufnummer und physikalische Schnittstelle.
Status	Zustand der Schnittstelle. Möglich sind folgende Schnittstellenzustände: • Idle (Schnittstelle ist im Ruhezustand.) • Call Initiated (Schnittstelle ist bereit.) • Overlap Sending (externe Ziffernaussendung) • Outgoing Call Proc (Wahlende) • Call Request (Warten auf Alert) • Call Present (Schnittstelle wird gerufen.) • Active (Schnittstelle ist im Gesprächszustand.) • Hold (Schnittstelle ist im Zustand Halten.) • Disconnect Indication (Anforderung zum Trennen eines aktiven Gesprächs) • Direct (Schnittstelle ist im Modus Direktansprechen.) • Intrusion (Aufschalten wird aktiviert.) • Call Back A (Rückruf Teilnehmer A) • Call Back B (Rückruf Teilnehmer B) • Busy (Schnittstelle ist besetzt.) • Fehler (Fehlerstatus) • Disconnect PI (Warten auf Trennen von PI (Progress Indicator)) • Sensor (Signal wurde von Sensor ausgesendet.) • Conference Master (Konferenz-Master) • Paging (Personensuche) • Help Dial (Assoziierte Wahl wird verwendet.) • Remote (Schnittstelle durch Remote Service oder DISA belegt.) • ACD (Anrufverteilung) • Unbekannter Zustand

Parameter	Beschreibung
Ereignis	Ereignis Möglich sind folgende Events: • Setup (Leitungsschnittstelle: Kommende oder gehende Belegung) • Setup Ackn (Leitungsschnittstelle: Belegungsquittung) • Info (Leitungsschnittstelle: Info (Rufnummernziffern)) • Call Proc (Leitungsschnittstelle: Unbewertetes Wahlende) • Progress (Leitungsschnittstelle: Zusatzinformation für Verbindungsaufbau) • Alert (Leitungsschnittstelle: Bewertetes Wahlende) • Connect (Leitungsschnittstelle: Anschaltung B-Kanal) • Connect Ackn (Leitungsschnittstelle: Quittung zu B-Kanal-Anschaltung) • Disconnect (Leitungsschnittstelle: Trenn-Anforderung) • Release (Leitungsschnittstelle: Trenn-Quittung) • Release Compl (Leitungsschnittstelle: Verbindung ausgelöst) • Monitor On (Leitungs-/Teilnehmerschnittstelle: Anrufüberwachung gestartet) • Monitor Off (Leitungs-/Teilnehmerschnittstelle: Anrufüberwachung gestoppt) • Off Hook (Teilnehmerschnittstelle: Hörer abgenommen) • On Hook (Teilnehmerschnittstelle: Hörer aufgelegt) • Digit (Teilnehmerschnittstelle: Ziffern werden gewählt)
Autom. Aktualisierung	Bei aktiviertem Flag erfolgt eine automatische Aktualisierung der Anzeige der Anrufüberwachung. Standardwert: Aktiviert
Sekunden bis zur nächsten Aktualisierung	Zeit in Sekunden nach deren Ablauf eine Aktualisierung der Anrufüberwachung erfolgt.

28.2.5.12 Traces > Lizenz-Komponente

Diese Funktion dient zur Überwachung des systeminternen Lizenzagenten CLA (Customer License Agent).

Änderungen der Einstellungen sollten nur nach Aufforderung durch den zuständigen Service-Support erfolgen.

Parameterbeschreibung der Registerkarten:

- **Ändern der CLA Trace Komponente**

Parameter	Beschreibung
Paketname	Name der Lizenz-Trace-Komponente.
Trace-Level	Definition der Detailtiefe der Aufzeichnung der Lizenz-Trace-Komponente Standardwert: Standard
Trace-Level: niedrig	Niedrige Detailtiefe für die Trace-Aufzeichnung.
Trace-Level: Standard	Mittlere Detailtiefe für die Trace-Aufzeichnung.

Parameter	Beschreibung
Trace-Level: Alle	Hohe Detailtiefe für die Trace-Aufzeichnung.
Trace-Level: Aus	Lizenz-Trace-Komponente gestoppt.

28.2.5.13 Traces > Trace-Profile

Trace-Profile enthalten vordefinierte Trace-Komponenten zur Überwachung kompletter Funktionseinheiten des Kommunikationssystems.

Parameterbeschreibung der Registerkarten:

- **Alle Trace-Profile anzeigen**
- **Trace-Profil hinzufügen (leeres Profil)**
- **Trace-Profil hinzufügen (mit aktuellen Trace-Einstellungen)**
- **Alle Trace-Profile stoppen**
- **Trace-Profil starten/stoppen**

Parameter	Beschreibung
Profil-Name	Name des Trace-Profils
Profil gestartet	Anzeige, ob Trace-Profil gestartet wurde.
Profil schreibgeschützt	Anzeige, ob Trace-Profil schreibgeschützt ist (Alle standardmäßig vorhandenen Trace-Profile sind schreibgeschützt.).
Trace-Komponente	Name der Trace-Komponente
Enthalten	Bei aktiviertem Flag wird die Trace-Komponente in das neue, hinzuzufügende Trace-Profil übernommen. Standardwert: Aktiviert
Level	Detailtiefe der Aufzeichnung der Trace-Komponente (Trace-Level 0 = geringste Detailtiefe bis Trace-Level 9 = größte Detailtiefe)

28.2.5.14 Traces > Trace-Komponenten

Anhand von Trace-Komponenten werden die Prozess- und Zustandsinformationen einzelner Komponenten des Kommunikationssystems aufgezeichnet.

Parameterbeschreibung der Registerkarten:

- **Alle Trace-Komponenten anzeigen**
- **Gestartete Trace-Komponenten anzeigen**
- **Gestoppte Trace-Komponenten anzeigen**
- **Trace-Komponenten ändern**
- **Alle Trace-Komponenten stoppen**
- **Trace-Komponenten starten/stoppen**
- **Standard-Trace-Einstellungen**

Parameter	Beschreibung
Subsystem-Name	Name der Trace-Komponente
Trace-Komponenten-Index	Fortlaufende Nummer
Trace-Level	Trace-Detailtiefe (Trace-Level 0 = niedrigste Detailtiefe bis Trace-Level 9 = höchste Detailtiefe)
Trace an	Bei aktiviertem Flag erfolgt eine Aufzeichnung der Daten der Trace-Komponente.

28.2.5.15 Traces > TCP Dump

Ein TCP-Dump dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung. Für die Diagnose der TCP-Dump-Dateien ist eine entsprechende Applikation erforderlich.

Parameterbeschreibung der Registerkarten:

- **Status TCP-Dump**

Parameter	Beschreibung
TCP-Dump starten	Startet den TCP-Dump
Start-Parameter	
Schnittstellenname	Schnittstelle, für die eine Auswertung des Datenverkehrs erfolgt. Die verfügbaren Schnittstellen werden unter **Interface-Details** angezeigt. Der Eintrag **any** bewirkt eine Auswertung des Datenverkehrs für alle verfügbaren Schnittstellen. Standardwert: any
Paketgröße	Größe der Datenpakete in Byte, die aufgezeichnet werden sollen. Der Eintrag **0** bedeutet, jedes Paket wird komplett aufgezeichnet. Wertebereich: 0 bis 2000000000, Standardwert: 0
Ende-Kriterien	
Anzahl der Pakete	Anzahl der Datenpakete, nach deren Erreichen der TCP-Dump beendet wird.
Zeit bis zur Beendigung (s)	Zeit in Sekunden, nach deren Ablauf der TCP-Dump beendet wird.
TCP-Dump beenden	Stoppen des TCP-Dump
TCP-Dump aufräumen	Löschen der im Kommunikationssystem gespeicherten TCP-Dump-Dateien
Autom. Aktualisierung	Bei aktiviertem Flag erfolgt eine automatische Aktualisierung der Statusanzeige. Standardwert: Aktiviert

28.2.5.16 Traces > rpcap Dämon

Ein RPCAP (Remote Packet Capture)-Dämon dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung. Über den RPCAP-Dämon wird ein Fernzugriff externer Applikationen auf die TCP/IP-Pakete der LAN-Schnittstellen des Kommunikationssystems ermöglicht. Ein RPCAP-Dämon wird häufig für Langzeit-Traces eingesetzt, da die Trace- Dateien auf einem PC und nicht im Kommunikationssystem abgelegt werden.

Anmerkung: Die in der Registerkarte genannten Sicherheitshinweise sind zu beachten.

Parameterbeschreibung der Registerkarten:

- **rpcap**

Parameter	Beschreibung
Adresse, an die gebunden werden soll	
IP-Adresse (numerisch oder literal)	IP-Adresse des HOST, auf dem die Aufzeichnungen erfolgen. Standardwert: 0.0.0.0
Port (bitte einen unbelegten Port auswählen)	Port des HOST, über den die Aufzeichnungen erfolgen.
Internes LAN tracen	Bei aktiviertem Flag erfolgt eine Aufzeichnung des Datenverkehrs zwischen zwei Baugruppen über die Schnittstelle eth9. Standardwert: Deaktiviert
Client-Identifikation für Zugriffskontrolle	
IP-Adresse (numerisch oder literal)	IP-Adresse des Remote-Clients, auf dem der Trace ausgegeben wird. Standardwert: 0.0.0.0

28.2.5.17 Traces > Kernel-Crash-Daten

Der Kernel Crash-Datendienst dient der automatischen Erfassung von Kernel-Crash-Daten. Er ist nur auf OSBiz X-Systemen mit V3-Mainboards verfügbar: OCCLA, OCCMA(R), OCCMB(R).

Der Dienst erfordert einen Speicherplatz von 200 MB. Die betroffenen Festplatten sind:

- SATA SSD 16GB (wenn keine NVMe SSD eingebaut ist)
- NVMe SSD

Es wird empfohlen, die Traces vor dem Start des Dienstes zu löschen, wenn Sie Speicherplatz freigeben möchten. Wenn der Platz nicht ausreicht, wird der Dienst keine Daten erfassen.

Parameterbeschreibung der Registerkarten:

- **Kernel-Crash-Daten**

Parameter	Beschreibung
Kernel Crash-Datendienst	Status des Dienstes: Grün: Der Dienst ist aktiviert. Grau: Der Dienst ist deaktiviert.
Start	Startet den Kernel Crash-Datendienst.
Anhalten	Stoppt den Kernel Crash-Datendienst.

Beim Starten oder Stoppen des Kernel Crash-Datendienstes wird automatisch ein Neustart des Systems eingeleitet. Der Dienst behält seinen Status nach dem Neustart des Systems bei.

Wenn der Dienst aktiviert ist, sind nach einem Systemneustart mit dem Grund WATCHDOG oder KERNEL_OOPS Kernel-Crash-Daten im oso-Diagnosespeicher verfügbar. Um Kernel-Crash-Daten zu sammeln, muss das Kontrollkästchen **CoreLog Protocol** unter **Servicezentrum** > **Diagnostik** > **Rückverfolgung** > **Diagnose-Protokolle** aktiviert sein.

Nach dem Sammeln der Kernel-Crash-Daten muss der Dienst manuell deaktiviert werden.

28.2.5.18 Traces > Medienserver-Trace

Anhand von Medienserver-Trace werden die Prozess- und Zustandsinformationen einzelner Medienserver-Komponenten des Kommunikationssystems aufgezeichnet.

Parameterbeschreibung der Registerkarten:

- **Trace-Komponente des Medienservers bearbeiten**

Parameter	Beschreibung
Package-Name	Name der Trace-Komponente Standardwert: Media Server
Trace-Level	Detaillierungsgrad des Trace (None, Unspecified, Default, Fatal, Error, Warning, Info, Unexpected, Debug, Fine, Finest)
Trace-Status	Status des Trace: Grün: Der Trace ist aktiviert. Grau: Der Trace ist deaktiviert.
Start	Startet den Medienserver-Trace.
Anhalten	Stoppt den Medienserver-Trace.

28.2.6 Events

Unter **Events** sind die Funktionen zum Anzeigen und Steuern der Ereignisse (Events) zusammengefasst. Dazu gehören z.B. die Event-Konfiguration und die E-Mail-Einstellungen.

28.2.6.1 Events > Event-Konfiguration

Parameterbeschreibung der Registerkarten:

- **Event-Konfiguration ändern**

Parameter	Beschreibung
Event-Datei-Einstellungen	
Max. Größe des Event-Buffers (Byte)	Anzeige der maximalen Größe des Event-Buffers in Byte
Max. Größe der Event-Datei (Byte)	Anzeige der maximalen Größe der Event-Protokolldatei in Byte
Event-Timer (s)	Anzeige der Zeit in Sekunden, nach deren Ablauf eine neue Event-Protokolldatei angelegt wird.
Event über LAN (XTracer)	
Event-Protokollierung über LAN (XTracer) aktivieren	Bei aktiviertem Flag werden Event-Protokollmeldungen über die LAN-Schnittstelle übertragen. Standardwert: Deaktiviert
Timer-Wert (s)	Anzeige der Zeit in Sekunden, nach deren Ablauf Event-Protokolldaten über die LAN-Schnittstelle übertragen werden.

28.2.6.2 Ereignisse > Event-Protokoll

Diese Funktion dient zum Herunterladen oder Löschen der Event-Protokolldatei.

Parameterbeschreibung der Registerkarten:

- **Laden über HTTP**
- **Event-Protokoll löschen**

28.2.6.3 Events > E-Mail

Parameterbeschreibung der Registerkarten:

- **E-Mail-Einstellungen bearbeiten**

Parameter	Beschreibung
E-Mail-Einstellungen	
Betreff	Text, der im Betreff-Feld der E-Mails angezeigt wird.
Empfänger-E-Mail-Adressen	
Empfänger 1	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.
Empfänger 2	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.

Parameter	Beschreibung
Empfänger 3	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.
Empfänger 4	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.
Empfänger 5	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.
Empfänger von Notfallbenachrichtigungen	
Empfänger für Notfälle	E-Mail-Adresse eines Sicherheitsbeauftragten vor Ort, an den eine E-Mail gesendet wird, wenn eine Notrufnummer gewählt wird.

28.2.6.4 Events > Reaktionstabelle

Anhand der Reaktionstabelle kann für jeden möglichen Event getrennt definiert werden, wie bei dessen Eintreten reagiert werden soll.

Parameterbeschreibung der Registerkarten:

- **Alle Events ändern**
- **Alle Events auf Werkseinstellung zurücksetzten**
- **Event bearbeiten**
- **Zugeordnetes Trace-Profil starten/stoppen**

Parameter	Beschreibung
Event-Name	Name des Events
SNMP-Trap senden	Bei aktiviertem Flag wird bei Eintreten des Events ein SNMP-Trap gesendet.
E-Mail senden	Bei aktiviertem Flag wird bei Eintreten des Events eine E-Mail an die unter **E-Mail-Einstellungen** bearbeiten eingetragenen E-Mail-Empfänger verschickt.
Zugeordnetes Trace-Profil	Trace-Profil, das bei Eintreten des Events gestartet oder gestoppt wird.
Trace-Profil starten	Bei aktiviertem Flag wird bei Eintreten des Events das ausgewählte Trace-Profil gestartet.
Trace-Profil stoppen	Bei aktiviertem Flag wird bei Eintreten des Events das ausgewählte Trace-Profil gestoppt.
Gateway neu starten	Zeigt an, ob bei Eintreten des Events das Kommunikationssystem neu gestartet wird.
Gateway neu starten: Ja	Bei Eintreten des Events erfolgt ein Neustart des Kommunikationssystems.
Gateway neu starten: Nein	Bei Eintreten des Events erfolgt kein Neustart des Kommunikationssystems.
OpenScape benachrichtigen	Zeigt an, ob bei Eintreten des Events eine Meldung an das Kommunikationssystem erfolgt.
OpenScape benachrichtigen: Ja	Bei Eintreten des Events erfolgt eine Meldung an das Kommunikationssystem.
OpenScape benachrichtigen: Nein	Bei Eintreten des Events erfolgt keine Meldung an das Kommunikationssystem.

28.2.6.5 Events > Diagnosie Logs

Hier werden die Diagnose Logs ((Protokolldateien) angezeigt, die bei kritischen Systemzuständen automatisch erzeugt wurden.

Parameterbeschreibung der Registerkarten:

- **Diagnose Logs holen**
- **Diagnose Logs löschen**

Parameter	Beschreibung
Dateiname	Name des im Kommunikationssystem gespeicherten Diagnose Logs ((Protokolldatei)
Größe (in Byte)	Größe der Diagnose Logs in Byte
Geändert	Änderungsdatum des Diagnose Logs
Attribute	Attribute des Diagnose Logs: • r = Leseberechtigung (Read) • w = Schreibberechtigung (Write)

28.2.6.6 Events > Alarm-Signalisierung

Hier werden die Teilnehmer (Systemtelefone mit Display, UP0 & HFA) ausgewählt, die benachrichtigt werden, wenn die Temperatur des Systems 55 Grad Celsius übersteigt. Werden 60 Grad Celsius überschritten, werden die für die Überhitzung verantwortlichen Baugruppen (z.B. OCAB, SLAD8/16) kontrolliert heruntergefahren oder abgeschaltet.

Parameterbeschreibung der Registerkarten:

- **Alarm-Signalisierung ändern**

Parameter	Beschreibung
Temperatur Alarm-Siganlisierungsports	
Teilnehmer 1	1. Ziel (Teilnehmer mit Systemtelefon).
Teilnehmer 2	2. Ziel (Teilnehmer mit Systemtelefon).
Teilnehmer 3	3. Ziel (Teilnehmer mit Systemtelefon).

28.2.7 Restart / Reload

Hier kann ein Restart (Neustart) oder ein Reload von OpenScape Business ausgelöst werden oder OpenScape Business X kontrolliert herunterfahren werden (Shutdown). Darüber hinaus kann ein Restart (Neustart) der UC Applikation (UC Smart oder UC Suite) oder der UC Booster Card (Application Board OCAB) ausgelöst werden. Um das kontrollierte Herunterfahren von OpenScape Business X über ein Systemtelefon zu ermöglichen, kann eine PIN definiert werden. Im Fall einer Vernetzung ist die Synchronisierung der vernetzten Kommunikationssysteme möglich.

28.2.7.1 Restart / Reload > Restart / Reload

Parameter	Beschreibung
System	
System neu starten	Kontrollierter Restart (Neustart) von OpenScape Business: • OpenScape Business S und OpenScape Business X: Es erfolgt ein kontrollierter Restart (Neustart) des Kommunikationssystems. Ist OpenScape Business X3/X5/X8 mit einer UC Booster Card (Application Board OCAB) bestückt, erfolgt auch ein kontrollierter Restart (Neustart) der UC Applikation (UC Smart oder UC Suite). • OpenScape Business UC Booster Server (Application Server): Es erfolgt ein kontrollierter Restart (Neustart) des OpenScape Business-Anteils und der UC Applikation (UC Suite).
System-Reload ausführen	Reload von OpenScape Business: • OpenScape Business S und OpenScape Business X: Es erfolgt ein Reload des Kommunikationssystems. Nach dem anschließenden Hochlauf befindet sich das Kommunikationssystem im Grundzustand. Alle länder- und kundenspezifischen Einstellungen wurden gelöscht (System-Länderkennzeichen = Deutschland). Das Kommunikationssystem hat die Standard-IP-Adresse 192.168.1.2 und den internen IP-Adressbereich 192.168.3.xxx. Die Lizenzierung bleibt erhalten. • OpenScape Business UC Booster Server: Es erfolgt ein Reload des OpenScape Business-Anteils. Nach dem anschließenden Hochlauf befindet sich der OpenScape Business-Anteil im Grundzustand. Alle kundenspezifischen Einstellungen des OpenScape Business-Anteils (zum Beispiel das Benutzerverzeichnis) wurden gelöscht. Die Lizenzierung bleibt erhalten. Das Betriebssystem wird nicht zurückgesetzt.
System herunterfahren	Kontrolliertes Herunterfahren von OpenScape Business X: • OpenScape Business X3/X5: Das anschließende Hochfahren des Kommunikationssystems ist ausschließlich durch Ziehen und anschließendes Stecken des Netzsteckers möglich. • OpenScape Business X8: Das anschließende Hochfahren des Kommunikationssystems ist ausschließlich durch Ausschalten und anschließendes Wiedereinschalten aller Stromversorgungen LUNA2 möglich.
Shutdown aktivieren/ deaktivieren	Definition einer PIN für die Aktivierung des Shutdowns (das kontrollierte Herunterfahren des Kommunikationssystems) über ein Systemtelefon
Application Board neu starten	Kontrollierter Restart (Neustart) des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite): Bei einem Restart des Application Boards OCAB werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.
Applikationen	

Parameter	Beschreibung
Sync-Netzwerk	Synchronisierung vernetzter Kommunikationssysteme: Nach der Änderung von Rufnummern, Durchwahlnummern oder Namen werden durch eine Synchronisierung die Daten in allen vernetzten Kommunikationssystemen aktualisiert.
UC Application neu starten	Kontrollierter Restart (Neustart) der UC Applikation (UC Smart oder UC Suite): Bei einem Restart der UC Applikation werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

28.2.8 SNMP

Unter **SNMP** sind die Funktionen zum Einrichten von Communities und Traps zusammengefasst. Durch Communities werden die Zugriffsberechtigungen auf die SNMP-Daten geregelt. Bei Problemen im System werden Traps erzeugt, um den Administrator über Fehler und Ausfälle zu informieren.

28.2.8.1 SNMP > Communities

Parameterbeschreibung der Registerkarten:

- **Communities anzeigen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SNMP-Kommunikationspartners. Bei der Adresse 127.0.0.1 ist die Kommunikation mit externen IP-Adressen gesperrt.
Community	Identifikation/Zugangspasswort, das für den SNMP-Nutzer verwendet wird. ***INFO:*** Zur Erhöhung der Sicherheit wird empfohlen, nicht den Standardwert **public** zu verwenden.
Type	Auswahl des Typs.
Typ: **Lesende Community**	Kommunikationspartner mit lesendem SNMP-Zugang.
Typ: **Lesende Community**	Kommunikationspartner mit lesendem und schreibendem SNMP-Zugang.
Typ: **Trap-Community**	Kommunikationspartner an den Fehlermeldungen (Traps) gesendet werden.

28.2.8.2 SNMP > Communities > Lesende Communities

Parameterbeschreibung der Registerkarten:

- **Lesende Communities anzeigen**
- **Lesende Community hinzufügen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SNMP-Kommunikationspartners. Bei der Adresse 127.0.0.1 ist die Kommunikation mit externen IP-Adressen gesperrt.
Community	Identifikation/Zugangspasswort, das für den SNMP-Nutzer verwendet wird. ***INFO:*** Zur Erhöhung der Sicherheit wird empfohlen, nicht den Standardwert **public** zu verwenden.

28.2.8.3 SNMP > Communities > Schreibende Communities

Parameterbeschreibung der Registerkarten:

- **Schreibende Communities anzeigen**
- **Schreibende Community hinzufügen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SNMP-Kommunikationspartners. Bei der Adresse 127.0.0.1 ist die Kommunikation mit externen IP-Adressen gesperrt.
Community	Identifikation/Zugangspasswort, das für den SNMP-Nutzer verwendet wird. ***INFO:*** Zur Erhöhung der Sicherheit wird empfohlen, nicht den Standardwert **public** zu verwenden.

28.2.8.4 SNMP > Communities > Trap Communities

Parameterbeschreibung der Registerkarten:

- **Trap-Communities anzeigen**
- **Trap-Community hinzufügen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SNMP-Kommunikationspartners. Bei der Adresse 127.0.0.1 ist die Kommunikation mit externen IP-Adressen gesperrt.
Community	Identifikation/Zugangspasswort, das für den SNMP-Nutzer verwendet wird. ***INFO:*** Zur Erhöhung der Sicherheit wird empfohlen, nicht den Standardwert **public** zu verwenden.

28.2.8.5 SNMP > Traps

Parameterbeschreibung der Registerkarten:

- **Alle Traps anzeigen**
- **Alle kritischen Traps anzeigen**

Parameter	Beschreibung
VarBind1 (Severity)	Klassifizierung des Traps: • Critical: Fehlermeldung. Der Fehler hat problematische Auswirkungen. • Major: Fehlermeldung. Der Fehler kann problematische Auswirkungen haben. • Minor: Fehlermeldung. Der Fehler hat keine problematischen Auswirkungen. • Warning: Meldung über einen möglicherweise problematischen Vorgang oder Zustand. • Cleared: Die Fehlermeldung wurde aufgehoben (zum Beispiel Port ist wieder in Betrieb) • Information: Reine Statusmeldung, keine Fehlermeldung
VarBind2 (Name)	Name des Traps
Generischer Name	Allgemeine Bezeichnung, wie zum Beispiel Enterprise Specific
Spezifischer Name	Typ des Traps: • 1 = Software • 2 = Hardware
Enterprise	(nicht benutzt)
Uhrzeit	Zeitpunkt des Fehlers
Index	Fortlaufende Nummer

28.2.9 Admin-Protokoll

Mit **Admin.-Protokoll** kann der Administrator die Konfiguration (z.B. die Sprache) für das Administrationsprotokoll ändern.

28.2.9.1 Admin-Protokoll > Konfiguration

Parameterbeschreibung der Registerkarte:

- **Konfiguration ändern**

Parameter	Beschreibung
Admin-Protokoll Sprache	Einstellung der gewünschten Sprache für das Admin.-Protokoll. Das Admin-Protokoll bietet eine Übersicht der am Kommunikationssystem durchgeführten Änderungen. Mögliche Sprachen: Deutsch, Englisch, Französisch, Spanisch, Italienisch, Portugiesisch, Niederländisch

28.2.9.2 Admin-Protokoll > Admin-Protokoll-Daten

Parameterbeschreibung der Registerkarte:

- **Laden über HTTP**

Parameter	Beschreibung
Laden über HTTP	Speichert das Admin.-Protokoll des Kommunikationssystems. Das Admin-Protokoll bietet die Möglichkeit zu erfahren, wann Änderungen am Kommunikationssystem durchgeführt worden sind und von wem diese gemacht wurden. Protokolliert werden Logins auf dem Kommunikationssystem.

28.2.10 Aktionen

Unter **Aktionen** sind die Funktionen zusammengefasst, die den Administrator bei häufig wiederkehrenden Administrationsaufgaben z.B. dem Löschen von Protokolldaten unterstützen.

28.2.10.1 Aktionen > Manuelle Aktionen > Diagnose-Protokolle

Parameterbeschreibung der Registerkarten:

- **Daten laden über HTTP**

Parameter	Beschreibung
Trace-Protokoll	Bei aktiviertem Flag werden Systemtrace-Protokolldateien heruntergeladen. Folgende Auswahlmöglichkeiten bestehen: • Gesamtes Protokoll: Die gesamten vorhandenen Systemtrace-Protokolldateien werden heruntergeladen. • Protokoll von heute: System Trace-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • Eigene Auswahl: Von: XXX Bis: YYY: Die System Trace-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Standardwert: Aktiviert, Gesamtes Protokoll
Event-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Angaben über Aktionen/ Events des Kommunikationssystems (Reset, Ein-/Ausschalten usw.) heruntergeladen. Standardwert: Aktiviert
Admin.-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Angaben über Administrationsvorgänge (Login-Versuche usw.) heruntergeladen. Standardwert: Aktiviert
Lizenz-Protokolle	Bei aktiviertem Flag werden Protokolldateien mit Meldungen über lizenzierungspflichtige Komponenten des Kommunikationssystems heruntergeladen. Standardwert: Aktiviert
Kunden-Trace	Bei aktiviertem Flag werden Protokolldateien mit Meldungen für den Kunden-Trace (Remote-Login, ITSP-Login usw.) heruntergeladen. Die Meldungen für den Kunden-Trace werden dabei in ausführlicherer Form dargestellt, als zum Beispiel im Trace-Protokoll. Standardwert: Aktiviert

Parameter	Beschreibung
Framework-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Meldungen des WBM heruntergeladen. Standardwert: Aktiviert
Diagnose-Protokoll	Bei aktiviertem Flag werden Diagnose-Protokolle des Kommunikationssystems heruntergeladen. Standardwert: Aktiviert
UC Suite-Protokolle	Bei aktiviertem Flag werden Protokolldateien mit Meldungen der UC Suite (UC Suite-, CSP- und MEB-Protokolle) heruntergeladen. Folgende Auswahlmöglichkeiten bestehen: • Gesamtes Protokoll: Alle vorhandenen UC Suite-, CSP- und MEB-Protokolldateien werden heruntergeladen. • Protokoll von heute: Die UC Suite-, CSP- und MEB-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • Eigene Auswahl: Von: XXX Bis: YYY: Die UC Suite-, CSP- und MEB-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst. Für die OpenScape Business-Protokolle gelten folgende Dateibezeichnungen: UC Suite-Protokolldateien = vs_jjjj_mm_tt.log, CSP-Protokolldateien = csptrace_jjjj_mm_tt.log, MEB-Protokolldateien = mebtrace_jjjj_mm_tt.log Standardwert: Deaktiviert
Applikationsprotokolle	Bei aktiviertem Flag werden Protokolldateien mit Meldungen des Applikationsanteils des Kommunikationssystems (zum Beispiel CSP-Protokolle) heruntergeladen. • Gesamtes Protokoll: Alle vorhandenen Protokolldateien werden heruntergeladen. • Protokoll von heute: Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • Eigene Auswahl: Von: XXX Bis: YYY: Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst. Standardwert: Deaktiviert
System-Diagnose-Protokolle	Bei aktiviertem Flag werden Diagnose-Protokolle des Kommunikationssystems heruntergeladen. Standardwert: Aktiviert
PPP-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Meldungen zum Point-to-Point-Protokoll heruntergeladen. Standardwert: Aktiviert
CoreLog-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Informationen über den letzten Zustand des Betriebssystems heruntergeladen. CoreLogs werden zum Beispiel bei Restarts erstellt. Standardwert: Deaktiviert

28.2.10.2 Aktionen > Manuelle Aktionen > DLI-Wartung

Parameterbeschreibung der Registerkarten:

- **DLI-Gerätewartung**

Parameter	Beschreibung
Gerät löschen	Wählen Sie das Systemtelefon aus, das gelöscht werden soll. Mit dieser Aktion wird das Systemtelefon aus der DLI-Datenbank gelöscht. **Anmerkung:** Vor einer DLI-Wartungsaktion (Löschen) müssen Sie sich vergewissern, dass das Gerät nicht mehr verwendet wird.
Rufnr	Rufnummer des Systemtelefons.
Gerätetyp	Typ des Systemtelefons.
IP-Adresse	IP-Adresse des Systemtelefons; direkter Link zum WBM des Systemtelefons.
MAC-Adresse	MAC-Adresse des Systemtelefons.
Aktuelle SW-Version	Aktuelle Software-Version des Systemtelefons.

28.2.10.3 Aktionen > Automatische Aktionen > Garbage Collection

Parameterbeschreibung der Registerkarten:

- **Aktion ändern**
- **Action starten/stoppen**

Parameter	Beschreibung
Aktion aktiviert	Bei aktiviertem Flag wird regelmäßig eine automatische Speicherbereinigung auf dem Kommunikationssystem durchgeführt. Nach Abschluss jeder Speicherbereinigung führt das Kommunikationssystem einen Restart (Neustart) durch. Standardwert: Deaktiviert
Startzeit nach Mitternacht	Zeitpunkt nach Mitternacht, an dem die Aktion Garbage Collection durchgeführt wird. Beispiel: Beispiel: Im Feld **Std.** wurde 3 und im Feld **Min.** 30 eingegeben. Das bedeutet, die Aktion Garbage Collection wird morgens um 3:30 Uhr gestartet. Standardwert: 3 Std, 00 Min.
Aktion an folgenden Wochentagen ausführen	Die Aktion Garbage Collection wird an den ausgewählten Wochentagen durchgeführt. Standardwert: Aktiviert

28.2.10.4 Aktionen > Automatische Aktionen > DLS Notification

Parameterbeschreibung der Registerkarten:

- **Aktion ändern**
- **Action starten/stoppen**

Parameter	Beschreibung
Aktion aktiviert	Bei aktiviertem Flag wird beim Hochlauf des Kommunikationssystems die automatische Anmeldung an einem externen DLS-Server initiiert. Standardwert: Deaktiviert
IP-Adresse	IP-Adresse des externen DLS-Servers Standardwert: 0.0.0.0
Port	Port des externen DLS-Servers Standardwert: 10444
Benutzername	Benutzername für die Anmeldung am externen DLS-Server
Kennwort	Passwort für die Anmeldung am externen DLS-Server

28.2.10.5 Aktionen > Automatische Aktionen > SDHC-Integritätsprüfung

Parameterbeschreibung der Registerkarten

- SDHC-Integritätsprüfung

Parameter	Beschreibung
SDHC-Integritätsprüfung	
Integritätsprüfung starten	Aktiviert die sofortige Integritätsprüfung der Karte.
Integritätsprüfung starten aktiv	Aktiviert einen geplanten Tag, Monat, ein geplantes Jahr und eine geplante Uhrzeit für die Integritätsprüfung der Karte.
Protokoll-Datei Das Ergebnis der letzten Dateiprüfungen wird ausgegeben.	
Status/Empfohlene Aktion Empfiehlt Aktionen für jede Integritätsprüfung der Karte.	

28.2.11 Plattform-Diagnose

Möglichkeit der Plattform-Diagnose (nur für Entwicklung).

28.2.12 Applikat.-Diagnose

Möglichkeit der Applikations-Diagnose (nur für Entwicklung).

28.2.12.1 Applikat.-Diagnose > Entwickler-Einstellungen > Trace-Konsolen-Ausgabe

Möglichkeit der Applikations-Diagnose (nur für Entwicklung).

28.2.12.2 Applikat.-Diagnose > Entwickler-Einstellungen > Übernahme des Write Tokens

Möglichkeit der Applikations-Diagnose (nur für Entwicklung).

28.2.12.3 Applikat.-Diagnose > Mainboard

Änderungen der Einstellungen sollten nur nach Aufforderung durch den zuständigen Service-Support erfolgen.

28.2.12.4 Applikat.-Diagnose > Entwickler-Einstellungen > SIP-Provider-Profile

Parameterbeschreibung der Tags:

- SIP-Provider-Profil hinzufügen
- SIP-Provider-Profile bearbeiten

Diese Seite ist für die Verwendung durch geschultes Fachpersonal während der Zertifizierung eines neuen ITSP vorgesehen. Bitte lesen Sie die Dokumente im Unify-Wiki: http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#How_to_get_a_new_VoIP_provider_released, um weitere Informationen zu erhalten.

28.2.13 IP-Diagnose

Möglichkeit der IP-Diagnose (nur für Entwicklung).

28.2.13.1 IP-Diagnose > Mainboard > ARP-Protokoll

Diese Funktion dient zur Anzeige der Daten des Address Resolution Protocol ARP. Die Mapping-Tabelle zeigt die Zuordnung der Netzwerkadressen zu den MAC-Adressen.

Parameterbeschreibung der Registerkarten:

- **ARP-Protokoll anzeigen**

Parameter	Beschreibung
IP-Adresse	Zeigt die Netzwerkadressen, die aktuell am Mainboard des Kommunikationssystems angeschlossen sind.
MAC-Adresse	Zeigt die zugehörige physikalische Adresse des angeschlossenen Netzwerkadressen
Type	Zeigt die Zuordnung der Adressen. Möglich ist eine feste (statisch) oder dynamische Zuordnung.
Schnittstelle	Interne Bezeichnung der vorhandenen LAN-Schnittstellen (zum Beispiel eth0, eth1, eth2, eth3)

28.2.13.2 IP-Diagnose > Mainboard > ICMP-Anforderung > Ping

Mittels dieser Funktion kann die Netzwerkverbindung zwischen dem Kommunikationssystem und einer frei wählbaren Ziel-Adresse mit Hilfe eines Ping-Befehls (Echoanforderung) überprüft werden.

Parameterbeschreibung der Registerkarten:

- **Execute Ping**

Parameter	Beschreibung
ICMP-Parameter	
Ziel-Adresse	IP-Adresse des Ziels, dessen Netzwerkverbindung zum Kommunikationssystem mit Hilfe von Echoanforderungspaketen überprüft wird. Standardwert: 127.0.0.1
Anzahl zu sendender Echoanforderungen	Anzahl der zu sendenden Echoanforderungspakete für die Überprüfung der Netzwerkverbindung Standardwert: 3

28.2.13.3 IP-Diagnose > Mainboard > ICMP-Anforderung > Traceroute

Mittels dieser Funktion wird anhand von ICMP-Echoanforderungen ermittelt, über welche Router Datenpakete bis zur abgefragten Ziel-Adresse vermittelt werden.

Parameterbeschreibung der Registerkarten:

- **Traceroute**

Parameter	Beschreibung
ICMP-Parameter	
Ziel-Adresse	IP-Adresse des Ziels, dessen Traceroute zum Kommunikationssystem mit Hilfe von ICMP-Echoanforderungen überprüft wird. Standardwert: 127.0.0.1

Parameter	Beschreibung
TOS-Byte	Anzeige, ob TOS (Type Of Service)-Bytes gesendet werden. TOS-Bytes geben Aufschluss über die Qualität eines Dienstes. Wertebereich: 0 bis 255, Standardwert: 0

28.2.14 Online-Benutzer

Web-Tool zur Fernsteuerung von OpenStage-Telefonen.

28.2.14.1 Online-Benutzer

Mit dem Online-Benutzer öffnet sich der Java Husim Phone Tester (jHPT). Dies ist ein Web-Tool zur Fernsteuerung von OpenStage-Telefonen über das Internet. Über eine Web-Oberfläche wird ein vorhandenes Systemtelefon so kontrolliert, dass reale Tastendrücke und Anzeigen des Kommunikationssystems übermittelt werden. Für das jHPT gibt es eine separate Dokumentation, die über die Hilfe-Funktion des Tools heruntergeladen werden kann (hier keine weitere Beschreibung der jHPT Seiten).

28.3 Telefonie

Unter **Telefonie** sind Funktionen für die Konfiguration der Telefonie zusammengefasst, um z.B. Teilnehmer oder das Call Management (CM) einzurichen.

28.3.1 Grundeinstellungen

Unter **Grundeinstellungen** sind Funktionen zusammengefasst, wie z.B. Systemflags, Einstellungen für Verzeichnisse und Kurzwahlziele, DynDNS, Quality of Service, Datum und Uhrzeit und Gebühren.

28.3.1.1 Grundeinstellungen > System > System Flags

Parameterbeschreibung der Registerkarten:

- **System Flags ändern**

Parameter	Beschreibung
Durchschalten bei AUL extern ein	Bei aktiviertem Flag wird ein Anruf bei einer externen Anrufumleitung sofort durchgeschaltet. Das Durchschalten erfolgt unabhängig davon, ob es sich um einen internen oder externen (HKZ/ISDN) Anruf handelt. Erfolgt die Anrufumleitung über eine ISDN-Amtsleitung und befindet sich das externe Anrufumleitungsziel in einem anderen Netz (zum Beispiel GSM-Netz), wird der Verbindungsaufbau vom ISDN-Amt mit dem Progress-Indikator Leaving ISDN gemeldet. Ab diesem Zeitpunkt entstehen Verbindungskosten für den Anrufer. Standardwert: Deaktiviert

Parameter	Beschreibung
Anrufumleitung nach HKZ erlaubt	Bei aktiviertem Flag folgen Anrufe über analoge Amtleitungen (HKZ) der externen Anrufumleitung. Standardwert: Aktiviert
Rufweiterschaltung nach AUL zum externen Ziel	Bei aktiviertem Flag gilt: Ist das externe Anrufumleitungsziel nicht erreichbar, erfolgt eine Rufweiterschaltung zum nächsten in der Rufzielliste eingetragenen Ziel. Standardwert: Deaktiviert
Konferenzton	Bei aktiviertem Flag werden die Teilnehmer einer Konferenz im Abstand von 20 Sekunden durch einen Sonderton darauf aufmerksam gemacht, dass sie sich in einer Konferenz befinden. Standardwert: Deaktiviert
Aufmerksamkeitssignalisierung bei AUN-Gruppen	Bei aktiviertem Flag wird ein Anruf für ein Mitglied einer Anrufübernahmegruppe bei den anderen Gruppenmitglieder optisch (Display) signalisiert. Wird der Anruf nicht innerhalb von vier Rufzyklen (4 x 5 Sekunden) angenommen, erhalten die anderen Gruppenmitglieder zusätzlich einen Hinweiston. Standardwert: Aktiviert
Sprachlautstärke für optiPoint/OpenStage erhöhen	Bei aktiviertem Flag wird für die optiPoint- und OpenStage-Telefone auf einen alternativen Dämpfungsplan umgeschaltet und damit eine höhere Sprachlautstärke erzielt. Standardwert: Deaktiviert
Endgerätetausch erlaubt	Bei aktiviertem Flag können Systemtelefone ohne Veränderung der logischen Konfiguration (Rufnummer, Name, Tastenprogrammierung usw.) physikalisch umgesteckt werden (Relocate/Rufnummerntausch). Standardwert: Deaktiviert
Mehr als 1 externer Konferenzteilnehmer	Bei aktiviertem Flag können mehrere externe Teilnehmer an einer Konferenz teilnehmen. Standardwert: Aktiviert
automatisches Leitungsvormerken	Bei aktiviertem Flag kann ein Teilnehmer eine Leitung vormerken, wenn ihm keine freie Amtsleitung zur Verfügung steht. Sobald diese Leitung frei wird, erhält er einen Wiederanruf und kann anschließend die externe Verbindung aufbauen. Standardwert: Deaktiviert
Wahlwiederholung mit PKZ	Bei aktiviertem Flag wird bei der Wahlwiederholung neben der Rufnummer auch eine vorher eingegebene PKZ wiederholt. Standardwert: Deaktiviert

Parameter	Beschreibung
Automatische Leitungsbelegung	Wenn dieses Flag aktiviert ist, so erfolgt mit Wahl einer Ziffer von einem Systemfernsprecher sofort eine Leitungsbelegung, und die gewünschte Rufnummer wird gewählt. Die Wahl der Zugangskennziffer ist dabei nicht erforderlich. Für die Anwahl eines internen Teilnehmers muss entweder • die Taste Intern betätigt, und die Teilnehmerrufnummer nachgewählt werden • oder die entsprechende DSS-Tasten betätigt werden. Diese Funktion ist nur dann verfügbar, wenn nur eine Richtung (siehe "Richtungen") konfiguriert ist. Sind im Kommunikationssystem noch Entry, ISDN oder a/b-Telefone angeschaltet, ist LCR mit automatischer Wahl nicht möglich.
Nur eingerichtete Nummer für MSN benutzen	Bei aktiviertem Flag können an einem S0-Bus die MSN (Multiple Subscriber Number) nur für bereits vorhandene interne Rufnummern eingerichtet werden (um eventuellen Gebührenmissbrauch zu verhindern). Standardwert: Deaktiviert
Wegeoptimierung	Bei aktiviertem Flag wird bei vernetzten Kommunikationssystemen eine Wegeoptimierung durchgeführt. Das Flag muss bei allen zu einer Vernetzung gehörenden Kommunikationssystemen aktiviert werden. Beispiel für zwei vernetzte Systeme (System 1 und System 2): Bei einem Anruf von Teilnehmer A (System 1) an Teilnehmer B (System 2) und anschließender Anrufumleitung zu Teilnehmer C (System 1) werden zwei Leitungen belegt. Durch Wegeoptimierung wird die Verbindung von A nach C automatisch über eine einzige Leitung geschaltet. Standardwert: Aktiviert
DTMF automatisch	Bei aktiviertem Flag wird nach jedem erfolgreichen gehenden Verbindungsaufbau automatisch in den DTMF-Modus (MFV-Modus) umgeschaltet. Damit wird zum Beispiel die Fernabfrage von Anrufbeantwortern ermöglicht. Standardwert: Aktiviert
Paging mit Zweierverbindung	Bei aktiviertem Flag ermöglicht Direktansprechen (Paging) einen internen Verbindungsaufbau, ohne dass der gerufene Teilnehmer den Hörer abhebt. Durch Abheben des Hörers erfolgt der Übergang zu einem normalen Zweiergespräch. Standardwert: Aktiviert
Ton vom Amt	Bei aktiviertem Flag wird eine Verbindung auch dann zum Amt oder zu einem vernetzten Kommunikationssystem durchgeschaltet, wenn von der Gegenseite kein Ton gesendet wird. Standardwert: Deaktiviert
R-Gesprächsschutz	Bei aktiviertem Flag werden R-Gespräche automatisch ausgelöst. Standardwert: Deaktiviert

Parameter	Beschreibung
Euroimpedanz	Bei aktiviertem Flag gelten folgende Impedanzwerte in Europa: a/b-Schnittstellen für den analogen Teilnehmeranschluss: Eingangsimpedanz = 270 Ohm + 750 Ohm || 150 nF, Nachbildimpedanz = 270 Ohm + 750 Ohm || 150 nF, Relativer Pegel A/D = 0 dBr, Relativer Pegel D/A = –7 - 7 dBr a/b-Schnittstellen für den analogen Amtsanschluss: Eingangsimpedanz = 270 Ohm + 750 Ohm || 150 nF, Nachbildimpedanz = 270 Ohm + 750 Ohm || 150 nF, Relativer Pegel A/D = –6 - 6 dBr, Relativer Pegel D/A = –1 - 1 dBr Standardwert: Deaktiviert
Verschiedene Phonemailansagen Tag/ Nacht	Bei aktiviertem Flag können (bei einem Kommunikationssystem mit Voicemail) verschiedene Voicemail-Ansagen für einen Teilnehmer aktiviert werden, indem verschiedene Rufnummern für diesen Teilnehmer an die Voicemail übermittelt werden. Voraussetzung dafür ist, dass für diesen Teilnehmer unterschiedlich Rufweiterschaltungen für Tag- und Nachtbetrieb konfiguriert werden. Standardwert: Deaktiviert
Internationale/nationale Kennzahl anzeigen	Bei aktiviertem Flag wird das Anzeigeformat von KWZ-Nummern bei kommenden Anrufen definiert, für die im KWZ-Speicher kein Name hinterlegt ist. Im Display des Telefons wird bei kommenden Anrufen die komplette Rufnummer angezeigt (Anlagenrufnummer + Durchwahl, inklusive Ortsnetzkennzahl und Ländervorwahl, falls vorhanden). Beispiel: Die KWZ-Nummer 06671234 wurde ohne Namen eingerichtet. Ortsnetzkennzahl = 02302, Anlagenrufnummer = 667, Durchwahl = 1234. Bei einem eingehenden Anruf von 6671234 wird im Display 023026671234 angezeigt. Standardwert: Deaktiviert
Leitungswechsel bei Direktruf	Mit diesem Flag wird das Verhalten einer Direktruftaste definiert, wenn eine aktive Gesprächsverbindung auf einer MULAP-Leitung vorliegt. Relevant für Teamschaltung / Team-Gruppe, Chef/Sekretär / Top-Gruppe, Basic-MULAP, Chef-MULAP. Nach dem Drücken einer Direktruftaste wird ein Leitungswechsel durchgeführt. Das Gespräch wird gehalten und kann nur an diesem Telefon wieder aufgenommen werden. Standardwert: Deaktiviert (nicht für USA, Kanada), Aktiviert (nur für USA, Kanada)
Automatische Wahlwiederholung	Im Fall eines besetzten Teilnehmers wird eine automatische Wahlwiederholung durchgeführt. Über den Zeitparameter Zeit für automatische Wahlwiederholung wird definiert, nach welcher Zeit die Wahlwiederholung aktiv wird. Standardwert: Deaktiviert
Knoten-Rufnummer bei Voice Mail	Bei aktiviertem Flag wird bei vernetzten Kommunikationssystemen definiert, ob die Knoten-Rufnummer bei der Identifizierung eines zentralen oder mehrerer dezentraler VoiceMail-Server mitzuliefern ist. Die Knotenrufnummer muss für die Identifizierung des oder der VoiceMail-Server mitgeliefert werden. Standardwert: Deaktiviert

Parameter	Beschreibung
Anrufübernahme nach Wiederanruf	Bei aktiviertem Flag werden Wiederanrufe und Rückrufe auch bei den anderen Mitgliedern einer Anrufübernahmegruppe signalisiert und können von diesen übernommen werden. Standardwert: Deaktiviert
Einstellbare CLIP	Bei aktiviertem Flag wird Anstelle der eigentlichen Rufnummer die unter Clip/Lin eingetragene Nummer zum gerufenen externen Anschluss übermittelt und am Display angezeigt. Bei leerem Eintrag Clip/Lin wird die Rufnummer übermittelt. Standardwert: Aktiviert
Anruferliste beim Zielteilnehmer im Falle Umleitung MULAP	Bei aktiviertem Flag werden bei einer Umleitung MULAP kommende Anrufe in der Anruferliste des Zielteilnehmers eingetragen. Standardwert: Deaktiviert
Rufweiterschaltung nach Deflect call / Single step transfer	Bei aktiviertem Flag gilt: Hat ein Teilnehmer eine Anrufumleitung zu einem internen Ziel aktiviert (Deflect Call), wird der Anruf bei diesem Ziel signalisiert. Nach abgelaufener Rufweiterschaltungszeit wird der Anruf bei einem in der Rufzielliste eingetragenen ersten Ziel und anschließend bei einem eventuell eingetragenen zweiten Ziel signalisiert. Beispiel: Für Teilnehmer A wurde ein Deflect Call auf Teilnehmer B ausgeführt. Das erste eingetragene Ziel in der Rufzielliste von Teilnehmer B ist Teilnehmer C und das zweite Ziel Teilnehmer D. Der Anruf wird bei Teilnehmer C und nach abgelaufener Rufweiterschaltungszeit bei Teilnehmer D signalisiert. Die Aktivierung dieses Flags ist nur sinnvoll, wenn auch das Flag Ermittlung des Ziels über Rufzielliste beim Deflect Call / Single Step Transfer aktiviert wird. Damit dieses Flag eine Wirkung hat, erfolgen die Umleitungsfunktion bei Anruf, Deflect und Single Step Call Transfer, und gelten vor allem für Anrufe, die über UC (Auto Attendant/ UCD-Gruppen) abgewickelt werden und bei denen diese Umleitungsfunktionen anwendbar sind. Standardwert: Aktiviert
Ermittlung des Ziels über Rufzielliste beim Deflect call / Single step transfer	Bei aktiviertem Flag gilt: Hat ein Teilnehmer eine Anrufumleitung zu einem internen Ziel aktiviert (Deflect Call) wird der Anruf bei diesem Ziel signalisiert und nach abgelaufener Rufweiterschaltungszeit bei einem in der Rufzielliste eingetragenen weiteren Ziel. Beispiel: Für Teilnehmer A wurde ein Deflect Call auf Teilnehmer B ausgeführt. Das erste eingetragene Ziel in der Rufzielliste von Teilnehmer B ist Teilnehmer C. Nach abgelaufener Rufweiterschaltungszeit wird der Anruf bei Teilnehmer C signalisiert. Damit dieses Flag eine Wirkung hat, erfolgen die Umleitungsfunktion bei Anruf, Deflect und Single Step Call Transfer, und gelten vor allem für Anrufe, die über UC (Auto Attendant/ UCD-Gruppen) abgewickelt werden und bei denen diese Umleitungsfunktionen anwendbar sind. Standardwert: Aktiviert
Hinweiston während Sprachaufzeichnung	Wenn das Flag aktiviert ist, gilt für OpenScape Business X: Wird während eines Gesprächs die Sprachaufzeichnung (Live Call Record) aktiviert, so wird bei aktiviertem Flag ein entsprechender Hinweiston ausgegeben. Standardwert: Aktiviert

Parameter	Beschreibung
E.164 Nummerierung	Über dieses Flag kann die Vernetzung der KDS von ortsübergreifenden oder weltweit aufgestellten Kundenanlagen ein- bzw. ausgeschaltet werden. Die Teilnehmer sind über eine öffentliche Rufnummer, d.h. die E.164-Rufnummer im nationalen oder internationalen Format (z.B. interne Calling Party Number im ISDN Format), erreichbar, ohne dass eine Knotenrufnummer vorgewählt werden muss. Jeder Teilnehmer repräsentiert sich mit seiner E.164 Rufnummer, die in optimierter Form dargestellt werden kann. Bei eingeschaltetem Flag wird die interne Rufnummer im E.164-Format übertragen. Ist dieses Flag gesetzt, so werden SIP-Teilnehmer mit der E.164-Langrufnummer (Standortnummer + interne Rufnummer z.B. 4923026673665) registriert. Standardwert: Deaktiviert
Erweiterte Schlüsselfunktionen	Wenn das Flag aktiviert ist – und nachdem eine beliebige Taste als "Shift-Taste" definiert wurde –, können auf der dann verfügbaren zweiten Tastenebene ausschließlich Rufnummern ohne LED-Unterstützung gespeichert werden. Beliebige Tastenfunktionen auf der ersten Tastenebene können programmiert werden. Die LED-Signalisierung gilt ausschließlich für die erste Tastenebene. Standardwert: Deaktiviert
A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungziel / RWS-Ziel	Bei aktiviertem Flag werden ob Rufnummer und Name eines Anrufers bei allen Mitgliedern einer Anrufübernahmegruppe, bei zugeschalteten Teilnehmern (Rufzuschaltung) und bei Umleitungs- und Rufweiterschaltungszielen angezeigt. Rufnummer und Name werden im Display angezeigt. Standardwert: Aktiviert
SPE Unterstützung	Bei aktiviertem Flag wird das Leistungsmerkmal Signaling and Payload Encryption SPE unterstützt. Die VoIP-Nutz- und Signalisierungsdatenströme vom und zum Kommunikationssystem und zwischen OpenStage-Systemtelefonen werden verschlüsselt. Standardwert: Deaktiviert **Anmerkung:** Wenn Sie den Cloud-Dienst Unify Video verwenden möchten, muss die **SPE-Unterstützung** deaktiviert werden, um die Leitung zu registrieren, es sei denn, es wurde ein SPE-Zertifikat in das System importiert.

Parameter	Beschreibung
SPE Advisory Ton	Bei aktiviertem Flag gilt: Bei aktiviertem System-Flag SPE Unterstützung und Verwendung eines OpenStage-Telefons 15, 20, 20 E oder 20 G wird ein Teilnehmer, zusätzlich zur Displayanzeige, durch einen Hinweiston auf eine unverschlüsselte Verbindung hingewiesen. Das Einschalten des Teilnehmer-Parameters Payload Security ist Voraussetzung für die Nutzung von SPE durch einen Teilnehmer. Bei Verwendung eines OpenStage-Telefons 40, 40 G, 60, 60 G, 80 oder 80 G ist kein Hinweiston zu hören. Der Zustand der Verbindung (verschlüsselt/unverschlüsselt) wird dauerhaft im Display angezeigt. Standardwert: Deaktiviert **Anmerkung:** Wenn Sie den Cloud-Service Unify Video nutzen möchten, muss der **SPE-Hinweiston** deaktiviert werden, um die Leitung registrieren zu können, es sei denn, es wurde ein SPE-Zertifikat in das System importiert.
SIP Prov. zu SIP Prov. transit	Bei aktiviertem Flag sind Transit-Leitungsverbindungen bei ITSP-Anschaltungen erlaubt. Eine Transit-Leitungsverbindung liegt vor, wenn ein Anruf zwei Leitungen desselben Kommunikationssystems belegt. Beispiel: Ein externer Anruf wird über einen ITSP an einen internen Teilnehmer geleitet. Der interne Teilnehmer übergibt dann den Anruf wieder über einen ITSP an ein externes Ziel. Dadurch entsteht eine Transit-Leitungsverbindung innerhalb des Kommunikationssystems. Für die Dauer des Anrufs werden zwei Leitungen belegt. Die sich ergebenden Transit-Leitungsverbindungen werden zugelassen. Standardwert: Deaktiviert
Wahl von * und # auf Leitungsschnittstellen	Bei aktiviertem Flag ist das Aktivieren und Deaktivieren von Centrex-Leistungsmerkmalen über IP-Leitungen (ITSP) und ISDN-Amtsleitungen möglich. Verschiedene Provider stellen Centrex (Central Office Exchange)-Leistungsmerkmale zur Verfügung, die anhand von Kennzahlen aktiviert und deaktiviert werden können. Die Eingabe einer Kennzahl muss im Wahlzustand erfolgen (zum Beispiel nach Eingabe der Leitungskennzahl). Die Eingabe beginnt immer mit * (Stern) oder # (Raute). Anschließend ist die eigentliche Kennzahl (Ziffern 0 bis 9) einzugeben und durch # (Raute) abzuschließen. Im Gesprächszustand ist das Aktivieren oder Deaktivieren von Centrex-Leistungsmerkmalen nicht möglich. Das Aktivieren und Deaktivieren von Centrex-Leistungsmerkmalen über IP-Leitungen (ITSP) und ISDN-Amtsleitungen ist möglich. Standardwert: Deaktiviert

Parameter	Beschreibung
Richtungskennzahl für MEX hinzufügen	Gilt nur für externe Anrufe, die über das ITSP Leistungsmerkmal "Mobile Extension (MEX)" eingeleitet werden. Bei aktiviertem Flag fügt das System für extern gehende Rufe automatisch die Amtskennziffer zur Rufnummer hinzu, wenn die Rufnummer aus mehr als 7 Ziffern besteht, da das System diese als externe Rufnummer interpretiert. Besteht die Rufnummer aus weniger als 7 Ziffern, wird die Amtskennziffer nicht hinzugefügt, da das System die Rufnummer als interne Rufnummer interpretiert. Ist das Flag deaktiviert, dann muss der Service Provider für alle extern gehenden Rufe die Amtskennziffer der Rufnummer hinzufügen. Standardwert: Deaktiviert
CMI MWI Hinweiston	Bei aktiviertem Flag ist der Hinweiston der Message Waiting Indication (MWI) für DECT-Telefone aktiviert (CMI: Cordless Multicell Integration). Bei neuen Nachrichten auf der Voice-Mailbox wird ein Hinweiston gesendet. Standardwert: Deaktiviert
Automatisches OpenStageTDM Telefon-Software-Update	Wenn dieses Flag aktiviert ist und die Softwareversion eines TDM-Telefons älter ist als die Softwareversion des Systems, wird die Software des Telefons automatisch aktualisiert. Standardwert: Aktiviert
Indirekte Richtungsverbindungen gemäß VBZ-Matrix einschränken	Wenn sich Niederlassungen einer Firma in verschiedenen Städten befinden, dann kann jede Niederlassung eine Leitung zum lokalen (staatlichen) Telekommunikationsanbieter haben. Zusätzlich können diese Niederlassungen über private Querverbindungen untereinander verbunden sein. Aufgrund staatlicher Auflagen (z. B. in Indien) kann es verboten sein, die folgende Verbindung zu schalten: Ein Teilnehmer benutzt die private Querverbindung von seinem Kommunikationssystem zum privaten Kommunikationssystem in der anderen Stadt und dann eine Leitung des staatlichen Telekommunikationsanbieters, um ein lokales externes Ziel zu erreichen. Stattdessen sollte für die Verbindung zwischen den Städten auch eine direkte Leitung des staatlichen Telekommunikationsanbieters benutzt werden. Diese Anforderung wurde wie folgt realisiert: • Verbindungen zwischen privaten Querleitungen können durch Konfigurieren der CON-Matrix eingeschränkt werden. • Für private Querleitungen, die die Funktionen Rufweiterleitung, Transfer und Konferenz beinhalten, wurde das Kennzeichen "Indirekte Trunk-Gruppenverbindungen gemäß VBZ-Matrix beschränken" eingeführt. Das Aktivieren/Deaktivieren dieses Flags hat die folgenden Auswirkungen: – Aktiviert: Anrufe zwischen Städten, die private Querleitungen verwenden, sind eingeschränkt. – Deaktiviert: Anrufe zwischen Städten, die private Querleitungen verwenden, sind erlaubt. Standardwert: Deaktiviert
Offene Nummerierung	

Parameter	Beschreibung
aktiv	Bei offener Nummerierung, wird ein Teilnehmer identifiziert durch die Knotenrufnummer, gefolgt von seiner Rufnummer oder Durchwahlnummer. Dadurch können Teilnehmern in unterschiedlichen Knoten die gleiche Rufnummer vergeben werden. In einem vernetzen System steht dieses Flag immer für alle Anlagen gleich. Standardwert: Deaktiviert
Knoten-Rufnummer	Bei offener Nummerierung ist hier die Knotenrufnummer einzutragen. Ein Teilnehmer kann aus anderen Knoten nur erreicht werden durch Wahl dieser Knotenrufnummer gefolgt von der Teilnehmerrufnummer. Wenn die Summe der Ziffern der Knotenrufnummer und Teilnehmerrufnummer mehr als 7 Zeichen beträgt, wird eine entsprechende Warnung angezeigt. Standardwert: Deaktiviert
Transiterlaubnis	
Leistungmerkmal Transit	Bei aktiviertem Flag sind Transitverbindungen erlaubt, die an bestimmte Leistungsmerkmale geknüpft sind, wie zum Beispiel externe Anrufumleitung, Übergeben und DISA-Anwendungen. Das ist unabhängig davon, ob es sich um Quer- oder Amt-zu-Amt-Verbindungen handelt. Standardwert: Aktiviert
Transit Durchwahl Quer	Bei aktiviertem Flag sind Transitverbindungen in Durchwahl bei Querverbindungen (vernetzte Kommunikationssysteme) erlaubt. Standardwert: Aktiviert
Transit Durchwahl Amt	Bei aktiviertem Flag sind Transitverbindungen in Durchwahl bei Amt-zu-Amt-Verbindungen erlaubt. Standardwert: Deaktiviert
Schalter Spezial	
CALL PROC nicht senden	Dieses Flag muss aktiviert werden, wenn der Service Provider keine Call Proceeding Messages (ISDN Message) vom Kommunikationssystem bekommen soll. Standardwert: Deaktiviert
Autom. zykl. Leistungsbelegung	Bei aktiviertem Flag belegen ausgehende Rufe bei fehlerhaftem Verbindungsaufbau (z.B. keine ACK-Quittung) zyklisch neue ISDN-Amtsleitungen. Leitungsnummern oder Richtungsnummern werden hochgezählt. Standardwert: Aktiviert
Einschränkung für UC-Anrufe	
Einschränkung für UC-Anrufe	Bei aktiviertem Flag werden alle vom System eingeleiteten UC-Anrufe (z.B. über den CallMe-Dienst) vor der Wahl geprüft, ob der anfordernde UC Benutzer die Berechtigung für diesen Anruf hat. Fehlt dem UC-Benutzer die Berechtigung, wird der Anruf nicht ausgeführt. Standardwert: Deaktiviert

28.3.1.2 Grundeinstellungen > System > Zeitarameter

In der Tabelle werden alle einstellbaren Zeitparameter aufgelistet (Spalte **Beschreibung**). Über die Spalten **Basis** und **Faktor** kann der Timer-Wert für den jeweiligen Zeitparameter eingestellt werden. Dabei ist die Zeit = Basis x Faktor. Wird in der Spalte **Faktor** der Wert 255 eingetragen, dann wird dieser Timer unwirksam.

Parameterbeschreibung der Registerkarten:

- **Zeitparameter ändern**

Parameter	Beschreibung
NoFe Nachwahlzeit Code Empfänger Anschaltzeit	Steuert die Dauer der Anschaltung der Codeempfänger bei MFV-Endgeräten und damit die Wahlaufnahmebereitschaft. Nach Ablauf dieses Zeitgliedes wird der Code-Empfänger freigegeben. Wertebereich: 5 - 15 s
Zeit für das Aktivieren von Leistungsmerkmalen NoFe	Wird aktiviert, wenn an einem Endgerät die Signaltaste betätigt wird. Sie dient zur Unterscheidung, ob ein Teilnehmer eine Rückfrage zurücknehmen will oder ein Leistungsmerkmal wie z.B. Konferenz aktivieren will. Wertebereich: 2 - 4 s
Wiederbelegungssperrzeit	Wird bei Leitungssätzen gestartet und verhindert eine sofortige gehende Belegung nach dem Auslösen während dieser Zeit. Wertebereich: 0 - 5 s
Rückrufverzögerungszeit	Wird gestartet, wenn ein Endgerät nach Ruhe wechselt. Nach Ablauf dieser Zeit wird geprüft, ob ein automatischer Rückruf auszuführen ist. Damit hat der Teilnehmer die Gelegenheit weitere gehende Gespräche zu führen. Wertebereich: 0 - 60 s
Dauer des Rückrufes	Wird ein automatischer Rückruf nicht innerhalb dieser Zeit beantwortet, so wird der Ruf beendet, und der Rückruf vertagt. Wertebereich: 15 - 60 s
Abwurfzeit für Wiederanruf	Wird ein Wiederanruf eines vor dem Melden übergebenen Gespräches nicht innerhalb dieser Zeit beantwortet, so erfolgt der Abwurf zum Vermittlungsplatz, falls dieses Abwurfkriterium ausgewählt wurde. Wertebereich: 20 - 600 s
Rufzeit während Übergeben vor Melden	Wird ein vor dem Melden (auf besetzten Teilnehmer) übergebenes Gespräch nicht innerhalb dieser Zeit beantwortet, so erfolgt der Wiederanruf bei der Nebenstelle, die das Gespräch übergeben hat. Wertebereich: 30 - 600 s
Wahlende bei unvollständiger Wahl (Österreich)	Überwachungstimer für Durchwahl. Erfolgt innerhalb dieser Zeit keine Wahl, so wird die Durchwahl als unvollständig bzw. als keine Wahl erkannt. (Gilt nur für Österreich). Wertebereich: 10 - 30 s

Parameter	Beschreibung
Wahlendezeit (keine Wahl)	Wird die Wahl nicht innerhalb einer bestimmten Zeit begonnen, so wird automatisch ein Wahlende erzeugt. Wertebereich: 5 - 15 s
Zeit zwischen 1. und 2. Ansage bei FDW	Fax/DuWa, analoge Durchwahl, Zeit nach Sprachansage. Standardwert: 15 s
Zeit für Parken + Übergang halten	Die Reaktivierung des geparkten Gesprächs muss innerhalb eines Timeouts erfolgen. Wird das geparkte Gespräch nicht innerhalb dieser bestimmten Zeit abgefragt (wiederaufgenommen), erfolgt ein automatischer Wiederanruf zu der Station, die das Gespräch geparkt hat. Mit dem Wiederanruf verlässt das Gespräch den Haltezustand und geht in einen Ruf über. Wertebereich: 60 - 255 s
Wahlende bei unvollständiger Wahl	Wird die Wahl nicht innerhalb einer bestimmten Zeit fortgesetzt, so wird automatisch ein Wahlende erzeugt. Wertebereich: 10 - 20 s
AB Tln Flashzeit Minimum	Zur Erkennung eines Flash-Zeichens wird eine Mindestzeit festgelegt, in der die Schleife unterbrochen sein muss. Standardwert: 0 s
NoFe Flashzeit Maximum	Zur Erkennung eines Flash-Zeichens wird eine Maximalzeit festgelegt, in der die Schleife unterbrochen sein darf. Standardwert: 0 s
Zeit für das Auslösen eines Wiederanrufes am VPL	Wird ein Wiederanruf am Vermittlungsplatz nicht innerhalb dieser Zeit angenommen, erfolgt Auslösen der Verbindung. Wertebereich: 30 - 180 s
HKZ NSA-Vorhaltezeit	Vorhaltezeit für Nummernschalter-Arbeitskontakt, dient zur Vermeidung von Wählgeräuschen im Hörer bei IWV-Apparaten (vor dem Impuls). Standardwert: 0 s
HKZ NSA-Nachhaltezeit	Nachhaltezeit für Nummernschalter-Arbeitskontakt, dient zur Vermeidung von Wählgeräuschen im Hörer bei IWV-Apparaten (nach dem Impuls). Standardwert: 0 s
Störausblendezeit für Ruf	Zeit zum Ausblenden von Leitungsstörungen bei IWV-Wahl. Standardwert: 0 s
Wahlende bei 1A Wahl	Gibt die Zeit an, nach der die letzte Ziffer beim 1A-Verfahren ausgewählt wird. Die Ausgabe einer Ziffer erfolgt nach Eingabe der nächsten Ziffer. Die letzte Ziffer wird nach Ablauf des Timers ausgegeben oder vom Teilnehmer mit dem Wahlendekennzeichen # gekennzeichnet. Wertebereich: 4 - 4,5 s

Parameter	Beschreibung
Gebührennachlaufzeit	Wird eine Leitung ausgelöst, so können während dieser Zeit eintreffende Gebühreninformationen (Gebührenimpulse) auf analogen Leitungen vom Kommunikationssystem ausgewertet werden. Die Leitung ist während dieser Zeit für gehende Verbindungen gesperrt. Standardwert: 0 s
Zwischenwahlzeit bei IWV	Erlaubte Pause zwischen einzelnen Ziffern bei IWV. Standardwert: 10 s
Wähltonüberwachungszeit	Dieser Timer gibt die Zeitspanne an, wie lange bei belegen eines Trunks mit Wählton auf diesen Ton maximal gewartet werden soll. Läuft dieser Timer ab, so liegt eine Störung dieser Amtsleitung vor. Läuft dieser Timer ab, so liegt eine Störung dieser Amtsleitung vor und der Satz geht in Störung. Standardwert: 10 s
Pausenzeit für IWV	Die IWV-Wahl erfolgt mittels Impuls-Pausen-Folgen, Erkennung von Pausen auf IWV-Leitungen. Standardwert: 0 s
Impulszeit für IWV	Die IWV-Wahl erfolgt mittels Impuls-Pausen-Folgen. Erkennung von Impulsen auf IWV-Leitungen. Standardwert: 0 s
Flashzeit für PABX	Unterbrechungszeit für Teilnehmerschleife zum Auslösen von Steuerfunktionen (z.B. Rückfrage) in der Anlage. Standardwert: 0 s
Flashzeit für Amtsbetrieb	Unterbrechungszeit für Teilnehmerschleife zum Auslösen von Steuerfunktionen (z.B. Rückfrage) auf der HKZ-Leitung. Standardwert: 0 s
Minimale Impulszeit bei IWV-NoFe	Die IWV-Wahl erfolgt mittels Impuls-Pausen-Folgen. Erkennung von Impulsen vom IWV-Telefon. Standardwert: 0 s
Maximale Impulszeit bei IWV-NoFe	Die IWV-Wahl erfolgt mittels Impuls-Pausen-Folgen. Erkennung von Impulsen vom IWV-Telefon. Standardwert: 80 ms
Sendezeit für MFV-Zeichen	Länderabhängige Dauer von MFV-Wahlzeichen. Standardwert: 80 ms
Pausenzeit zwischen MFV-Zeichen	Länderabhängige Pause zwischen MFV-Wahlzeichen. Standardwert: 80 ms
MOH Verzögerungstimer	Wird eine Verbindung gehalten, so wird MOH geschaltet, sofern dies konfiguriert wurde. Das Einschalten der MOH erfolgt jedoch erst nach Ablauf dieser Zeit, damit insbesondere beim Einleiten von Leistungsmerkmalen wie z.B. Konferenz keine MOH eingeschaltet wird. Wertebereich: 1 - 5 s

Parameter	Beschreibung
Pausenzeit vor Wahl (nur für Entwicklung)	Ist bei analogen Amtsleitungen keine Hörzeichenüberwachung möglich oder erwünscht, kann die Wahl automatisch nach dieser Zeit gestartet werden. Standardwert: 3 s
Gebührenpause in Min	Zeit zwischen Gebührenimpulsen. Standardwert: 0 min.
Gebührenimpuls in Min	Dauer von Gebührenimpulsen. Standardwert: 0 min.
NSA Meldepulszeit	Nummernschalter-Arbeitskontakt (IWV-Leitungen). Standardwert: 0 s
NSA Belegungspulszeit	Nummernschalter-Arbeitskontakt (IWV-Leitungen). Standardwert: 0 s
Auslösen falls keine Wahl erfolgt	Erfolgt eine Leitungsbelegung und innerhalb einer bestimmten Zeit keine Wahl, so wird die Verbindung ausgelöst. Der anfordernde Teilnehmer bekommt Besetztton signalisiert. Wertebereich: 5 - 30 s
IWV NoFe Minimale Zwischenwahlzeit	Zeit zwischen Wahlziffern bei IWV-Telefonen. Standardwert: 0 ms
MFV NoFe Flash Entprellzeit	Verhindert Mehrfach-Erkennung von Flash-Tastendruck. Standardwert: 0 ms
MFV-Beruhigungszeit Zeit	Wartezeit zur Vermeidung von Störungen von DTMF-Zeichen auf abgehenden Leitungen. Standardwert 100 ms
Flash-Beruhigungszeit (siehe Hilfe)	Wartezeit nach Flash auf analogen Leitungen. Standardwert: 1 s
Zykluslänge für Wiederinbetriebnahme	Zeit für Restart von analogen Leitungen, nachdem kein Wählton erkannt wurde. Standardwert: 120 s
Wahlpausenlänge	Gibt die Pausenzeit an, welche zwischen zwei Ziffern eingehalten werden soll, wenn ein Pausenkennzeichen erkannt wird. Wertebereich: 1 - 5 s
Störausblendezeit für Ruf bei PABX-Betrieb	Zeit zum Ausblenden von Leitungsstörungen. Standardwert: 0 s
Künstliches Wahlende	Bei Externwahl werden nach dem künstlichen Wahlende empfangene Ziffern als Rückfrage interpretiert. Wertebereich: 5 - 15 s

Parameter	Beschreibung
Zeit für automatische Wahlwiederholung	Nach Ablauf des Timers wird im Falle eines besetzten Teilnehmers eine automatische Wahlwiederholung durchgeführt. Voraussetzung dafür ist die Auswahl der Option Automatische Wahlwiederholung unter Flags. Wertebereich: 10 - 650 s
Störausblendung für den ersten Polaritätswechsel (FRK/SPA)	Zeit zum Ausblenden von Leitungsstörungen. Standardwert: 0 ms
Verzögerungszeit bis zur Ansage vor Melden	Stellt die Verzögerungszeit ein, nach der sich das Ansagegerät meldet. Wertebereich: 1,5 - 30 s
Zeit zwischen HT-Auswertung und der Wahl Trunk-HKZ	Legt die Zeit zwischen der Hörzeichenerkennung und der Wahl der ersten Ziffer über HKZ ins Amt fest. Wertebereich: 0 - 2 s
Die Pausenl. nach der Wahl des 2.AKZ	Legt die Pause fest, welche nach der Wahl des 2. Amtskennzeichens oder der Internationalen Kennzahl eingelegt wird. Übergang zum nächsten Vermittlungsknoten. Wertebereich: 1 - 5 s
Zeit bis zum Aufmerksamkeitston bei HKZ-Transit-Verbindungen	Transit-Verbindungen werden in Abhängigkeit der verwendeten Satztypen zeitlich überwacht. Dies erfolgt mit dem Ziel, dass eine Verbindung nicht unendlich lange bestehen bleibt. Wenn mindestens ein Satztyp dieser Transit-Verbindung über eine Auslöse-Erkennung verfügt, erfolgt in der Regel keine zeitliche Überwachung (Ausnahme siehe unten stehende Tabelle). Bei dem Satztyp HKZ gibt es keine Auslöseerkennung. Es gibt jedoch eine HW-Option für Silent Reversal. Damit wird eine Auslöseerkennung bei HKZ möglich. Die Tabelle für Transitüberwachung (für die US-spezifischen Satztypen gilt) zeigt für welche Satztypen eine Timer-Überwachung erfolgt. Die Dauer der Überwachung ist konfigurierbar. Bei der Verwendung von HKZ mit Silent Reversal ist jedoch zu beachten, dass es Rufnummern gibt, bei denen u. U. kein Melden erkannt wird, und damit auch kein Auslösen erkannt werden kann. Bei diesen Rufnummern handelt es sich in der Regel um Ansagedienste. Hier muss der Betreiber des Kommunikationssystems explizit drauf hingewiesen werden. Wertebereich: 120 s - 42 min
Zeit vom Aufmerksamkeitston bis zum Auslösen...	Erfolgt eine zeitliche Überwachung von Transit-Verbindungen, so erfolgt nach Ablauf des Überwachungstimers ein Aufmerksamkeitston. Damit das Gespräch beendet werden kann, wird die Verbindung nicht sofort getrennt, sondern erst nach Ablauf dieser Zeit. Wertebereich: 10 - 650
Auslösetimer für HKZ	Ein Ruf einer HKZ-Leitung über Durchwahl (DuWa) wird nach dieser Zeit ausgelöst, wenn kein Gespräch zustande kommt. Wertebereich: 30 s - 254 min
Nach Halten wird ein Aufmerksamkeitston geschaltet (Italien)	Nach Ablauf dieser Zeit erfolgt bei gehaltenen Verbindungen ein Anklopfen bei der haltenden Nebenstelle (ITL). Wertebereich: 30 - 180 s

Parameter	Beschreibung
LCR: Künstliches Wahlende	Wartezeit nach der letzten Ziffer bis Wahlende angenommen wird (Blockwahl LCR). Standardwert: 5 s
Überwachung eines UCD-Rufes auf einer analogen Leitung	Zeit für das Auslösen eines HKZ-Anrufes auf eine UCD-Gruppe, wenn es zu keinem Verbindungsaufbau gekommen ist. Wertebereich: 10 - 3810 s
Überwachung eines Übergeben vor Melden an eine UCD-Gruppe (nur für Entwicklung)	Erfolgt ein Übergeben vor Melden eines Gespräches auf eine UCD-Gruppe, so wird der Timer gestartet. Wird der übergebene Ruf nicht beantwortet, so erfolgt nach Timerablauf ein Wiederanruf. Wertebereich: 10 - 3810 s
Verzögerungs-Timer für PC-VPL	Zeit bis Update Message zum PC-Vermittlungsplatz (Business Attendant) gesendet wird. Wertebereich: 300 ms
USBS Timer Intervall	Für den Zugang über S0-Port, TA-S0, TA-RS232 und TA-API wird der User Signalling Bearer Service (USBS) auf Basis der ETS 300 716 verwendet. Wertebereich: 1 - 60 s
Timer für Toll Fraud Monitoring	Wird eine Verbindung in Transit geschaltet, so erfolgt nach Ablauf dieser Zeit eine Signalisierung am Display des Vermittlungsplatzes. Dieser kann dann ggf. einzelne Leitungen freischalten. Dies ist eine Möglichkeit um Transit-Verbindungen zeitlich zu überwachen. Wertebereich: 0 - 650 s
Sonderbesetztton, wenn ZielTln. Ruf nicht annimmt	Nach Ablauf dieses Timers erhält der rufende Tln. den Sonderbesetztton, wenn der gerufene interne Tln. nicht abnimmt. Wertebereich: 30 - 120 s
Sonderbesetztton wenn Ltg. ohne Wahl belegt wird	Belegt ein Teilnehmer gehend eine Leitung und wählt anschließend nicht weiter, dann erhält er nach Ablauf des Zeitgliedes den Sonderbesetztton. Wertebereich: 20 - 60 s
Rufzeit übergeben vor Melden auf besetzten Tln.	Nach Ablauf dieses Timers wird ein Teilnehmer A, der von Tln. B zu einem besetzten Tln. C übergeben wurde, zurück auf Tln. B geleitet. Wertebereich: 15 - 180 s
Fehlersignalisierungs-Intervall	Mit der Fehlersignalisierungszeit wird ein Intervall mit dem Wertebereich von 1 Min. bis 15 Min. definiert. Kommastellen werden auf volle Minuten abgerundet, Werte kleiner als 1 Min. oder größer als 15 Min. werden als 15 Min. bewertet. Zyklisch werden nach Ablauf des Intervalls die aktuell im Event Log eingetragenen Class-B-Fehler an das Remote Center übermittelt. Wertebereich: 60 - 900 s

28.3.1.3 Grundeinstellungen > System > Display

Parameterbeschreibung der Registerkarten:

- **Display ändern**

Parameter	Beschreibung
Name/Rufnummer anzeigen	Es kann konfiguriert werden, welche der folgenden Daten bei Anrufen auf den Displays aller angeschlossenen Telefone angezeigt werden sollen: Nur Rufnummer, oder Name (falls vorhanden), oder Name und Rufnummer gleichzeitig. Falls ein Telefon eine dieser Einstellungen nicht unterstützt, wird z. B. anstatt der gleichzeitigen Anzeige des Namens und der Rufnummer nur die Rufnummer angezeigt. OpenStage-Telefone sind für die gleichzeitige Anzeige des Namens und der Rufnummer geeignet. Standardwert: Name und Rufnummer
Name / Algorithmus	Der vollständige Namen wird über drei separate Felder unterstützt: Vorname, Nachname und Anzeigename. Das Feld "Anzeigename" kann bis zu 16 Zeichen, die Felder "Name" und "Nachname" können bis zu 32 Zeichen enthalten. Für den Anzeigenamen kann einer der folgenden Algorithmen verwendet werden: • <nachname>, < vorname> • <nachname>, <initiale des vornamens.\> • <vorname>, <nachname> • <initiale des vornamens>, <nachname> • <nachname> Standardwert: <nachname>, < vorname> **Wichtig:** Die Option **<vorname>, <nachname>** wird für MULAP-Benutzer in UC Suite nicht erkannt. Wenn diese Option verwendet wird, erscheinen der Vorname und Nachname des UC Suite Benutzers zusammen im Feld Vorname im UC-Benutzerverzeichnis und das Feld Nachname bleibt leer. Verwenden Sie in diesem Fall den Standardwert der Option, wobei ein Komma als Trennzeichen verwendet wird.
Übergeben vor Melden	Bei Übergeben vor Melden kann entweder die Rufnummer des Übergebenen oder die Rufnummer des Übergebenden beim angerufenen Teilnehmer angezeigt werden. Ein mit „Übergeben vor Melden“ übergebenes Gespräch kann vom angerufenen Teilnehmer nicht abgewiesen werden. Bei Wahl von „Übergebener“ wird am Display vor Zustandekommen der Verbindung und nach Auslösen der übergebende Teilnehmer angezeigt. Bei Wahl von Übergebender wird am Display der übergebende Teilnehmer angezeigt, solange dieser mit dem Empfangsteilnehmer verbunden ist. Nachdem der Übergebende aufgelegt hat und eine Verbindung zum Übergebenen besteht, springt das Display vom übergebenden zum übergebenen Teilnehmer um. Standardwert: Übergeben an

Parameter	Beschreibung
Wiederanruf	Erfolgt nach Übergabe eines Anrufs ein Wiederanruf, kann beim Empfangsteilnehmer entweder die Nummer des Übergebenden oder die Nummer des Teilnehmers angezeigt werden, von dem der Wiederanruf ausgeht. Die Übergabe eines Gesprächs wird bei einem internen Teilnehmer B angezeigt. C empfängt einen Rufton, bis entweder B antwortet oder A zurückruft. Unter diesem Punkt kann konfiguriert werden, ob im Display des Übergabeziels B der Teilnehmer A (Anrufer) oder C (Übergeben-Ziel) angezeigt wird. Geht von Teilnehmer A ein Wiederanruf aus, so bekommen beide Teilnehmer „meldet sich nicht“ im Display angezeigt. Standardwert: Übergeben-Ziel
Datum/Uhrzeit-Format	Das Datum kann in unterschiedlichen Formaten angezeigt werden. Standardwert: Europa - 24 Stunden-Format
Anruferliste, Modus	Bei Aktivierung von Interne und externe Rufe oder Nur externe Rufe werden alle nicht entgegengenommene Anrufe in einer Liste gespeichert, deren Inhalt dann später über eine Systemprozedur abgerufen werden kann. Bei Aktivierung von Externe Rufe und Gespräche werden auch angenommene Gespräche in der Anruferliste gespeichert. Es erfolgt kein Austragen einer Rufnummer aus der Anruferliste, weder bei kommenden noch bei gehenden Gesprächen. Wenn alle Speicherplätze der Anruferliste bereits vergeben sind, wird beim Speichern einer weiteren Rufnummer der älteste Eintrag überschrieben. Nicht angenommene Gespräche werden angezeigt, wie es bisher im Leistungsmerkmal Anruferliste beschrieben ist. Angenommene Gespräche werden so angezeigt, wie es über die Funktionalität der Anruferliste Rufnummer speichern üblich ist. Wird ein von extern kommender Anruf über den AutoAttendant an einen internen Teilnehmer vermittelt und der Teilnehmer ist gerade besetzt oder hat die Anrufumleitung aktiviert, erfolgt kein Eintrag in der Anruferliste. Standardwert: Nur externe Anrufe
Rufnummern-Unterdrückung	Bei aktiviertem Flag wird die Anzeige der Rufnummer im ISDN verhindert, d.h. der Gesprächspartner erhält keine Rufnummernanzeige (das Leistungsmerkmal muss auch bei der Telekom aktiviert sein). Es gibt Anrufszenarien, bei denen ein Anrufer über das Amt auf Präsentation eingeschränkt gesetzt wurde. Wenn dieses Flag aktiviert ist, wird die Rufnummer des Anrufers beim Angerufenen angezeigt. Wenn dieses Flag deaktiviert ist, wird der Text Rufnummer unbekannt angezeigt. Das Flag hängt immer von den Amtseinstellungen jedes Providers ab. Standardwert: Deaktiviert

Parameter	Beschreibung
Internes Telefonbuch	Teilnehmer können auf ein Online-Telefonbuch zugreifen, das die Namen und Teilnehmerrufnummer aller internen Nebenstellen enthält. An den systemspezifischen Display-Endgeräten gibt es die Möglichkeit, sich alle vorhandenen internen Teilnehmer mit Namen und Rufnummer anzusehen, gezielt zu suchen und anschließend den gewünschten Teilnehmer anzurufen. Bei Endgeräten mit alphanumerischer Tastatur kann diese zur gezielten Suche benutzt werden. Wählen Sie aus der Liste die entsprechende Option aus: kein: kein Zugriff auf das Telefonbuch möglich, intern: Zugriff auf das interne Telefonbuch (Teilnehmer, Gruppen und KWZ (Kurzwahlziele)) möglich, LDAP: Zugriff auf die Telefonbuchinformationen des LDAP-Servers. Der LDAP-Zugriff muss über LDAP eingerichtet sein; alle: Teilnehmer kann zwischen dem Zugriff auf das interne Telefonbuch oder LDAP-Telefonbuch wählen. Standardwert: Intern
Internes Telefonbuch über Unified-Verzeichnis	Ist dieses Flag aktiviert, kann der Benutzer in allen Verzeichnissen nach Kontakten suchen. Die Suchanfragen werden als Anforderungen an das Unified-Verzeichnis verarbeitet. Wenn das Flag nicht aktiviert ist, werden die Suchanfragen lokal vom System verarbeitet. Standardwert: Aktiviert
Schalter	
Gesprächsdauer anzeigen	Bei gehenden externen Gesprächen werden keine Gebühreninformationen angezeigt. Bei UP0/E-Endgeräten mit Display wird dann die aktuelle Gesprächsdauer angezeigt. Der Startpunkt der Zeiterfassung wird bei analogen Leitungen über einen Timer gesetzt (5 s nach Wahlende), bei digitalen Amtsleitungen mit CONNECT. Bei S0-Endgeräten wird vom Kommunikationssystem keine Anzeige der Gesprächsdauer unterstützt. Standardwert: Deaktiviert
DTMF verdeckte Anzeige	PIN-Code-Eingaben werden an Systemtelefonen mit Display verdeckt angezeigt. Standardwert: Aktiviert
Displayanzeige bei Info-Meldung	Vorliegende Info-Meldungen werden am Display der Systemtelefone angezeigt. Standardwert: Aktiviert
Rufnummer transparent weiterreichen	Im Falle einer Anrufumleitung oder Rufweiterschaltung zu einem externen Teilnehmer werden dem gerufenen Teilnehmer die Rufnummer des rufenden Teilnehmers angezeigt. In einem vernetzten System ist die Option in dem Knoten zu setzen, an dem ein Amtsanschluss angeschaltet ist. Voraussetzung für das Funktionieren des LM ist die freigeschaltete Clip-No-Screening-Funktion im Amt, die kostenpflichtig ist. Dieses Flag arbeitet wechselwirksam mit dem Flag TIn-RufNr unterdrücken unter Richtungen zusammen. Standardwert: Deaktiviert

Parameter	Beschreibung
SST mit Übergabeoption (für Rufnr. des Anrufers)	Wenn das Flag aktiviert ist und der Benutzer (während eines aktiven Anrufs) die Menüoption "Übertragung starten?" wählt, wird die Übertragung als Einzelschritt-Übergabe ausgeführt (kein Rückfragegespräch). Entscheidet sich der Benutzer, zuerst eine Rückfrage durchzuführen (z. B. Option „Enquiry?“) und danach den neuen Anruf an den gehaltenen Teilnehmer weiterzuleiten, erfolgt die Übertragung als normale Übergabe ohne Rückfrage. Bei einer Einzelschritt-Übergabe wird die rufende Nummer beim Klingeln des Mobilgeräts am externen Ziel angezeigt, d. h., der angerufene Teilnehmer sieht die rufende Nummer und nicht die Nummer des übergebenden Teilnehmers, wenn der Anruf von einem Systemgerät übergeben wird. Das Flag "Rufnummer transparent weiterreichen" muss ebenfalls aktiviert sein. Standardwert: Deaktiviert **Anmerkung:** Wenn der übergebene Teilnehmer ein externes Gerät ist, muss die Funktion "CLIP no screening" (Teilnehmerrufnummer unterdrücken) vom Netzanbieter unterstützt werden und aktiviert sein. Andernfalls wird aus dem Amt die Standard-Durchwahl des Systems verwendet, oder der Anruf wird vom Amt abgelehnt.

28.3.1.4 Grundeinstellungen > System > DISA

Parameterbeschreibung der Registerkarten:

- **DISA ändern**

Parameter	Beschreibung
DISA	
Durchwahl	Rufnummer, unter der die DISA-Funktion von extern erreicht werden kann. Die Rufnummer kann für externe und interne Nutzung unterschiedlich sein.
Sicherheits Modus	Um die DISA-Funktionen nutzen zu können, muss der Teilnehmer ein Kennwort eingeben. Über die Optionen im Sicherheitsmodus kann festgelegt werden, ob der Teilnehmer nach Eingabe des Kennworts zunächst warten muss oder ob er # (Raute) eingeben muss. Standardwert: Nach Timeout
DISA intern	
Rufnummer	DISA Intern bezieht sich auf die Nutzung an einem anderen, mittels IP-vernetzten Knoten.
Mobility Callback	
Durchwahl	Die Authentifizierung mittels Passwort entfällt, wenn ein als Mobility-Rufnummer erkannter Anruf von extern auf die Mobility Callback-Durchwahlnummer erfolgt. In diesem Fall wird direkt der interne Wählton angeschaltet. Hierfür muss das Endgerät des externen Teilnehmers seine Rufnummer übermitteln. Diese Rufnummer wird dann gegen die Mobility-Liste geprüft.

28.3.1.5 Grundeinstellungen > System > Abwurf/Attendant/Hotline

Parameterbeschreibung der Registerkarten:

- **Intercept/Vermittlung/Hotline bearbeiten**

Parameter	Beschreibung
Abwurfplatz	
Tag/Nacht	Rufnummer des Abwurfplatzes. Der Abwurfplatz kann für die Tag und Nacht getrennt festgelegt werden. Darüber hinaus besteht die Möglichkeit, bei der Aktivierung der Nachtschaltung auch ein beliebiges Ziel anzugeben (variable Nachtschaltung).
Zentraler Abwurfplatz	
Richtung	Richtungsindex für den zentralen Abwurfplatz bei vernetzten Kommunikationssystemen
Rufnummer	Rufnummer des zentralen Abwurfplatzes bei vernetzten Kommunikationssystemen
Abwurf zum Abwurfplatz	
Im Freifall	Der Ruf folgt der festgelegten Prozedur für Kommende Rufe. Ist das Ende der Tabelle erreicht, so wird geprüft, ob Abwurf nach Zeit erfolgen soll oder nicht. Gegebenenfalls wird nach der unter Rufweiterschaltung festgelegten Anzahl von Ruftönen der Abwurfplatz gerufen. Aus einem Sammelanschluss erfolgt kein Abwurf. Der Ruf wird wieder zum ersten Sammelanschluss-Teilnehmer weitergeschaltet und verbleibt im Sammelanschluss. Standardwert: Aktiviert
bei Besetzt	Im Besetztfall wird zunächst geprüft, ob angeklopft werden kann oder nicht. Wenn nicht angeklopft werden darf (Anklopfschutz oder Abwurfkriterium), so folgt der Ruf dem Call Management/Anrufrouting. Kann der Ruf bei keinem Teilnehmer signalisiert werden, so wird geprüft, ob Abwurf erfolgt oder ausgelöst wird (B-Signalisierung ins Amt). Ist ein analoger Fernsprecher mit Anklopfschutz besetzt, so wird bei allen Satztypen ausgelöst. Bei MFV-Durchwahl und bei HKZ erfolgt immer Abwurf. Standardwert: Deaktiviert
Bei Falschwahl	Wenn eine falsche Rufnummer gewählt wird, wird geprüft, ob Abwurf erfolgen soll. Bei MFV-Durchwahl erfolgt immer Abwurf. Standardwert: Aktiviert
Bei unvollständiger Wahl	Wenn die gewählte Teilnehmerrufnummer nicht vollständig ist, wird nach Ablauf der voreingestellten Zeit der Abwurfplatz gerufen. Die Zeit kann im Feld Wahlende bei unvollständiger Wahl unter Zeitparameter eingestellt werden. Standardwert: Aktiviert

Parameter	Beschreibung
Bei nicht beantwortetem Wiederanruf	Wird ein externer Anruf nach Übergeben vor Melden von Teilnehmer A auf Teilnehmer B von Teilnehmer B nicht abgefragt und erfolgt nach Wiederanruf auf Teilnehmer A ebenfalls kein Melden, so wird nach Ablauf der voreingestellten Zeit der Abwurfplatz gerufen. Die Zeit kann im Feld Wahlende bei unvollständiger Wahl unter Zeitparameter eingestellt werden. Wenn das Flag nicht aktiviert ist, wird nach Ablauf der eingestellten Zeit das Gespräch ausgelöst. Standardwert: Deaktiviert
Bei Ablehnung	Falls ein interner Teilnehmer den Anruf mit "Ruf abweisen" ablehnt, so folgt der Ruf dem Call Management/Anrufrouting. Kann der Ruf bei keinem Teilnehmer signalisiert werden, so wird geprüft, ob Abwurf erfolgt oder ausgelöst wird (B-Signalisierung ins Amt). Standardwert: Aktiviert
Abwurf bei Codeschloss	
Rufnummer	Wenn bei einem Teilnehmer das Codeschloss aktiviert ist und es wird von diesem Teilnehmer eine Bündelkennzahl gewählt, wird der Anruf unverzüglich zum eingetragenen Abwurfziel umgeleitet. Somit wird ein Anruf bei Wahl einer Nummer, für die der Teilnehmer keine Berechtigung hat, bei der angegebenen Teilnehmerrufnummer signalisiert. Die Funktion Abwurf bei Codeschloss lässt sich individuell für jeden Teilnehmer über die Teilnehmerflags einstellen.
Berechtigung vermittelter Leitungen	
Berechtigung vermittelter Leitungen	In dieses Feld muss ein vollamtsberechtigter Teilnehmer eingestellt werden, sonst wird der Anrufumleitung zu externen Zielen nicht durchgeführt.
Platzkennzahl	
Interne Rufnummer	Über diese Rufnummer kann der Abwurfplatz von internen Geräten aus erreicht werden. Wertebereich: Freie Eingabe einer beliebigen Ziffer, sofern sie nicht bereits im Wahlplan verwendet wird.
Rufnummer extern	Über diese Rufnummer wird der Abwurfplatz in Durchwahl oder aus dem Anlagennetz (CorNet-N bzw. CorNet-NQ) erreicht.
Hotline	
Röchel-Zeit	Wenn ein Teilnehmer den Telefonhörer abnimmt, dann wird nach Ablauf der Röchel-Zeit die Hotline automatisch gerufen, allerdings nur, wenn innerhalb dieser Zeit vom Teilnehmer keine Ziffer eingegeben wird. Die Röchel-Zeit wird in Sekunden angegeben.
Ziel-Ruf-Nr. 1 bis 6	Systemweit können 6 Hotline-Ziele eingetragen werden, die Auswahl erfolgt je Teilnehmer (siehe Teilnehmer/Teilnehmer-Parameter ändern)
Vermittlungsplatz	

Parameter	Beschreibung
Anrufe in der Warteschlange	Hier kann die Anzahl der maximal wartenden Anrufe ausgewählt werden. Erreicht die Anzahl der Teilnehmer in der Warteschlange des Vermittlungsplatzes diesen numerischen Wert, so erfolgt eine Rufweiterschaltung zu einem konfigurierbaren Überlaufziel. Wertebereich: 1-15
Wartezeit	Hier kann eine Wartezeit in Sekunden eingegeben werden. Nach Überschreitung dieser Zeit erfolgt eine Rufweiterschaltung zu einem über das Call Management festgelegten Überlaufziel.
Schnellvermitteln	Ist dieses Flag gesetzt, kann die Vermittlung einen Anruf durch Eingabe der entsprechenden Teilnehmerrufnummer an einen anderen Teilnehmer übergeben. Schnellvermitteln kann nur aktiviert werden, wenn das systemweite Flag **DTMF automatisch** ausgeschaltet ist. Standardwert: Deaktiviert
Unbewählt vermitteln	Ein berechtigter Teilnehmer (Vermittlungsplatz VPL) hat die Möglichkeit, einem internen Teilnehmer mit nicht ausreichender Amtsberechtigung eine unbewählte Amtsleitung zuzuteilen, um diesem Teilnehmer das Führen genau eines externen Gespräches zu ermöglichen. Nach der Übergabe der vermittelten Leitung an den nicht ausreichend berechtigten Teilnehmer erfolgt eine Wahlkontrolle anhand einer zusätzlichen Amtsberechtigung für vermittelte Leitungen. Nur wenn diese zusätzliche Amtsberechtigung ausreicht, d.h. wenn der Teilnehmer z.B. eine gültige Nummer gemäß Verbots- oder Erlaubnisliste für vermittelte Leitungen wählt, wird die gehende externe Verbindung zugelassen. Der Teilnehmer wählt auf einer vermittelten Leitung selbst die Belegungskennzahl. Es ist im Kommunikationssystem über einen Referenzteilnehmer eine Amtsberechtigung für vermittelte Leitungen pro Richtung konfigurierbar. Der Standard-Referenzteilnehmer ist der erste logische Teilnehmerport bzw. der Vermittlungsplatz. Die Standardberechtigung steht auf volle Amtsberechtigung für alle Richtungen. Standardwert: Deaktiviert
Sonstige Kriterien	
Anklopfen im Besetzfall	Ist dieses Flag aktiviert, ist bei sämtlichen Teilnehmern im Kommunikationssystem das Leistungsmerkmal "Anklopfen" aktiv ist. Standardwert: Aktiviert
Sofortiges Einschalten für Vermittlungsanrufe	Nur relevant in CorNet-vernetzten Systemen. Wenn das Flag gesetzt ist, kann nur ein rufender VPL (System A) beim Teilnehmer B (System B) anklopfen. Alle anderen Teilnehmer des System A können im System B nicht anklopfen. Für die Teilnehmer innerhalb des Systems B gilt die Bedingung des Anklopfschutzes (siehe Teilnehmersicht: Flags) für den jeweiligen Teilnehmer. Wenn das Flag nicht gesetzt ist, können alle Anrufe auf besetzte Teilnehmer in einem anderen System sofort anklopfen, wenn der Teilnehmer nicht Anklopfschutz aktiviert hat. Das Flag muss gesetzt werden, wenn erreicht werden soll, dass ein rufender VPL bei einem besetzten Teilnehmer sofort in den Wartezustand gesetzt wird und anklopfen kann. Wenn das Flag nicht gesetzt wird, dann bekommt der VPL den Besetztton und geht erst nach einigen Sekunden in den Wartezustand. Standardwert: Deaktiviert

Parameter	Beschreibung
Aufschalten durch VPL	Ist dieses Flag aktiviert, ist der Abwurfplatz für das Leistungsmerkmal "Aufschalten" berechtigt. Damit kann er sich in ein Gespräch eines internen Teilnehmers einschalten. Standardwert: Aktiviert

28.3.1.6 Grundeinstellungen > System > LDAP

Parameterbeschreibung der Registerkarten:

- **LDAP ändern**

Parameter	Beschreibung
LDAP-Zugang	
IP-Adresse des LDAP-Servers	IP-Adresse des LDAP-Servers, von dem die Telefonbuchinformation geholt werden soll.
Port-Nummer des LDAP-Zugangs	Port-Nummer für den LDAP-Zugang. Standardwert: 389
Benutzername/Kennwort	Unter Windows Server ADS ist ein Anonymus-Zugriff nicht möglich. In diesem Fall hier Benutzernamen und Kennwort für die LDAP-Anbindung eingeben. Wertebereich: max. 48 Zeichen.
LDAP-Server-Parameter	
Basis DN	DN = Distinguished Name; Suchbasis für die Suchanfrage an den LDAP-Server (ASCII, 100 Zeichen), z.B. ou=com, cn=unify, cn=de
Suchanfrage	Muster für die Suchanfrage an den LDAP-Server. Als Platzhalter für den zu suchenden Namen muss das Zeichen $ eingegeben werden. Beachten Sie, dass ein Suchmuster nicht mit einem regulären Ausdruck beginnen kann. Wertebereich: ASCII, 50 Zeichen Standardwert: cn=$*
Ergebnisattribut Name	Das Ergebnisattribut Name unterstützt Zeichen des Zeichensatzes ISO-8859-1 mit Codewerten im Bereich von 0x20 bis 0x80 (ASCII-Zeichen), sowie die Zeichen Ä, Å, Æ, Ñ, Õ, Ö, Ø, Ü, ß, ä, õ, ö, ü. Die Anzeige der Zeichen ist abhängig von der Spracheinstellung des Teilnehmers und dem verwendeten Endgerät. Wertebereich: ASCII, 24 Zeichen Standardwert: cn

Parameter	Beschreibung
Ergebnisattribut Rufnummer	Im Ergebnisattribut Rufnummer dürfen bis zu 25 Wahlziffern (0...9, *, #) und bis zu 6 Zeichen zur Formatierung (+,(), Leerzeichen, -) zurückgeliefert werden. Die Rufnummer muss im kanonischen Rufnummernformat vorliegen (z.B. +49 (89) 70070) Wertebereich: ASCII, 25 Zeichen Standardwert: telephoneNumber
Sortieren der Suchergebnisse	Die Suchergebnisse werden alphabetisch sortiert nach Name angezeigt. Standardwert: Aktiviert
LDAP-Rufnummernauswertung	
LDAP-Belegungskennzahl	Die Belegungskennzahl entspricht der gewählten Richtungskennzahl. Standardwert: 0 (Default-Richtungskennzahl der ersten Richtung)
LDAP-Rufnummernprefix	Das hier angegebene Präfix wird der gefundenen Rufnummer vorangestellt. Wertebereich: ASCII, 5 Zeichen

Anmerkung: Damit die LDAP-Ressourcen angezeigt werden können, müssen Sie im Menü **Display** unter **Grundeinstellungen** > **Display** > **Internes Telefonbuch** die entsprechende Option auswählen. Für weitere Informationen siehe Kapitel 28.3.1.3 Grundeinstellungen > System > Display.

28.3.1.7 Grundeinstellungen > System > Texts

Parameterbeschreibung der Registerkarten:

- **Texte ändern**

Parameter	Beschreibung
Zurücksetzen auf Default-Werte	Info- und Antwort-Texte auf die voreingestellten Werte einer bestimmten Sprache zurücksetzen. Die Rücksetzung erfolgt durch Auswahl der Sprache in der Aufklappliste.
Info-Texte	Kurznachrichten, die ein Teilnehmer an einen anderen Teilnehmer senden kann. Standardmäßig sind im Kommunikationssystem zehn solcher Texte vorkonfiguriert. Jede dieser Standard-Meldungen kann überschrieben werden. Dabei sind allerdings immer nur zehn Meldungen verfügbar. Der Teilnehmer kann auf diese Info-Texte über den Menüpunkt Infos senden? am Systemtelefon zugreifen. Teilnehmer mit Endgeräten, die eine alphanumerische Tastatur haben, können darüber hinaus auch selbst Meldungen erstellen; allerdings können sie die Standard-Meldungen nicht ändern. Wertebereich: maximal 24 alphanumerische Zeichen

Parameter	Beschreibung
Antwort-Texte	Kurznachrichten, die der Teilnehmer einem Anrufer bei Abwesenheit zukommen lassen kann. Es stehen 10 Standard-Texte zur Verfügung. Jede dieser Standard-Meldungen kann überschrieben werden. Teilnehmer mit Endgeräten, die eine alphanumerische Tastatur haben, können darüber hinaus auch selbst Meldungen erstellen; allerdings können sie die Standard-Meldungen nicht ändern. Zumeist wird der Teilnehmer die bestehenden Meldungen nur um bestimmte Zusatzinformationen ergänzen wollen. Bei Texten mit einem Doppelpunkt hat der Teilnehmer die Möglichkeit, eine Nachricht, eine Nummer oder ein Datum zu ergänzen. Der Teilnehmer kann auf die Antwort-Texte über den Menüpunkt Hinweismeldung an? am Systemtelefonen zugreifen. Wertebereich: maximal 24 alphanumerische Zeichen

28.3.1.8 Grundeinstellungen > System > Flexible Menüs

Flexible Menüs ermöglichen die kundenindividuelle Anpassung der Menüpunkte im Servicemenü der Systemtelefone. Bei aktiviertem Kontrollkästchen in der **Ausblendliste** wird dieser Menüpunkt nicht angezeigt. Diese Einstellung gilt systemweit für alle Systemtelefone. Ausgeblendete Funktionen können weiterhin per Kennziffer aktiviert werden.

28.3.1.9 Grundeinstellungen > System > Kurzwahlziele

Es können bis zu 8000 Telefonbucheinträge manuell eingerichtet oder geändert werden. Bei den Kurzwahlzielen handelt es sich um zentrale Kurzwahlnummern (RNGZ). Durch Klicken auf einen Spaltennamen werden die Einträge in der entsprechenden Spalte sortiert.

Parameterbeschreibung der Registerkarten:

- **Kurzwahlziel ändern**

Parameter	Beschreibung
Kurzwahl	Nummer, die vom Teilnehmer gewählt wird. Die Kurzwahl-Nummern müssen vierstellig sein (`0000-7999`, führende Nullen verwenden).
Rufnummer	Wählbare Rufnummer der gewünschten Zielstelle, d.h. mit einer Richtungs- oder Leitungskennzahl (z.B. 0, 9, 81 oder 801). Wertebereich: max. 31 Ziffern
Name	Name für das Kurzwahlziel, wie er im internen Telefonbuch gespeichert und bei Anwahl des dazugehörigen Kurzwahlziels angezeigt werden soll. Kommende Rufe (mit CLIP) werden mit den gespeicherten Kurzwahlzielen verglichen und als Name des Kurzwahlziels angezeigt, wenn der Displayparameter Name bzw. Name und Rufnummer aktiviert ist. Wertebereich: max. 16 Zeichen

Parameter	Beschreibung
Suchen	Wird in die Suchfelder **Kurzwahl**, **Rufnummer** oder **Name** ein Suchbegriff eingegeben und anschließend die Return-Taste gedrückt, werden alle Treffer angezeigt, die den Suchbegriff enthalten. Mit der Eingabe von `521` als Rufnummer werden z. B. die Treffer `+495213535` und `+498967521` angezeigt oder mit `co` als Name die Treffer `Collins`, `Mcoin` und `Branco`. Alle Einträge werden angezeigt, wenn in allen Suchfeldern nichts eingetragen ist und anschließend die Return-Taste gedrückt wird.
Schaltflächen	
Übernehmen	Neue Einträge hinzufügen oder vorhandene Einträge ändern.
Rückgängig	Änderungen für vorhandene Einträge zurücksetzen (vor Übernehmen).

Parameterbeschreibung der Registerkarten:

- **Textdatei (csv/xml) importieren/exportieren über HTTP**

Parameter	Beschreibung
CSV/XML-Datei über HTTP importieren	Kurzwahlziele können über eine XML-Datei im UTF-8-Format importiert werden. Bereits bestehende Kurzwahlnummern werden vor dem Import gelöscht. Eine XML-Vorlage für den Import von Kurzwahlnummern findet sich unter **Service-Center** > **Dokumente** > **CSV Vorlagen.**
XML-Datei über HTTP exportieren	Kurzwahlziele können als XML-Datei im UTF-8-Format exportiert werden. Es werden immer alle Datensätze exportiert. **Anmerkung:** Der Import von Kurzwahllisten aus CSV-Dateien wird nicht mehr empfohlen und nur noch bei Bestandskunden unterstützt.

28.3.1.10 Grundeinstellungen > System > Service Codes

Leistungsmerkmale können über das Telefon mittels Servicekennzahlen aktiviert und deaktiviert werden. Die Standard-Servicekennzahlen können geändert werden, wobei zu beachten ist, dass die Vergabe der Kennzahlen konsistent ist.

Zusätzlich können die beiden Kennzahlen geändert werden, die bei IWV-Telefonen und ISDN-Endgeräten den * (Stern, Standard: `75`) und die # (Raute, Standard: `76`) ersetzen (Substitutionen).

28.3.1.11 Grundeinstellungen > System > HFA-Registrierungs-Passwort

Parameterbeschreibung der Registerkarten:

- **HFA-Registrierungs-Passwort**

Parameter	Beschreibung
Voraussetzung für die Wirksamkeit dieser Parameter ist, dass die Systemtelefone den DLI des Systems nutzen und dieser die Systemtelefone mit den erforderlichen Parametern versorgen kann.	
HFA-Registrierungs-Passwort ändern Das HFA-Registrierungs-Passwort kann vom Administrator geändert werden	
Authentifizierung für HFA-Geräte durchsetzen	In der Aufklappliste stehen die folgenden Optionen zur Verfügung: • **Nein** (Standardwert) – es wird keine Authentifizierung verwendet Wenn diese Option ausgewählt ist, sind die Kennwortfelder deaktiviert. Durch Klicken auf die Schaltfläche **Übernehmen** wird die Authentifizierung deaktiviert. • **Nur Nicht-Deskshare-Geräte mit DLI** – das Kennwort wird nur für die System-Clients übernommen, die DLI konfiguriert haben. Das Kennwort wird in der System-DB für diese Geräte festgelegt und von DLI an die richtigen Geräte verteilt. • **Nur Deskshare-Geräte mit DLI** – das Kennwort wird nur für die Deskshare-Geräte übernommen, die DLI konfiguriert haben. Das Kennwort wird in der System-DB für diese Geräte festgelegt und von DLI an die richtigen Geräte verteilt. • **Alle Nicht-Deskshare-Geräte** – das Kennwort wird für alle System-Clientsübernommen. Das Kennwort wird in der System-DB für alle diese Geräte festgelegt und von DLI an die richtigen Geräte verteilt. Bei den System-Clients, für die kein DLI konfiguriert ist, muss das Kennwort manuell eingegeben werden, damit sie in Betrieb genommen werden können. • **Alle Deskshare-Geräte** – das Kennwort wird für alle aktivierten Geräte übernommen. Das Kennwort wird in der System-DB für alle diese Geräte festgelegt und von DLI an die richtigen Geräte verteilt. Bei den Deskshare-Geräten, für die kein DLI konfiguriert ist, muss das Kennwort manuell eingegeben werden, damit sie in Betrieb genommen werden können.
Kennwort	Das Kennwort muss in dieses Feld eingegeben werden. Das Kennwort muss mindestens 8 Zeichen lang sein und mindestens 1 Ziffer und/oder 1 Buchstaben enthalten.
Kennwort bestätigen	Das Kennwort muss in diesem Feld zu Prüfzwecken erneut eingegeben werden.

28.3.1.12 Grundeinstellungen > Gateway

Parameterbeschreibung der Registerkarten:

- **Gateway-Eigenschaften ändern**

Parameter	Beschreibung
Allgemeines	

Parameter	Beschreibung
Kunden-Name	Frei wählbarer Name des Kunden, nur für Informationszwecke (optional) Wertebereich: max. 15 Zeichen.
Vertragsnummer	Frei wählbare Zeichenfolge, für Informationszwecke (optional) Wertebereich: unbegrenzt
System-Name	Frei wählbarer Name des Kommunikationssystems. Diese Zeichenfolge wird im Display aller Systemtelefone angezeigt. Wertebereich: max. 24 Zeichen.
Gateway-Standort	Frei wählbare Zeichenfolge zur Angabe des Aufstellungsorts des Kommunikationssystems. Diese Information hilft einem Servicetechniker, das Kommunikationssystem zu finden, wenn ein physischer Zugang zum Kommunikationssystem nötig ist. (optional) Wertebereich: unbegrenzt
Kontakt-Adresse	Frei wählbare Zeichenfolge zur Angabe einer Kontaktperson, die bei Problemen mit dem Kommunikationssystem angesprochen werden kann. (optional) Wertebereich: unbegrenzt
System-Länderkennzeichen	Auswahl des Landes, in dem das Kommunikationssystem betrieben wird; das Ändern des System-Länderkennzeichens erfordert einen Reboot, der automatisch durchgeführt wird.
Gateway-IP-Adresse	Anzeige der IP-Adresse des Kommunikationssystems, z.B. 192.168.1.2.
Gateway-Netzmaske	Anzeige der Netzmaske des Kommunikationssystems, z.B. 255.255.255.0.
Internationales Präfix	Angabe des Präfix für internationale Wahl, z.B. 00 für Deutschland oder 011 für USA.
Nationales Präfix	Angabe des Präfix für nationale Wahl, z.B. 0.
Produkt	Auswahl des erworbenen Produkts (OpenScape Business oder Octopus F X)
Gateway-Standort	
Ländervorwahl	Angabe der Ländervorwahl, z.B. 49 für Deutschland oder 1 für USA.
Ortskennzahl	Angabe der Ortsnetzkennzahl, z.B. 89 für München.
Anlagenrufnummer	Angabe der Anlagenrufnummer (Kopf-Nr. ohne Tln.-Durchwahl), z.B. 7007
Vernetzungsparameter	
Knoten ID	Für jeden Knoten in einem vernetzten System muss eine eindeutige Knoten-ID vergeben werden. Damit sind die einzelnen Knoten im vernetzten System eindeutig identifizierbar. Wertebereich: 1 bis 100
Interner Wählton	

Parameter	Beschreibung
Dauerton	Ist dieses Flag aktiviert, ist der interne Wählton keine Tonfolge sondern ein Dauerton. Der interne Wählton ertönt, sobald man den Telefonhörer abgenommen und noch keine Ziffer gewählt hat. Standard: deaktiviert

28.3.1.13 Grundeinstellungen > DynDNS > DynDNS Service

Parameterbeschreibung der Registerkarten:

- **DynDNS Konfiguration anzeigen**
- **DynDNS Konfiguration ändern**

Parameter	Beschreibung
DynDNS aktivieren	Mit Hilfe des DynDNS-Service kann von verschiedenen Orten auf das Gateway zugegriffen werden, ohne dass die aktuelle IP-Adresse des Gateways bekannt sein muss. Der DynDNS-Service kann hier aktiviert werden.
Benutzerdefinierte Domäne	Kontrollkästchen muss aktiviert werden, wenn der DynDNS-Anbieter nicht in der Liste **Domainname** enthalten ist.
Benutzername	Benutzername des DynDNS-Accounts beim DynDNS-Anbieter. Das Einrichten von DynDNS-Accounts ist z.B. unter der Internet-Adresse `http://www.dyndns.org/account/create.html` möglich.
Kennwort	Passwort des DynDNS-Accounts beim DynDNS-Anbieter. Bei der Eingabe werden aus Sicherheitsgründen nur Platzhalterzeichen angezeigt.
Passwort wiederholen	Wiederholung des Passworts des Benutzerkontos beim DynDNS-Service. Bei der Eingabe werden aus Sicherheitsgründen nur Platzhalterzeichen angezeigt.
Hostname	Eingabe des beim DynDNS-Anbieter registrierten Hostnamens ohne den Domainnamen, z.B. myhost. Der komplette Subdomain-Name setzt sich aus dem Hostnamen und dem Domainnamen zusammen, z.B. myhost.dyndns.org.
Domänen-Name	Auswahl des DynDNS-Anbieters aus einer Liste (z.B. dyndns.org) oder manuelle Eingabe des DynDNS-Anbieters (falls Kontrollkästchen **Benutzerdefinierte Domäne** aktiviert ist).

Parameter	Beschreibung

Update-URL	Eingabe der Update-URL eines nicht in der Liste enthaltenen DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.
	Beispiel einer Update-URL:
	`http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
	Beispiel einer Update-URL mit Base64 verschlüsselter Authentifizierung:
	`https://<b64><username>:<pass></b64>@members.dyndns.org/nic/update?hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG`
	<b64>...</b64> für Base64 codierte Parameter

Zuletzt aktualisiert	Zeitpunkt der letzten Aktualisierung beim DynDNS-Service.
IP-Adresse beim DynDNS	IP-Adresse beim DynDNS-Anbieter, auf die Anfragen für Ihre eingerichtete DynDNS-Subdomain geroutet werden.
Eigene dynamische IP-Adresse	Anzeige der aktuellen IP-Adresse des Kommunikationssystems, die vom Internet Service-Provider zugewiesen wurde.
Wildcard aktivieren	Wird diese Option aktiviert, werden Anfragen nach Sub-Subdomains wie beliebig.myhost.dyndns.org auf myhost.dyndns.org geroutet.
Mail Exchanger	Der Mail Exchanger (MX-Record) gibt innerhalb des DNS an, an welche IP-Adresse oder an welchen Domainnamen E-Mails für die eingerichtete DynDNS-Subdomain zu schicken sind. Hinter dem angegebenen Ziel muss sich ein Mailserver befinden.
Backup MX	Wird diese Option aktiviert, werden E-Mails, die nicht an den angegebenen Mail-Exchanger zugestellt werden können, weil dieser beispielsweise temporär nicht verfügbar ist, beim DynDNS-Service zwischengespeichert und zugestellt, wenn der eigene Mail Exchanger wieder verfügbar ist.
HTTPS für die Aktualisierung verwenden	Wird diese Option aktiviert, wird für die Aktualisierung die sichere verschlüsselte HTTPS-Verbindung gewählt.

28.3.1.14 Grundeinstellungen > DynDNS > Aktualisierungszeit der DNS-Namen

Parameterbeschreibung der Registerkarten:

- **Aktualisierungszeit ändern**

Parameter	Beschreibung
DNS-Namen aktualisieren	Diese Option gilt nur für VPN. Nach Ablauf der Zeit, die in „Timer-Wert für Aktualisierung der DNS-Namen“ eingestellt ist, überprüft die VPN-Komponente, ob sich eventuell verwendete DNS-Namen in der VPN Konfiguration zu neuen IP-Adressen auflösen (VPN mit dynamischen IP Adressen). In dem Fall wird VPN mit den neuen IP-Adressen rekonfiguriert.

Parameter	Beschreibung
Timer-Wert für Aktualisierung der DNS-Namen (s)	Sekundenanzahl für das Intervall zwischen zwei Aktualisierungen. Wertebereich: 60 bis 1800, Standardwert: 180

28.3.1.15 Grundeinstellungen > Quality of Service

Beim IP-Datenverkehr werden die IP-Pakete, die das Kommunikationssystem selbst generiert, in fünf Gruppen aufgeteilt. Für vier dieser Gruppen kann eingestellt werden, mit welchem Codepunkt die Pakete markiert werden sollen. Der übrige Datenverkehr wird nicht proirisiert (also 00 markiert).

Prioritätsklasse	ToS-Wert Binär	ToS-Wert Hexadezimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60
CS4	100-000-00	80
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Manuelle Eingabe	xxx-xxx-00	0-63 (dezimal)

Parameterbeschreibung der Registerkarten:

- **Quality of Service ändern**

Parameter	Beschreibung
Prioritätsklasse für Signalisierungsdaten	Call Signaling für den Verbindungsaufbau bei H.323/SIP Standardwert: AF31
Prioritätsklasse für Fax/ Modem-Payload	Data Payload, zum Beispiel für IP-Vernetzung mit Fax oder Modem Standardwert: EF
Prioritätsklasse für Netzwerksteuerung	Network Control, zum Beispiel SNMP-Traps Standardwert: CS7
Prioritätsklasse für Sprach-Payload	Voice-Payload für die IP-Telefonie (Voice over IP) Standardwert: EF

28.3.1.16 Grundeinstellungen > Datum und Uhrzeit > Datum und Uhrzeit

Parameterbeschreibung der Registerkarten:

- **Datum und Uhrzeit setzen**

Parameter	Beschreibung
Datum und Uhrzeit	
Tag	Auswahl des Tages.
Monat	Auswahl des Monats.
Jahr	Eingabe des Jahrs.
STD:MM:SS	Eingabe der Uhrzeit im 24-Stunden Format.

28.3.1.17 Grundeinstellungen > Datum und Uhrzeit > Zeitzonen-Einstellungen

Parameterbeschreibung der Registerkarten:

- **Zeitzonen-Einstellungen ändern**

Parameter	Beschreibung
Zeitzone	Lokale Zeitzone, in welcher sich das System befindet

28.3.1.18 Grundeinstellungen > Datum und Uhrzeit > SNTP-Einstellungen

Parameterbeschreibung der Registerkarten:

- **Einstellungen ändern**

Parameter	Beschreibung
SNTP-Client Eingabe der Zugangsdaten für einen externen Zeitserver (SNTP) zur netzweiten Synchronisation der Systemuhr.	

Parameter	Beschreibung
Administrativer Zustand des SNTP-Client	Verbindung des Kommunikationssystems zum SNTP-Server aktivieren oder deaktivieren Standardwert: aus
IP-Adresse/DNS-Name des externen Zeitservers	IP-Adresse oder DNS-Name des SNTP-Servers. Standardwert: 0.de.pool.ntp.org
Pollzeit für externen Zeitserver	Intervall für die Synchronisation von Datum und Uhrzeit mit dem SNTP-Server. Standardwert: 4 Std.

28.3.1.19 Grundeinstellungen > Port-Verwaltung

Die dargestellten Ports dienen zur Identifizierung der Netzwerkprotokolle und entsprechenden Netzwerkdienste. Einige der Ports, die das Kommunikationssystem selbst verwendet, können hier geändert werden. Dadurch kann z.B. in einem Netzwerk die Kommunikation auf das Kundennetz abgestimmt werden, wenn die Ports bereits anderweitig verwendet werden. Wenn an der Portverwaltung Änderungen vorgenommen werden, muss dies in der Regel an allen Komponenten (Telefone, Anlagen etc.) gleichzeitig geändert werden, damit die Funktionalität gewährleistet bleibt.

Parameterbeschreibung der Registerkarten:

- **Globale Port-Manager-Einstellungen ändern**

Parameter	Beschreibung
Protokoll-Name	Dienst.
Portnummer	Portnummer des Dienstes (konfigurierbar).
Port-Typ	Zur Information wird der Port-Typ angezeigt; Single: ein einzelner Port; Min: Untergrenze für ein Port-Bereich.
Dienste	
CSP	CSTA Service Provider, IP-Port für alle Applikationen, die sich mit dem CSP verbinden wollen. Standardwert: 8800
HFA	Steuerung von HFA-Clients (CorNet-TC Serverport). Standardwert: 4060
HFA_EXT	Steuerung von HFA-Clients (CorNet-TC Serverport) für System Device@Home. Standardwert: 4062
HFA_TLS	CorNet-TC über TLS. Standardwert: 4061
HFA_TLS_EXT	CorNet-TC via TLS für System Device@Home. Standardwert: 4063

Parameter	Beschreibung
MEB_SIP	MediaExtensionBridge, Callsignalling für SIPQ Trunking. Standardwert: 15060
RTP_MIN	RTP/RTCP- und T.38-Ports (MediaBasePort). Standardwert: 29100
SIP	Rufsignalisierung für SIP-Endgeräte und SIP-basiertes Trunking. Standardwert: 5060
SIP_EXT	Rufsignalisierung für SIP-Endgeräte und ITSP-Trunking für SIP-Gerät@Home. Standardwert: 5070
SIPS	Sichere Rufsignalisierung für SIPQ Trunking. Standardwert: 5061
SIP_TLS_SUB	Sichere Rufsignalisierung für SIP-Teilnehmer. Standardwert: 5062
SIP_TLS_SUB_EXT	Sichere Rufsignalisierung für SIP-Teilnehmer für SIP-Gerät@Home. Standardwert: 5071
VSL_MULTISITE	Multi-Site-Verbindungen. Standardwert: 8778

28.3.1.20 Grundeinstellungen > Gebühren > Gebühren Ausgabe

Parameterbeschreibung der Registerkarten:

- **Gebühren Ausgabe ändern**

Parameter	Beschreibung
Format des Gesprächsdatensatzes	
Komprimiertes Ausgabeformat	Standardwert: Aktiviert
Letzten 4 Ziffern unterdrücken	Ersetzen der letzten 4 Ziffern des Feldes Rufnummer durch Fragezeichen zum Schutz der Privatsphäre. Standardwert: Deaktiviert
Kommende Gespräche protokollieren	Standardwert: Deaktiviert
Anrufdauerprotokollierung ein	Protokollierung der Gesprächsdauer in Stunden, Minuten und Sekunden. Standardwert: Aktiviert

Parameter	Beschreibung
Anrufprotokoll ein	Bei eingehenden Anrufen wird unmittelbar nach Rufbeginn ein Verbindungsdatensatz angelegt, um z.B. für eine Anruferliste oder über eine PC-Auswertung des Datensatzes Zusatzinformationen zu den Anrufern zu übermitteln. Standardwert: Deaktiviert
Ausgabe der MSN	Protokollierung der benutzten MSN (Nur IDSN) Standardwert: Deaktiviert
Dezimalformat	(nicht in USA) Format der Gebührenanzeige, ist länderindividuell zu konfigurieren. In Deutschland wird immer das Dezimalformat verwendet. Gleichfalls bedeutet diese Dezimaldarstellung, dass der Multiplikator in Hundertstel angegeben wird. Der Multiplikator gibt an, mit welchem Betrag eine Tarifeinheit multipliziert wird, um den Währungsbetrag zu erhalten (z.B. 0,06 Euro statt 6 Cent). Standardwert: Aktiviert
Beträge statt Einheiten ausgeben	Es werden Geldbeträge statt Tarifeinheiten ausgegeben (z.B. 4,50 EUR statt 75 Einheiten). Standardwert: Aktiviert
Gehend ohne Verbindung	Protokollierung gehender Gespräche, welche nicht angenommen wurden. Standardwert: Deaktiviert
LCR-Rufnummer gehend bzw. angewählte Rufnummer kommend	Ist dieses Flag aktiviert, wird der Gebührendatensatz um ein zusätzliches Rufnummernfeld erweitert. Er beinhaltet: • bei gehendem Ruf die LCR-Rufnummer, die ggf. nach Umwandlung durch LCR tatsächlich ins Amt gesendet wurde, bzw. • bei kommendem Ruf die interne Rufnummer des Wunschteilnehmers, d.h. des ersten angewählten Teilnehmers. Es wird auch dann ein Gebührendatensatz ausgegeben, wenn ein Anruf auf einen besetzten Teilnehmer erfolgt. Dieser Verbindungsdatensatz entspricht in seinem Format dem Datensatz eines freien Teilnehmers mit dem Unterschied, dass die Ruf-/Gesprächsdauer auf „0“ gesetzt ist. Standardwert: Deaktiviert
Gesprächsdatenerfassung zentral (GEZ)	
Ausgabe: keine	Keine Übertragung von Verbindungsdaten Standardwert: HTTP
Ausgabe: HTTPS	Übertragung von Verbindungsdaten an mitgelieferten Gebührenmanager oder andere Accounting-SW Standardwert: HTTP
Ausgabe: LAN-TCP-Client	Übertragung von Verbindungsdaten an externen Server via TCP/IP Standardwert: HTTP

Parameter	Beschreibung
TCP-Client	Festlegen von IP-Adresse und Portnummer eines externen Gebührenservers. Bei anfallenden Gebühren initiiert das Kommunikationssystem eine TCP/IP-Verbindung zum externen Gebührenserver. Nach dem Verbindungsaufbau werden die Gebührendaten übertragen. Die Verbindung bleibt permanent bestehen, weitere anfallende Gebühren werden übertragen, wobei jeder Datensatz separat verschickt wird.

28.3.1.21 Grundeinstellungen > Gebühren > Gebühren Faktoren

Parameterbeschreibung der Registerkarten:

- **Gebührenfaktoren ändern**

Parameter	Beschreibung
Gebührenfaktor pro Richtung	Die Gebühreninformation kann in Form von Tarifeinheiten (Zählimpulse) oder Währungseinheiten (Geldbeträge) angeboten werden. Beide Formen werden unterstützt, aber es werden nur Währungseinheiten am Display angezeigt. Bei Übermittlung der Information in Form von Gebühreneinheiten wird ein Umrechnungsfaktor benutzt. Diese Gebührenfaktoren werden pro Richtung eingestellt und gelten sowohl für Amtsgespräche als auch im Netzverbund, gehend und kommend.
Richtungen	Anzeige der im System vorhandenen Richtungen
Multiplikator	Dieser Multiplikator wird verwendet zur Umrechnung von Tarifeinheiten in Währungsbeträge. Wertebereich: 0 bis 65534, Standardwert: 6
Multipl. ISDN	Faktor zur zur Umrechnung empfangener bzw. zu versendender Währungsbeträge in Tarifeinheiten und umgekehrt. Nur für Richtungen mit Protokoll QSIG. Wertebereich: 1 bis 65535, Standardwert: 6
Währung	Kurzbezeichnung der Währung, z.B. EUR. Dies ist mit dem angeschlossenen Kommunikationssystem abzustimmen. Die Konfiguration des Währungsstrings ist unabhängig von dem Währungsstring für die Anzeige bei den Endgeräten. Hinweis: Der Parameter hat nur Bedeutung bei Richtungen mit Protokoll QSIG. Bei anderen Protokollen ist der Parameter wirkungslos und die vorgegebene Einstellung (Standardeinstellung) ist dann beizubehalten. Wertebereich: max. 3 Zeichen.
Währungsbetrag	In der Spalte Währungsbetrag wird festgelegt, ob Währungsbeträge oder Tarifeinheiten auf der Richtung ausgetauscht werden. Bei aktivierter Option wird der Währungsbetrag versendet und empfangen (siehe Spalte Multipl. ISDN). Anderenfalls werden Tarifeinheiten versendet und empfangen. Dies ist mit dem angeschlossenen Kommunikationssystem abzustimmen. Wenn auf der Richtung Gebührenimpulse ausgetauscht werden, so sollte als Währung ein leerer String konfiguriert werden. Hinweis: Der Parameter hat nur Bedeutung bei Richtungen mit Protokoll QSIG. Bei anderen Protokollen ist der Parameter wirkungslos und die vorgegebene Einstellung (Standardeinstellung) ist dann beizubehalten.

Parameter	Beschreibung
Gebührenmode: **keine Gebühren**	Über die Richtung werden keine Gebühren empfangen, z.B. USA Amtsleitungen. Parameter ist nicht relevant bei Richtungen mit Protokoll QSIG.
Gebührenmode: **während Verbindung**	Gebühren werden nur während der Verbindung empfangen, nicht beim Verbindungsabbau.
Gebührenmode: **am Ende der Verbindung**	Gebühren werden nur bei Verbindungsende empfangen.
Gebührenmode: **während / am Ende der Verbindung**	Gebühren werden während einer Verbindung und bei Verbindungsabbau empfangen.
Währung	Währungskennzeichen für die Gebührenanzeige bei den Endgeräten.
Rechengenauigkeit	Ist so einzustellen, dass die Genauigkeit des Kommunikationssystems mindestens gleich groß ist als jene der vom Amt gesendeten Geldbeträge. Falls die maximal möglichen drei Nachkommastellen nicht ausreichen, wird automatisch gerundet. "Über Gebührenimpulse" ist zu wählen bei Richtungen mit Protokoll QSIG.

28.3.1.22 Grundeinstellungen > Gebühren > Gebühren Projekt Kennzahlen

Parameterbeschreibung der Registerkarten:

- **Projektkennzahlen ändern**

Parameter	Beschreibung
Prüfverfahren	
Prüfverfahren: Keine Prüfung	Keine Prüfung eingegebener Projekt-Kennzahlen unterzogen. Diese Option kann bei Richtungen mit Pflicht-Eingabe nicht verwendet werden.
Prüfverfahren: Listen-Prüfung	Eingegebene PKZ werden an Hand der PKZ-Listen auf Gültigkeit geprüft.
Prüfverfahren: Prüfung der Stellenzahl	Eingegebene PKZ werden auf ihre Stellenanzahl geprüft.
Anzahl der zu prüfenden Stellen	Gültige Stellenanzahl für PKZ. Wertebereich: 1 bis 11, Standardwert: 5
PKZ-Listen	
Liste	Für Listenprüfung können maximal 1000 PKZ eingegeben werden.
Projektkennzahl	Wertebereich: max. 11 Ziffern

28.3.1.23 Grundeinstellungen > Wiedergabegerät für Sprachnachrichten/Ansagen

Parameterbeschreibung der Registerkarten:

- **Wiedergabegerät für Sprachnachrichten/Ansagen ändern**

Parameter	Beschreibung
Sprachnachricht	
Präfix	Rufnummer der Sprachbox.
Wiedergabegerät für Ansagen	
Rufnummer	Rufnummer des Wiedergabegeräts (Announcement Player).

28.3.1.24 Grundeinstellungen > Telefonparameter-Bereitstellung

Parameterbeschreibung der Registerkarten:

- **Telefonparameter-Bereitstellung bearbeiten**

Parameter	Beschreibung
Telefonparameter-Bereitstellung Voraussetzung für die Wirksamkeit dieser Parameter ist, dass die Systemtelefone den DLI des Systems nutzen und dieser die Systemtelefone mit den erforderlichen Parametern versorgen kann. Die Parameter der Systemtelefone werden aktualisiert, sobald sich ein Systemtelefon neu mit dem System verbindet oder neu gestartet wird oder das System neu gestartet wird. Die einzelnen Parameter können direkt am Systemtelefon oder mit dem WBM des Systemtelefons konfiguriert werden. Die Einstellungen für den PC-Ethernet-Port und für die Codec-Priorisierung werden vom DLI nicht überschrieben, wenn sie direkt am Systemtelefon oder mit dem WBM des Systemtelefons konfiguriert wurden.	
Aktivieren der Telefonparameter-Bereitstellung	Ist dieses Flag aktiviert, sind die nachfolgenden Optionen zur Bearbeitung aktiviert.
SW an @Home-Geräte verteilen	Wenn dieses Flag aktiviert ist, werden Berechtigungen für die Softwareaktualisierung über DLI für HFA@Home-Geräte erteilt.
Telefonparameter Die folgenden Telefoneinstellungen können hier geändert werden.	
PC Port	Ist dieses Flag aktiviert, wird der PC Ethernet Port aller aktiven Systemtelefone eingeschaltet. Standard: deaktiviert
Codec-Einstellung ist "geringe Bandbreite bevorzugt"	Ist dieses Flag aktiviert, gilt für alle Systemtelefone die folgende Codec-Priorisierung: G.729 - G.711 - G.722 Ist dieses Flag deaktiviert, gilt die folgende Codec-Priorisierung: G.722 - G.711 - G.729 **Anmerkung:** CP100 unterstützt G.722 nicht Standard: deaktiviert

Parameter	Beschreibung
Bilder für Anrufer anzeigen	Ist dieses Flag aktiviert, wird an Systemtelefonen mit großem Farbdisplay bei einem ankommenden Ruf das Bild des Anrufers angezeigt, sofern es über UC Smart oder UC Suite in das System geladen wurde. Standard: deaktiviert
Telefonparametereinstellungen anwenden	
Telefonparametereinstellungen auf alle Telefone anwenden	Wenn Sie dieses Flag aktivieren, werden alle lokal verwalteten Einstellungen überschrieben. Standard: deaktiviert

Parameterbeschreibung der Registerkarten:

- **Geräte-Info**

  Folgende Informationen für jedes Gerät werden hier erwähnt:

  Rufnummer, Anzeige, Gerätetyp, IP-Adresse, MAC-Adresse, Aktuelle SW-Version, HW-Version, PC-Port, Codec-Einstellung.

Parameterbeschreibung der Registerkarten:

- **Admin-Passwort ändern**

  Der Administrator kann das Passwort für den Zugriff auf das WBM des Telefons konfigurieren.

Parameter	Beschreibung
Voraussetzung für die Wirksamkeit dieser Parameter ist, dass die Systemtelefone den DLI des Systems nutzen und dieser die Systemtelefone mit den erforderlichen Parametern versorgen kann.	
Admin-Passwort ändern Das Standard-Passwort kann vom Administrator zentral für alle über DLI verbundenen Geräte geändert werden.	
Kennwort	Das Passwort muss in dieses Feld eingegeben werden. Das Passwort muss mindestens 6 Zeichen lang sein.
Passwort bestätigen	Das Passwort muss in diesem Feld zu Prüfzwecken erneut eingegeben werden.

Parameterbeschreibung der Registerkarten:

- **Kanonische Wahleinstellungen**

  Der Administrator kann die kanonischen Wahleinstellungen an alle Desk Phone CP HFA-Geräte verteilen, die DLI konfiguriert haben.

  Bitte beachten Sie, dass die Werte der im WBM konfigurierten kanonischen Wahleinstellungen immer die lokalen (Telefon-) Einstellungen überschreiben.

Parameter	Beschreibung
Kanonische Wahleinstellungen	
Landeskennzahl	Erforderlich - Interner Code für den Telefonstandort. Wenn sie nicht gesetzt ist, findet keine Umwandlung statt. Maximale Länge: 5 Zeichen.

Parameter	Beschreibung
Nationale Vorwahlziffer	Benötigt - Vorwahlziffer für PSTN-Wahl innerhalb des Landes. Wert: Maximale Länge: 5 Zeichen.
Lokaler Nationaler Code	Benötigt - PSTN-Vorwahl für den Standort des Telefons. Maximale Länge 6 Zeichen.
Minimale Länge der lokalen Nummer	Benötigt - PSTN Ortsnetzlänge der Nummern. Reichweite: 0-50
Maximale Länge der lokalen Nummer	Optional - PSTN-Ortsnetzlänge der Nummern Ein Wert von 0 bedeutet, dass diese neue Regel nicht angewendet wird. Reichweite: 0-50
Lokaler Unternehmensknoten	Optional - Vorwahl des lokalen Unternehmensnetzes für ein Telefon als Nebenstelle. Maximale Länge 10 Zeichen.
PSTN-Kennzahl	Optional - Liste der Ziffern für den PSTN-Zugang. Maximale Länge 10 Zeichen.
Internationale Kennzahl	Benötigt - Liste der PSTN-Zugangscodes für das internationale Gateway. Maximale Länge 5 Zeichen.
Betreiberkennzahl	Optional - Liste der Nebenstellennummern für die Betreiber. Maximale Länge 50 Zeichen.
Notrufnummern	Optional - Liste der Nummern, die für Notrufe verwendet werden Maximale Länge 50 Zeichen.
Initiale Durchwahlziffern / Initiale Ziffern	Optional - Liste der Anfangsziffern für die Nebenstelle im lokalen Unternehmensnetz (definiert durch den lokalen Unternehmensknoten). Maximale Länge 50 Zeichen.
Erwarte Wählnummer	Optional - Der Wert gibt an, wann ein PSTN-Zugangscode + nationale Vorwahlziffer beibehalten und nicht in den internationalen Zugangscode umgewandelt wird. Wahr/Falsch mit dem Standardwert Falsch.
Kanonisches Zifferblatt	
Internrufnummern	Dropdown-Liste mit den folgenden Optionen: Lokales Unternehmensformular (Standard), Knoten immer hinzufügen, Externe Nummern verwenden. Integer.
Externe Rufnummern	Dropdown-Liste mit den folgenden Optionen: Lokales öffentliches Formular (Standard), nationales öffentliches Formular, internationales öffentliches Formular. Integer.
Externe Kennzahl	Dropdown-Liste mit den folgenden Optionen: Nicht erforderlich (Standard), Für externe Nummern. Integer.
Internationale Gateway-Kennzahl	Dropdown-Liste mit den folgenden Optionen: Verwenden Sie den nationalen Code (Standard), lassen Sie als +. Integer.
Kanonische Wählhilfe	
Ortsvorwahl 1-5	Optional - ein lokaler Knotencode im Unternehmensnetz. Maximale Länge 10 Zeichen.
Internationaler Code 1-5	Optional - der internationale Code entspricht dem lokalen Code. Maximale Länge 30 Zeichen.

28.3.1.25 Grundeinstellungen > Power Management

Parameterbeschreibung der Registerkarten:

- **Power Management ein-/ausschalten**

Parameter	Beschreibung
Power Management Das Power-Management kann nur aktiviert werden, wenn sich die LAN-Schnittstellen des Systems im Ethernet-Link-Modus **Auto** befinden. Im Energiesparzustand wechseln die LAN-Schnittstellen des Systems automatisch in den 100Mbit/s-Vollduplex-Modus. Die LAN-Schnittstellen der angeschlossenen Infrastruktur sollten sich ebenfalls im Autosense-Modus befinden.	
Power Management ein-/ ausschalten	Schaltet das System in den Energiesparzustand.
Beginn des LowPowerModes	Startzeitpunkt des Energiesparzustand.
Ende des LowPowerModes	Endzeitpunkt des Energiesparzustand.
IP Bandbreite wird auf 100MBit/s FDX reduziert	Anzeige der Datenrate im Energiesparzustand.

28.3.1.26 Grundinstallation> Massendaten

- Parameterbeschreibung der Registerkarten:

Parameter	Beschreibung
Port	Portnummer. Nicht editierbares Feld.
Gültigkeit	Es gibt zwei Arten der Validierung: den Front-End-Konsistenz Check und den Back-End-Konsistenz Check: a. Der **Front-End-Konsistenz Check** validiert Daten aus den Feldern im Fenster für den Assistenten "Massendaten" validiert, indem sie auf Inkonsistenzen und Konflikte geprüft werden. Eine rote Anzeige erscheint im Feld "Gültigkeit" unter den jeweiligen Nummern. Wenn Sie mit der Maus auf ein Popup-Fenster zeigen, erhalten Sie genaue Angaben zum Konflikt. b. Beim **Back-End-Konsistenz Check** werden die Daten aus den Feldern im Fenster für den Assistenten "Massendaten" validiert, indem die Daten mit den vorhandenen aber nicht anzeigbaren Daten im System verglichen werden. Dazu gehören Gruppen, MULAP, Voicemail, nationaler und internationaler Zugriff, VSL-Nummern, Richtungskennzahlen und Leitungskennzahlen (z. B. Amtszugang).
Rufnr.	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.
Dual-Mode-Nr.	Mobile Rufnummer des Teilnehmers.
UC Mobilnr.	Persönliche Mobiltelefonnummer des Benutzers von UC Smart oder UC Suite. Die Nummer ist im kanonischen Format, z. B.: +49 89 7007 100. Diese Nummer wird in der Ansicht **Eigene persönliche Daten** des Benutzers im **Benutzerverzeichnis** angezeigt.
E-Mail-Adresse	E-Mail-Adresse des Teilnehmers.

Parameter	Beschreibung
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt.
Vorname	Frei wählbarer Vorname des Teilnehmers.
Nachname	Frei wählbarer Nachname des Teilnehmers.
Gerätetyp	Der dem Benutzer zugeordnete Gerätetyp. Nicht editierbares Feld.
Typ	Typ des Teilnehmers.
Typ: **Frei**	Der Rufnummer ist (noch) kein Teilnehmer zugeordnet.
Typ: **System-Client**	Ein System-Client ist ein IP-Teilnehmer, der über CorNet-IP alle Leistungsmerkmale des Kommunikationssystems nutzen kann (früher HFA System-Client).
Typ: **SIP-Client**	Ein SIP-Client ist ein IP-Teilnehmer, der das Protokoll SIP nutzt. Er kann über SIP nur einen eingeschränkten Leistungsumfang des Kommunikationssystems nutzen.
Typ: **Deskshare User**	Ein Deskshare User ist ein IP-Teilnehmer, der sich auf einem anderen IP-Systemtelefon anmelden kann (Mobile Login) und dieses Telefon wie sein eigenes Telefon nutzen kann (inkl. Rufnummer).
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax DuWa	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA)
Status	Zeigt den Status des Geräts an. Aktiv oder inaktiv.

28.3.2 Sicherheit

Unter **Sicherheit** sind die sicherheitsrelevanten Einstellungen zusammengefasst. Dazu gehören Einstellungen für Firewall, Filter, VPN und SSL.

28.3.2.1 Sicherheit > Anwendungsfirewall

Parameterbeschreibung der Registerkarten:

- **Dienste anzeigen**
- **Dienst hinzufügen**
- **Alle Dienste löschen**

Parameter	Beschreibung
Application Firewall	Die Anwendungsfirewall wird verwendet, um den Zugriff auf bestimmte Dienste wie FTP oder LDAP einzuschränken. Es ist standardmäßig deaktiviert und kann durch Definieren geeigneter Regeln aktiviert werden. Die folgenden Dienste können von der Anwendungsfirewall entweder blockiert oder auf bestimmte IP-Adressen oder IP-Adressbereiche beschränkt werden: **Dienst / Ports** HTTPS / 443 Postgres / 5432 LDAP / 389 Manager E / 7000 ssh (standardmäßig gesperrt) / 22 FTP / 21, 40000 - 40040 OBSERVER / Der OBSERVER-Dienst ermöglichte den Zugriff von einer OpenScape Observer-Anwendung die nicht mehr unterstützt wird. Nur die aufgeführten Dienste können über ein Auswahlmenü im Expertenmodus gesperrt werden. Telefonmerkmale wie SIP, HFA usw. können über die Anwendungsfirewall nicht blockiert werden. Ein Dienst kann mehrfach ausgewählt werden; Jedes Mal können unterschiedliche IP-Beschränkungen angegeben werden. **Anmerkung:** Wenn die Anwendungsfirewall aktiviert ist, werden Dienste standardmäßig erst blockiert, wenn eine Regel für diesen Dienst hinzugefügt wird. Zu diesem Zeitpunkt können nur IP-Adressen, die in der Regel enthalten sind, auf diesen bestimmten Dienst zugreifen. Die Anwendungsfirewall kann den Zugriff auf Merkmale zwischen Knoten einschränken, wenn das System mit anderen OpenScape Business-Systemen vernetzt ist. Wenn in diesem Fall eine Regel für den POSTGRES-Dienst hinzugefügt wird, fügen Sie der POSTGRES-Regel manuell die IP-Adressen der anderen OpenScape Business-Netzwerkknoten hinzu, um den korrekten Betrieb der Überlebensfähigkeit sicherzustellen.
Regelname	Vorname für die Regel
Regel aktiviert	Die Regel ist aktiviert.
Untere Grenze des Quell-IP-Adressbereichs	Die untere Grenze der blockierten IP-Adressen.
Obere Grenze des Quell-IP-Adressbereichs	Die obere Grenze der blockierten IP-Adressen.

28.3.2.2 Sicherheit > Deployment- und Licensing-Client (DLSC)

Um DLS-Funktionen nutzen zu können, muss das Kommunikationssystem dem externen DLS den Zugriff auf die Konfigurationsdaten gewähren. Das Kommunikationssystem wird dann als Deployment und Licensing Client betrieben. Der externe DLS-Server wird unter > Mainboard > DHCP-Modus > DHCPServer > Globale Einstellungen eingerichtet.

Parameterbeschreibung der Registerkarten:

- **DLSC-Grundeinstellung**
- **DLSC kontaktieren**
- **DLSC Bootstrapping zurücksetzen**

Parameter	Beschreibung
Status	
Sichere Kommunikation mit dem DLS-Client	Anzeige ob (und wieviel) eine sichere Kommunikation mit dem DLS-Client aktiviert bzw. deaktiviert (0) ist
DLS-Client	
Zeitinterval für ContactMe-Antwort	Standardwert: 0
PIN für DLS-Bootstrapping erforderlich	Erhöhte Sicherheitsstufe durch PIN-Eingabe auf beiden Seiten
Bootstrap PIN	Wertebereich: min. 8 bis max. 32 Zeichen
DLS-Server	
IP-Adresse des DLS-Servers	Eintrag der IP-Adresse des externen DLS_Servers.
Port des DLS-Servers	Port-Eingabe des externen DLS-Servers Standardwert: 18443
Port für sichere Verbindung zum DLS-Server	Anzeige der Portnummer für eine sichere Verbindung

28.3.2.3 Sicherheit > Deployment- und Licensing-Client (DLSC) > DLSC Client-Zertifikat

Parameterbeschreibung der Registerkarten:

- **Zertifikatsinformationen**

Parameter	Beschreibung
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS
Seriennummer des Zertifikats	Anzeige der festgelegten Seriennummer.

Parameter	Beschreibung
Seriennummer des Zertifikats (hex)	Anzeige der festgelegten Seriennummer im Hexadezimalformat.
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus Wertebereich: sha256RSA, sha512RSA
Beginn der Zertifikatsgültigkeit (GMT)	Anzeige des Beginns der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
Ende der Zertifikatsgültigkeit (GMT)	Anzeige des Endes der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
CRL-Verteilerpunkt	Anzeige der optionalen URL, von der aus Zertifikatssperrlisten (CRL) verteilt werden
Ausgestellt durch CA	Die Zertifizierungsstelle, die das Zertifikat signiert hat
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Antragsteller	Anzeige der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z.B. im Feld Land (C) DE für Deutschland)
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig
Daten des öffentl. Schlüssels	Öffentliche Schlüsseldaten des für die Verschlüsselung verwendeten Zertifikats
Länge des öffentl. Schlüssels	Wertebereich: 1024, 1536, 2048
Öffentlicher Schlüssel	Verschlüsselung mit Hilfe öffentlicher Schlüssel, die von einer dritten Partei nach dem X.509-Standard bestätigt werden. Die hohe Sicherheit wird dadurch garantiert, dass der Schlüssel zur Dechiffrierung nochmals individuell festgelegt werden muss und nur beim Anwender gespeichert ist.
Fingerabdruck	Der verwendete öffentliche Schlüssel sowie der Fingerabdruck werden hexadezimal dargestellt.

28.3.2.4 Sicherheit > Deployment- und Licensing-Client (DLSC) > DLSC CA -Zertifikat

Parameterbeschreibung der Registerkarten:

- **Zertifikatsinformationen**

Parameter	Beschreibung
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS.
Seriennummer des Zertifikats	Anzeige der festgelegten Seriennummer.
Seriennummer des Zertifikats (hex)	Anzeige der festgelegten Seriennummer im Hexadezimalformat.
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus. Wertebereich: sha256RSA, sha512RSA
Beginn der Zertifikatsgültigkeit (GMT)	Anzeige des Beginns der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
Ende der Zertifikatsgültigkeit (GMT)	Anzeige des Endes der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
CRL-Verteilerpunkt	Anzeige der optionalen URL, von der aus Zertifikatssperrlisten (CRL) verteilt werden.
Ausgestellt durch CA	Die Zertifizierungsstelle, die das Zertifikat signiert hat
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Antragsteller	Anzeige der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z.B. im Feld Land (C) DE für Deutschland).
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig.
Daten des öffentl. Schlüssels	Öffentliche Schlüsseldaten des für die Verschlüsselung verwendeten Zertifikats

Parameter	Beschreibung
Länge des öffentl. Schlüssels	Wertebereich: 1024, 1536, 2048
Öffentlicher Schlüssel	Verschlüsselung mit Hilfe öffentlicher Schlüssel, die von einer dritten Partei nach dem X.509-Standard bestätigt werden. Die hohe Sicherheit wird dadurch garantiert, dass der Schlüssel zur Dechiffrierung nochmals individuell festgelegt werden muss und nur beim Anwender gespeichert ist.
Fingerabdruck	Der verwendete öffentliche Schlüssel sowie der Fingerabdruck werden hexadezimal dargestellt.
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS.

28.3.2.5 Sicherheit > Signaling- und Payload-Encryption

Parameterbeschreibung der Registerkarten:

- **SPE Sicherheitseinstellungen ändern**

Parameter	Beschreibung
Minimale Länge des RSA-Schlüssels	Minimale Länge des RSA-Schlüssels in den Zertifikaten. Je größer dieser Wert ist, desto sicherer ist der Schlüssel Wertebereich: 512, 1024, 2048 Standard: 1024
Zertifikatüberprüfung	Schaltet die Zertifikatsprüfung komplett ein oder aus. Ein Abschalten der Zertifikatsprüfung wird nicht empfohlen. Standard: Ein
Subjectname überprüfen	Durch Überprüfen des Subjectname im Zertifikat eines Gateways kann dessen Identität überprüft werden. Der Subjectname enthält die IP-Adresse oder den DNS-Namen (DNS: Domain Name System) des jeweiligen Gateways Standard: deaktiviert
CRL-Überprüfung	Mit Hilfe einer Zertifikatssperrliste (CRL: Certificate Revocation List) kann festgestellt werden, ob ein Zertifikat gesperrt/widerrufen wurde und warum. Erklärt eine Zertifizierungsstelle (CA: Certificate Authority) ein Zertifikat für ungültig, trägt es dessen Seriennummer in seine Liste ein. Während der Zertifikatsüberprüfung kann diese Liste über das Internet bei der Zertifizierungsstelle abgefragt werden Standard: deaktiviert
Sichere Neuverhandlung erzwingen (RFC 5746)	Dieses Verfahren verbessert die Sicherheit bei der Neuverhandlung der Verschlüsselungsparameter von TLS-Verbindungen. Es kann nur eingesetzt werden, wenn es auf allen verbundenen Servern ebenfalls unterstützt wird. (OpenScape Business, OpenScape 4000 und OpenScape Voice unterstützen dieses verbesserte Verfahren, HiPath 3000 unterstützt es nicht). Standard: deaktiviert

Parameter	Beschreibung
Maximales Intervall für Schlüssel-Neuverhandlung (Stunden)	Dieses Intervall legt fest, wie lange ein bestimmter Schlüssel für die Verschlüsselung der Signalisierungs- und Nutzdaten verwendet werden soll. Nach Ablauf dieser Zeitdauer wird ein neuer Schlüssel festgelegt Wertebereich: 6 bis 48 Standard: 24

28.3.2.6 Sicherheit > Signaling- und Payload-Encryption > SPE-Zertifikat

Parameterbeschreibung der Registerkarte:

- **SPE Zertifikat und privaten Schlüssel importieren (Datei PKCS#12)**

Parameter	Beschreibung
Entschlüsselungspasswort	Eingabe des Kennworts, das bei der Erstellung der PKCS#12-Datei verwendet wurde.
Datei mit Zertifikat und privatem Schlüssel (PEM- oder PKCS#12-Format)	Auswahl der Datei, die die zu importierenden Zertifikats-Daten enthält.

28.3.2.7 Sicherheit > Signaling- und Payload-Encryption > SPE CA-Zertifikate

Es können z.B. von einer Kunden PKI-Zertifizierungsstelle (RA/CA) bis zu 16 vertrauenswürdige CA-Zertifikate einzeln importiert werden.

Parameterbeschreibung der Registerkarte:

- **Vertrauenswürdiges CA-Zertifikat (X.509 Datei) für SPE importieren**

Parameter	Beschreibung
Datei mit Zertifikat (PEM oder Binär-Format)	Auswahl der zu importierenden PEM- oder Binär-Datei.
CRL Distribution Point (CDP) Protokoll	Protokollauswahl für die CRL-Listen (Zertifikatswiderrufslisten) Wertebereich: LDAP oder HTTP
CDP (ohne z.B. ldap://)	Ein CDP ist eine optionale Zertifikatserweiterung. Ein empfangenes Zertifikat wird nur gegen die CRLs geprüft, für die der CDP konfiguriert wurde.

28.3.2.8 Sicherheit > VPN

Parameterbeschreibung der Registerkarten:

- **Allgemeine Informationen anzeigen**
- **Aktivieren der konfigurierten VPN-Tabellen**
- **Ipsec ein-/ausschalten**

Parameter	Beschreibung
Verschlüsselungsalgorithmen	Verwendete Verschlüsselungsalgorithmen Wertebereich: AES, 3DES
Hash-Algorithmen	Standardisierte kryptologische Hashfunktion zur Berechnung eines eindeutligen Prüfwerts (digitale Signatur) Wertebereich: MD5, SHA1, SHA2
Public-Key-Algorithmen	Asymetrisches Verschlüsselungsverfahren Wertebereich: RSA
Diffie-Hellman-Gruppen	Verfahren zum Austausch von Schlüssel Wertebereich: DH-Gruppe 2, DH-Gruppe 5
Schaltflächen	
Sofort aktivieren	Die VPN-Tabellen können aktiviert werden. Warnhinweise beachten!
Ipsec aktivieren / deaktivieren	IPsec kann aktiviert oder deaktiviert werden. Warnhinweise beachten!

28.3.2.9 Sicherheit > VPN > Lightweight CA

Parameterbeschreibung der Registerkarten:

- **CA-Zertifikat generieren**

Parameter	Beschreibung
Name des Zertifikats	Frei einzugebener Name des zu generierenden Zertifikates
Seriennummer des Zertifikats	Eingabe einer von Ihnen festgelegten Seriennummer. Die Nummer muss eine positive ganze Zahl sein.
Signatur-Algorithmus-Typ	Auswahl des für dieses Zertifikat zu verwendenden Signaturalgorithmus Wertebereich: sha25RSA, sha512RSA
Länge des öffentl. Schlüssels	Auswahl einer für dieses Zertifikat verwendeten Schlüssellänge Wertebereich: 2048
Beginn der Zertifikatsgültigkeit (GMT) Zeitpunkt, ab dem das Zertifikat gültig sein soll. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.	
Ende der Zertifikatsgültigkeit (GMT) Zeitpunkt, bis zu dem das Zertifikat gültig sein soll. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.	

Parameter	Beschreibung
Antragsteller	
Eingabe der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z.B. im Feld Land (C) DE für Deutschland).	
Alternativer Antragsteller	
Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und einem anderen Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.	
Format des DN-Namens	Dies wird normalerweise auch als Common Name RDN im Betreff des Hauptzertifikats angegeben.
Anderes Format	Andere Namen, als Allgemeiner Name angegeben
Erweiterung Alternativer Antragstellername	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.
CRL-Verteilungspunkt-Typ	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
CRL-Verteilerpunkt	Angabe einer URL, von der aus Zertifikatssperrlisten (CRL) verteilt werden.
Zertifikat erzeugen	

28.3.2.10 Sicherheit > VPN > Zertifikatsverwaltung

Parameterbeschreibung der Registerkarten:

- **Zertifikat aus Datei anzeigen**

Parameter	Beschreibung
PKCS#12-Format	Falls das Zertifikat in einer PKCS#12-Datei gespeichert ist, müssen Sie dieses Feld aktivieren.
Entschlüsselungspasswort	Wenn das Feld PKCS#12-Format aktiviert wurde, müssen Sie in diesem Feld das gleiche Kennwort angeben, das bei der Dateierstellung verwendet wurde.
Datei mit dem Zertifikat	Tragen Sie in diesem Feld den Pfad und den Dateinamen des Zertifikats ein. Klicken Sie auf Durchsuchen, falls Sie den Speicherort nicht genau kennen. Ein Suchdialog wird angezeigt.

28.3.2.11 Sicherheit > VPN > Zertifikatsverwaltung > Trusted CA Zertifikate > Aktive Zertifikate

Parameterbeschreibung der Registerkarte:

- **Trusted CA-Zertifikat importieren (X.509)**

Parameter	Beschreibung
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS
Seriennummer des Zertifikats	Anzeige der festgelegten Seriennummer.
Seriennummer des Zertifikats (hex)	Anzeige der festgelegten Seriennummer im Hexadezimalformat.
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus Wertebereich: sha256RSA, sha512RSA
Beginn der Zertifikatsgültigkeit (GMT)	Anzeige des Beginns der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
Ende der Zertifikatsgültigkeit (GMT)	Anzeige des Endes der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
CRL-Verteilerpunkt	Anzeige der optionalen URL, von der aus Zertifikatssperrlisten (CRL) verteilt werden
Ausgestellt durch CA	Die Zertifizierungsstelle, die das Zertifikat signiert hat
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Antragsteller	Anzeige der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z.B. im Feld Land (C) DE für Deutschland)
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig
Daten des öffentl. Schlüssels	Öffentliche Schlüsseldaten des für die Verschlüsselung verwendeten Zertifikats
Länge des öffentl. Schlüssels	Wertebereich: 1024, 1536, 2048

Parameter	Beschreibung
Öffentlicher Schlüssel	Verschlüsselung mit Hilfe öffentlicher Schlüssel, die von einer dritten Partei nach dem X.509-Standard bestätigt werden. Die hohe Sicherheit wird dadurch garantiert, dass der Schlüssel zur Dechiffrierung nochmals individuell festgelegt werden muss und nur beim Anwender gespeichert ist.
Fingerabdruck	Der verwendete öffentliche Schlüssel sowie der Fingerabdruck werden hexadezimal dargestellt.

28.3.2.12 Sicherheit > VPN > Zertifikatsverwaltung > Trusted CA Zertifikate > Konfigurierte Zertifikate

Parameterbeschreibung der Registerkarte:

- **Trusted CA-Zertifikat importieren (X.509)**

Parameter	Beschreibung
Name des Zertifikats	Eingabe des Namens, den das Zertifikat haben soll.
Datei mit dem Zertifikat	Pfad und Dateiname des Zertifikats. Beim Klicken auf "Durchsuchen" wird ein Suchdialog angezeigt, um den Speicherort der Datei zu finden.

28.3.2.13 Sicherheit > VPN > Peer-Zertifikate

Parameterbeschreibung der Registerkarten:

- **Zertifikatsanforderung (CSR) generieren**
- **Peer-Zertifikat importieren (PKCS#12)**

Parameter	Beschreibung
Name der Zertifikatsanforderung	Ein CA-signiertes Peer-Zertifikat (das auf einem CA-Zertifikat basiert) kann erzeugt werden. Voraussetzung ist, dass mindestens ein CA-Zertifikat generiert wurde. Das erzeugte Zertifikat wird in einer PKCS#12-Datei gespeichert. PKCS#12-Dateien (PKCS#12 Personal Information Exchange Syntax Standard) speichern Zertifikate mit dem privaten Schlüssel. Eine PKCS#12-Datei enthält also die entscheidenden Daten für persönliche Ver- und Entschlüsselung.
Signatur-Algorithmus-Typ	Wählen Sie den für dieses Zertifikat zu verwendenden Signaturalgorithmus aus. Wertebereich: sha25RSA, sha512RSA
Länge des öffentl. Schlüssels	Wertebereich: 2048
Antragsteller	Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 (z.B. im Feld Land (C) DE für Deutschland).
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname

Parameter	Beschreibung
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.
Format des DN-Namens	Dies wird normalerweise auch als Common Name RDN im Betreff des Hauptzertifikats angegeben.
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Anderes Format	Andere Namen, als Allgemeiner Name angegeben
Erweiterung Alternativer Antragstellername	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
Alternativer Antragstellername	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig.
Peer-Zertifikat importieren [PKCS#12]	
Name des Zertifikats	Eingabe des Namens, den das Zertifikat haben soll.
Entschlüsselungspasswort	Kennwort zur Entschlüsselung des Peer-Zertifikats Wertebereich: min. 7 und max. 32 Zeichen
Datei mit dem Zertifikat	Klicken Sie auf Durchsuchen. Ein Suchdialog wird angezeigt.
Fingerabdruck des Zertifikats anzeigen	Klicken Sie auf diese Schaltfläche, um die Integrität des Zertifikats zu überprüfen.
Zertifikat aus Datei importieren	Klicken Sie auf diese Schaltfläche, um ein Zertifikat zu importieren.

28.3.2.14 Sicherheit > VPN > Dienste > Aktive Dienste

Parameterbeschreibung der Registerkarte:

- **Ipsec-Dienste anzeigen**

Parameter	Beschreibung
Name des Dienstes	Dieses Feld enthält die Namen der konfigurierten Dienste.

Parameter	Beschreibung
Status im IP-Stack	
Quell-Port	Anzeige der Quell-Port-Nummer. Wird als Port die "0" angezeigt, so entspricht das einem beliebigen bzw. unbekannten Port.
Ziel-Port	Anzeige der Ziel-Port-Nummer. Wird als Port die "0" angezeigt, so entspricht das einem beliebigen bzw. unbekannten Port.
IP-Protokoll	Anzeige des für die Übertragung verwendeten IP-Protokolls.
Zugehörige 'pass'-Regel	Anzeige der zugehörigen "Pass"-Regel. Die Zuordnung von Regeln und Diensten erfolgt bei den Regeln.
Zugehörige 'deny'-Regel	Anzeige der zugehörigen "Deny"-Regel. Die Zuordnung von Regeln und Diensten erfolgt bei den Regeln.

28.3.2.15 Sicherheit > VPN > Dienste > Konfigurierte Dienste

Parameterbeschreibung der Registerkarten:

- **Ipsec-Dienste anzeigen**
- **Ipsec-Dienste hinzufügen**
- **Ipsec-Dienste ändern**
- **Ipsec-Dienste umbenennen**
- **Ipsec-Dienste löschen**

Parameter	Beschreibung
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten Dienstes. Geben Sie eine Zeichenkette in dieses Feld ein.
Quell-Port	Nummer des Ports, der für die Übertragung der Daten auf der Sendeseite verwendet werden soll. Wird als Port die "0" eingetragen, so entspricht das einem beliebigen bzw. unbekannten Port.
Ziel-Port	Nummer des Ports, der für die Übertragung der Daten auf der Empfängerseite verwendet werden soll. Wird als Port die "0" eingetragen, so entspricht das einem beliebigen bzw. unbekannten Port.
IP-Protokoll	Für die Übertragung zu verwendende IP-Protokoll Wertebereich: ICMP, TCP, UDP
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten Dienstes.
Quell-Port	Nummer des Ports, der für die Übertragung der Daten auf der Sendeseite verwendet werden soll. Wird als Port die "0" eingetragen, so entspricht das einem beliebigen bzw. unbekannten Port.
Ziel-Port	Nummer des Ports, der für die Übertragung der Daten auf der Empfängerseite verwendet werden soll. Wird als Port die "0" eingetragen, so entspricht das einem beliebigen bzw. unbekannten Port.
IP-Protokoll	Wählen Sie die für die Übertragung verwendete IP-Protokoll aus Wertebereich: ICMP, TCP, UDP

Parameter	Beschreibung
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten Dienstes.
	Löschen ist nur möglich wenn dem Dienst keine Regel zugeordnet ist.

28.3.2.16 Sicherheit > VPN > Tunnel > Aktive Tunnel

Parameterbeschreibung der Registerkarten:

- **Allgemeine Tunneldaten anzeigen**
- **Regeln für alle Tunnel anzeigen**

Parameter	Beschreibung
Name des Tunnels	Dieses Feld enthält den Namen des konfigurierten Tunnels.
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Endpunkttyp des lokalen Tunnel	Anzeige der Endpunktadresse auf der Tunnel-Sendeseite (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Anzeige der Endpunktadresse im lokalen Tunnel.
Endpunkttyp des Remote Tunnel	Anzeige des Endpunkttyps des Remote-Tunnels.
Endpunktadresse des Remote Tunnel	Anzeige der Empfängeradresse des Remote-Tunnels. Wird die Adresse 0.0.0.0 angezeigt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z. B. Teleworker).
Vorgeschlagene Lebensdauer der Session-Keys	Anzeige der akzeptierten Gültigkeitsdauer für die Sitzungsschlüssel (Session Keys), die verwendet werden. Nach Ablauf dieser Zeit werden keine Daten mehr innerhalb dieser Sitzung ausgetauscht. Als Ersatz für ungültig gewordene Sitzungsschlüssel werden automatisch neue Sitzungsschlüssel ausgehandelt.
Vorgeschlagene Lebensdauer der Schlüsseltausch-Session	Anzeige der akzeptierten Gültigkeitsdauer für die Schlüsseltausch-Session. Nach Ablauf der Schlüsseltausch-Session werden automatisch neue Schlüssel für die Schlüsseltausch-Session durch IKE (Verschlüsselungsprotokoll) ausgehandelt.
Zugehörige Regeln: **Zugehörige Senderegel**	Einrichtung der Senderegel unter VPN>Regeln
Zugehörige Regeln: **Zugehörige Empfangsregel**	Einrichtung der Empfangsregel unter VPN>Regeln
Tunneldaten	
Name des Tunnels	Dieses Feld enthält den Namen des konfigurierten Tunnels.
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv

Parameter	Beschreibung
Endpunkttyp des lokalen Tunnel	Anzeige der Endpunktadresse auf der Tunnel-Sendeseite (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Anzeige der Endpunktadresse im lokalen Tunnel.
Endpunkttyp des Remote Tunnel	Anzeige des Endpunkttyps des Remote-Tunnels.
Endpunktadresse des Remote Tunnel	Anzeige der Empfängeradresse des Remote-Tunnels. Wird die Adresse 0.0.0.0 angezeigt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z. B. Teleworker).
Regeldaten	
Zielstelle	Statusanzeige im Ziel. Wertebereich: Senden/Empfangen
Priorität	Anzeige der Priorität für die Abarbeitungsfolge. Die höchste Priorität wird mit 1 angegeben. Für jede Regel einer Richtung ist eine eigene Priorität zu vergeben. Eine Regel und die dazugehörige Regel der Gegenrichtung müssen stets die gleiche Priorität haben. Die Regel für die Gegenrichtung können Sie nur über den entsprechenden Menüpunkt einrichten.
Aktion für die Regel	Zeigt an, wie die IP-Pakete durch diese Regel behandelt werden: "pass" bedeutet, dass die IP-Pakete weitergeleitet werden; "deny" bedeutet, dass sie nicht weitergeleitet werden.
Verschlüsselung erforderlich	Anzeige einer Verschlüsselung für diese Regel. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	Statusanzeige in der Regel. Wertebereich: Aktiviert / Deaktiviert
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Quelladresse Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Anzeige ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.	
Type	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereiches)	Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Eingabemaske ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.

Parameter	Beschreibung
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/ Zieladressen erforderlich ist.
Zieladresse	
Type	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereiches)	Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Eingabemaske ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/ Zieladressen erforderlich ist.
Dienstdaten Anzeige des Dienstes, auf den die Verschlüsselung beschränkt wird. Soll die Verschlüsselung nicht auf einen Dienst beschränkt sein, wählen Sie "Beliebiger Dienst" aus.	
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten Dienstes.
Quell-Port	Anzeige des Tunnels in Empfangsrichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Wählen Sie Keine Tunnelzuordnung, falls in Empfangsrichtung kein Tunnel zugeordnet werden soll.
Ziel-Port	Anzeige des Tunnels in Senderichtung, für den diese Regel gilt. In diesen Tunnel werden die IP-Pakete, die zum Netz gesendet werden müssen, hineingeschickt. Wählen Sie Keine Tunnelzuordnung, falls in Senderichtung kein Tunnel zugeordnet werden soll.
IP-Protokoll	Wählen Sie die für die Übertragung verwendete IP-Protokoll aus Wertebereich: ICMP, TCP, UDP

28.3.2.17 Sicherheit > VPN > Tunnel > Konfigurierte Tunnel

Parameterbeschreibung der Registerkarten:

- **Allgemeine Tunneldaten anzeigen**
- **Regeln für alle Tunnel anzeigen**
- **Tunnel hinzufügen / Tunneldaten ändern**
- **Schlüsselaustauschdaten**

Parameter	Beschreibung
	Ein Tunnel bezeichnet einen Transport von verschlüsselten Datenpaketen zu einem fest definierten Endpunkt. Aktive Tunnel sind konfigurierte Tunnel nach einer Aktivierung der Konfiguration. Insgesamt lassen sich bis zu 256 Tunnel pro Gateway einrichten.

Parameter	Beschreibung
Name des Tunnels	Dieses Feld enthält den Namen des konfigurierten Tunnels.
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Endpunkttyp des lokalen Tunnel	Anzeige der Endpunktadresse auf der Tunnel-Sendeseite (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Anzeige der Endpunktadresse im lokalen Tunnel.
Endpunkttyp des Remote Tunnel	Anzeige des Endpunkttyps des Remote-Tunnels.
Endpunktadresse des Remote Tunnel	Anzeige der Empfängeradresse des Remote-Tunnels. Wird die Adresse 0.0.0.0 angezeigt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z. B. Teleworker).
Vorgeschlagene Lebensdauer der Session-Keys	Anzeige der akzeptierten Gültigkeitsdauer für die Sitzungsschlüssel (Session Keys), die verwendet werden. Nach Ablauf dieser Zeit werden keine Daten mehr innerhalb dieser Sitzung ausgetauscht. Als Ersatz für ungültig gewordene Sitzungsschlüssel werden automatisch neue Sitzungsschlüssel ausgehandelt.
Vorgeschlagene Lebensdauer der Schlüsseltausch-Session	Anzeige der akzeptierten Gültigkeitsdauer für die Schlüsseltausch-Session. Nach Ablauf der Schlüsseltausch-Session werden automatisch neue Schlüssel für die Schlüsseltausch-Session durch IKE (Verschlüsselungsprotokoll) ausgehandelt.
Zugehörige Regeln: **Zugehörige Senderegel**	Einrichtung der Senderegel unter VPN>Regeln
Zugehörige Regeln: **Zugehörige Empfangsregel**	Einrichtung der Empfangsregel unter VPN>Regeln
Tunneldaten	
Name des Tunnels	Dieses Feld enthält den Namen des konfigurierten Tunnels.
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Endpunkttyp des lokalen Tunnel	Anzeige der Endpunktadresse auf der Tunnel-Sendeseite (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Anzeige der Endpunktadresse im lokalen Tunnel.
Endpunkttyp des Remote Tunnel	Anzeige des Endpunkttyps des Remote-Tunnels.
Endpunktadresse des Remote Tunnel	Anzeige der Empfängeradresse des Remote-Tunnels. Wird die Adresse 0.0.0.0 angezeigt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z. B. Teleworker).

Parameter	Beschreibung
Regeldaten	
Zielstelle	Statusanzeige im Ziel. Wertebereich: Senden/Empfangen
Priorität	Anzeige der Priorität für die Abarbeitungsfolge. Die höchste Priorität wird mit 1 angegeben. Für jede Regel einer Richtung ist eine eigene Priorität zu vergeben. Eine Regel und die dazugehörige Regel der Gegenrichtung müssen stets die gleiche Priorität haben. Die Regel für die Gegenrichtung können Sie nur über den entsprechenden Menüpunkt einrichten.
Aktion für die Regel	Zeigt an, wie die IP-Pakete durch diese Regel behandelt werden: "pass" bedeutet, dass die IP-Pakete weitergeleitet werden; "deny" bedeutet, dass sie nicht weitergeleitet werden.
Verschlüsselung erforderlich	Anzeige einer Verschlüsselung für diese Regel. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	Statusanzeige in der Regel. Wertebereich: Aktiviert / Deaktiviert
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Quelladresse Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Anzeige ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.	
Type	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereiches)	Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Eingabemaske ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/ Zieladressen erforderlich ist.
Zieladresse	
Type	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).

Parameter	Beschreibung
Adresse (unterste des Bereiches)	Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Eingabemaske ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/ Zieladressen erforderlich ist.
Dienstdaten Anzeige des Dienstes, auf den die Verschlüsselung beschränkt wird. Soll die Verschlüsselung nicht auf einen Dienst beschränkt sein, wählen Sie "Beliebiger Dienst" aus.	
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten Dienstes.
Quell-Port	Anzeige des Tunnels in Empfangsrichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Wählen Sie Keine Tunnelzuordnung, falls in Empfangsrichtung kein Tunnel zugeordnet werden soll.
Ziel-Port	Anzeige des Tunnels in Senderichtung, für den diese Regel gilt. In diesen Tunnel werden die IP-Pakete, die zum Netz gesendet werden müssen, hineingeschickt. Wählen Sie Keine Tunnelzuordnung, falls in Senderichtung kein Tunnel zugeordnet werden soll.
IP-Protokoll	Für die Übertragung zu verwendende IP-Protokoll Wertebereich: ICMP, TCP, UDP
Name des Tunnels	Dieses Feld enthält den Namen des neu konfigurierten Tunnels.
Remote-Service über VPN ermöglichen: **(aktivierbar über Service-Code)**	Dieses Feld ankreuzen, wenn der VPN-Tunnel zur Fernadministration genutzt werden soll.
Endpunkttyp des lokalen Tunnel	Wählen Sie den Typ der Endpunktadresse auf der Tunnel-Sendeseite aus (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Tragen Sie die Senderadresse in dem zum Endpunkttyp passenden Format ein.
Endpunkttyp des Remote Tunnel	Typ der Endpunktadresse auf der Tunnel-Empfängerseite (Angabe der IP-Adresse unterstützt).
Endpunktadresse des Remote Tunnel	Empfängeradresse in dem zum Endpunkttyp passenden Format. Wird die Adresse 0.0.0.0 eingestellt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z. B. Teleworker).
Session-Key-Handhabung	Unter Session-Key-Handhabung wird das Verfahren für den Schlüsselaustausch eingetragen (Automatisch, mit dem IKE-Protokoll).
Vorgeschlagene Verschlüsselungsalgorithmen	Welche Algorithmen dürfen verwendet werden Wertebereich: AES, 3DES

Parameter	Beschreibung
Vorgeschlagene Hash-Algorithmen	Welche Hash-Algorithmen (Prüfalgorithmen) verwendet werden dürfen. Die ausgewählten Algorithmen werden vom Initiator der IKE-Aushandlung angeboten. Wertebereich: MD5, SHA1, SHA2
Vorgeschlagene Lebensdauer der Session-Keys	Gültigkeitsdauer für die Sitzungsschlüssel (Session Keys), die verwendet werden. Nach Ablauf dieser Zeit werden keine Daten mehr innerhalb dieser Sitzung ausgetauscht. Als Ersatz für ungültig gewordene Sitzungsschlüssel werden automatisch neue Sitzungsschlüssel ausgehandelt
Vorgeschlagene Lebensdauer der Schlüsseltausch-Session	Gültigkeitsdauer für die Schlüsseltausch-Session. Nach Ablauf der Schlüsseltausch-Session werden automatisch neue Schlüssel für die Schlüsseltausch-Session durch IKE ausgehandelt
Vorgeschlagene Datenvolumen der Session-Keys	Maximales Datenvolumen für die Sitzungsschlüssel (Session Keys). Nach Überschreiten des Datenvolumens wird automatisch ein neuer Session-Key mittels IKE ausgehandelt. Bei der Auswahl von "unbegrenzt" wird die Datenmenge nicht begrenzt
'Perfect Forward Secrecy' aktivieren	Es wird empfohlen, diese Option immer anzukreuzen, da hiermit ein verbesserter Sicherheitsmechanismus für den Datentransfer über den Tunnel aktiviert wird
Authentifizierungsverfahren für die VPN-Peers	Authentifizierungsverfahren für die VPN-Teilnehmer. Möglich sind digitale Signaturen (Authentifizierung über Zertifikate) und Pre-Shared Keys (Authentifizierung über selbstdefinierte manuelle Schlüssel)
Pre-Shared Key	Dieses Feld ist nur vorhanden, wenn das Authentifizierungsverfahren auf Pre-Shared Keys gesetzt ist. Hier ist das Kennwort einzutragen, das von den VPN-Teilnehmern an beiden Endpunkten des Tunnels verwendet werden muss. Es sollten mindestens 12 Zeichen verwendet werden
Wiederholung des Pre-Shared Key	Dieses Feld ist nur vorhanden, wenn das Authentifizierungsverfahren auf Pre-Shared Keys gesetzt ist.
Liste der CA-Zertifikate	Diese Optionen sind nur vorhanden, wenn das Authentifizierungsverfahren auf Digitale Signaturen gesetzt ist. Die VPN-Teilnehmer können jedes Zertifikat zur Authentifizierung verwenden, dass von einem der angekreuzten CA-Zertifikate ausgestellt (signiert) wurde
Vorgeschlagene Diffie-Hellman-Gruppen	Die VPN-Teilnehmer können jedes angekreuzte Verfahren zum Schlüsselaustausch verwenden

Anmerkung: Das Hinzufügen/Löschen eines VPN-Tunnels muss abschließend unter "VPN > Aktivieren der konfigurierten VPN-Tabellen" aktiviert werden.

28.3.2.18 Sicherheit > VPN > Regeln > Aktive Regeln

Parameterbeschreibung der Registerkarte:

- **Regeln anzeigen**

Parameter	Beschreibung
Priorität	Anzeige der Priorität für die Abarbeitungsfolge als Ziffer. Die höchste Priorität wird mit 1 angegeben. Für jede Regel einer Richtung ist eine eigene Priorität zu vergeben. Eine Regel und die dazugehörige Regel der Gegenrichtung müssen stets die gleiche Priorität haben.
Service	Anzeige des Dienstes, auf den die Verschlüsselung beschränkt wird. Ist die Verschlüsselung nicht auf einen Dienst beschränkt, so wird "Beliebiger Dienst" angezeigt.
Aktion für die Regel	Zeigt an, wie die IP-Pakete durch diese Regel behandelt werden: "pass" bedeutet, dass die IP-Pakete weitergeleitet werden; "deny" bedeutet, dass sie nicht weitergeleitet werden.
Verschlüsselung erforderlich	Anzeige der Verschlüsselung. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	Statusanzeige in der Regel. Wertebereich: Aktivierung / Deaktivierung
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: Aktivierung / Deaktivierung
Quelladresse	
Type	Anzeige des Typs für die Quelladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (unterste des Bereiches)	Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Eingabemaske ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/ Zieladressen erforderlich ist.
Zieladresse	
Type	Anzeige des Typs für die Zieladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (oberste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/ Zieladressen erforderlich ist.
Tunnel für die Verschlüsselung	
Tunnel auf der Empfangsseite	Anzeige des Tunnels in Empfangsrichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Anzeige: Keine Tunnelzuordnung (falls in Empfangsrichtung kein Tunnel zugeordnet wurde).

Parameter	Beschreibung
Tunnel auf der Sendeseite	Anzeige des Tunnels in Senderichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Anzeige: Keine Tunnelzuordnung (falls in Senderichtung kein Tunnel zugeordnet wurde).

28.3.2.19 Sicherheit > VPN > Regeln > Konfigurierte Regeln

Regeln legen fest, was mit einem IP-Paket geschehen soll. Die Regelaktion Pass bedeutet, dass das IP-Paket weitertransportiert (durchgelassen) wird. Die Regelaktion Deny bedeutet, dass das IP-Paket nicht weitertransportiert (ignoriert) wird. Es kann jeweils ausgewählt werden, ob das IP-Paket einen (verschlüsselten) VPN-Tunnel benutzt oder nicht. Das Kommunikationssystem kann 640 Regeln verwalten, davon sind 6 Regeln vorbelegt (Default-Regeln) und 634 frei zur Vergabe.

Parameterbeschreibung der Registerkarten:

- **Regeln anzeigen**
- **Regel hinzufügen**
- **Regel ändern**
- **Regel für Gegenrichtung hinzufügen**
- **Regel löschen**

Parameter	Beschreibung
Priorität	Anzeige der Priorität für die Abarbeitungsfolge als Ziffer. Die höchste Priorität wird mit 1 angegeben. Für jede Regel einer Richtung ist eine eigene Priorität zu vergeben. Eine Regel und die dazugehörige Regel der Gegenrichtung müssen stets die gleiche Priorität haben.
Service	Anzeige des Dienstes, auf den die Verschlüsselung beschränkt wird. Ist die Verschlüsselung nicht auf einen Dienst beschränkt, so wird "Beliebiger Dienst" angezeigt.
Aktion für die Regel	Zeigt an, wie die IP-Pakete durch diese Regel behandelt werden: "pass" bedeutet, dass die IP-Pakete weitergeleitet werden; "deny" bedeutet, dass sie nicht weitergeleitet werden.
Verschlüsselung erforderlich	Anzeige der Verschlüsselung. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	Statusanzeige in der Regel. Wertebereich: Aktiviert / Deaktiviert
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: Aktivierung / Deaktivierung
Quelladresse	
Type	Anzeige des Typs für die Quelladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name

Parameter	Beschreibung
Adresse (unterste des Bereiches)	Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Eingabemaske ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/ Zieladressen erforderlich ist.
Zieladresse	
Type	Anzeige des Typs für die Zieladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (oberste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/ Zieladressen erforderlich ist.
Tunnel für die Verschlüsselung	
Tunnel auf der Empfangsseite	Anzeige des Tunnels in Empfangsrichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Anzeige: Keine Tunnelzuordnung (falls in Empfangsrichtung kein Tunnel zugeordnet wurde).
Tunnel auf der Sendeseite	Anzeige des Tunnels in Senderichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Anzeige: Keine Tunnelzuordnung (falls in Senderichtung kein Tunnel zugeordnet wurde).

28.3.2.20 Sicherheit > VPN > Public Key Infrastructure (PKI)

Der PKI-Server bezeichnet einen Server, der digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI (Public Key Infrastruktur) ausgestellten Zertifikate werden zur Absicherung der Kommunikation verwendet. Über die vom PKI-Server konfigurierte PKI-URL wird bei Verwendung von Zertifikaten (digitalen Signaturen) versucht, die CRL herunterzuladen.

Parameterbeschreibung der Registerkarten:

- **PKI-Server anzeigen**
- **PKI-Server hinzufügen**

Parameter	Beschreibung
Name des PKI-Servers	Geben Sie einen leicht wiedererkennbaren Namen für den Server ein.
PKI-Servertyp	Wählen Sie die Aufgabe des Servers aus (möglich sind LDAP und Enrollment).

Parameter	Beschreibung
URL des PKI-Servers	Tragen Sie die URL des Servers ein (z.B.: LDAP://139.21.92.144:389).

28.3.2.21 Sicherheit > SSL > Zertifikatsgenerierung

Der Administrationszugriff erfolgt verschlüsselt über HTTPS unter Verwendung des TLS 1.2-Protokolls. Zertifikate dienen zur Authentifizierung der Verbindung. Standardmäßig wird ein selbstsigniertes Zertifikat verwendet. Zur Erhöhung der Sicherheit kann ein Kundenspezifisches Zertifikat von einer Zertifizierungsstelle (CA) verwendet werden. Das Kommunikationssystem authentifiziert sich gegenüber dem Admin-Client mit Hilfe der im WBM generierten oder importierten Zertifikate. Im Browser kann ein solches Zertifikat als vertrauliches Zertifikat importiert werden, um Warnmeldungen des Browsers beim Verbinden zum SSL-Server zu vermeiden.

Parameterbeschreibung der Registerkarten:

- **CA-Zertifikat generieren**
- **Selbstsigniertes Zertifikat generieren**

Parameter	Beschreibung
Name des Zertifikats	Name des zu generierenden Zertifikats.
Seriennummer des Zertifikats	Seriennummer für das Zertifikat. Die Nummer muss eine positive ganze Zahl sein
Signatur-Algorithmus-Typ	Zu verwendender Signaturalgorithmus Wertebereich: sha256RSA, sha512RSA
Länge des öffentl. Schlüssels	Wertebereich, Standardwert: 2048
Beginn der Zertifikatsgültigkeit (GMT) Zeitpunkt, ab dem das Zertifikat gültig sein soll. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.	
Tag, Monat, Jahr, Std., Min., S.	Einheiten für die Zeiteingabe der Zertifikatsgültigkeit
Ende der Zertifikatsgültigkeit (GMT) Zeitpunkt, bis zu dem das Zertifikat gültig sein soll. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.	
Tag, Monat, Jahr, Std., Min., S.	Einheiten für die Zeiteingabe der Zertifikatsgültigkeit
Antragsteller Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 (z.B. im Feld Land (C) DE für Deutschland). Alle vier Felder müssen ausgefüllt werden.	
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname

Parameter	Beschreibung
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Alternativer Antragsteller Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.	
Format des DN-Namens	Dies wird normalerweise auch als Common Name RDN im Betreff des Hauptzertifikats angegeben.
Anderes Format	Andere Namen, als Allgemeiner Name angegeben
Erweiterung Alternativer Antragstellername	(optional) Wertebereich, Standardwert: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform ResourceIndicator, Andere
Alternativer Antragstellername	
CRL-Verteilungspunkt-Typ	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
CRL-Verteilerpunkt	Hier kann (optional mit einer URL) die Stelle angegeben werden, von der aus Zertifikatssperrlisten (CRL) verteilt werden.

28.3.2.22 Sicherheit > SSL > Zertifikatsverwaltung

Parameterbeschreibung der Registerkarte:

- **Zertifikat aus Datei anzeigen**

Parameter	Beschreibung
PKCS#12-Format	Falls das Zertifikat in einer PKCS#12-Datei gespeichert ist, muss dieses Feld aktiviert sein.
Entschlüsselungspasswort	Wenn das Feld PKCS#12-Format aktiviert wurde, muss in diesem Feld das gleiche Kennwort angegeben sein, das bei der Dateierstellung verwendet wurde.
Datei mit dem Zertifikat	Eingabe von Pfad und den Dateinamen des Zertifikats. Ggf. auf Durchsuchen klicken, um den Speicherort zu definieren.

28.3.2.23 Sicherheit > SSL > Zertifikatsverwaltung > Server-Zertifikate

Parameterbeschreibung der Registerkarten:

- **Zertifikatsanforderung (CSR) generieren**
- **Server-Zertifikat importieren (PKCS#12)**
- **Zertifikat anzeigen**
- **Zertifikat löschen**
- **Zertifikat exportieren (X.509)**

- **Verlängertes Zertifikat importieren (X.509)**
- **Zertifikat aktivieren**

Parameter	Beschreibung
Name der Zertifikatsanforderung	Name des zu generierenden Zertifikats.
Signatur-Algorithmus-Typ	Für dieses Zertifikat zu verwendender Signaturalgorithmus Wertebereich: sha256RSA, sha512RSA
Länge des öffentl. Schlüssels	Wertebereich: 2048
Antragsteller Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 (z.B. im Feld Land (C) DE für Deutschland). Alle vier Felder müssen ausgefüllt werden.	
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Alternativer Antragsteller Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z.B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.	
Format des DN-Namens	Dies wird normalerweise auch als Common Name RDN im Betreff des Hauptzertifikats angegeben.
Anderes Format	Andere Namen, als Allgemeiner Name angegeben
Erweiterung Alternativer Antragstellername	(optional) Wertebereich, Standardwert: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
Alternativer Antragstellername	(optional)
Name des Zertifikats	Name des zu importierenden Zertifikats .
Entschlüsselungspasswort	Kennwort, das bei der Dateierstellung verwendet wurde. Wertebereich: 7 bis 32 Zeichen
Datei mit dem Zertifikat	Im Feld **Datei mit dem Zertifikat** kann das gewünschte Zertifikat eingegeben werden oder über das Feld Durchsuchen ausgewählt werden. Zuerst muss der **Fingerabdruck** des Zertifikats angezeigt werden, dann kann es importiert werden.

28.3.2.24 Sicherheit > Web Sicherheit

Parameterbeschreibung der Registerkarte:

- **Web-Zugriffsfilter**

Parameter	Beschreibung
Web-Clients	Nur in Verbindung mit UC Suite: Aktivieren und Deaktivieren des Web-Zugriffs durch Mobiltelefone und mobile Applikationen (myPortal for Mobile/Tablet, myPortal to go, Application Launcher und 3rd party Applikationen via Web Service) Info: Nutzung von Web Clients in Verbindung mit UC Smart über Experten-Modus > Applikationen > UC Smart > Grundeinstellungen
Zugriff per HTTPS	Nur verschlüsselte Verbindungen erlaubt.
Zugriff per HTTP	Unverschlüsselte Verbindungen erlaubt.
Anmeldedaten im Endgerät speichern	Wenn aktiviert, müssen Anmeldedaten nicht bei jedem Start der Applikation eingegeben werden

28.3.2.25 Sicherheit > SQL Sicherheit

Parameterbeschreibung der Registerkarte:

- **SQL-Zugangskennwort**

Parameter	Beschreibung
Neu generieren	Es wird ein verschlüsseltes SQL-Passwort erstellt, das der Benutzer nicht kennt.
Default aktivieren	Das Standard-SQL-Passwort wird aktiviert.

28.3.3 Netzwerkschnittstellen

Unter **Netzwerkschnittstellen** sind Funktionen zusammengefasst, wie z.B. die Konfiguration der einzelnen LAN-Schnittstellen. Die Schnittstellen können unabhängig voneinander konfiguriert werden.

28.3.3.1 Netzwerkschnittstellen > Mainboard > Host-Name

Parameterbeschreibung der Registerkarten:

- **Host-Name ändern**

Parameter	Beschreibung
Host-Name	Host-Name des Kommunikationssystems - frei wählbar. Beispiel: `commsystem` Sind Name und IP-Adresse des Kommunikationssystems in einem DNS-Server hinterlegt, kann eine Namensauflösung erfolgen. Der Name des Kommunikationssystems setzt sich zusammen aus Host-Name und Domänen-Name. Beispiel: `commsystem.mynet.home`

28.3.3.2 Netzwerkschnittstellen > Hauptplatine > LAN 1 (WAN)

Parameterbeschreibung der Registerkarten:

- **LAN 1-Modus anzeigen**
- **LAN 1-Schnittstelle bearbeiten**
- **ACD bearbeiten**

Parameter	Beschreibung
Internet Service Provider-Auswahl	Auswahl, um festzulegen, wie der Zugriff auf einen ISP (Internet Service Provider) über die WAN-Schnittstelle erfolgt.
Internet Service Provider-Auswahl: Nicht konfiguriert oder deaktiviert	Die WAN-Schnittstelle wird nicht verwendet.
Internet Service Provider-Auswahl: LAN-Verbindungstyp TCP/IP	Die WAN-Schnittstelle dient dem Zugriff auf einen ISP, der bereits in einem externen Internetrouter konfiguriert ist. Das Kommunikationssystem und der Internetrouter müssen sich nicht im selben LAN-Segment befinden, sondern die WAN-Schnittstelle muss mit dem LAN-Segment des Internetrouters verbunden sein.
Internet Service Provider-Auswahl: T-Online, T-DSL Business, …	Das Kommunikationssystem fungiert als Internetrouter. Die WAN-Schnittstelle wird für den Zugriff auf einen vorkonfigurierten ISP verwendet.
Internet Service Provider-Auswahl: Anbieter-PPPoE	Das Kommunikationssystem fungiert als Internetrouter. Die WAN-Schnittstelle wird für den Zugriff auf einen ISP über PPPoE verwendet. PPPoE ist das am häufigsten von DSL-Modems verwendete Protokoll.
Internet Service Provider-Auswahl: Anbieter-PPTP	Das Kommunikationssystem fungiert als Internetrouter. Die WAN-Schnittstelle wird für den Zugriff auf einen ISP über PPTP verwendet. Diese Variante ist zum Beispiel in Österreich üblich.
Internetzugang über einen externen Router	Der Zugriff auf das Internet erfolgt über einen externen Router. Diese Flagge wird intern vom **Internetkonfigurationsassistenten** erwendet und sollte nicht geändert werden.
Automatische Adresskonfiguration (über DHCP)	Ein externer DHCP-Server (evtl. der DHCP-Server des Internetrouters) weist dem Kommunikationssystem eine IP-Adresse zu.
IP-Adresse des Standardrouters annehmen	Der externe DHCP-Server übermittelt die IP-Adresse des Standardrouters (z.B. des Internetrouters) an das Kommunikationssystem.

Parameter	Beschreibung
IP Adresse des DNS Servers annehmen	Der externe DHCP-Server übermittelt die IP-Adresse des DNS-Servers an das Kommunikationssystem.
IP Adresse des SNTP Servers annehmen	Der externe DHCP-Server übermittelt die IP-Adresse des SNTP-Servers an das Kommunikationssystem.
IP-Adresse	IP Adresse des LAN Servers annehmen.
Subnetzmaske:	Netzmaske des LAN-Segments.
MAC-Adresse	Zeigt die MAC-Adresse der LAN-Schnittstelle an.
Ethernet-Link-Modus	WAN-Schnittstellenmodus.
Ethernet-Link-Modus: Auto	Automatisches Umschalten zwischen 100 und 1000 Mbps Vollduplex-Modus.
Ethernet-Link-Modus: 100HDX	100 Mbps, Vollduplex.
Ethernet-Link-Modus: 100FDX	100 Mbps, Vollduplex.
Ethernet-Link-Modus: 1000FDX	1000 Mbps, Vollduplex.
NAT	NAT (Network Address Translation) ist eingeschaltet. Diese Aufgabe wird in der Regel bereits vom externen Router übernommen.
Bandbreitensteuerung für Sprachverbindungen	Dieses Feld aktiviert die Bandbreitensteuerung für Sprachverbindungen.
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.
Verwendete Bandbreite für Sprache/Fax (%)	Prozentsatz der verfügbaren Bandbreite für Sprach-/Faxverbindungen. Wertebereich, Standardwert: 0 - 100, 80
IEEE802.1p/q Tagging	Ist dieses Kontrollkästchen aktiviert, wird zu Priorisierungszwecken ein "Diensttyp" in die Ethernet-Pakete (Layer 2) aufgenommen. Die Option ist standardmäßig deaktiviert.
IEEE802.1p/q VLAN ID	Geben Sie die ID des VLANs ein, wenn der verwendete Switch Probleme mit dem Standardwert "0" hat.
Layer 2 QoS-Klasse	
Signaldaten	Prioritätsklasse für den Verbindungsaufbau. 0 = niedrigste Priorität / 7 = höchste Priorität. Wertebereich, Standardwert: 0 - 7, 3
Fax-/Modem-Nutzlast	Prioritätsklasse für die Fax- und Modem-Daten der IP-Verbindung. 0 = niedrigste Priorität / 7 = höchste Priorität. Wertebereich, Standardwert: 0 - 7, 5

Parameter	Beschreibung
Netzwerksteuerung	Prioritätsklasse für die Netzwerksteuerungsdaten (z. B. Übertragung von SNMP-Traps). 0 = niedrigste Priorität / 7 = höchste Priorität. Wertebereich, Standardwert: 0 - 7, 0
Sprachnutzlast	Prioritätsklasse für die Sprachdaten der IP-Verbindung. 0 = niedrigste Priorität / 7 = höchste Priorität. Wertebereich, Standardwert: 0 - 7, 5
Internetzugangsdaten für…	
Verbindungs-ID / Benutzername / T-Online-Nummer / Unterbenutzernummer / Suffix / Internetzugangskonto / DSL-Login …	Zugangsdaten des Internet Service Providers.
CHAP-Kennwort	Passwort für den Zugang zum Internet Service Provider.
Passwort erneut eingeben	Passwort für den Zugang zum Internet Service Provider.
IP-Parameter	
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des ISP-Servers, wenn der ISP eine statische IP-Adresse verwendet.
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die von Ihrem ISP für den Internetzugang zugewiesen wurde.
IP-Adressenverhandlung	Auswahl, um festzulegen, wie die Verbindungspartner die IP-Adresse beim Verbindungsaufbau verhandeln sollen.
IP-Adressenverhandlung: konfigurierte IP-Adresse	Nur die konfigurierte IP-Adresse ist möglich.
IP-Adressenverhandlung: akzeptiert jede IP-Adresse	Jede vom Partner vorgeschlagene Adresse wird akzeptiert.
IP-Adressenverhandlung: neue IP-Adresse anfordern	Bei jeder Verbindung wird eine neue IP-Adresse angefordert.
DNS-Anfrage	
Internetzugang mit DNS-Anfrage	Der DNS-Server wird automatisch ermittelt.
IP-Adresse des primären DNS-Servers	Ein spezieller DNS-Server wird ausgewählt.
Allgemeine PPP-Parameter	
Standardrouter	Die hier erstellte PPP-Verbindung wird als Routing-Ziel verwendet.
IP-Header-Komprimierung	Der TCP-Header ist komprimiert. UDP- und RTP-Header werden immer komprimiert.

Parameter	Beschreibung
LCP-Echo-Anfrage senden	Eine LCP-Echo-Anfrage wird gesendet. Mit dieser Funktion wird überprüft, ob die Verbindung noch aktiv ist.
Automatische PPP-Wiederverbindung	Die PPP-Verbindung wird nach einem Verbindungsabbruch automatisch wiederhergestellt (z.B. bei ISP-Zugang mit Flatrate und erzwungener Trennung nach 24-Stunden).
PPTP-Parameter	
Lokale IP-Adresse der Steuerverbindung	IP-Adresse, die von Ihrem ISP für die PPTP-Verbindung zugewiesen wurde.
Remote-IP-Adresse der Steuerverbindung	IP-Adresse des Servers Ihres ISP für die PPTP-Verbindung.
Remote-Subnetzmaske für die Steuerverbindung	Subnetzmaske, die von Ihrem ISP für die PPTP-Verbindung zugewiesen wurde.
Kurzer Halt	
Kurzer Halt	Für die PPP-Verbindung ist die Betriebsart "Kurzer Halt" eingeschaltet. Der folgende Eintrag ist nur möglich, wenn der Short-Hold-Modus aktiviert ist.
Kurze Haltezeit (Sek)	Dauer ohne Datenübertragung, nach der die PPP-Verbindung gelöscht werden soll. Der Kurzhaltetimer wird nur von ausgehenden Paketen ausgelöst. Wertebereich, Standardwert: 10 - 9999, 60
Authentifizierung	
PPP-Authentifizierung	PPP-Authentifizierung ist aktiviert. Die Einstellung muss gemäß den Vorgaben des ISP erfolgen.
PPP-Benutzername	Frei auswählbarer Benutzername zur Authentifizierung über PAP oder CHAP.
PAP-Authentifizierungsmode	Aktivierung und Art der PAP-Authentifizierung für die PPP-Verbindung: Nicht verwendet, PAP-Client, PAP-Host.
PAP-Kennwort	Passwort für PAP-Authentifizierung.
CHAP-Authentifizierungsmode	Aktivierung und Art der CHAP-Authentifizierung für die PPP-Verbindung: Nicht verwendet, CHAP-Client, CHAP-Host, CHAP-Client und -Host.
CHAP-Kennwort	Passwort für CHAP-Authentifizierung.
Datenkomprimierung	
DEFLATE - Datenkomprimierung	Für die Komprimierung von PPP Datenpaketen mit dem Komprimierungsalgorithmus DEFLATE.
COMPRESS-Datenkomprimierung	Für die Komprimierung von PPP Datenpaketen mit dem Komprimierungsalgorithmus COMPRESS.
Address Translation	
NAT	NAT (Network Address Translation) ist eingeschaltet. Die folgenden Protokolle werden unterstützt: TCP, UDP und ICMP (nur im passiven Modus).
Adresszuordnung	wird gelöscht.

Parameter	Beschreibung
Router-Einstellungen	
Vollzeitschaltung	Je nach Tarifmodell kann die Vollzeitschaltung (permanente Verbindung) zum ISP aktiviert oder deaktiviert werden. Die Vollzeitschaltung sollte für ein zeitbasiertes Tarifmodell deaktiviert und für ein Pauschaltarifmodell aktiviert werden.
Kurze Haltezeit (Sek)	Ist Vollzeitschaltung deaktiviert (zeitbasiertes Tarifmodell), geben Sie die Dauer der Inaktivität ein, nach der die Verbindung abgebrochen werden soll (z. B. 60 Sekunden). Wertebereich, Standardwert: 10 - 9999, 60
Erzwungene Trennung um (Stunde:min)	Ist Vollzeitschaltung aktiviert (Pauschaltarifmodell), geben Sie den Zeitpunkt an, zu dem die Internetverbindung deaktiviert werden soll (z. B. 04:59).
Verbindungszeit	Zeigt die verstrichene Verbindungszeit in Tagen-Stunden-Minuten-Sekunden an.
QoS-Parameter der Schnittstelle	
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.
Bandbreitensteuerung für Sprachverbindungen	Die Bandbreitensteuerung verhindert, dass die verfügbaren Übertragungsraten mit Sprachverbindungen innerhalb einer Multilink-Verbindung überbucht werden. Mit anderen Worten, wenn Header-Komprimierung aktiv ist, sind maximal 5 Sprachverbindungen über einen B-Kanal zulässig. Dieses Feld aktiviert die Bandbreitensteuerung für Sprachverbindungen. Dabei werden nur Sprachverbindungen mit den im Sprachgateway konfigurierten Routen berücksichtigt.
Verwendete Bandbreite für Sprache/Fax (%)	Prozentsatz der verfügbaren Bandbreite für Sprach-/Faxverbindungen. Wertebereich, Standardwert: 0 - 100, 80

Parameterbeschreibung der Registerkarten:

- **ACD bearbeiten**

Parameter	Beschreibung
Verbindungszeit	Zeigt die verstrichene Verbindungszeit in Tagen-Stunden-Minuten-Sekunden an.
Wiederverbindung erzwingen bei	Zeitpunkt, zu dem die Verbindung gelöscht und wiederhergestellt werden soll.
ACD aktivieren	Aktivieren Sie die automatische Deaktivierung, um eine Unterbrechung der Verbindung durch den ISP zu einem ungünstigen Zeitpunkt zu verhindern.

28.3.3.3 Netzwerkschnittstellen > Mainboard > LAN 2

Parameterbeschreibung der Registerkarten:

- **LAN 2-Schnittstelle bearbeiten**

Parameter	Beschreibung
Internetzugang über einen externen Router	Der Zugang zum Internet erfolgt über einen externen Router.
Schnittstelle aktiviert	Die LAN-Schnittstelle ist aktiviert.
IP-Adresse	IP-Adresse des Kommunikationssystems.
Netzmaske:	Netzmaske des LAN-Segments, in dem sich das Kommunikationssystem befindet.
MAC-Adresse	Anzeige der MAC-Adresse des Kommunikationssystems.
Ethernet-Link-Modus	Modus der LAN-Schnittstelle.
Ethernet-Link-Modus: **Auto**	Automatisches Umschalten zwischen 100 und 1000 Mbit/s Vollduplex-Betrieb. In diesem Modus kann das Power-Management aktiviert werden. Nach der Migration auf V2R3 oder höher muss für die gewünschte Ethernet-Verbindung über die Netzwerkschnittstellenseite oben auf "Übernehmen" gedrückt werden, damit der Wert auf "Auto" gesetzt wird. Anderenfalls müssen die Systeme vor der Migration auf "Auto" oder 100 gesetzt werden.
Ethernet-Link-Modus: **100HDX**	100 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: **100FDX**	100 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: **1000FDX**	1000 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
IEEE802.1p/q-Tagging	Ist dieses Kontrollkästchen aktiviert, so wird in den Ethernet-Paketen (Layer 2) ein "Type of Service" zur Priorisierung mitgegeben. Die Option ist standardmäßig ausgeschaltet.
IEEE802.1p/q-VLAN-ID	Die ID-Nummer des VLAN, ist nur anzugeben, falls der verwendete Switch Probleme mit dem Standardwert „0“ hat.
Layer 2-QoS-Klasse	
Signalisierungsdaten	Prioritätsklasse für den Verbindungsaufbau. 0 = geringste Priorität / 7= höchste Priorität. Wertebereich, Standardwert: 0 - 7, 3
Fax/Modem-Payload	Prioritätsklasse für die Fax- und Modemdaten der IP-Verbindung. 0 = geringste Priorität / 7= höchste Priorität. Wertebereich, Standardwert: 0 - 7, 5
Netzwerksteuerung	Prioritätsklasse für die Daten der Netzwerksteuerung (z.B. Übermittlung von SNMP-Traps). 0 = geringste Priorität / 7= höchste Priorität. Wertebereich, Standardwert: 0 - 7, 0

Parameter	Beschreibung
Sprach-Payload	Prioritätsklasse für die Sprachdaten. 0 = geringste Priorität / 7= höchste Priorität. Wertebereich, Standardwert: 0 - 7, 5

28.3.3.4 Netzwerkschnittstellen > Mainboard > LAN 3 (Admin)

Parameterbeschreibung der Registerkarten:

- **LAN 3-Schnittstelle bearbeiten**

Parameter	Beschreibung
Schnittstelle aktiviert	Die LAN-Schnittstelle ist aktiviert.
Automatische Adresskonfiguration (mit DHCP)	Ein externer DHCP-Server weist dem Kommunikationssystem eine IP-Adresse zu.
IP-Adresse des Default Routers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des Default-Routers (z.B. Internet-Router) mit.
IP-Adresse des DNS-Servers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des DNS-Servers mit.
IP-Adresse des SNTP-Servers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des SNTP-Servers mit.
IP-Adresse	IP-Adresse der LAN-Schnittstelle.
Netzmaske:	Netzmaske des LAN-Segments.
MAC-Adresse	Anzeige der MAC-Adresse der LAN-Schnittstelle.
Ethernet-Link-Modus	Modus der LAN-Schnittstelle.
Ethernet-Link-Modus: **Auto**	Automatisches Umschalten zwischen 100 und 1000 Mbit/s Vollduplex-Betrieb.
Ethernet-Link-Modus: **100HDX**	100 Mbit/s, Vollduplex.
Ethernet-Link-Modus: **100FDX**	100 Mbit/s, Vollduplex.
Ethernet-Link-Modus: **1000FDX**	1000 Mbit/s, Vollduplex.

28.3.3.5 Netzwerkschnittstellen > Mainboard > FTP-Server

Parameterbeschreibung der Registerkarten:

- **FTP-Server Parameter ändern**

Parameter	Beschreibung
FTP-Server freigeben	Ist das Kontrollkästchen aktiviert, ist der interne FTP-Server freigegeben.
Download-Nutzer 'Phone'	
Name	Name für den Zugang der IP-Telefone zum FTP-Server, um aktuelle Software-Updates herunterladen zu können. Der Name kann nicht geändert werden.
Neues Kennwort	Kennwort für den Zugang der IP-Telefone zum FTP-Server. Wird das vordefinierte Kennwort geändert, muss das Kennwort auch an den IP-Telefonen geändert werden.
Kennwort bestätigen	Kennwort für den Zugang der IP-Telefone zum FTP-Server.
Download-Nutzer 'FTP_Admin'	
Name	Name für den Zugang des Administrators zum FTP-Server. Der Name kann nicht geändert werden.
Neues Kennwort	Kennwort für den Zugang des Administrators zum FTP-Server.
Kennwort bestätigen	Kennwort für den Zugang des Administrators zum FTP-Server.

28.3.3.6 Netzwerkschnittstellen > Mainboard > DHCP Modus

Parameterbeschreibung der Registerkarten:

- **DHCP Mode ändern**

Parameter	Beschreibung
Kein DHCP	Ist das Optionsfeld aktiviert, ist der interne DHCP-Server ausgeschaltet.
DHCP-Server	Ist das Optionsfeld aktiviert, ist der interne DHCP-Server eingeschaltet.
DHCP Relay-Agent	Ist das Optionsfeld aktiviert, fungiert das Kommunikationssystem als DHCP-Relay-Agent. Die DHCP-Anfragen der IP-Teilnehmer werden vom Kommunikationssystem an den eigentlichen DHCP-Server weitergeleitet. DHCP-Server und IP-Teilnehmer müssen sich nicht im selben Netzwerksegment befinden.

28.3.3.7 Netzwerkschnittstellen > Hauptplatine > DHCP-Modus > DHCP-Server > Globale Parameter

Die netzwerksspezifischen Daten werden vom DHCP-Server an die IP-Stationen übertragen.

Parameterbeschreibung der Registerkarten::

- **Globale Parameter ändern**

Parameter	Beschreibung
DHCP-Server aktivieren	Gibt an, dass der interne DHCP-Server aktiviert ist und seine globalen Parameter konfiguriert werden können. Kann nicht geändert werden.

Parameter	Beschreibung
Nur Mitel-/Unify-Geräte	Gibt an, dass der interne DHCP-Server nur Anfragen von Mitel- und Unify Phone-Geräten akzeptiert. Wenn der Client mehr als eine Antwort erhält, z. B. vom OpenScape Business DHCP-Server und von einem anderen Server im Netzwerk, bevorzugt er die Antwort, die von OpenScape Business empfangen wird, wenn kompatible Geräte verwendet werden: • OpenScape DeskPhone CP x00 mit Software-Release V1R8.4.0 (HFA) / V1R11.6.0 (SIP) oder höher • OpenScape DeskPhone CP x10 mit Software Release V2R0.18.0 (HFA oder SIP) oder höher • Mitel MiVoice 69xx / 68xx (SIP)
Subnetzmaske:	Die Subnetzmaske definiert die Größe des Subnetzes. Beispiel: `255.255.255.0`.
Broadcast-Adresse	Mit der Broadcast-Adresse können alle IP-Stationen eines Netzwerks oder Subnetzes vom DHCP-Server angesprochen werden (optional). Beispiel: `0.0.0.0`.
Standardgateway	
Gateway 1	IP-Adresse, unter der das Standardgateway erreicht werden kann. Wenn ein Internet-Router im Netzwerk verwendet wird, ist der Internetrouter das Standardgateway. Beispiel: `192.168.1.1`. Wenn das Kommunikationssystem direkt mit einem Internetmodem verbunden ist, ist das Kommunikationssystem das Standardgateway. Beispiel: `192.168.1.2`.
Gateway 2	IP-Adresse, unter der ein zweites Standardgateway (Router) erreicht werden kann (optional).
Gateway 3	IP-Adresse, unter der ein drittes Standardgateway (Router) erreicht werden kann (optional).
DNS-Server	
Domänenname	Domänenname des internen Netzwerks, max. 80 Zeichen, z. B. `mynet.home` (optional).
Server 1	IP-Adresse, unter der der DNS-Server erreicht werden kann. Wenn das Kommunikationssystem direkt mit einem Internetmodem verbunden ist, darf der Standardwert `0.0.0.0` nicht geändert werden. Das Kommunikationssystem verwendet es, um automatisch eine Verbindung mit einem DNS-Server aus dem Internet herzustellen. Ein externer DNS-Server kann ebenfalls eingegeben werden. Beispiel: der DNS-Server des Internetrouters (`192.168.1.1)` oder ein DNS-Server aus dem Internet (`google-public-dns-a.google.com`).
Server 2	IP-Adresse, unter der ein zweiter DNS-Server erreicht werden kann (optional).
Server 3	IP-Adresse, unter der ein dritter DNS-Server erreicht werden kann (optional).
Lease-Zeit in Stunden (0 unendlich)	Maximale Gültigkeitsdauer in Stunden, 0;unendliche Lebensdauer (Standard: 1 Stunde).

Parameter	Beschreibung
Dynamisches DNS-Update aktivieren	Wenn dieses Kontrollkästchen aktiviert ist, wird der DNS-Server möglicherweise dynamisch aktualisiert. Standard: Nicht aktiviert. **Anmerkung:** Wenn die Option Dynamische DNS-Aktualisierung aktiviert ist, ist es zwingend erforderlich, den **Domänennamen** im entsprechenden Feld für den IP-Adresspool zu konfigurieren.
Interne DLI verwenden	Wenn dieses Kontrollkästchen aktiviert ist, wird der interne DLI verwendet. Wenn das Kontrollkästchen deaktiviert ist, erscheinen die Parameter für einen externen DLS-Server. Standard: Aktiviert.
Externer DLS-Server	
IP-Adresse	IP-Adresse, unter der der externe DLS-Server erreicht werden kann.
Port	Port, über den der externe DLS-Server erreicht werden kann.

28.3.3.8 Netzwerkschnittstellen > Hauptplatine > DHCP-Modus > DHCP-Server > IP-Adresspools

Parameterbeschreibung der Registerkarten::

- **IP-Adresspools anzeigen**
- **IP-Adresspool hinzufügen**
- **IP-Adresspool bearbeiten**
- **IP-Adresspool löschen**

Parameter	Beschreibung
Subnetzadresse	Die Subnetzadresse definiert den maximalen IP-Adressbereich. Beispiel: `192.168.1.0`.
Subnetzmaske:	Die Subnetzmaske definiert die Größe des Subnetzes. Standardeinstellung: `255.255.255.0`.
Adressbereich	
Adressbereich 1	Untere und obere Grenzen des IP-Adressbereichs des Subnetzes. Beispiel: von `192.168.1.50` bis `192.168.1.254`.
Adressbereich 2	Untere und obere Grenzen eines zweiten IP-Adressbereichs innerhalb desselben Subnetzes (optional).
Adressbereich 3	Unter- und Obergrenzen eines dritten IP-Adressbereichs innerhalb desselben Subnetzes (optional).
Standardgateway	

Parameter	Beschreibung
Gateway 1	IP-Adresse, unter der das Standardgateway erreicht werden kann. Wenn ein Internet-Router im Netzwerk verwendet wird, ist der Internetrouter das Standardgateway. Beispiel: `192.168.1.1`. Wenn das Kommunikationssystem direkt mit einem Internetmodem verbunden ist, ist das Kommunikationssystem das Standardgateway. Beispiel: `192.168.1.2`.
Gateway 2	IP-Adresse, unter der ein zweites Standardgateway (Router) erreicht werden kann (optional).
Gateway 3	IP-Adresse, unter der ein drittes Standardgateway (Router) erreicht werden kann (optional).
Broadcast-Adresse	Mit der Broadcast-Adresse können alle IP-Stationen eines Netzwerks oder Subnetzes vom DHCP-Server angesprochen werden (optional). Standardwert: `0.0.0.0`.
Domänenname	Domänenname des internen Netzwerks, max. 80 Zeichen, z. B. `mynet.home` (optional).
DNS-Server	
Server 1	IP-Adresse, unter der der DNS-Server erreicht werden kann. Wenn das Kommunikationssystem direkt mit einem Internetmodem verbunden ist, darf der Standardwert `0.0.0.0` nicht geändert werden. Das Kommunikationssystem verwendet es, um automatisch eine Verbindung mit einem DNS-Server aus dem Internet herzustellen. Ein externer DNS-Server kann ebenfalls eingegeben werden. Beispiel: der DNS-Server des Internetrouters (`192.168.1.1)` oder ein DNS-Server aus dem Internet (`google-public-dns-a.google.com`).
Server 2	IP-Adresse, unter der ein zweiter DNS-Server erreicht werden kann (optional).
Server 3	IP-Adresse, unter der ein dritter DNS-Server erreicht werden kann (optional).
Verbesserte Sicherheit	
Relay-Option	Eine hexadezimale Zahl, die vom Administrator für zusätzliche Sicherheit konfiguriert wurde. Der Wert dieses Feldes ist standardmäßig leer, und diese Option wird nicht berücksichtigt, wenn sie nicht konfiguriert ist.
Lease-Zeit in Stunden (0 unendlich)	Maximale Gültigkeitsdauer in Stunden, 0;unendliche Lebensdauer (Standard: 1 Stunde).

28.3.3.9 Netzwerk-Schnittstellen > Hauptplatine > DHCP-Modus > DHCP-Server > Statische IP-Adressen

Parameterbeschreibung der Registerkarten::

- **Statische IP-Adresse anzeigen**
- **Statische IP-Adresse hinzufügen**
- **Statische IP-Adresse bearbeiten**

- **Statische IP-Adresse löschen**

Parameter	Beschreibung
Hostname	Name oder Beschreibung der IP-Station (z.B. PC oder Server), die eine feste IP-Adresse empfangen soll. Beispiel: `Druckserver`.
IP-Adresse	Gewünschte feste IP-Adresse. Beispiel: `192.168.1.10`.
Client-Kennung	MAC-Adresse der IP-Station ex. Mitel SIP-DECT RFP-Gerät.
Subnetzmaske:	Netzmaske des Subnetzes. Beispiel: `255.255.255.0`.
Standardgateway	
Gateway 1	IP-Adresse, unter der das Standardgateway erreicht werden kann. Wenn ein Internet-Router im Netzwerk verwendet wird, ist der Internetrouter das Standardgateway. Beispiel: `192.168.1.1`. Wenn das Kommunikationssystem direkt mit einem Internetmodem verbunden ist, ist das Kommunikationssystem das Standardgateway. Beispiel: `192.168.1.2`.
Standardgateway 1	IP-Adresse, unter der ein zweites Standardgateway (Router) erreicht werden kann (optional).
Standardgateway 1	IP-Adresse, unter der ein drittes Standardgateway (Router) erreicht werden kann (optional).
Broadcast-Adresse	Mit der Broadcast-Adresse können alle IP-Stationen eines Netzwerks oder Subnetzes vom DHCP-Server angesprochen werden (optional). Beispiel: `0.0.0.0`.
Domänenname	Domänenname des internen Netzwerks, max. 80 Zeichen, z. B. `mynet.home` (optional).
DNS-Server	
Server 1	IP-Adresse, unter der der DNS-Server erreicht werden kann. Wenn das Kommunikationssystem direkt mit einem Internetmodem verbunden ist, darf der Standardwert `0.0.0.0` nicht geändert werden. Das Kommunikationssystem verwendet es, um automatisch eine Verbindung mit einem DNS-Server aus dem Internet herzustellen. Ein externer DNS-Server kann ebenfalls eingegeben werden. Beispiel: der DNS-Server des Internetrouters (`192.168.1.1)` oder ein DNS-Server aus dem Internet (`google-public-dns-a.google.com`).
Server 2	IP-Adresse, unter der ein zweiter DNS-Server erreicht werden kann (optional).
Server 3	IP-Adresse, unter der ein dritter DNS-Server erreicht werden kann (optional).
Verbesserte Sicherheit	
Relay-Option	Eine hexadezimale Zahl, die vom Administrator für zusätzliche Sicherheit konfiguriert wurde.
Lease-Zeit in Stunden (0 unendlich)	Maximale Gültigkeitsdauer in Stunden, 0;unendliche Lebensdauer (Standard: 1 Stunde).

28.3.3.10 Netzwerkschnittstellen > Hauptplatine > DHCP-Modus > DHCP Server > Letzte aktive Leasing

Die von einem DHCP-Server zugewiesene IP-Adresse bleibt für eine IP-Station bis zum Ablauf der "Lease-Periode" gültig, auch wenn die IP-Station während dieser Zeit ausgeschaltet ist. Hier werden die letzten aktiven Zuweisungen angezeigt.

Parameterbeschreibung der Registerkarten::

- **Lease anzeigen**
- **Lease löschen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse, die der IP-Station vom DHCP-Server zugewiesen wird.
MAC-Adresse	MAC-Adresse der IP-Station, der eine IP-Adresse zugewiesen wurde.
Client-ID	Client-ID der IP-Station. Wenn die Client-ID nicht verfügbar ist, wird die MAC-Adresse der IP-Station angezeigt.
Hostname	Name oder Rufnummer der IP-Station, der eine IP-Adresse zugeordnet wurde.
Start der Lease	Startzeit der Zuweisung. Der IP-Station wird ab diesem Zeitpunkt eine IP-Adresse zugewiesen.
Ende der Lease	Endzeit der Zuweisung. Nach dieser Perode muss die IP-Station eine neue Anfrage für eine IP-Adresse senden.

28.3.3.11 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP Server > Alle Leases

Die von einem DHCP-Server zugewiesene IP-Adresse bleibt für einen IP-Teilnehmer so lange gültig wie es die "Lease-Dauer" vorsieht, auch wenn der IP-Teilnehmer zwischenzeitlich ausgeschaltet ist. Hier werden alle Zuweisungen angezeigt.

Parameterbeschreibung der Registerkarten:

- **Lease anzeigen**
- **Lease löschen**

Parameter	Beschreibung
IP-Adresse	Vom DHCP-Server zugewiesene IP-Adresse des IP-Teilnehmers.
MAC-Adresse	MAC-Adresse des IP-Teilnehmers, dem eine IP-Adresse zugwiesen wurde.
Client-ID	Client-ID des IP-Teilnehmers. Ist die Client-ID nicht verfügbar, wird die MAC-Adresse des IP-Teilnehmers angezeigt.
Hostname	Name oder Rufnummer des IP-Teilnehmers, dem eine IP-Adresse zugwiesen wurde.
Start der Lease	Startzeitpunkt der Zuweisung. Der IP-Teilnehmer hat ab diesem Zeitpunkt eine IP-Adresse zugewiesen bekommen.

Parameter	Beschreibung
Ende der Lease	Endzeitpunkt der Zuweisung. Danach startet der IT-Teilnehmer eine neue Anfrage nach einer IP-Adresse.

28.3.3.12 Netzwerkschnittstellen > Application Board > Host-Name

Parameterbeschreibung der Registerkarten:

- **Host-Name ändern**

Parameter	Beschreibung
Host-Name	Host-Name des Application Boards - frei wählbar. Beispiel: `applboard` Sind Name und IP-Adresse des Application Boards in einem DNS-Server hinterlegt, kann eine Namensauflösung erfolgen. Der Name des Application Boards setzt sich zusammen aus Host-Name und Domänen-Name. Beispiel: `applboard.mynet.home`

28.3.3.13 Netzwerkschnittstellen > Application Board > LAN 1

Parameterbeschreibung der Registerkarten:

- **LAN 1-Schnittstelle ändern**

Parameter	Beschreibung
Schnittstelle aktiviert	Ist dieses Kontrollkästchen aktiviert, ist die LAN 1-Schnittstelle des Application Boards aktiv.
Automatische Adresskonfiguration (mit DHCP)	Ist dieses Kontrollkästchen aktiviert, werden der LAN 1-Schnittstelle automatisch vom DHCP-Server die IP-Adresse und die Netzmaske zugewiesen. Zusätzlich kann gewählt werden, ob weitere netzwerkspezifische Parameter vom DHCP-Server übernommen werden.
IP-Adresse des Default Routers übernehmen	Ist dieses Kontrollkästchen aktiviert, wird vom DHCP-Server die IP-Adresse des Default Routers übernommen.
IP-Adresse des DNS-Servers übernehmen	Ist dieses Kontrollkästchen aktiviert, wird vom DHCP-Server die IP-Adresse des DNS-Servers übernommen.
IP-Adresse des SNTP-Servers übernehmen	Ist dieses Kontrollkästchen aktiviert, wird vom DHCP-Server die IP-Adresse des SNTP-Servers übernommen.
IP-Adresse	IP-Adresse, unter der das Application Board zu erreichen ist.
Netzmaske:	Netzmaske, unter der das Application Board zu erreichen ist.
MAC-Adresse	MAC-Adresse des Application Boards (nicht editierbar).
Ethernet-Link-Modus	Modus der LAN 1-Schnittstelle.
Ethernet-Link-Modus: **Auto**	Automatisches Umschalten zwischen 100 und 1000 Mbit/s Vollduplex-Betrieb. In diesem Modus kann das Power-Management aktiviert werden.

Parameter	Beschreibung
Ethernet-Link-Modus: **100HDX**	100 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: **100FDX**	100 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: **1000FDX**	1000 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.

28.3.3.14 Netzwerkschnittstellen > Application Board > LAN 2

Parameterbeschreibung der Registerkarten:

- **LAN 2-Schnittstelle ändern**

Parameter	Beschreibung
Schnittstelle aktiviert	Ist dieses Kontrollkästchen aktiviert, ist die LAN 2-Schnittstelle des Application Boards aktiv.
IP-Adresse	IP-Adresse, unter der das Application Board zu erreichen ist.
Netzmaske:	Netzmaske, unter der das Application Board zu erreichen ist.
MAC-Adresse	MAC-Adresse des Application Boards (nicht editierbar).
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Es sind Werte von 576 bis 1500 erlaubt.
Ethernet-Link-Modus	Modus die LAN 2-Schnittstelle.
Ethernet-Link-Modus: **Auto**	Vollduplex-Modus. In diesem Modus kann das Power-Management aktiviert werden.
Ethernet-Link-Modus: **100HDX**	100 Mbit/s Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: **100FDX**	100 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: **1000FDX**	1000 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
IEEE802.1p/q-Tagging	Ist dieses Kontrollkästchen aktiviert, wird das Ethernet-Format festgelegt, das vom Application Board gesendet wird. Die Option ist standardmäßig ausgeschaltet.
IEEE802.1p/q-VLAN-ID	Geben Sie als ID-Nummer des VLAN einen vom Standardwert "0" abweichenden Wert ein, wenn der verwendete Switch Probleme mit dem Standardwert "0" hat.
Layer 2-QoS-Klasse	
Signalisierungsdaten	Prioritätsklasse für den Verbindungsaufbau. 0 = geringste Priorität / 7= höchste Priorität.

Parameter	Beschreibung
Fax/Modem-Payload	Prioritätsklasse für die Fax- und Modemdaten der IP-Verbindung. 0 = geringste Priorität / 7= höchste Priorität.
Netzwerksteuerung	Prioritätsklasse für die Daten der Netzwerksteuerung (z.B. Übermittlung von SNMP-Traps). 0 = geringste Priorität / 7= höchste Priorität.
Sprach-Payload	Prioritätsklasse für die Sprachdaten der IP-Verbindung. 0 = geringste Priorität / 7= höchste Priorität.

28.3.4 Routing

Unter **Routing** werden die Routing-Tabellen verwaltet. In kleinen Netzen kann eine Routing-Tabelle auf jedem Router vom Administrator manuell gepflegt werden. In größeren Netzen wird diese Aufgabe mithilfe eines Protokolls automatisiert, das Routing-Informationen im Netz verteilt.

28.3.4.1 Routing > IP-Routing > Mainboard > Statische Routen

Das Kommunikationssystem unterstützt ausschließlich statische Routen. Statische Routen verbinden zwei IP-Geräte miteinander. Sie werden manuell angelegt.

Je nach Applikation ist es ggf. nötig, für das System (Mainboard) und die UC Booster Card (Application Board) unterschiedliche Routen einzustellen.

Parameterbeschreibung der Registerkarten:

- **Statische Routentabelle anzeigen**
- **Statische Route hinzufügen**
- **Statische Route ändern**
- **Statische Route löschen**

Parameter	Beschreibung
Route-Index	Der Route-Index wird automatisch vergeben und nur zur Information angezeigt. Er kann nicht geändert werden.
Route-Name	Name oder Beschreibung der statischen Route, frei wählbar.
Ziel-Netzwerk/Host	IP-Adresse des Zielnetzes.
Netzmaske:	Subnetzmaske des Zielnetzes.
Route-Gateway	IP-Adresse des nächsten Routers auf dieser Route oder IP-Adresse der lokalen oder entfernten Schnittstelle eines PSTN-Partners.

28.3.4.2 Routing > IP-Routing > Mainboard > Default Router

Je nach Applikation ist es ggf. nötig, für das System (Mainboard) und die UC Booster Card (Application Board) ein unterschiedliches Default-Routing einzustellen.

Parameterbeschreibung der Registerkarten:

- **Default Router ändern**

Parameter	Beschreibung
Default-Routing über	IP-Routing über einen Default Router aktivieren oder deaktivieren.
Keine Schnittstelle	IP-Routing über einen Default Router deaktiviert.
LAN	IP-Routing über einen Default Router aktiviert.
IP-Adresse des Default Routers	IP-Adresse des Default Routers, sofern im Feld **Default Routing über** als Schnittstelle **LAN** ausgewählt ist. Beispiel: IP-Adresse des Internet-Routers, `192.168.1.1`.

28.3.4.3 Routing > IP-Routing > Mainboard > DNS-Server

Sie können die IP-Adresse des DNS-Servers anzeigen und gegebenenfalls ändern. Die Einstellung ist für Trunking mit dynamischen IP-Adressen notwendig.

Parameterbeschreibung der Registerkarten:

- **DNS-Einstellungen ändern**

Parameter	Beschreibung
IP-Adresse des DNS-Servers	IP-Adresse, unter der der DNS-Server erreichbar ist. Ist das Kommunikationssystem direkt mit einem Internet-Modem verbunden, muss der Standardwert `0.0.0.0` nicht geändert werden. Das Kommunikationssystem verbindet sich so automatisch mit einem DNS-Server aus dem Internet. Es kann auch ein externer DNS-Server eingetragen werden. Beispiel: der DNS-Server des Internet-Routers (`192.168.1.1)` oder ein DNS-Server aus dem Internet (`google-public-dns-a.google.com`). Im Falle eines OpenScape Business S-Systems ist ein Systemneustart erforderlich, damit die Änderungen wirksam werden.

28.3.4.4 Routing > IP-Routing > Application Board > Statische Routen

Je nach Applikation ist es ggf. nötig, für das System (Mainboard) und die UC Booster Card (Application Board) unterschiedliche Routen einzustellen.

Parameterbeschreibung der Registerkarten:

- **Statische Routentabelle anzeigen**
- **Statische Route hinzufügen**
- **Statische Route ändern**

- **Statische Route löschen**

Parameter	Beschreibung
Route-Index	Der Route-Index wird automatisch vergeben und nur zur Information angezeigt. Er kann nicht geändert werden.
Route-Name	Name oder Beschreibung der statischen Route, frei wählbar (optional) Wertebereich: max. 35 Zeichen.
Ziel-Netzwerk/Host	IP-Adresse des Zielnetzes.
Netzmaske:	Subnetzmaske des Zielnetzes.
Route-Gateway	IP-Adresse des nächsten Routers auf dieser Route oder IP-Adresse der lokalen oder entfernten Schnittstelle eines PSTN-Partners.

28.3.4.5 Routing > IP-Routing > Application Board > Default Router

Je nach Applikation ist es ggf. nötig, für das System (Mainboard) und die UC Booster Card (Application Board) ein unterschiedliches Default-Routing einzustellen.

Parameterbeschreibung der Registerkarten:

- **Standard-Router ändern**

Parameter	Beschreibung
Default-Routing über	IP-Routing über einen Default Router aktivieren oder deaktivieren.
Keine Schnittstelle	IP-Routing über einen Default Router deaktiviert.
LAN	IP-Routing über einen Default Router aktiviert.
IP-Adresse des Default Routers	IP-Adresse des Default Routers, sofern im Feld Default Routing über als Schnittstelle LAN ausgewählt ist.

28.3.4.6 Routing > NAT

Sie können eine NAT-Regel für die Netzwerk-Adressübersetzung anzeigen, hinzufügen, ändern und löschen. Über den NAT-Tabelleneditor können Sie bequem alle vorhandenen und weitere NAT-Einträge für die Netzwerk-Adressübersetzung auf einmal bearbeiten.

Parameterbeschreibung der Registerkarten:

- **NAT hinzufügen**
- **NAT-Tabelleneditor**

Parameter	Beschreibung
NAT-Regel aktiv	
Beschreibung	
Lokale IP-Adresse	Lokale Zieladresse im LAN.

Parameter	Beschreibung
Lokaler Port	Lokale Port-Nummer des eingestellten Protokolls im LAN.
Globaler Port	Port-Nummer des eingestellten Protokolls.
Protokoll	Zu verwendendes Transportprotokoll. Das eingestellte Transportprotokoll gilt sowohl für die lokalen als auch für die globalen Adress-Angaben.
Protokoll: **TCP**	TCP (Transmission Control Protocol) TCP ist ein zuverlässiges, verbindungsorientiertes Protokoll für die Übertragung von IP-Paketen. Vor Übertragungsbeginn wird ein virtueller Kanal zwischen den beiden Endpunkten der Netzwerkverbindung aufgebaut. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP wird hauptsächlich in den Bereichen WorldWideWeb, E-Mail und Peer-to-Peer-Netzwerke eingesetzt. Zusätzlich wird es auch für die Rufsignalisierung bei der IP-Telefonie verwendet, da es die Eigenschaft besitzt, dass Datenverluste bei der Übertragung erkannt und automatisch behoben werden.
Protokoll: **UDP**	UDP (User Datagram Protocol) UDP ist ein einfaches, verbindungsloses Protokoll für die Übertragung von IP-Paketen. Vor Übertragungsbeginn wird kein virtueller Kanal wie bei TCP zur Gegenstelle aufgebaut, wodurch die PCs schneller mit dem Datenaustausch beginnen können. Zur Adressierung der Sprachpakete wird bei UDP die Portnummer des Dienstes mitgesendet, der die Daten erhalten soll. Es wird hauptsächlich im Bereich DNS und für die Sprachübertragung bei der IP-Telefonie eingesetzt. Da bei einem verbindungslosen Protokoll allerdings nicht kontrolliert wird, ob die Gegenstelle die Daten auch wirklich erhalten hat, kann dies zu Verlusten bei der Sprachübertragung führen.

28.3.4.7 Routing > PSTN

Mit diesen Parametern wird eine IP-Remote-Verbindung (DFÜ-Verbindung) über das klassische Telefonnetz eingerichtet.

Parameterbeschreibung der Registerkarten:

- **Globale PSTN-Daten ändern**

Parameter	Beschreibung
Router-Rufnummer (interne Rufnummer)	Durchwahl des Systems auswählen. Alle Anwendungen, die die Routerfunktion nutzen, sind unter dieser Durchwahl von außen erreichbar. Externe Routingpartner, die keine Rufnummer übermitteln, müssen jeweils andere Rufnummern benutzen. Diese Rufnummern werden als MSN konfiguriert.
Wahlwiederholung	
Anzahl Wahlwiederholungen	Wiederholungsversuche, die das System zum Aufbau einer Verbindung unternehmen soll. Wertebereich: 0 bis 255
Wahlwiederholungspause (s)	Pause zwischen den Wahlwiederholungen in Sekunden. Wertebereich: 1 - 1,.000

Parameter	Beschreibung
Scripting	
Kennung 1 für Scripting	Erster Teil der Kennung für die Anmeldung bei Internet-Providern. Der Internet-Provider fordert Einträge zu Host, Nutzer-Identifikation und ein Passwort, z.B Host=ERT005, Nutzer=KJUMBERT, Passwort=123456. Die Einträge sind wie folgt: Kennung 1 für Scripting: HOST:ERT005 - Host Kennung 2 für Scripting: USER:KJUMBERT - Neues Passwort für Scripting: PASSWORT:123456.
Kennung 2 für Scripting	Zweiter Teil der Kennung für die Anmeldung bei Internet-Providern.
Neues Passwort für Scripting	Kennwort für die Anmeldung bei Internet-Providern.

28.3.4.8 Routing > PSTN > PPP-Protokoll

Parameterbeschreibung der Registerkarten:

- **Laden über HTTP**

Parameter	Beschreibung
Laden	Das PPP-Logfile kann über HTTP geladen werden. Je nach Einstellung des Browsers wird angezeigt, ob das heruntergeladene Logfile gespeichert oder im Default-Editor geöffnet werden soll.

28.3.4.9 Routing > PSTN > PSTN-Partner

Parameterbeschreibung der Registerkarten:

- **PSTN-Partner hinzufügen**
- **PSTN-Partner anzeigen**
- **PSTN-Partner ändern**

Parameter	Beschreibung
Name des Partners	Name des PSTN-Partners. Folgende PSTN-Partner stehen zur Verfügung: • Default PSTN - nicht konfigurierbar • PSTN Partner 1: Default für CLA, Funktion umkonfigurierbar • PSTN Partner 2: Default für ISDN, Funktion umkonfigurierbar • PSTN Partner 3: Name und Funktion frei konfigurierbar • PSTN Partner 4: Name und Funktion frei konfigurierbar Wertebereich: 1 bis 14 Zeichen
Art der PSTN-Verbindung	Einrichten der PSTN-Anbindung: (Standardauswahl: Aktiviert).
Art der PSTN-Verbindung: Nicht konfiguriert	PSTN-Partner kann vorkonfiguriert werden. Ein Verbindungsaufbau über diesen PSTN-Partner wird mit dieser Einstellung jedoch verhindert.

Parameter	Beschreibung
Art der PSTN-Verbindung: Aktiv	PSTN-Partner ist aktiviert. Ein Verbindungsaufbau über diesen PSTN-Partner wird mit dieser Einstellung erlaubt.
Art der PSTN-Verbindung: DSL Fallback	Nutzung des DSL-Zugangs für die PSTN-Verbindung (Default Router ist der DSL-Zugang)
IP-Parameter	
IP-Adresse des PSTN-Partners	IP-Adresse des Host-PC auf der Gegenseite, zu dem die PSTN-Verbindung aufgebaut wird.
IP-Adresse der lokalen PSTN-Schnittstelle	IP-Adresse des lokalen Kommunikationssystems, die für die PSTN-Verbindung benutzt werden soll.
IP-Address-Aushandlung	Aushandlung der IP-Adresse zwischen den Verbindungspartnern beim Verbindungsaufbau.
IP-Adress-Aushandlung: **konfigurierte IP-Adresse nutzen**	Nur die konfigurierte IP-Adresse des PSTN-Partners wird akzeptiert.
IP-Adress-Aushandlung: **jede IP-Adresse akzeptieren**	Keine IP-Adress-Aushandlung
IP-Adress-Aushandlung: **neue IP-Adresse anfordern**	IP-Adresse wird ausgehandelt
Allgemeine PPP-Parameter	
Default-Router	Der hier eingerichtete PSTN-Partner soll nicht nur vorkonfiguriert, sondern als Routing-Ziel verwendet werden. Es kann nur einen Default-Router geben. Entweder ist dies ein DSL-Zugang oder der hier eingerichtete PSTN-Partner.
Internet-Zugang mit DNS-Abfrage	Der Zugang soll als Internetzugang benutzt werden. Es darf nur ein Internetzugang pro System aktiviert werden darf (entweder ein PSTN-Partner oder ein DSL-Zugang).
Service-Eintrag	Bei einem Ruf zur MSN des PSTN-Partners soll die Rufnummernüberprüfung ausgeschaltet sein. Der Service-Eintrag kann nur aktiviert werden, wenn der PSTN-Partner eine MSN-Nummer hat und eine PAP- oder CHAP-Authentifizierung aktiviert wurde.
MSN/Durchwahl (interne Rufnummer)	Konfiguration der MSN-Nummer. Übermittelt der Partner seine Rufnummer, so muss diese konfiguriert sein, sonst wird der Ruf abgewiesen. Sind hingegen Rufnummern des Partners konfiguriert, aber der Partner übermittelt keine, so kommt die Verbindung trotzdem zustande.
B-Kanäle	Anzahl der verwendeten B-Kanäle. Wertebereich: 1 oder 2

Parameter	Beschreibung
Rückruf	Ein Anruf wird abgelehnt und der Partner danach sofort zurückgerufen. Dies verhindert das Einwählen von nicht autorisierten Gegenstellen. Die anrufende Stelle muss im D-Kanal der ISDN-Verbindung die Rufnummer übertragen und die Einwahl durch das System erlauben. Beim PSTN-Partner muss diese Rufnummer mit gehender Richtung konfiguriert sein. Ist "Rückruf" aktiviert, werden nur gehende Verbindungen von diesem Partner akzeptiert. Ist die Gegenstelle ebenfalls ein Gateway, und ist für diese Verbindung ebenfalls "Rückruf" aktiviert, kann keine Verbindung aufgebaut werden, weil keiner der Partner einen einkommenden Verbindungsaufbau akzeptiert. Ist bei einer solchen Fehlkonfiguration nur "Rückruf ohne Wahlwiederholung" aktiviert, so kann sie erkannt werden, und ein ständiger Verbindungsaufbau wird unterdrückt. Ist jedoch Wahlwiederholung aktiviert, wird das Problem nicht erkannt.
V.34-Gegenstelle	Akzeptieren einer V.34-Gegenstelle (z.B. ein Modem).
PPP automatisch wieder verbinden	PPP Verbindung wird nach einem Verbindungsabbau automatisch wieder aufgebaut (z.B. bei ISP-Zugang mit Flat-Rate und Zwangstrennung nach 24 Stunden).
LCP-Echo-Anforderung senden	Eine LCP-Echo-Anforderung wird gesendet. Diese Funktion dient der Prüfung, ob die Verbindung noch aktiv ist.
Short-Hold-Modus	
Short-Hold-Modus	Die Betriebsart „Short Hold“ ist für die PPP-Verbindung eingeschaltet. Die nachfolgenden Eingaben sind nur bei eingeschaltetem Short-Hold Modus möglich.
Short-Hold-Zeit (s)	Zeit ohne Datenübertragungen, nach der die PPP-Verbindung getrennt werden soll. Der Short-Hold-Timer wird nur von ausgehenden Paketen getriggert. Wertebereich: 10 bis 9999
Short-Hold-Gebührentaktauswertung	Geben Sie an, ob der Short-Hold-Betrieb unter Berücksichtigung des Gebührentaktes optimiert werden soll. Für Anrufe über PPP erfolgt eine Gebührentaktauswertung (Auswertung der Facility Meldungen mit AoC-Info-Elementen). Werden vom Internet-Service-Provider keine Gebühreneinformationen geliefert, so wird als Default-Timeout-Wert 0 Sekunden verwendet.
Authentifizierung	
PPP-Authentifizierung	PPP-Authentifizierung wird aktiviert.
PPP-Benutzername	Frei wählbarer Benutzername, der bei der Authentifizierung durch PAP oder CHAP verwendet werden soll.
PAP-Authentifizierungsmode	Aktivierung und Art der PAP-Authentifizierung für die PPP-Verbindung: nicht benutzt, PAP-Client, PAP-Host.
PAP-Kennwort	Kennwort für die PAP-Authentifizierung.
CHAP-Authentifizierungsmode	Aktivierung und Art der CHAP-Authentifizierung für die PPP-Verbindung: Nicht benutzt, CHAP-Client, CHAP-Host, CHAP-Client und -Host.

Parameter	Beschreibung
CHAP-Kennwort	Kennwort für die CHAP-Authentifizierung.
Header-Komprimierung	
IP-Header-Komprimierung	Die Komprimierung des IP/TCP bzw. IP/UDP/RTP-Header ist aktiviert. Die Header-Komprimierung verbessert die Datenübertragung in Voice-over-PPP-Szenarien. Es werden alle Voice-Pakete komprimiert, deren UDP-Portnummern im eingestellten Bereich liegen.
Datenkomprimierung	
DEFLATE-Datenkomprimierung	Komprimierung mit dem DEFLATE-Algorithmus
COMPRESS-Datenkomprimierung	Komprimierung mit dem COMPRESS-Algorithmus
Addressübersetzung	
Netzwerkadress-Übersetzung (NAT)	NAT (Network Adress Translation) ist eingeschaltet. Folgende Protokolle werden unterstützt: TCP, UDP und ICMP (nur im Passivmodus).
Address-Mapping	Adress-Mapping ist aktiviert.
QoS-Parameter der Schnittstelle	
Bandbreitensteuerung für Sprach-Verbindungen	Die Bandbreitensteuerung verhindert das Überbuchen der verfügbaren Übertragungsraten mit Sprachverbindungen innerhalb einer Multilink-Verbindung. d.h. bei aktivierter Header-Kompression werden maximal 5 Sprachverbindungen (G.729 / 60ms o. G.723 / 60ms) über einen B-Kanal zugelassen. Dieses Feld aktiviert die Bandbreitensteuerung für Sprach-Verbindungen. Es werden dabei nur Sprachverbindungen betrachtet, deren Routen im Sprachgateway eingerichtet wurden.
Bandbreite für Sprach-/Fax-Verbindungen (%)	Prozentangabe für die verfügbare Bandbreite für Sprach-/Fax-Verbindungen. Wertebereich, Standardwert: 0 - 95, 80

Parameterbeschreibung der Registerkarten:

- **Auf Lieferzustand zurücksetzen**

Parameter	Beschreibung
Übernehmen	Die Werte für den gewählten PSTN-Partner werden auf die Lieferzustandswerte zurückgesetzt.

Parameterbeschreibung der Registerkarten:

- **Rufnummer hinzufügen**
- **Rufnummer ändern**
- **Rufnummer löschen**

Parameter	Beschreibung
Rufnummer	Rufnummer, unter der ein PSTN-Partner erreichbar ist. Sie muss innerhalb der Gesamtkonfiguration eindeutig sein und kann aus bis zu 22 Dezimalziffern (0 bis 9) bestehen. Es können Bindestriche verwendet werden. Zu jedem PSTN-Partner können bis zu fünf Rufnummern konfiguriert werden. Bei Übermittlung der Rufnummer wird diese überprüft und es werden nur Anrufe entgegengenommen, wenn für die eingehende Rufnummer ein PSTN-Partner mit der entsprechenden Rufberechtigung definiert ist.
Rufrichtung	Zustandekommen der Verbindung unter der oben eingetragenen Rufnummer.
Anrufrichtung: Gesperrt	Die Nummer ist nicht verwendbar.
Rufrichtung : kommend	Der Partner darf anrufen, aber nicht angerufen werden.
Anrufrichtung: gehend	Der Partner darf angerufen werden, aber nicht anrufen.
Rufrichtung : Kommend und gehend	Der Partner darf angerufen werden und kann anrufen.
Löschen	Die gewählte Rufnummer wird gelöscht.

28.3.5 LCR

Unter **LCR** werden die Funktionen für LCR wie Berechtigungen, Wahlpläne, Wegetabellen und Wahlregeln zusammengefasst.

28.3.5.1 LCR > LCR-Flags

Parameterbeschreibung der Registerkarte:

- **LCR Flags ändern**

Parameter	Beschreibung
LCR Flags	
LCR freigeben	LCR wird freigegeben und somit die automatische Wegesuche aktiviert.
LCR Daten zurücksetzen	
Löschen der konfigurierten LCR Daten und Initialisierung mit LCR Standard Daten	Wird dieses Optionsfeld aktiviert, werden die konfigurierten LCR-Einträge (Wahlpläne, Wegetabellen, Wahlregeln) gelöscht und durch die Standard-Einträge ersetzt.

Tipp: Bei Fehlkonfiguration im LCR besteht die Gefahr, dass gehende Verbindungen nicht oder nur eingeschränkt möglich sind.

Zugehörige Konzepte

Teilnehmerdaten auf Seite 160

28.3.5.2 LCR > Berechtigungen

Parameterbeschreibung der Registerkarte:

- **LCR Berechtigungen ändern**

Parameter	Beschreibung
Index	Hierarchische Indexliste
Rufnummer	Rufnummer
Name	Name des Teilnehmers
Berechtigungsgruppe	Jeder Teilnehmer wird einer LCR-Berechtigunggruppe (Class Of Service COS) zugewiesen. Standardmäßig sind alle Teilnehmer mit maximaler LCR-Berechtigung (15) eingetragen Wertebereich: 1 bis 15

Tipp: Ein Teilnehmer kann einen Weg nur dann belegen, wenn seine Berechtigung größer oder gleich der LCR-Berechtigung in der Wegetabelle ist.

28.3.5.3 LCR > Wahlplan

Parameterbeschreibung der Registerkarten:

- **Wahlplan ändern**
- **Wahlplan anzeigen**

Parameter	Beschreibung
Rufnummernplan	Im Wahlplan wird nach Mustern gesucht, die auf die gewählten Ziffern zutreffen. Das Ergebnis dient als Kriterium für die Auswahl der Wegetabelle. Dabei wird ebenfalls überprüft, ob die Berechtigung des Teilnehmers für diese Richtung zutrifft. Für Externverbindungen wird jede Rufnummer einschließlich der Kennzahl (bis max. zur 24 Zeichen incl. Feldtrennzeichen) im Wahlplan überprüft. Der Wahlplan ermittelt dann für den Teilnehmer eine Wegetabelle, die der Teilnehmer für den Verbindungsaufbau zugewiesen bekommt. Über die Wegetabelle werden bis zu 16 Wege (Routen) angelegt. Die Wahlregeltabelle legt fest, wie die vom Teilnehmer ausgesuchten Ziffern umgesetzt und vom Kommunikationssystem gewählt werden.
Name	Über die Spalte „Name“ kann jedem Profil wie z.B. Ortsgespräch, Ferngespräch, Ausland ein Name zugeordnet werden. Ob die Spalte „Name“ angezeigt wird, hängt von der jeweiligen Version des Kommunikationssystems ab. Für den Namen sollte ein sprechender Name gewählt werden. Eine Name darf auch mehrfach verwendet werden. Über den Rufnummern-Assistenten werden automatisch entsprechende Namen vergeben.

Parameter	Beschreibung
Gewählte Ziffern	Anhand dieses Schemas wird die Rufnummer ausgewertet, um in die entsprechende Wegetabelle zu verzweigen. Es können die Feldtrennzeichen C und - sowie die Platzhalter X, N und Z verwendet werden. 0...9 feste Ziffern - Feldtrennzeichen (Auswertung durch die Wahlregel); X - Platzhalter für eine Ziffer zwischen 0...9; N - Platzhalter für eine Ziffer zwischen 2...9; Z - Platzhalter für eine oder mehrere Ziffern bis Wahlende; C - simulierter Wählton (kann max. 3 mal eingetragen werden)
Wegetabelle	In der Spalte Wegetabelle wird angegeben, welche Wegetabelle für das Profil verwendet werden soll. Der Pfeil verlinkt zur Definition der jeweiligen Wegetabelle. Wertebereich: 1 bis 254, davon 1 bis 15 vorbelegt
PKZ	In dieser Spalte wird über Ankreuzen entschieden, ob eine erzwungene PKZ-Eingabe nach der Belegungskennzahl erfolgen soll oder nicht (in USA.: nach Wahlende). Wenn nicht ausgewählt, wird die PKZ erst nach der kompletten Wahl des Wahlplans angefordert, wenn dies für die Richtung eingerichtet ist.
Amtsberechtigung	Wenn markiert, dann unterliegen die gewählten Ziffern der Wahlkontrolle (Berechtigung). Dies gilt sowohl für die Vernetzung, als auch für standalone Kommunikationssysteme. Damit können einzelne Rufnummern von der Wahlkontrolle ausgenommen werden. Wenn die Wahlkontrolle durchgeführt werden soll, so gelten die bekannten Regeln über die Verbots- und Erlaubnislisten.
Notruf	Wenn eine hier als Notrufnummer eingerichtete Nummer (Spalte Notbetrieb angekreuzt) angewählt wird und es keine freie Leitung gibt, dann wird eine nicht als Notrufnummer benutzte Leitung (Spalte Notbetrieb nicht angekreuzt) getrennt und diese dann automatisch für den Notruf bereitgestellt.

28.3.5.4 LCR > Wegetabelle

Parameterbeschreibung der Registerkarten:

- **Wegetabelle ändern**

Parameter	Beschreibung
Wegetabellen	Den im Wahlplan definierten Rufnummern wird über die Wegetabellen hier eine Aktion (Wahl) zugeordnet. Wertebereich: 254 Wegetabellen
Index	Die Wegetabelle wird von oben nach unten in hierarchischer Reihenfolge durchsucht. Es wird jeweils überprüft, ob die Richtung frei ist bzw. der Teilnehmer die erforderliche LCR-Berechtigung (Class Of Service COS) hat. Ist dies der Fall, erfolgt die Wahl gemäß der in der Wegetabelle eingetragenen Wahlregel. Wertebereich: 1 bis 16
Dedizierte Richtung	Es wird die Richtung verwendet, die dem Teilnehmer fest zugewiesen wurde (z.B. über die Zuweisung der Richtung beim Multisite Management.

Parameter	Beschreibung
Richtung	Die zu belegende Richtung, siehe "Leitungen/Vernetzung > Richtungen" Standardwert: Im System konfigurierter Richtungsnamen
Wahlregel	Durch die LCR-Wahlregeln können eingegebene Rufnummern zur Weiterverarbeitung in beliebige neue Ziffernfolgen umgewandelt werden. Durch Ziffernumwandlung wird der Zugang zu verschiedenen Netzanbietern ermöglicht. Definition unter "Wahlregel". Wertebereich: 254 Wahlregeln
Min. Ber.	Die min. Berechtigung beschreibt die LCR-Berechtigung, die ein Teilnehmer mindestens haben muss, um die zugehörige Route verwenden zu dürfen. Hier lässt sich z.B. festlegen, dass ein Teilnehmer nur über einen bestimmten Carrier oder nur zu bestimmten Zeiten telefonieren darf, während andere Teilnehmer eine Ausweichmöglichkeit auf andere Routen erhalten. Der Wert für die maximale Berechtigung ist 15. Wertebereich: 1 bis 15
Warnung	Wenn der primäre Verbindungsweg in der Wegetabelle belegt ist, wird LCR den nächsten (möglicherweise kostspieligeren) in der Tabelle konfigurierten Weg wählen. Dies kann dem Anwender durch ein akustisches und/oder optisches Signal angezeigt werden. Wertebereich: Keine, Ton, Display, Display + Ton
Dediziertes Gateway	Der Parameter definiert die Art, wie in einem IP-Netzverbund der Zielpartner-Knoten identifiziert wird. Wertebereich: Nein, Erzwungen, Mehrere Standorte
Dediziertes Gateway: **Nein**	Der Partner-Knoten wird anhand der Ziel-Rufnummer identifiziert.
Dediziertes Gateway: **Erzwungen**	Es wird zwingend zu dem Gateway geroutet, das in der Spalte **GW Knoten-ID** durch seine Knoten-ID definiert ist.
Dediziertes Gateway: **Mehrere Standorte**	Anruferorientierte Bestimmung des Partner-Knotens: Es wird zu dem Gateway geroutet, das dem jeweiligen Anrufer per Multigateway-Wizard oder in der Eingabemaske **Teilnehmer** > **Workpointclient Daten ändern** > **ID des Sekundärsystems** zugewiesen wurde. Für Anrufer ohne einen diesbezüglichen Eintrag wird zu dem Gateway geroutet, das in der Spalte **GW Knoten-ID** durch seine Knoten-ID definiert ist (default).
GW Knoten-ID	Angabe der Gateway-Knoten-ID für die Auswahl **Erzwungen** oder **Mehrere Standorte** des Parameters **Dediziertes Gateway**.
Schaltflächen	
Blauer Pfeil in Spalte **Wahlregel**	Zeigt die Seite mit den **Wahlregel**-Parametern an.

28.3.5.5 LCR > Wahlregel

Parameterbeschreibung der Registerkarte:

- **Wahlregel ändern**

Parameter	Beschreibung
	Durch die LCR-Wahlregeln können eingegebene Rufnummern zur Weiterverarbeitung in beliebige neue Ziffernfolgen umgewandelt werden. Durch Ziffernumwandlung wird der Zugang zu verschiedenen Netzanbietern ermöglicht. Die verwendete Wahlregel wird bestimmt durch den Eintrag in der Wegetabelle.
Regelname	Frei definierbarrer Name der Wahlregel, einige Wahlregeln sind vordefiniert Wertebereich: max. 16 Zeichen
Wahlregelformat	Programm für die zu wählenden Ziffern. Der einzelnen Programmschritte werden von links nach rechts abgearbeitet. Die Zeichen für den Programmcode stehen für folgende Funktionen:
A	Restliche Felder wiederholen (aussenden). "A" bewirkt, dass alle nachfolgenden Ziffernfelder gesendet werden. Bezugspunkt ist das letzte Feldtrennzeichen im Feld gewählte Ziffern im Wahlplan. Wird "A" ohne expliziten Bezug eingetragen, bezeichnet dies alle Ziffern nach dem Acces Code, d. h, "A" entspricht dann "E2A"
B	Wird für die Multi-Gateway-Vernetzung genutzt, wenn eine von extern angerufene Rufnummer vom TON (Type Of Number) "unknown" ist, um sie zum Multi-Gateway-Knoten zu routen. Damit diese Rufnummer eindeutig ist, wird sie entsprechend der TON im LCR auf national oder international erweitert. Dies ist erforderlich, wenn die Durchwahlnummern nicht eindeutig sind und ins nationale oder internationale Format konfiguriert werden müssen.
D (n)	Ziffernfolge wählen (1 bis 25 Ziffern). "D" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen.
E (n)	Aussenden des Feldinhaltes (1 bis 10). "E" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen. Die Reihenfolge von "E" in Abhängigkeit von (n) ist beliebig. Ein bestimmtes Feld darf mehrmals, auch aufeinanderfolgend, angesprochen werden. "E" darf mit Ausnahme von "E1" (Access Code) von beliebigen anderen Parametern eingeschlossen sein. Bei schritthaltender Wahl (Gegensatz zur Blockwahl) darf das letzte Element in der Wahlregel nicht E(n) heißen, sondern E(n)A.
M (n)	Autorisierungscode (1 bis 16). Dieser Buchstabe darf nicht an der letzten Stelle stehen.
P (n)	P(n) darfin der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen. P(n) darf von beliebigen anderen Parametern eingeschlossen sein. (1- bis 60-fache der systemweiten Pauseneinheit).
S	Switch, Umschalten des Wahlverfahrens von IWV auf MFV (bei CONNECT, PROGRESS oder CALL PROC mit PI). "S" darf in der Zeichenkette nur einmal vorkommen und darf nicht an der letzten Stelle stehen. Nach "S" darf nicht mehr der Parameter "C" verwendet werden.
C	Carrier "C" darf in der Zeichenkette nur einmal vorkommen. Die nachfolgenden Zeichen werden ohne Wahlpause gesendet und für den Carrierzugang bei "Single Stage", "Two Stage", "DICS" und "PRI" verwendet.
U	Anwenden des Wahlverfahrens SUB-Adresse. "U" darf in der Zeichenkette nur einmal vorkommen und darf nicht an der letzten Stelle stehen. Nach "U" dürfen die Parameter "S", "P" "M" und "C" nicht mehr verwendet werden.

Parameter	Beschreibung
N (n) (Nur für USA!)	Netz-SFG-Gruppe (1 bis 5) oder Bandnummer (1).
L (Nur für USA!):	"L" darf nur am Ende der Zeichenkette vorkommen. "L" bewirkt, dass der Anruf als Notruf behandelt wird.
Verfahren des Netzanbieters	Auswahl des jeweiligen Netzanbieters
unbekannt	Keine explizite Angabe über einen Netzanbieter.
Hauptnetzanbieter	Bei einer Belegung über den Hauptnetzanbieter erfolgt die einfache Wahl durch Blockwahl oder Wahl einzelner Ziffern in das öffentliche Netz.
MCL Single Stage	Bei MCL Single Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt und anschließend die Rufnummer gewählt. Die Wahl erfolgt dabei bei ISDN im D-Kanal bzw. als normale Wahl bei HKZ.
MCL Two Stage	Bei MCL Two Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt. Nach einer Synchronisationsphase wird zunächst ein ebenfalls konfigurierbarer Autorisierungscode und darauffolgend die Ziel-Rufnummer als DTMF-Zeichen gesendet. Bei Synchronisation durch Zeit muss eine Pause von 2 bis 12 s programmiert werden.
Corporate Network	Ein Corporate Network ist direkt an OpenScape Business angeschlossen. Die LCR-Funktion bestimmt aus der vom Teilnehmer gewählten Nummer die entsprechende Richtung und routet das Gespräch entweder über das Leitungsbündel des öffentliches Amtes oder über das Leitungsbündel mit dem firmeneigenen Netz.
Dial In Control Server	Bei dieser Art LCR wird mit einem Präfix der gewünschte Netzanbieter über einen Dial-In Control Server (DICS) angewählt und dabei die Rufnummer und ein konfigurierbarer Authorisierungscode in der Subadresse übermittelt. Die Wahl erfolgt dabei im D-Kanal.
Primary Rate Interface (Primärmultiplexschnittstelle) (nur für USA)	Beim Primary Rate Interface erfolgt die Auswahl des Netzanbieters bzw. des Calling Service in der SETUP-Meldung über die folgenden Informationselemente: Network Specific Facility, Operator System Access und Transit Network Selection.
Type	Type of Number [TON]; hier können pro Wahlregel folgende Nummerntypen der „Called Party Number“ über die Klappliste ausgewählt werden: Anlagenrufnummer, Ortsnetzkennzahl, Ländervorwahl. Als Default-Eintrag ist „Unbekannt“ vorgegeben. Der Type of Number wird nur bei E.164 gesetzt. Bei einer Vernetzung steht der Parameter auf "unbekannt".

28.3.5.6 LCR > Multisite

Parameterbeschreibung der Registerkarte:

- **Bereich ändern**

Parameter	Beschreibung
Ortskennzahl	Eingabe der Ortsvorwahl für einen Standort (inkl. führender Null, z.B. `069` für Frankfurt und `030` für Berlin). Es können unterschiedliche oder auch gleiche Ortsvorwahlen eingetragen werden.

Parameter	Beschreibung
Bereich	Eingabe des Namens für einen Standort (z.B. die zu den Ortvorwahlen passenden Städte `Frankfurt` und `Berlin` oder bei gleichen Ortsvorwahlen die Abteilungsbezeichnungen `Service` und `Vertrieb`).
Dedizierte Richtung	Auswahl der Richtung bzw. der ITSP-Registrierung für diesen Standort.
Löschen	Löscht die markierten Standorteinträge.
Schaltflächen	
Speichern	Sichert die Änderungen.

Parameterbeschreibung der Registerkarte:

- **Teilnehmer/Gruppen ändern**

Parameter	Beschreibung
Bereich	Auswahl des Standorts für den Teilnehmer oder die Gruppe.
Dedizierte Richtung	Auswahl der Richtung bzw. der ITSP-Registrierung für den Teilnehmer oder die Gruppe.
Suche	Suche nach Teilnehmern und Gruppen, indem der Suchbegriff in die Suchfelder **Rufnr**, **DuWa** oder **Name** eingegeben und anschließend die Return-Taste gedrückt wird. Alle Teilnehmer und Gruppen werden aufgelistet, wenn alle Suchfelder leer sind und anschließend die Return-Taste gedrückt wird. Über die Auswahl **Typ** lassen sich alle Teilnehmer-Typen anzeigen (z.B. **SIP Clients** oder **System Clients**).

28.3.6 Sprachgateway

Unter **Sprachgateway** sind die Funktionen für die IP-Telefonie zusammengefasst.

28.3.6.1 Sprachgateway > SIP-Parameter

Parameterbeschreibung der Registerkarten:

- **SIP-Parameter ändern**

Parameter	Beschreibung
SIP Transport-Protokoll	
SIP über TCP	TCP (Transmission Control Protocol) TCP ist ein obligatorisches Transportprotokoll für SIP und kann hier nicht deaktiviert werden.
SIP über UDP	UDP (User Datagram Protocol) UDP ist das standardmäßige Transportprotokoll für SIP, das deaktiviert werden kann, wenn kein Endpunkt/ Trunk/ITSP es verwendet. Es wird ausdrücklich empfohlen, das UDP aktiviert bleibt.

Parameter	Beschreibung
SIP über TLS	TLS (Transport Layer Security) TLS ist ein sicheres Transportprotokoll für SIP und kann hier nicht deaktiviert werden.
SIP-Registrar	
Dauer der Registrierung (s)	Intervall (in Sekunden) innerhalb dessen die Registrierung eines SIP-Endpunkts wiederholt werden muss. Der Intervallwert sollte nicht zu hoch eingestellt werden, weil die Registrierung dazu benötigt wird, festzustellen, ob ein Endpunkt außer Betrieb ist. (Der Registrierungszeitraum für ITSP-Trunks wird in den ITSP-Profilen konfiguriert). Wertebereich, Standardwert: 10 - 86400, 120
RFC 3261 Timer-Werte	
Transaction Timeout (ms)	Gibt die Wartezeit (in Millisekunden) vor einer Neuübertragung der Invite-Antwort für den Zeitgeber D für die Spezifikation RFC 3261 an. Diese Einstellung ist für die Invite-Clienttransaktion relevant. Wertebereich, Standardwert: 2000 - 64000, 32000
SIP-Session-Timer	
RFC 4028 verwenden	RFC 4028 definiert eine Erweiterung des Session Initiation Protocols (SIP). Diese Erweiterung erlaubt einen periodischen Refresh von SIP-Sessions. Die User-Agents und die Proxies können durch den Refresh ermitteln, ob die SIP-Session noch aktiv ist. Hier werden die Konfigurationsmöglichkeiten verwendet, um die Aktualisierung der Sitzung in der Leitungsschnittstelle zu steuern (für ITSPs siehe das dazugehörige Profil).
Session-Expires (s)	Definiert die Dauer einer SIP-Session. Der Standardwert ist „1800“. Der konfigurierte Wert wird für Trunking und ITSP-Schnittstellen verwendet. Wertebereich, Standardwert: 90 - 65535, 1800
Minimal-SE (s)	Definiert die kürzeste Dauer einer SIP-Session, die erlaubt ist. Der konfigurierte Wert wird für Trunking und ITSP-Schnittstellen verwendet. Wertebereich, Standardwert: 90 - 65535, 90
DNS Einträge	
Sperrzeit für nicht erreichbare Ziele (s)	Dieser Timer wird verwendet, um die Blacklist des SIP-Stack zu kontrollieren. Wenn ein durch DNS aufgelöster SIP-Server nicht reagiert, wird er für die Dauer der hier konfigurierten Zeit gesperrt. Der Standardwert ist 60 Sekunden. Falls redundante Server verwendet werden (Beispiel: DNS resultiert in mehreren Servern), wird ein höherer Wert empfohlen (z.B. 900).
Provider-Anrufe	
Maximal mögliche Anrufe über Provider	Hier wird die Anzahl der gleichzeitigen Gespräche über alle aktivierten Provider angezeigt. Der Wert wird entsprechend der verfügbaren Bandbreite und der ITSP-Konfiguration beim Einrichten konfiguriert.

28.3.6.2 Sprachgateway > ITSP Loc-ID Einstellungen

Parameterbeschreibung der Registerkarten:

- ITSP Loc-Info hinzufügen

  Die ITSP Loc-Info wird im SIP-Protokoll verwendet, um den Empfänger eines Notrufs über dessen geografischen Ursprung zu informieren. Im SIP-Protokoll wird das Format der Loc-ID-Info als RFC4119 & RFC5139 (XML-kodiertes Loc-Objekt im MIME-Text) festgelegt. Mit der ITSP Loc-ID können alle in den entsprechenden RFCs definierten Felder bestimmt werden, wohingegen in Ihrer bestimmten Bereitstellung nur eine Untermenge dieser Daten konfiguriert werden muss. (Beispiel: In der Schweiz wird nur das NAM-Feld für die Definition eines Ortes verwendet). Die für die Definition eines Ortes nötigen Daten erhalten Sie von Ihrem ITSP.

Parameter	Beschreibung
Loc-ID-Name	Der Name der Loc-ID.
Land	Das Land wird über den zweistelligen ISO-3166-Code identifiziert.
A1	Nationale Unterabteilungen (Staat, Region, Provinz, Präfektur)
A2	Landkreis, Gemeinde, Gun, Kreis
A3	Stadt, Gemeinde, Shi
A4	Stadt-Division, Bezirk, Stadtteil, Ward, Chou
A5	Nachbarschaft, Block
A6	Straße
PRD	Führende Straßenrichtung
POD	Trailing Straße Suffix
STS	Straße Suffix
HNO	Hausnummer, nur numerischer Teil
HNS	Hausnummer Suffix
LMK	Wahrzeichen oder Vanity Adresse
LOC	Zusätzliche Informationen Standort
FLR	Floor
NAM	Name (Wohnung, Geschäft oder Büroangestellter)
PC	Postleitzahl
ROOM	Raum
PLC	Art des Orts
PCN	Name der Postgemeinschaft
POBOX	Postfach
ADDCODE	Zusatzcode
SEAT	Sitz (Schreibtisch, Kabine, Workstation)

Parameter	Beschreibung
RD	Hauptstraßennetzes Name
RDSEC	Straßenabschnitt
RDBR	Zweig Straße Name
RDSUBBR	Sub-Zweig Straße Name
PRM	Straßenname pre-Modifikator
POM	Straßenname Post-Modifikator
Erweiterte Einstellungen aktivieren	Wenn aktiviert, können die erweiterten Parameterfelder konfiguriert werden.
BLD	Gebäude (Struktur)
UNIT	Einheit (Wohnung, Suite)

28.3.6.3 Sprachgateway > Codec-Parameter

Parameterbeschreibung der Registerkarten:

- **Codec-Parameter ändern**

Parameter	Beschreibung
Codec	Die Parameter für die Codecs G.711 A-law, G.711 µ-law, G.729A und G.729AB können bearbeiten werden.
Codec: G.711 A-law	G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt. Das A-law-Verfahren ist ein primär in Europa verwendetes Digitalisierungsverfahren für analoge Audiosignale im Telekommunikationsbereich.
Codec: G.711 µ-law	G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt. In Nordamerika und Japan wird das ähnliche µ-law-Verfahren eingesetzt, das dem A-law ähnelt, jedoch nicht kompatibel ist. Zur Kommunikation, z.B. bei einem Telefongespräch zwischen Europa und USA, müssen die digitalen Daten durch entsprechende Konverter umgesetzt werden.
Codec: G.729A	Sprachkodierung mit 8 Kbit/s.
Codec: G.729AB	Sprachkodierung mit 8 Kbit/s. Auffüllen von Sprachpausen mit Komfortrauschen.
Priorität	Den Audio-Codecs können Prioritäten von 1 (hoch) bis 4 (niedrig) zugewiesen werden. Das Kommunikationssystem versucht automatisch, für jede Verbindung einen Audio-Codec mit einer möglichst hohen Priorität zu verwenden. Wird ein Audio-Codec mit geringer Sprachkomprimierung (guter Sprachqualität) verwendet, wird das Netz höher ausgelastet. Bei intensiver IP-Telefonie kann das bei einem durch Datentransfer bereits ausgelasteten Netz zu einer Verschlechterung der Sprachqualität führen.
Sprechpausenerkennung (VAD)	Aktivieren der Sprechpausenerkennung (VAD, Voice Activity Detection). Bei langen Sprechpausen kann somit die Last auf das Netz reduziert werden.

Parameter	Beschreibung
Rahmengröße	Für jeden Codec kann die Rahmengröße (Größe des IP-Pakets) von 10 bis zu 90 Millisekunden angegeben werden. Damit legen Sie die Abtastrate fest, mit der das Sprachsignal in IP-Pakete zerlegt wird. Ein höherer Wert (z. B. 90 ms) bedeutet einerseits ein besseres Verhältnis von Nutzdaten zum IP-Paket-Overhead, andererseits aber eine größere Verzögerung bei der Übertragung. Die einstellbaren Werte sind von den Codecs abhängig. Für die Vernetzung von OpenScape Business mit OpenScape Voice über SIP-Q V2: Cordless IP und OpenScape Mobile Connect unterstützen nur eine Framelänge von 20 ms für den G.711 Codec. Wenn es im Netzverbund eines dieser beiden Produkte gibt, muss hier die Rahmengröße auf 20 ms eingestellt werden. Wertebereich, Standardwert: 10 - max. 90, 20
Erweiterte DSP-Kanäle	
Nur G.711 verwenden	Nur die Protokolle G.711 A-law, G.711 µ-law werden verwendet. Bei G.711 werden weniger DSP-Ressourcen benötigt, dann sind mehr gleichzeitige Gespräche möglich.
T.38-Fax	
T.38-Fax	Legt fest, ob das T.38-Faxprotokoll zum Einsatz kommen soll. Für System mit Booster-Karte und/oder Booster-Server: Bei aktiviertem Flag wird die Fehlerkorrektur während im T.38-Protokoll durchgeführt. Ein Popup-Fenster wird angezeigt, um den Benutzer darüber zu informieren, dass ein manueller Neustart des Systems oder OCAB/Booster Servers erforderlich ist.
FillBitRemoval verwenden	Legt fest, ob bei Verwendung des T.38-Faxprotokolls Füllbits beim Senden gelöscht und beim Empfangen wiederhergestellt werden sollen. Dadurch lässt sich Bandbreite sparen.
Max. UDP-Datagramm-Größe für T.38-Fax (Byte)	Maximale Größe eines T.38-UDP-Datagramms in Bytes. Wertebereich, Standardwert: 1 - 1472, 1472
Verwendete Fehlerkorrektur für T.38-Fax (UDP)	Legt fest, welche Methode zur Fehlerkorrektur eingesetzt werden soll. Werte: t38UDPFEC, t38UDPRedundancy Für System mit Booster-Karte und/oder Booster-Server: Wenn eine Option ausgewählt ist, wird ein Popup-Fenster angezeigt, um den Benutzer darüber zu informieren, dass ein manueller Neustart des Systems oder OCAB/Booster Servers erforderlich ist. Standardwert: t38UDPRedundancy
T.30 Fax	
ECM aktivieren	Für System mit Booster-Karte und/oder Booster-Server: Bei aktiviertem Flag wird die Fehlerkorrektur im T.30-Protokoll durchgeführt. Ein Popup-Fenster wird angezeigt, um den Benutzer darüber zu informieren, dass ein manueller Neustart des Systems oder OCAB/Booster Servers erforderlich ist. Standardwert: Aktiviert

Parameter	Beschreibung
VoIP-Kompatibilitätsmodus	Für System mit Booster-Karte und/oder Booster-Server: Dieses Flag sollte aktiviert werden, wenn Probleme mit der Faxübertragung in VoIP-Netzwerken auftreten. Ein Popup-Fenster wird angezeigt, um den Benutzer darüber zu informieren, dass ein manueller Neustart des Systems oder OCAB/Booster Servers erforderlich ist. Standardwert: Deaktiviert
Sonstiges	
ClearChannel	Ein ClearChannel ist ein offener Kanal, bei dem die Endpunkte für das Protokoll im Kanal verantwortlich sind. Der Parameter legt fest, ob die ClearChannel-Interface-Funktionalität aktiviert sein soll oder nicht. Der Parameter legt fest, ob die ClearChannel-Interface-Funktionalität aktiviert sein soll oder nicht.
Rahmengröße	In diesem Feld können Sie die Sampling-Rate bestimmen. Möglich sind 10, 20, 30, 40, 50 und 60 Millisekunden (ms). Wertebereich, Standardwert: 10 - 60, 20
RFC2833 RFC2833 legt fest, wie die Tonsignale übermittelt werden.	
Übertragung von Fax/ Modem Tönen nach RFC2833	Übertragung outband (über die SIP-Signalisierung), empfohlene Betriebsweise um Töne sicher zu übertragen
Übertragung von DTMF Tönen nach RFC2833	Übertragung outband (über die SIP-Signalisierung), empfohlene Betriebsweise um Töne sicher zu übertragen
Payload Type für RFC2833	Anpassung ggf. abhängig vom Kommunikationspartner erforderlich Wertebereich, Standardwert: 96 - 126, 98
Redundante Übertragung der RFC2833 Töne nach RFC2198	Dient zur Erhöhung der Übertragungssicherheit

28.3.6.4 Sprachgateway > Ziel-Codec-Parameter

Für bestimmte Kommunikationspartner können Prioritäten für die Verwendung der Audio-Codecs definiert werden.

Parameterbeschreibung der Registerkarten:

- **Ziel-Codec-Parameter hinzufügen**

Parameter	Beschreibung
Codec: G.711 A-law	G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt. Das A-law-Verfahren ist ein primär in Europa verwendetes Digitalisierungsverfahren für analoge Audiosignale im Telekommunikationsbereich.

Parameter	Beschreibung
Codec: G.711 µ-law	G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt. In Nordamerika und Japan wird das ähnliche µ-law-Verfahren eingesetzt, das dem A-law ähnelt, jedoch nicht kompatibel ist. Zur Kommunikation, z.B. bei einem Telefongespräch zwischen Europa und USA, müssen die digitalen Daten durch entsprechende Konverter umgesetzt werden.
Codec: G.729A	Sprachkodierung mit 8 Kbit/s.
Codec: G.729AB	Sprachkodierung mit 8 Kbit/s. Auffüllen von Sprachpausen mit Komfortrauschen.
Priorität	Den Audio-Codecs können Prioritäten von 1 (hoch) bis 4 (niedrig) zugewiesen werden. Das Kommunikationssystem versucht automatisch, für jede Verbindung einen Audio-Codec mit einer möglichst hohen Priorität zu verwenden. Wird ein Audio-Codec mit geringer Sprachkomprimierung (guter Sprachqualität) verwendet, wird das Netz höher ausgelastet. Bei intensiver IP-Telefonie kann das bei einem durch Datentransfer bereits ausgelasteten Netz zu einer Verschlechterung der Sprachqualität führen.
Zielstelle	
Ziel-Adress-Typ	Anzeige des Typs des Ziels, dem die eingestellten Prioritäten der Audio-Codecs zugeordnet werden sollen.
IP-Adresse	IP-Adresse des Ziels, für das die eingestellten Prioritäten der Audio-Codecs gelten sollen (z.B. vernetzter Knoten, SIP Server)

28.3.6.5 Voice Gateway > Internet-Telefonie-Dienstanbieter

Parameterbeschreibung der Registerkarten:

- **Internet Telefonie Service Provider hinzufügen**
- **Internettelefonie-Dienstanbieter bearbeiten**
- **Internettelefonie-Dienstanbieter löschen**

Parameter	Beschreibung
Basisvorlage	Auswahl einer leeren Vorlage (Standard) oder einer vordefinierten Beispielkonfiguration für einen bestimmten Dienstanbieter. Diese lässt sich individuell anpassen und als neues ITSP speichern.
Anbietername	Gewünschter Name des ITSP. Der konfigurierte ITSP wird in der Liste der ITSPs unter diesem Namen erscheinen.
Anbieter aktivieren	Der ITSP ist aktiviert.
Anbieterkennung im System	Zuweisung einer eindeutigen Bezeichnung im System. Maximal 8 ITSPs können gleichzeitig aktiv sein. Wertebereich: Anbieter 1-8
Domänenname	Gateway-Domänenname des ITSP Oft nicht identisch mit dem Web-Domänennamen.

Parameter	Beschreibung
Transportprotokoll	Gewünschtes Transportprotokoll. Es kann zwischen UDP und TCP gewählt werden.
Transportsicherheit	Die möglichen Werte sind **traditionell (upd oder tcp)** für traditionelle Anrufe mit udp/tcp oder **secure (tls)** für sichere Anrufe mit TLS. Standardwert: **traditionell (udp oder tcp)**
Mediensicherheit	Die möglichen Werte sind **nur RTP** (nur AVP-Profil wird unterstützt) oder **nur SDES** (nur SAVP-Profil wird unterstützt). Standardwert: **Nur RTP**
Anbieter-Registrar	
Registrar verwenden	Muss ausgewählt werden, wenn der Trunk mit Registrierung arbeitet (Standard = Aus).
IP-Adresse / Hostname	Hostname oder IP-Adresse des externen Registrar-Servers.
Port	Portnummer des externen Registrar-Servers, z.B. 5060. Geben Sie Port 00 ein, wenn das ITSP DNSSRV verwendet.
Neuregistrierungsintervall beim Anbieter (Sek.)	Intervall (in Sekunden), in dem die ITSP-Registrierung wiederholt wird. Der Wert des Intervalls darf nicht 0 betragen und darf nicht zu hoch eingestellt werden, da bei Wiederholung der Registrierung am ITSP auch ein Verbindungsabbruch erkannt und bei Bedarf eine alternative Route (über ISDN oder einen alternativen Anbieter) ausgewählt werden kann. Standardwert: 120 Sekunden
Anbieter-Proxy	
IP-Adresse / Hostname	Domänenname oder IP-Adresse des Proxy-Servers (z. B., sip-voice.de). Der Eintrag ist obligatorisch und ist in der Regel identisch mit dem Anbieter-Registrar-Eintrag.
Port	Portnummer des Proxy-Servers (z. B. 5060). In der Regel ist dies identisch mit der Portnummer des Anbietes. Geben Sie Port 0 ein, wenn der ITSP mehrere Server und DNSSRV verwendet.
Ausgehender Anbieter-Proxy	
Ausgehenden Proxy verwenden	Nur gesetzt, wenn der ITSP einen ausgehenden Proxy verwendet, der sich vom Anbieter-Proxy unterscheidet. Standardmäßig deaktiviert.
IP-Adresse / Hostname	Domänenname oder IP-Adresse des ausgehenden Proxys.
Port	Portnummer des ausgehenden Proxys. Geben Sie Port 0 ein, wenn der ITSP mehrere Server und DNSSRV verwendet.
Eingehender Anbieter-Proxy	
Eingehenden Proxy verwenden	Nur festlegen, ob der ITSP optional Anfragen von einem zweiten Server sendet. Standardmäßig deaktiviert.
IP-Adresse / Hostname	Domänenname oder IP-Adresse des zweiten ITSP-Servers

Parameter	Beschreibung
Port	Portnummer des zweiten ITSP-Servers. Geben Sie Port 0 ein, wenn das ITSP DNSSRV verwendet.
Anbieter-STUN	
STUN verwenden	Nur gesetzt, wenn der ITSP einen STUN-Server verwendet. Die systemweite Einstellung unter der STUN-Konfiguration gilt als STUN-Modus für alle ITSPs (Standard = Aus).
IP-Adresse / Hostname	Hostname oder IP-Adresse des STUN-Servers.
Port	STUN-Portnummer des STUN-Servers.
Erweiterte SIP-Provider-Daten	
Erweiterte SIP-Provider-Daten anzeigen	Durch Aktivieren dieser Flagge stehen einige zusätzliche Konfigurationsparameter zur Verfügung, um den SIP-Stack zu steuern und den Inhalt von SIP-Header-Feldern anzupassen.
CLIP / CLIR	Das System stellt verschiedene Parameter zur Verfügung, um das Format der SIP-Header-Felder entsprechend den Bedürfnissen des nativen Trunks zu steuern Die Inhalte der folgenden Header-Felder, die die Quelle eines Aufrufs beschreiben, kann gesteuert werden: • Von: DisplayPart <sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>
Ausgehender CLIP in Von Header - Anzeigeteil	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer - die für eine Station konfigurierte Nummer. Welche Nummer in den "Routenparametern" verwendet wird, können Sie definieren • Konto - der Benutzername, der dem nativen Trunk zugewiesen ist • anzeigename
Ausgehender CLIP in Von Header - Benutzerteil:	Mögliche Einstellungen: • Rufnummer • Konto
Ausgehender Von Header - Domänen-/Hostteil:	Ändern Sie den Domänen-/Hostteil des URI, der mit der IP-Adresse des Systems ausgefüllt werden soll. Dieser Parameter beeinflusst den Hostteil aller drei Header-Felder Von:, PAI und PPI Mögliche Einstellungen: • domänenname • lokale IP-Adresse • öffentliche IP-Adresse

Parameter	Beschreibung
Umleitung: Von enthält die ursprüngliche Rufnummer:	Wird aufgrund der Anrufweiterleitung ein ausgehender Anruf aufgebaut, kann das System Informationen über den ursprünglichen Anrufer bereitstellen. Wenn aktiviert, sendet das System den ursprünglichen Anrufer (A-Ext) im Von: Header-Feld, andernfalls sendet es die Nummer der Weiterleitungsstation.
Umleitung: PAI enthält die ursprüngliche Rufnummer des Anrufers	Wird aufgrund der Anrufweiterleitung ein ausgehender Anruf aufgebaut, kann das System Informationen über den ursprünglichen Anrufer bereitstellen. Wenn aktiviert, sendet das System den ursprünglichen Anrufer (A-Ext) im P-Asserted-Id Header-Feld, andernfalls sendet es die Nummer der Weiterleitungsstation. Wenn Sie diese Flagge setzen, sendet das System den ursprünglichen Anrufer im P-Asserted_ID: Header-Feld und P-Preferred-ID:.
Ausgehender CLIP in P-Asserted-Id Header - Anzeigeteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer - die für eine Station konfigurierte Nummer. Welche Nummer in den "Routenparametern" verwendet wird, können Sie definieren • Konto - der Benutzername, der dem nativen Trunk zugewiesen ist • anzeigename
Ausgehender CLIP in P-Asserted-Id Header - Benutzerteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer • Konto
Ausgehender CLIP in P-Preferred-Id Header - Anzeigeteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer - die für eine Station konfigurierte Nummer. Welche Nummer in den "Routenparametern" verwendet wird, können Sie definieren • Konto - der Benutzername, der dem nativen Trunk zugewiesen ist • anzeigename
Ausgehender CLIP in P-Preferred-Id Header - Benutzerteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer • Konto
Ausgehender CLIP in Umleitung Header - Anzeigeteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer - die für eine Station konfigurierte Nummer. Welche Nummer in den "Routenparametern" verwendet wird, können Sie definieren • Konto - der Benutzername, der dem nativen Trunk zugewiesen ist • anzeigename

Parameter	Beschreibung
Ausgehender CLIP in Umleitung Header - Benutzerteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer • Konto
Ausgehender CLIP in Verlauf-Info Header - Benutzerteil:	Mögliche Einstellungen: • weglassen • callnumber
CLIR Ausgehender in Von Header - Anzeigeteil:	Mögliche Einstellungen: • Weglassen • Rufnummer • Konto • Anonym **Von: Anonym <sip: ...@...>**
CLIR Ausgehender in Von Header - Benutzerteil:	Mögliche Einstellungen: • Rufnummer • Konto • Völlig anonym**Von: ...<sip:anonymous@anonymous.invalid>** • Benutzer anonym **Von: ... <sip:anonymous@...>**
CLIR ausgehender Datenschutz-Header	Mögliche Einstellungen: • Weglassen • Id **Datenschutz: id** • Benutzer **Datenschutz: user** • Benutzer, id **Datenschutz: user;id**
COLP / TIP für ausgehende Anrufe unterstützt:	In ISDN wurde das Merkmal COLP (Connect Line Identification Presentation) eingeführt. In SIP wird dieses Merkmal manchmal als TIP (Termination Identification Presentation) bezeichnet. RFD3324 (Abschnitt 5.) definiert einen Mechanismus zum Transport der Identität der akzeptierenden Partei (C) im P-Asserted-Identity Header-Feld der 200 OK response: Mögliche Einstellungen: • COLP unterstützt • COLP nicht unterstützt
Formatierung von Rufnummern	

Parameter	Beschreibung
Eingehender Anruf - Nummer des angerufenen Teilnehmers:	Diese Flagge bezieht sich auf die Zieladresse eines Anrufs. Standardmäßig wird dies aus dem **Benutzerteil** des **AN: Header**-Felds übernommen. Mögliche Einstellungen: • Anfragezeile **INVITE sip: +498970070@...** • An Header-Anzeigeteil **An: +498970070 <sip:+** • An Header-Benutzerteil **An: <sip: +498970070@...** • P-Called-Party-Id Header-Anzeigeteil **P-Called-Party-ID: +498970070 <sip:..** • P-Called-Party-Id Header-Benutzerteil **P-Called-Party-ID: <sip: +498970070@..**
Eingehender Anruf - Nummer des Anrufers:	Diese Flagge bezieht sich auf die Quellenadresse eines Anrufs. Standardmäßig nimmt das System den Anrufer aus dem Von Header-Benutzerteil heraus. Mögliche Einstellungen: • automatisch • Von Header-Anzeigeteil **Von: +498970070 <sip:+** • Von Header-Benutzerteil **Von: <sip: +498970070@...** • P-Asserted-Id Header-Anzeigeteil **P-Asserted-ID: +498970070 <sip:..** • P-Asserted-Id Header-Benutzerteil **P-Asserted-ID: <sip: +498970070@..** Im automatischen Modus sucht das System zunächst im Benutzerteil der P-Asserted-Identity, falls vorhanden. Wenn keine P-Asserted-Identity vorhanden ist, wird der Benutzerteil des Von: Header-Feldes genommen.
Eingehender Anruf - Typ der Nummer (anrufend):	Mögliche Einstellungen: • automatisch • international
Eingehender Anruf - Typ der Nummer (angerufen):	Mögliche Einstellungen: • automatisch • international • national

Parameter	Beschreibung
Ausgehender Anruf - Typ der Nummer (anrufend):	Mögliche Einstellungen: • automatisch • international • national
Ausgehender Anruf - Typ der Nummer (angerufen):	Mögliche Einstellungen: • automatisch • international • national
Zuordnung der Anbieternummer:	Mögliche Einstellungen: • auf jeden Fall • Nur eingehend angerufen (falls konfiguriert) • aus
CLIP keine Screening-Unterstützung:	Mögliche Einstellungen: • nicht unterstützt • CLIP in Von / vertrauenswürdige Nummer in PAI • Unterstützt-Keine Sonderbehandlung • CLIP in Von / DuWa-Nummer in PAI
Ruf-Nr. mit internationaler/ nationaler Vorwahl:	Mögliche Einstellungen: • Nein • Ja
Angerufene Nummer im E164-Format:	Mögliche Einstellungen: • Nein • Ja
Routenoptimierung:	Mögliche Einstellungen: • nicht erlaubt • erlaubt • erlaubt (lokale IP in Kontakt)
MEX unterstützt:	Mögliche Einstellungen: • Nein • Ja
Kontakt-URI enthält:	Dieser Parameter wird verwendet, um den Inhalt des Benutzerteils der Kontakt-URI zu konfigurieren **Kontakt: sip:UserPart@HostPart:port** Mögliche Einstellungen: • Rufnummer: Der Benutzerteil der Kontakt-URI enthält die Rufnummer • Registrierungs-AOR: Die Kontakt-URI enthält den account=user-Teil der Registrierung.

Parameter	Beschreibung
Im Kontakt-URI verwendeter TCP-Port:	Dieser Parameter wird verwendet, um den im Hostteil der Kontakt-URI verwendeten tcp-port zu konfigurieren **Kontakt: sip:UserPart@HostPart:port** Mögliche Einstellungen: • ephem.src-port: Standardmäßig wird der ephemere tcp src-Port verwendet • SIP-Server-Port: Der SIP-Server-Port wird in der Kontakt-URI verwendet
Registrierung	
Register-Kontakt enthält IP-Adresse:	Mögliche Einstellungen: • localIPAddr • domainName
ContactUriWithProtocol:	aktivieren/deaktivieren
BNC-Registrierung (SIPconnect):	Mögliche Einstellungen: • normale Registrierung • BNC-Registrierung
Neuregistrierungsintervall nach Ausfall (Sek.):	
Neuregistrierungsmodus:	Mögliche Einstellungen: • kontinuierlich • SIPConnect
Neuregistrierung nach Anrufausfall:	Mögliche Einstellungen: • CallFailureIsNoRegFailure • CallFailureIsRegFailure
Sicherheit	
UDP-Modus:	Mögliche Einstellungen: • symmetrisches UDP • asymmetrisches UDP
Zugelassene Peer-Auswahl:	Mögliche Einstellungen: • Nur konfigurierte Server vertrauen • Vertrauensserver, die in SIP-Antworten empfangen wurden
Verschiedenes	
Direkte Nutzlast:	Bei einer direkten ITSP-Verbindung MUSS dieser Parameter auf false gesetzt werden. Wenn ein externer SBC vor OpenScape Business verwendet wird, wird dieser Parameter auf true gesetzt.

Parameter	Beschreibung
Vermeidung von Medienneuverhandlungen:	Bei einer direkten ITSP-Verbindung MUSS dieser Parameter auf true gesetzt werden. Wenn der Media-Handling-Parameter Direct Payload auf true gesetzt ist, hat dieser Parameter KEINE Wirkung. (z. B. in Fällen, in denen ein externer SBC vor dem OpenScape Business-System verwendet wird)
Attribut Richtung ändern:	Mögliche Einstellungen: • Attribut behalten • zu sendrecv wechseln
Attribut zur Unterdrückung von Stille:	Mögliche Einstellungen: • unterstützt • nicht unterstützt
Mediasec-Erweiterung:	Mögliche Einstellungen: • unterstützt • nicht unterstützt
SDP-Filter:	Mögliche Einstellungen: • Standardmäßig • Kompatibilitätsprofil • Offnen
UseRouteURIAuthentication:	True legt das Verhalten für die Verwendung der Route-URI anstelle der Anfrage-URI im (Proxy-) Authorization-Header für INVITE oder INFO fest (nicht für REGISTER). Die Anfrage-URI wird verwendet, wenn keine Route-URI vorhanden ist. Für ITSPs MUSS dieser Parameter auf true gesetzt werden.
100 Rel ignorieren:	Ein 'Supported: 100rel'-Header-Feld ignorieren, wenn es in INVITE empfangen wird. Da 100rel das Interworking mit Nicht-SIP-Teilnehmern stören kann, SOLLTE dieser Parameter auf true gesetzt werden
100 Rel unterstützen	Wenn dieses Flag gesetzt ist, fügt das System einen unterstützten 100rel-Header in die ausgehende Einladung ein. Damit kann der ITSP zuverlässige vorläufige Antworten, gefolgt von UPDATE-Nachrichten, senden. Dieser Parameter ist für die OpenScape Business V3 Mainboard-Familie und den Server uneingeschränkt nutzbar.
UseViaRPort:	Wenn auf true gesetzt, wird der rport-Parameter zum Via-Header hinzugefügt. *Via: SIP/2.0/UDP 192.168.138.1:5060;rport;* Wenn auf false gesetzt, wird dem Via-Header kein rport-Parameter hinzugefügt. *Via: SIP/2.0/UDP 192.168.138.1:5060;*

Parameter	Beschreibung
UPDATE unterstützt:	Wenn auf true gesetzt, wird UPDATE abhängig vom Inhalt des Allow-Header-Feldes verwendet. Wenn UPDATE im empfangenen Allow-Header-Feld nicht gesetzt ist, sendet der SIP-Stack nie ein UPDATE. Wenn auf false gesetzt, wird die UPDATE-Methode nie verwendet (stattdessen wird ein re-INVITE verwendet) Für ITSP MUSS dieser Parameter auf true gesetzt werden (Standard)
P-Early-Media Header-Unterstützung:	Mögliche Einstellungen: • nicht unterstützt • unterstützt
Unterstützung für Sitzungstijmer:	Mögliche Einstellungen: • nicht aktiv • auffrischungsrichtlinie Remote
Automatischen 183 Antworttimer senden (Sek):	Mit diesem Timer wird nach Ablauf der Zeit eine vorläufige Antwort (183) ausgelöst, wenn keine Fortschrittsinformationen vom System verfügbar sind. Dies ist notwendig, da einige Plattformen die Überwachungs-Timer nicht stoppen, wenn sie einen 100-Versuch erhalten (z. B. Broadsoft) 0 wird keine automatische Antwort gesendet; alle Antworten werden vom System ausgelöst 1-10 Timeout in sec, Timer wird beim Empfang einer INVITE-Anfrage vom ITSP gestartet. Bei Ablauf des Timers wird vom SIP-Stack eine 183 gesendet 0 (Standard)
UDP-Keep Alive:	Mögliche Einstellungen: • UdpKeepAliveON • UdpKeepAliveOFF • SendAliveOptions
Keep-Alive-Intervall für OPTIONEN (Sek.):	Mit diesem Parameter wird das Intervall für das Senden von SIP OPTIONS festgelegt 60 (Standard)
Erneute Registrierung bei OPTIONEN-Ausfall:	Mögliche Einstellungen: • NoRegisterOnFailure • RegisterOnFailure
Antwort auf OPTIONEN:	Mögliche Einstellungen: • Vollständige Antwort • Ohne Körper
Schaltflächen	
ITSP neu starten	Leitet eine neue Registrierung beim ITSP ein (nur mit aktiviertem ITSP möglich).

Parameterbeschreibung der Registerkarten:

- **STUN-Konfiguration bearbeiten**

Parameter	Beschreibung
STUN-Modus	Diese Einstellung gilt global für alle ITSPs, sofern STUN für sie aktiviert ist. Ob STUN benötigt wird oder nicht, hängt von der ITSP Infrastruktur und dem verwendeten Internet Router ab. STUN ist nicht erforderlich, wenn das ITSP NAT Traversal im eigenen Netzwerk auflöst. STUN stellt sicher, dass in SIP-Nachrichten anstelle der internen IP-Adresse die öffentlich zugängliche IP-Adresse verwendet wird.
STUN-Modus: Immer	STUN ist immer aktiv.
STUN-Modus: Automatisch	Der NAT-Typ des Routers zum Internet wird automatisch überprüft. Falls STUN erforderlich ist, wird es aktiviert. Ist kein STUN erforderlich oder möglich, wird STUN deaktiviert. Dies ist die empfohlene Standardeinstellung.
STUN-Modus: Statische IP-Adresse verwenden	Wenn das ITSP statische IP-Authentifizierung erfordert, ist eine statische IP-Adresse (öffentliche IP-Adresse) im DSL-Modem oder Internet-Router erforderlich. Die statische IP-Adresse und der Port müssen zusätzlich angegeben werden.
STUN-Modus: Verwenden Sie statische IP, öffentliche IP-Adresse	Statische IP-Adresse des DSL-Modems oder des Internet-Routers.
STUN-Modus: Statische IP, öffentlichen SIP-Port verwenden	Port des DSL-Modems oder des Internet-Routers.
STUN-Modus: Router zum Erhalt des Ports	Wenn keiner der oben genannten STUN-Modi funktioniert, sollte dieser Modus ausprobiert werden. Einige Modems und Internetrouter ändern den RTP-Port nicht für NAT und benötigen diesen Modus für den ordnungsgemäßen Betrieb.
Nat-Typ erkannt	Ist ein ITSP aktiv, wird hier der NAT-Typ angezeigt.
Default STUN Server	
IP-Adresse / Hostname	IP-Adresse oder Hostname des STUN-Servers (z. B. `stun.serviceprovider.com`). Dieser STUN Server wird für SIP@Home Wenn kein ITSP verwendet wird oder der gebrauchte ITSP keinen STUN Server anbietet.
Port	Port des STUN-Servers (z. B. `3478`)

Parameterbeschreibung der Registerkarten:

- **NAT-Typerkennung**

Parameter	Beschreibung
Automatische Aktivierung	Ermöglicht die automatische Erkennung des NAT-Typs.
NAT-Typerkennung starten	Startet die Erkennung des NAT-Typs manuell.

Parameterbeschreibung der Registerkarten:

- **Internettelefonie-Station hinzufügen**
- **Internettelefonie-Station bearbeiten**

- **Internettelefonie-Station löschen**

Parameter	Beschreibung
Internettelefonie-Station	Zugriffsdaten des vom ITSP zugewiesenen Kontos. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: SIP-Benutzer, SIP-ID usw. Möglicherweise müssen Sie hier auch die ITSP Kundennummer eingeben. Bei statischer IP-Authentifizierung muss hier die PABX-Nummer eingegeben werden.
Autorisierungsname	Der vom ITSP zugewiesene Autorisierungsname. Dies ist oft identisch mit dem Internettelefonie-Abonnenten.
Kennwort	Passwort vom ITSP zugewiesen. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: Kennwort, SIP-Kennwort usw.
Passwort bestätigen	Passwort vom ITSP zugewiesen. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: Kennwort, SIP-Kennwort usw.

Parameterbeschreibung der Registerkarten:

- **MSN-Eintrag hinzufügen**
- **MSN-Eintrag bearbeiten**
- **MSN-Eintrag löschen**
- **Alle MSN-Einträge löschen**

Parameter	Beschreibung
Internettelefonie-Telefonnummer / **Internettelefonie-Telefonnummer** / **Internettelefonie-Telefonnummer**	(Einzel) Rufnummer, die vom ITSP zugewiesen wird.
DuWa / **Interne Rufnummer**	Zugewiesene interne Rufnummer.
Standardeintrag	Die Aktivierung als Standardeintrag ermöglicht Benutzern, die keine eigene Internettelefonnummer haben, Anrufe über diese Nummer zu tätigen. Die Option kann nur für ein MSN ausgewählt werden. (nur für Unterstützung von Sprachanrufen, nicht Fax)
Internettelefonie-Station / **Internettelefonie-Station**	Zeigt die Internettelefonie-Station an

Parameterbeschreibung der Registerkarten:

- **DID-Bereich hinzufügen**
- **DID-Bereich bearbeiten**
- **DID-Bereich löschen**

Parameter	Beschreibung
PABX-Nummer	Vom ITSP zugewiesene Kopfnummer (ohne DID-Nummer)
Direktwahlband nach innen von ... bis	Bereich der vom ITSP zugewiesenen DID-Nummern
Beginn des internen Rufnummernbereichs	Erste interne Nummer, ab der eine automatische Zuweisung von Rufnummern gewünscht ist.

Parameter	Beschreibung
Direktwahlband automatisch Stationen zuweisen	Wenn ausgewählt, werden die DID-Nummern automatisch aufsteigend den internen Rufnummern zugeordnet und die entsprechenden MSN-Einträge generiert.

28.3.6.6 Sprachgateway > Networking > Knoten

Parameterbeschreibung der Registerkarten:

- **Networking-Knoten hinzufügen**
- **Networking-Knoten ändern**
- **Networking-Knoten löschen**

Parameter	Beschreibung
Knoten ID	Nur für manuelle Konfiguration ohne Wizard z.B. bei offener Nummerierung: Eingabe einer Knotennummer, die im Netzverbund eindeutig ist.
IP-Adresse	Nur für manuelle Konfiguration ohne Wizard z.B. bei offener Nummerierung: IP- Adresse des Knotens
Knotenüberwachung	Die Auswahl der Knotenüberwachung bewirkt eine periodische Überprüfung der Kommunikation mit dem Knoten. Voraussetzung ist, dass die Knotenüberwachung auch im anderen Knoten aktiviert ist.
Verschlüsselungseinstellung des Knoten	Durch die Auswahl von "sicher" wird die Verschlüsselung für die Sprachkommunikation mit dem Knoten aktiviert. Hierzu muss zusätzlich im System "Signaling und Payload Encryption" eingerichtet werden. Wertebereich: traditionell, sicher

28.3.6.7 Sprachgateway > Networking > Routing

Parameterbeschreibung der Registerkarten:

- **Rufnummer hinzufügen**
- **Alle Rufnummern löschen**

Parameter	Beschreibung
Knoten ID	Auswahl der Knotennummer
Rufnummer	Nur für manuelle Konfiguration ohne Wizard z.B. bei offener Nummerierung: Angabe der Kennzahl über die der Knoten erreichbar ist.

28.3.6.8 Sprachgateway > SIPQ-Verbindung

Über die SIP-Q-Verbindung werden die Parameter für zwei mögliche externe SIP-Q-Richtungen definiert. Über diese können beliebige externe SIP-Server wie z.B. OpenScape 4000 oder OpenScape Voice angeschaltet werden. Entsprechende Beispiele sind in den vorhandenen Templates eingepflegt.

Parameterbeschreibung der Registerkarten:

- **SIPQ-Verbindung hinzufügen**
- **SIPQ-Verbindung bearbeiten**
- **SIPQ-Verbindung löschen**

Parameter	Beschreibung
Template verwenden	Template, das als Basis verwendet werden soll.
Name	Name des externen SIP Servers (Template-Name).
Trunk aktivieren	Die Verbindung zum externen SIP-Server ist aktiviert. Standardwert: Deaktiviert
Trunk-ID im System	Auswahl zwischen zwei externen SIP-Q-Verbindungen. Wenn vorhanden, ist eine der beiden SIPQ-Verbindungen immer mit der UC Booster Card oder dem UC Booster Server belegt.
Name der Remote-Domäne	Hostname oder IP-Adresse des externen SIP-Servers. Der Wert ist in der Regel identisch mit dem Wert bei **IP-Adresse/Host-Name**.
SIP-Server	
IP Adresse/Host-Name	Hostname oder IP-Adresse des externen SIP-Servers.
Port	SIP-Port des externen SIP-Servers. Wertebereich: 0 oder 1024-65535, Standardwert: 5060
Sicherer Transport	Bei Anschaltung an OpenScape 4000 oder OpenScape Voice kann die verschlüsselte SIP-Signalisierung aktiviert werden (Signalling and Payload Encryption feature). Standardwert: Deaktiviert
SIP-Registrar	
Provider Registrar verwenden	Externer SIP-Server erfordert eine Registrierung. Standardwert: Deaktiviert
IP Adresse/Host-Name	Hostname oder IP-Adresse des Registrar-Servers.
Port	Portnummer des Registrar-Servers. Wertebereich: 0 oder 1024-65535, Standardwert: 5060
Registrierungsintervall (s)	Intervall (in Sekunden), in dem die Registrierung wiederholt wird. Wertebereich: 30 bis 86400, Standardwert: 300
Outbound Proxy/Inbound Proxy	
Provider Outbound/Inbound Proxy verwenden	Aktivierung des Outbound Proxy: Bestimmte Redundanz-Szenarien (z.B. mit OpenScape Branch Proxy) erfordern die Abwicklung der SIP-Signalisierung über einen Outbound Proxy. Aktivierung des Inbound Proxy: In bestimmeten Redundanz-Szenarien (z.B. mit OpenScape Voice) erfolgt die ankommende Signalisierung von einem separaten SIP-Server (Inbound proxy). Standardwerte: jeweils deaktiviert
IP Adresse/Host-Name	Hostname oder IP-Adresse des Outbound bzw. Inbound Proxy.

Parameter	Beschreibung
Port	Portnummer des Outbound bzw. Inbound Proxy. Wertebereiche: 0 oder 1024-65535

Parameterbeschreibung der Registerkarten:

- **SIPQ-Verbindungsteilnehmer hinzufügen**
- **SIPQ-Verbindungsteilnehmer bearbeiten**
- **SIPQ-Verbindungsteilnehmer löschen**

Parameter	Beschreibung
Benutzer-ID	Eingabe der Benutzer-ID für den Zugang zum SIP-Server.
Autorisierungsname / **Realm**	Eingabe des Autorisierungsnamens oder der Realm für den Zugang zum SIP-Server.
Kennwort	Eingabe des Kennworts für den Zugang zum SIP-Server.
Kennwort bestätigen	Wiederholung des Kennworts für den Zugang zum SIP-Server.

28.3.6.9 Sprach-Gateway > Nativer SIP-Server-Trunk

Hier werden die Parameter für 10 mögliche externe native SIP-Routen definiert. Über diese Routen kann jeder externe SIP-Server verbunden werden.

Parameterbeschreibung der Registerkarten:

- **Native SIP Server-Trunk hinzufügen**
- **Nativen SIP-Server-Trunk bearbeiten**
- **Native SIP Server-Trunk löschen**

Parameter	Beschreibung
Basisvorlage	Vorlage, die als Basis verwendet werden soll.
Stammname	Name des externen SIP-Servers (Vorlagenname).
Trunk aktivieren	Die Verbindung zum externen SIP-Server wird aktiviert. Standardwert: Deaktiviert
Stammkennung im System	Auswahl von 10 externen nativen SIP-Verbindungen. Ausgegraute Elemente werden von bereits konfigurierten ITSPs belegt (Max. 8 ITSPs möglich, in diesem Fall sind noch 2 Native SIP Verbindungen übrig).
Remote-Domänenname	Hostname oder IP-Adresse des externen SIP-Servers. Der Wert ist in der Regel identisch mit dem Wert bei **IP-Adresse / Hostname**. Beispiel: Der konfigurierte **Remote-Domänenname** wird im Hostteil der Felder From und PAI/PPI-Header verwendet (siehe unten): Von: sip: +49...@DomainName P-Asserted-Identity: sip: +49...@DomainName

Parameter	Beschreibung
Transportprotokoll	Auswahl des UDP- oder TCP-Protokolls.
Transportsicherheit	Wählen Sie zwischen tranditionalem UDP oder TCP und Secure TLS.
Mediensicherheit	Wählen Sie zwischen nur RTP, nur SDES und DTLS-SRTP. DTLS-SRTP ist ein Protokoll, das Datagram Transport Layer Security (DTLS) mit Secure Real-Time Transport Protocol (SRTP) kombiniert, um verschlüsselte und authentifizierte Medien-Streaming über das Internet bereitzustellen. **Anmerkung:** In neuen Bereitstellungen (ab V3R4) ist DTLS-SRTP Standard. Der Wechsel zu DTLS-SRTP von nur RT oder nur SDES erfordert einen Trunk-Neustart, damit er wirksam wird. **Anmerkung:** Restriktive Firewall-Einstellungen können sporadische oder dauerhafte Probleme mit der Sprachverbindung verursachen. Deaktivieren Sie in diesem Fall die Option DTLS-SRTP.
SIP-Server	
IP-Adresse / Hostname	Hostname oder IP-Adresse des externen SIP-Servers.
Port	SIP-Port des externen SIP-Servers. Standardwert: 5060, geben Sie Port 0 ein, wenn das ITSP DNSSRV verwendet
SIP-Registrar	
Registrar verwenden	Muss ausgewählt werden, wenn der Trunk mit Registrierung arbeitet (Standard = Aus)
IP-Adresse / Hostname	Hostname oder IP-Adresse des externen Registrar-Servers
Port	Port des externen Registrar-Servers standardwert: 5060, geben Sie Port 0 ein, wenn DNSSRV verwendet ist
Wiederregistrierungsintervall	Das Intervall, in dem eine Registrierung wiederholt wird (Standard = 600)
STUN-Server	
STUN verwenden	Muss ausgewählt werden, wenn der Trunk mit STUN arbeitet (Standard = Aus)
IP-Adresse / Hostname	Hostname oder IP-Adresse des STUN-Servers
Port	Port des STUN-Servers
Erweiterte SIP-Daten	
Erweiterte SIP-Daten anzeigen	Durch Aktivieren dieser Flagge stehen einige zusätzliche Konfigurationsparameter zur Verfügung, um den SIP-Stack zu steuern und den Inhalt von SIP-Header-Feldern anzupassen

Parameter	Beschreibung
CLIP / CLIR	Das System stellt verschiedene Parameter zur Verfügung, um das Format der SIP-Header-Felder entsprechend den Bedürfnissen des nativen Trunks zu steuern Die Inhalte der folgenden Header-Felder, die die Quelle eines Aufrufs beschreiben, kann gesteuert werden: • Von: DisplayPart <sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>
Ausgehender CLIP in Von Header - Anzeigeteil	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer - die für eine Station konfigurierte Nummer. Welche Nummer in den "Routenparametern" verwendet wird, können Sie definieren • Konto - der Benutzername, der dem nativen Trunk zugewiesen ist • anzeigename
Ausgehender CLIP in Von Header - Benutzerteil:	Mögliche Einstellungen: • Rufnummer • Konto
Ausgehender Von Header - Domänen-/Hostteil:	Ändern Sie den Domänen-/Hostteil des URI, der mit der IP-Adresse des Systems ausgefüllt werden soll. Dieser Parameter beeinflusst den Hostteil aller drei Header-Dateien Von:, PAI und PPI Mögliche Einstellungen: • domänenname • lokale IP-Adresse • öffentliche IP-Adresse
Umleitung: Von enthält die ursprüngliche Rufnummer:	Wird aufgrund der Anrufweiterleitung ein ausgehender Anruf aufgebaut, kann das System Informationen über den ursprünglichen Anrufer bereitstellen. Wenn auf true gesetzt, sendet das System den ursprünglichen Anrufer (A-Ext) im Von: Header-Feld, andernfalls sendet es die Nummer der Weiterleitungsstation.
Umleitung: PAI enthält die ursprüngliche Rufnummer des Anrufers	Wird aufgrund der Anrufweiterleitung ein ausgehender Anruf aufgebaut, kann das System Informationen über den ursprünglichen Anrufer bereitstellen. Wenn auf true gesetzt, sendet das System den ursprünglichen Anrufer (A-Ext) im P-Asserted-Id Header-Feld, andernfalls sendet es die Nummer der Weiterleitungsstation. Wenn Sie diese Flagge setzen, sendet das System den ursprünglichen Anrufer im P-Asserted_ID: Header-Feld und P-Preferred-ID:.
Ausgehender CLIP in P-Asserted-Id Header - Anzeigeteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer - die für eine Station konfigurierte Nummer. Welche Nummer in den "Routenparametern" verwendet wird, können Sie definieren • Konto - der Benutzername, der dem nativen Trunk zugewiesen ist • anzeigename

Parameter	Beschreibung
Ausgehender CLIP in P-Asserted-Id Header - Benutzerteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer • Konto
Ausgehender CLIP in P-Preferred-Id Header - Anzeigeteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer - die für eine Station konfigurierte Nummer. Welche Nummer in den "Routenparametern" verwendet wird, können Sie definieren • Konto - der Benutzername, der dem nativen Trunk zugewiesen ist • anzeigename
Ausgehender CLIP in P-Preferred-Id Header - Benutzerteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer • Konto
Ausgehender CLIP in Umleitung Header - Anzeigeteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer - die für eine Station konfigurierte Nummer. Welche Nummer in den "Routenparametern" verwendet wird, können Sie definieren • Konto - der Benutzername, der dem nativen Trunk zugewiesen ist • anzeigename
Ausgehender CLIP in Umleitung Header - Benutzerteil:	Mögliche Einstellungen: • Weglassen - Feld wird weggelassen • Rufnummer • Konto
Ausgehender CLIP in Verlauf-Info Header - Benutzerteil:	Mögliche Einstellungen: • weglassen • callnumber
CLIR Ausgehender in Von Header - Anzeigeteil:	Mögliche Einstellungen: • Weglassen • Rufnummer • Konto • Anonym **Von: Anonym <sip: ...@...>**
CLIR Ausgehender in Von Header - Benutzerteil:	Mögliche Einstellungen: • Rufnummer • Konto • Vollständig anonym **Von: ...<sip:anonymous@anonymous.invalid>** • Benutzer anonym **Von: ... <sip:anonymous@...>**
CLIR ausgehender Datenschutz-Header	Mögliche Einstellungen: • Weglassen • Id **Datenschutz: id** • Benutzer **Datenschutz: user** • Benutzer, id **Datenschutz: user;id**

Parameter	Beschreibung
COLP / TIP für ausgehende Anrufe unterstützt:	In ISDN wurde das Merkmal COLP (Connect Line Identification Presentation) eingeführt. In SIP wird dieses Merkmal manchmal als TIP (Termination Identification Presentation) bezeichnet. RFD3324 (Abschnitt 5.) definiert einen Mechanismus zum Transport der Identität der akzeptierenden Partei (C) im P-Asserted-Identity Header-Feld der 200 OK response: Mögliche Einstellungen: • COLP unterstützt • COLP nicht unterstützt
Formatierung von Rufnummern	
Eingehender Anruf - Nummer des angerufenen Teilnehmers:	Diese Flagge bezieht sich auf die Zieladresse eines Anrufs. Standardmäßig wird dies aus dem **Benutzerteil** des **AN: Header-Felds** übernommen. Mögliche Einstellungen: • Anfragezeile **INVITE sip: +498970070@...** • An Header-Anzeigeteil **An: +498970070 <sip:+** • An Header-Benutzerteil **An: <sip: +498970070@...** • P-Called-Party-Id Header-Anzeigeteil **P-Called-Party-ID: +498970070 <sip:..** • P-Called-Party-Id Header-Benutzerteil **P-Called-Party-ID: <sip: +498970070@..**
Eingehender Anruf - Nummer des Anrufers:	Diese Flagge bezieht sich auf die Quellenadresse eines Anrufs. Standardmäßig nimmt das System den Anrufer aus dem Von Header-Benutzerteil heraus. Mögliche Einstellungen: • automatisch • Von Header-Anzeigeteil **Von: +498970070 <sip:+** • Von Header-Benutzerteil **Von: <sip: +498970070@...** • P-Asserted-Id Header-Anzeigeteil **P-Asserted-ID: +498970070 <sip:..** • P-Asserted-Id Header-Benutzerteil **P-Asserted-ID: <sip: +498970070@..** Im automatischen Modus sucht das System zunächst im Benutzerteil der P-Asserted-Identity, falls vorhanden. Wenn keine P-Asserted-Identity vorhanden ist, wird der Benutzerteil des Von: Header-Felds übernommen.

Parameter	Beschreibung
Kontakt-URI enthält:	Dieser Parameter wird verwendet, um den Inhalt des Benutzerteils der Kontakt-URI zu konfigurieren **Kontakt: sip:UserPart@HostPart:port** Mögliche Einstellungen: • Rufnummer: Der Benutzerteil der Kontakt-URI enthält die Rufnummer • Registrierungs-AOR: Die Kontakt-URI enthält den account=user-Teil der Registrierung.
Im Kontakt-URI verwendeter TCP-Port:	Dieser Parameter wird verwendet, um den im Hostteil der Kontakt-URI verwendeten tcp-port zu konfigurieren **Kontakt: sip:UserPart@HostPart:port** Mögliche Einstellungen: • ephem.src-port: Standardmäßig wird der ephemere tcp src-Port verwendet • SIP-Server-Port: Der SIP-Server-Port wird in der Kontakt-URI verwendet

Parameterbeschreibung der Registerkarten:

- **Nativen SIP-Server-Trunk-Benutzer hinzufügen**
- **Nativen SIP-Server-Trunk-Benutzer bearbeiten**
- **Nativen SIP-Server-Trunk-Benutzer löschen**

Parameter	Beschreibung
UserId	Eingabe der Benutzer-ID für den Zugriff auf den SIP-Server.
Autorisierungsname	Eingabe des Autorisierungsnamens für den Zugriff auf den SIP-Server.
Kennwort	Eingabe des Passworts für den Zugriff auf den SIP-Server.
Passwort bestätigen	Wiederholung des Passworts für den Zugriff auf den SIP-Server.

28.3.7 Teilnehmer

Unter **Teilnehmer** sind die Funktionen für alle Teilnehmer zusammengefasst. Dazu gehören z.B. Name und Rufnummer der Teilnehmer, aber auch die Tastenprogrammierung.

28.3.7.1 Teilnehmer > Teilnehmer > UP0 Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.

Parameter	Beschreibung
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten Endgeräts.
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax DID	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **UP0 Master/Slave**

  Diese Registerkarte gibt es nur bei OpenScape Business X8, da bei diesem System die Slave-Ports dynamisch verwaltet werden. Bei OpenScape Business X1/X3/X5 sind die Slave-Ports fest zugeordnet.

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Slave-Zone hinzufügen	Ist dieses Kontrollkästchen aktiviert, wird dem ausgewählten Master-Port vorbereitend ein Slave-Port zugeordnet. Nach Speichern der Auswahl mit **Übernehmen** können vorab Rufnummer, Durchwahl und Name des Slave-Systemtelefons konfiguriert werden. Wird anschließend an dem Slave-Adapter des Master-Systemtelefons das Slave-Systemtelefon angeschlossen, wird es dem zuvor ausgewählten Slave-Port zugewiesen. Wird das Slave-Systemtelefon ohne vordefiniertem Slave-Port angeschlossen, wird automatisch der nächste freie Port (ab Port 384) belegt.
Slave-Zone löschen	Ist dieses Kontrollkästchen aktiviert, wird die Vorkonfiguration des Slave-Systemtelefons gelöscht. Ist ein Slave-Systemtelefon an dem Slave-Adapter des Master-Systemtelefons angeschlossen, ist das Kontrollkästchen ausgegraut. Die Vorkonfiguration kann nicht gelöscht werden.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **Endgeräte Info**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.

Parameter	Beschreibung
Name	Name des Teilnehmers.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten Endgerätes.
Aktuelle SW-Version	Software-Version des zugeordneten Endgerätes (sofern verfügbar).
HW Version	Hardware-Version des zugeordneten Endgerätes (sofern verfügbar).
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.2 Station > Station > IP-Clients

Parameterbeschreibung der Registerkarten:

- **Abonnenten bearbeiten**

Parameter	Beschreibung
Rufnummer	Interne Rufnummer des Teilnehmers.
DID	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Display	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Typ	Typ des Teilnehmers.
Typ: **Kein Port**	Diese Rufnummer ist noch keiner Station zugewiesen.
Typ: **System-Client**	Ein System-Client ist eine IP-Station, die über CorNet-IP alle Funktionen des Kommunikationssystems nutzen kann (früher als HFA-System-Client bezeichnet).
Typ: **RAS-Benutzer**	Ein RAS-Benutzer (Remote Access Service-Benutzer) erhält über die ISDN-Verbindung Internetzugang zum IP-Netzwerk. Dadurch kann das Kommunikationssystem aus der Ferne gewartet und lizenziert werden.

Parameter	Beschreibung
Typ: **SIP-Client**	Ein SIP-Client ist eine IP-Station, die das SIP-Protokoll verwendet. Er kann über SIP nur auf eingeschränkte Funktionen des Kommunikationssystems zugreifen.
Typ: **Deskshare-Benutzer**	Ein Deskshare-Benutzer ist ein IP-Benutzer, der sich an einem anderen IP-Systemtelefon anmelden (mobile Anmeldung) und dieses Telefon dann als sein eigenes Telefon (einschließlich der Rufnummer) verwenden kann.
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA)
Aktiv	Gibt an, ob die Station betriebsbereit ist.
Faxrufnummer	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax-DID	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der externe Faxnachrichten vom Teilnehmer empfangen werden können.
ITSP-Standort-ID	Die ITSP-Standort-ID einer Station.
Suche	Sie können ausgewählte Teilnehmer auch anzeigen lassen, indem Sie einen Suchbegriff in die **Suchfelder** eingeben und die Eingabetaste drücken. Die Teilnehmer, die dem Suchbegriff entsprechen, werden angezeigt. Wenn Sie alle **Suchfelder** leer lassen und die Eingabetaste drücken, werden alle Teilnehmer erneut aufgelistet.
Elemente pro Seite	Auswahl, um festzulegen, ob 10, 25, 50 oder 100 Elemente pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in der Spalte **Call no**	Öffnet die Seite mit den Registerkarten **Stationsparameter bearbeiten**, **Stationsmerkmale bearbeiten**, **Workpoint Client Daten bearbeiten** und **Gruppe/CFW bearbeiten**.
>	Blättert eine Seite weiter.
<	Blättert eine Seite zurück.
>|	Blättert zum Ende der Liste.
|<	Blättert zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **Geräte-Infos**

Bitte beachten Sie, dass die Sortierung für alle Spalten streng alphabetisch erfolgt. Es gibt keine spaltenspezifische numerische Sortierung für bestimmte Datentypen wie **IP-Adresse** oder **Aktuelle SW-Version**.

Parameter	Beschreibung
Rufnummer	Interne Rufnummer des Teilnehmers.
Display	Name des Teilnehmers.

Parameter	Beschreibung
Gerätetyp	Zeigt den mit der Station verbundenen Gerätetyp an.
IP-Adresse	IP-Adresse des verbundenen Geräts; direkter Link zum WBM des IP-Telefons.
MAC-Adresse	MAC-Adresse des verbundenen Telefons.
Aktuelle SW-Version	Softwareversion des verbundenen Geräts (falls verfügbar).
HW-Version	Hardwareversion des verbundenen Geräts (falls verfügbar).
PC-Port	Ist dieses Flag aktiviert, wird der PC Ethernet Port aller aktiven Systemtelefone eingeschaltet. Standard: deaktiviert
Codec-Einstellung	Ist dieses Flag aktiviert, gilt für alle Systemtelefone die folgende Codec-Priorisierung: G.729 - G.711 - G.722 Ist dieses Flag deaktiviert, gilt die folgende Codec-Priorisierung: G.722 - G.711 - G.729 **Anmerkung:** CP100 unterstützt G.722 nicht Standard: deaktiviert
Elemente pro Seite	Auswahl, um festzulegen, ob 10, 25, 50 oder 100 Elemente pro Seite angezeigt werden sollen.
Schaltflächen	
>	Blättert eine Seite weiter.
<	Blättert eine Seite zurück.
>|	Blättert zum Ende der Liste.
|<	Blättert zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **Sekundäres Gateway**

Parameter	Beschreibung
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Knoten-ID	Jedem Knoten in einem vernetzten System muss eine eindeutige Knoten-ID zugewiesen werden. Dadurch können die einzelnen Knoten in einem vernetzten System eindeutig identifiziert werden.
Fallback-Telefonie	Gibt an, ob die Funktion aktiviert ist.
Fallback-Rufnummer	Die Rufnummer der Station, die im Falle eines Ausfalls verwendet wird.
Fallback-Rufnummern-DID	Die interne Rufnummer der Station, die im Falle eines Ausfalls verwendet wird.

Parameterbeschreibung der Registerkarten:

- **Fallback Hosting**

Parameter	Beschreibung
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Primäre Knoten-ID	Die eindeutige Knoten-ID, für die die Station ursprünglich konfiguriert wurde.
Fallback-Rufnummer	Die Rufnummer der Station, die im Falle eines Ausfalls verwendet wird.
Fallback-Rufnummern-DID	Die interne Rufnummer der Station, die im Falle eines Ausfalls verwendet wird.

28.3.7.3 Station > Station > Analog Stations

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers. **Anmerkung:** Rufnummern, die mit einem Stern (*) beginnen, können nicht als Faxziel verwendet werden.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten Endgeräts.
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

Parameter	Beschreibung
Fax DID	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.4 Teilnehmer > Teilnehmer > ISDN-Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen

Parameter	Beschreibung
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten Endgeräts.
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax DID	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.5 Teilnehmer > Teilnehmer > DECT-Teilnehmer > SLC-Rufnummer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.

Parameter	Beschreibung
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten Endgeräts. Basisstationen werden als S0-Teilnehmer angezeigt.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Parameter	Standardansicht für alle Teilnehmer, Einstellungen nicht verändern
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.6 Teilnehmer > Teilnehmer > DECT-Teilnehmer > DECT-Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.

Parameter	Beschreibung
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten Endgeräts. DECT-Teilnehmer werden als Comfort-PP angezeigt.
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax DID	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.7 Teilnehmer > Teilnehmer > IVM/EVM Ports > EVM

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Voicemail-Ports.
Durchwahl	Durchwahlnummer des Voicemail-Ports, sofern vorhanden.
Vorname	Frei wählbarer Vorname des Voicemail-Ports. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Voicemail-Ports. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Voicemail-Ports. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA).
Aktiv	Zeigt an, ob der Voicemail-Port betriebsbereit ist.
Gerätetyp	Bei EVM wird S0-Teilnehmer angezeigt.
Zugang	Anzeige des internen Ports für die Voicemail.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Teilnehmertyp	Für die EVM ist "Phonemail" zu wählen, für Company AutoAttendant auf "Standard" stellen.
Parameter	Standardansicht für alle Voicemail-Ports, Einstellungen nicht verändern (z.B. "Sprache" ist nicht die Sprache der Voicemail-Ansagen).
Suche	Sie können sich auch ausgewählte Voicemail-Ports anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Voicemail-Ports werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Voicemail-Ports aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.

Parameter	Beschreibung
|<	Springt zum Anfang der Liste.

28.3.7.8 Teilnehmer > Teilnehmer > Virtuale Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des virtuellen Teilnehmers.
Durchwahl	Durchwahlnummer des virtuellen Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Type	Frei oder Virtueller Teilnehmer (bei Mobility Entry feste Anzeige)
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA)
Aktiv	Zeigt an, ob der virtuelle Teilnehmer betriebsbereit ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.9 Teilnehmer > Teilnehmer > Teilnehmer-Parameter

Parameterbeschreibung der Registerkarten:

- **Teilnehmer-Parameter ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Display	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Durchwahl	Durchwahlnummer des Teilnehmers.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten Endgeräts.
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Gerätebereitstellung	Dieses Menü ist nur für SIP-Teilnehmer sichtbar und die folgenden Werte sind verfügbar: • **Standard** (Standardwert) • **Mitel SIP DECT-Gerät** (Das spezifische SIP-Gerät wird für das Mitel SIP DECT verwendet). **Anmerkung:** Die **Mitel SIP DECT-Gerät**e-Option wird ausschließlich auf V3-Hardware und OSBiz S Systemen unterstützt.
Mitel SIP DECT Konfiguration: Dieses Menü wird nur sichtbar, wenn **Mitel SIP DECT-Gerät** unter **Gerätebereitstellung** ausgewählt ist.	
PIN	Der PIN-Code des Geräts.
Tastensperre Aktiviert	Aktivieren (Ja) oder deaktivieren (Nein) Sie die Tastensperre des Geräts.
Tastensperr-PIN	Die PIN für die Tastensperre.

Parameter	Beschreibung
Zeit der Tastensperre	Die Zeit, nach der die Tastensperre aktiviert wird.
Persönliches Verzeichnis anzeigen	Wählen Sie, ob das persönliche Verzeichnis sichtbar (Ja) oder nicht sichtbar (Nein) ist.
Fax	
Rufnummer	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Durchwahl	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der externe Faxnachrichten vom Teilnehmer empfangen werden können.
Mobility	
Typ	Typ des Teilnehmers: • Mobility Teilnehmer • Virtuelle Teilnehmer • SFB-Teilnehmer • Vertrauenswürdiger externer Teilnehmer: virtueller Teilnehmertyp, der verwendet werden soll, um einen vertrauenswürdigen externen Benutzer zu erstellen
Rufnummer der Mobil-/Sfb-/ Vertrauens-Außenstation	Nur für SIP-Clients und mobile Teilnehmer: Für One-Number-Service dient diese Rufnummer zur Authentifizierung des DISA-Zugangs per Mobilfunk. Geben Sie hier die zugehörige Mobilfunk-Rufnummer des Teilnehmers mit Amtskennziffer ein (z. B. 0017312345678). **Anmerkung:** Das Feld **Rufnummer des vertrauenswürdigen externen Teilnehmers** ist obligatorisch. Wenn Sie die Konfiguration mit einem leeren Feld für die **Rufnummer des vertrauenswürdigen externen Teilnehmers** anwenden, wird folgende Warnmeldung angezeigt: *„Die Rufnummer des vertrauenswürdigen externen Teilnehmers darf nicht leer sein!*“. Nachdem Sie bei der ersten Meldung auf **OK** geklickt haben, wird eine zweite Meldung angezeigt*: „Die Eingabe konnte nicht verarbeitet werden, bitte überprüfen Sie dies*“.
Web Feature ID	Die Web Feature ID legt fest, wie sich der Teilnehmer am mobilen web Client einloggen soll (Benutzername). Auswahl zwischen "keine" (nur Mobility Entry) und "automatisch" (interne Rufnummer des Teilnehmers) oder Auswahl der Rufnummer des Clients bzw. des Telefons aus der Klappliste.
Parameter	
Teilnehmertyp	Typ des angeschlossenen Endgeräts (Klappliste)
Teilnehmertyp: **Standard**	Systemtelefone oder analoge Telefone
Teilnehmertyp: **Fax**	Faxgerät, z.B. kein Aufschalten möglich

Parameter	Beschreibung
Teilnehmertyp: **Lautsprecher**	Für eine über den a/b-Port realisierte Durchsage-Einrichtung
Teilnehmertyp: **Anrufbeantworter**	Nur bei analog: Ist an dieser Schnittstelle ein Anrufbeantworter angeschlossen, kann mit dieser Einstellung von jedem Endgerät ein Gespräch vom Anrufbeantworter übernommen werden, auch wenn der Anrufbeantworter das Gespräch bereits angenommen hat. Dazu muss am Endgerät eine Taste mit der internen Rufnummer dieses analogen Teilnehmers programmiert werden. Dieser Eintrag sollte außer für Anrufbeantworter auch für virtuelle Ports gewählt werden, bei denen keine physikalischen Geräte eingerichtet sind. Hierdurch wird verhindert, dass das Kommunikationssystem den Port auf dessen Betriebszustand prüft. Nur für virtuelle Ports: Wurde im Manager E ein Teilnehmer ohne Zugang als Typ Anrufbeantworter konfiguriert, muss der Port zusätzlich als virtueller Port konfiguriert sein. Ansonsten ist er im WBM nicht als Teilnehmer sichtbar.
Teilnehmertyp: **AB Tln MW LED**	Für analoge Telefone (NoFe = Normalfernsprecher) mit Message Waiting-LED Nicht für U.S.
Teilnehmertyp: **Teilnehmer mit Impulsschleife**	Bei Verwendung eines Impulsschleifen-Endgerätes mit Türöffner-Funktion
Teilnehmertyp: **Modem**	Bei dieser Einstellung ist kein Aufschalten möglich. Sie ist vorgesehen für Modems.
	Wenn ein Fax- oder Modem-Teilnehmer gelöscht wird (Ruf-Nr. und Durchwahl werden gelöscht), muss auch der Stationstyp wieder auf Standard gesetzt werden.
Sprache	Sprache für die Menüsteuerung des Endgeräts (Systemtelefons).
Rufsignalisierung intern	Hier können jedem Teilnehmer eine von insgesamt acht internen Rufsignalisierungen zugewiesen werden. Damit wird zusätzlich zu dem externen Rufton nun ein interner Rufton zugewiesen, der bei einem internen Anruf übertragen wird. Standardwert: Rufart 1
Rufsignalisierung extern	Drei verschiedene Rufarten für die Signalisierung externer Anrufe können hier ausgewählt werden: – Systemtelefone: Rufart 1 = Externer Anruf (z. B. doppelter Ruf), Rufart 2 = Externer Anruf CO 2 (z. B. dreifacher Ruf), Rufart 3 = Externer Anruf CO 3 (z. B. kurz/lang/kurz) – Analoge Endgeräte, Deutschland: Rufart 1 = Externer Anruf, Rufart 2 = Wiederanruf, Rufart 3 = Türklingelruf – Analoge Endgeräte, andere Länder: Rufart 1 = Externer Anruf, Rufart 2 = Externer Anruf, Rufart 3 = Externer Anruf Standardwert: Rufart 1
Berechtigung (LCR)	Ein Teilnehmer kann einen Weg nur dann belegen, wenn seine Berechtigung größer oder gleich der LCR-Berechtigung in der Wegetabelle ist, das heißt ein Teilnehmer mit Berechtigung 7 kann einen Weg mit Berechtigung 8 nicht belegen. Standardmäßig sind alle Teilnehmer mit maximaler LCR-Berechtigung (15) eingetragen. Standardwert: 15

Parameter	Beschreibung
Hotline Modus	Auswahl der Hotline-Optionen
Hotline Modus: **aus**	Hotline-Funktion ausgeschaltet.
Hotline Modus: **Röcheln**	Der Ruf zur Hotline erfolgt nach einer vorgegebenen Wartezeit (Röchelzeit), siehe Telefonie/Grundeinstellungen/System/Abwurf-VPL-Hotline
Hotline, Modus: **Hotline**	Hotline-Funktion eingeschaltet. Beim Abheben des Hörers wird sofort die Verbindung zum Hotline-Ziel aufgebaut, siehe Telefonie/Grundeinstellungen/System/Abwurf-VPL-Hotline
Hotline	Auswahl der Hotline-Ziele, siehe Telefonie/Grundeinstellungen/System/Abwurf-VPL-Hotline
Hotline: **keine**	Kein Ziel definiert
Hotline: **Ziffern 1 bis 6**	Hotline-Ziele, siehe Telefonie/Grundeinstellungen/System/Abwurf-VPL-Hotline
Payload Security (für IP-System-Clients)	Aktivieren oder Deaktivieren der Verschlüsselung von Telefongesprächen (SPE). Dazu müssen alle beteiligten Teilnehmer SPE aktiviert haben. Standard-Wert: Ein
Payload Security (für TDM-/ Analoge Telefone)	Gibt an, ob der spezifische Endpunkt aus Sicht der Infrastruktur gesichert ist oder nicht, da die Payload Security nur für IP-Telefone funktioniert. Wenn dieser Parameter auf „Ein“ gesetzt ist und das Flag SPE Support System aktiviert ist, wird angezeigt, ob der Verbindungspfad zwischen dieser Station und einer IP-Station verschlüsselt ist oder nicht. Wenn der Parameter auf „Aus“ gesetzt ist, werden keine Informationen angezeigt. Standardwert: Aus
MWI-Protokoll	Auswahl des MWI-Protokolls für analoge Teilnehmer. Verfügbar nur für SLMAVx (OpenScape Business X8), 4SLAV onboard und SLAVx OpenScape Business X3, X5.
MWI-Protokoll: Comtel3	ComTel3-Protokoll ausgewählt. Standardwert.
MWI-Protokoll: Hochspannung	Hochspannungsprotokoll ausgewählt. Verfügbar nur für SLMAVx (OpenScape Business X8).
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die **Suche**-Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.
<	Springt einen Teilnehmer zurück.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer-Flags ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.

Parameter	Beschreibung
Name	Name des Teilnehmers.
Teilnehmer-Flags	
Aufschaltberechtigung ein	Wenn dieses Flag aktiviert ist, kann sich der Teilnehmer in die laufende Verbindung eines internen Teilnehmers aufschalten (bzw. diese überschreiben). Die beteiligten Teilnehmer werden durch einen Aufmerksamkeitston und durch eine Displaymeldung über das Aufschalten informiert. Standardwert: Deaktiviert
Anrufschutz durchbrechen	Bei aktiviertem Flag gilt: Trifft der Teilnehmer auf einen internen Teilnehmer mit aktiviertem Anrufschutz, kann er den Anrufschutz durchbrechen. Nach fünf Sekunden wird dem gerufenen Teilnehmer der Anruf signalisiert. Bei deaktiviertem Flag kann der Anrufschutz nicht durchbrochen werden. Trifft der Teilnehmer auf einen internen Teilnehmer mit aktiviertem Anrufschutz, erhält er den Besetztton. Standardwert: Deaktiviert
AUL extern erlaubt	Bei aktiviertem Flag kann der Teilnehmer eine Anrufumleitung zu einem externen Ziel aktivieren. Die bei der Ausführung einer externen Anrufumleitung anfallenden Gebühren werden dem Teilnehmer zugewiesen, der die Anrufumleitung aktiviert hat. Standardwert: Aktiviert
Direktansprechschutz aus	Bei aktiviertem Flag kann der Teilnehmer direkt angesprochen werden. Ermöglicht wird damit ein interner Verbindungsaufbau, ohne dass der Teilnehmer den Hörer abhebt. Der Lautsprecher des Teilnehmers wird dabei automatisch eingeschaltet. Standardwert: Aktiviert
DISA-Berechtigung	Bei aktiviertem Flag kann der Teilnehmer von extern über DISA (Direct Inward System Access) – wie als interner Teilnehmer – Funktionen des Kommunikationssystems aktivieren oder deaktivieren und gehende externe Verbindungen aufbauen. Dazu gehört zum Beispiel das Aktivieren und Deaktivieren einer Anrufumleitung, des Anrufschutzes und des Codeschlosses. Standardwert: Deaktiviert
Transit schalten durch Auflegen	Bei aktiviertem Flag kann der Teilnehmer ein externes Gespräch an einen anderen externen Teilnehmer durch Auflegen übergeben. Beispiel: Der Teilnehmer ist Konferenzleiter und legt auf: Verbleiben interne Teilnehmer in der Konferenz, wird der am längsten teilnehmende interne Teilnehmer automatisch zum Konferenzleiter. Verbleiben ausschließlich externe Teilnehmer in der Konferenz, wird die Konferenz beendet und alle Verbindungen werden getrennt. Standardwert: Deaktiviert
Codeschloss zurücksetzen	Bei aktiviertem Flag kann der Teilnehmer das individuelle Codeschloss anderer interner Teilnehmer auf den Standardcode zurücksetzen. Standardwert: Deaktiviert

Parameter	Beschreibung
Kommendes CLIP für Analog (nur für analoge Teilnehmer)	Bei aktiviertem Flag wird im Telefondisplay des analogen Teilnehmers die Rufnummer des Anrufers angezeigt. Voraussetzung dafür ist, dass das analoge Telefon des Teilnehmers CLIP (Calling Line Identification Presentation) unterstützt. Standardwert: Aktiviert
Zugriff für Fangen	Bei aktiviertem Flag kann der Teilnehmer unerwünschte externe Anrufer über das ISDN-Amt identifizieren lassen. Voraussetzung dafür ist, dass die Freischaltung der Leistungsmerkmals "Fangen" (Malicious Call Identification MCID) beim Netzbetreiber beantragt wurde und erfolgt ist. Nach der Freischaltung des Leistungsmerkmals "Fangen" durch den Netzbetreiber ist folgendes zu beachten: Bei jeder kommenden Verbindung vom ISDN-Amt wird nach Auflegen des Anrufers das Auslösen der Verbindung zum gerufenen Teilnehmer für eine bestimmte Zeit verzögert. Diese Zeitverzögerung stellt sicher, dass der gerufene Teilnehmer das Leistungsmerkmal "Fangen" aktivieren kann. Dadurch wird die Verfügbarkeit der ISDN-Amtsleitungen reduziert. Standardwert: Deaktiviert
Eintrag in Telefonbuch	Wenn dieses Flag aktiviert ist, werden der Name und die Nummer des Teilnehmers im Systemverzeichnis (einschließlich ODS) angezeigt. Standardwert: Aktiviert
Editieren der Wahl	Bei aktiviertem Flag kann der Teilnehmer die über die Wähltastatur eingegebenen Ziffern der Rufnummer vor der Wahlaussendung ändern (editieren). Voraussetzung dafür ist ein Systemtelefon mit Display. Standardwert: Deaktiviert
Keine Rufzuschaltung bei besetzt	Bei aktiviertem Flag gilt: Der Zustand des rufzuschaltenden Teilnehmers bestimmt, ob eine Rufzuschaltung durchgeführt wird. Der rufzuschaltende Teilnehmer ist frei: Alle zugeschalteten Teilnehmer werden sofort gerufen. Beim rufzuschaltenden Teilnehmer kann angeklopft werden: Alle zugeschalteten Teilnehmer werden nach 5 Sekunden gerufen. Beim rufzuschaltenden Teilnehmer kann nicht angerufen oder angeklopft werden: Es erfolgt keine Rufzuschaltung. Standardwert: Deaktiviert
Assoziierte Wahl/Dienste	Assoziierte Wahl: Bei aktiviertem Flag kann der Teilnehmer für einen anderen internen Teilnehmer eine Rufnummer wählen, so als würde der andere Teilnehmer selbst wählen. Assoziierte Dienste: Bei aktiviertem Flag kann der Teilnehmer für einen anderen internen Teilnehmer Leistungsmerkmale steuern, so als würde der andere Teilnehmer die Leistungsmerkmale selbst steuern. Dazu gehört zum Beispiel das Aktivieren und Deaktivieren einer Anrufumleitung, einer Rufzuschaltung und des Codeschlosses. Standardwert: Deaktiviert
Anklopfschutz ein	Bei aktiviertem Flag gilt: Führt der Teilnehmer ein Gespräch, erhält er keine Informationen über weitere kommende Anrufe mittels Anklopfton und Displaymeldung. Standardwert: Aktiviert

Parameter	Beschreibung
Diskret Ansprechen	Bei aktiviertem Flag kann sich der Teilnehmer in die bestehende Gesprächsverbindung eines internen Teilnehmers einschalten. Er kann unbemerkt mithören und mit dem internen Teilnehmer sprechen, ohne dass der andere Teilnehmer dies hört. Voraussetzung dafür ist, dass es sich um eine Zweierverbindung handelt. Bei Rückfragegesprächen oder Konferenzen ist kein diskretes Ansprechen möglich. Standardwert: Deaktiviert
Schutz Diskretes Anspr.	Bei aktiviertem Flag kann der Teilnehmer nicht diskret angesprochen werden. Standardwert: Deaktiviert
DTMF-basierte Leistungsmerkmalaktivierung	Nur relevant für Mobility Entry Teilnehmer: Um im Gesprächszustand Leistungsmerkmale aktivieren zu können, muss dieses Flag gesetzt sein. Der Code Receiver bleibt aktiv. (Achtung: begrenzte Ressourcen) Standardwert: Deaktiviert
Headset	Bei aktiviertem Flag kann beim Teilnehmer eine Kopfsprechgarnitur am Handapparat-Anschluss angeschlossen werden. Das Flag bewirkt, dass man Anrufe durch Drücken einer Headset-Taste am Systemtelefon bei aufliegendem Handapparat entgegennehmen kann. Der Einsatz einer Kopfsprechgarnitur am Headset-Anschluss eines Systemtelefons wird vom Kommunikationssystem automatisch erkannt, eine Berechtigungsfreigabe ist hier nicht erforderlich. Ist dieses Flag aktiviert, können Anrufe nicht über die Lautsprecher-Taste ausgelöst werden; es muss dann für das Auslösen von Verbindungen eine Trennen-Taste programmiert werden. Standardwert: Deaktiviert
Vertretermailbox aktiv	Ist das Flag aktiviert und ist der Angerufene nicht erreichbar, dann wird der Anruf auf die Mailbox des Vertreters umgeleitet und die Rufnummer des Anrufenden wird am Display des Vertreter-Endgeräts angezeigt. Standardwert: Deaktiviert
Anrufprio./Sof. Freiton Anklopfen	Bei aktiviertem Flag (Anrufpriorität/Sofortiger Freiton bei Anklopfen) werden Anrufe durch diesen Teilnehmer mit höherer Priorität beim Partner signalisiert. Die Priorität wird dabei gleich gesetzt mit der Priorität von externen Anrufen. Die priorisierten Anrufe werden somit vor bestehende Internrufe, jedoch nach bestehenden Externrufen eingereiht. Dabei ist zu beachten, dass bestehende Erstanrufe (nicht anklopfende Rufe) unabhängig von ihrer Rufart generell nicht verdrängt werden. Soll auch bei einem internen Anruf in einen anderen Knoten die Priorität entsprechend gesetzt werden, muss zusätzlich auch für die entsprechende Leitung das Leitungsflag „Anrufprio./Sof. Freiton Anklopfen“ (Bereich: Leitung Flags, Anrufprio./Sof. Freiton Anklopfen) gesetzt sein. Ist dieses Flag gesetzt, bekommt der Anrufer beim Anklopfen einen sofortigen Freiton anstatt des Besetztttons. Dieses hat keinen Einfluss auf die akustische Signalisierung. Die priorisierten Anrufe werden weiterhin wie ein Internruf signalisiert. Dieses Leistungsmerkmal ist wichtig bei Phonemail-Anschlüssen. Standardwert: Deaktiviert

Parameter	Beschreibung
Sprachaufzeichnung	Bei aktiviertem Flag kann der Teilnehmer während eines Gesprächs die Sprachaufzeichnung aktivieren. Über Flags, Schalter **Hinweiston bei Sprachaufzeichnung** kann zusätzlich angegeben werden, ob während der Sprachaufzeichnung ein Hinweiston ausgegeben werden soll. Unter PhoneMail muss ein geeignetes Live Recording Aufnahmegerät eingerichtet sein. Standardwert: Deaktiviert
Display-Ausgaben komprimieren	Bei aktiviertem Flag werden die Display-Ausgaben zum Zweck einer besseren Performance komprimiert. Ändert sich die Displayanzeige an einem UP0/E-Endgerät, aktualisiert das Kommunikationssystem nur die Daten, die sich von der vorhergehenden Anzeige unterscheiden. Bei Anschluss einer Anwendung (z.B. Smartset/TAPI) über einen RS-232-Adapter (Data- bzw. Control-Adapter) muss dieses Leistungsmerkmal deaktiviert sein. Bei Applikationen, die Rufnummerninformationen aus der Displayanzeige des Endgerätes beziehen, muss das Flag deaktiviert werden (d. h. unkomprimierte Ausgabe mit Rufnummer statt komprimierter Ausgabe mit Namen). Namen werden generell nur angezeigt, wenn unter Display "Name/Rufnummer anzeigen" das Flag "nur Rufnummer" deaktiviert ist. Standardwert: Aktiviert
Türfreigabe, DTMF	Bei aktiviertem Flag kann der Teilnehmer mittels DTMF/MFV-Code die Tür öffnen, wenn am betreffenden Port ein Tür-Relais angeschlossen ist. Standardwert: Deaktiviert
Automatische Rufannahme, CSTA (nur für OpenStage-SIP-Telefone)	Bei aktiviertem Flag gilt: Bei der Wahl oder der Rufannahme über myPortal oder myAttendant wird am zugehörigen SIP-Telefon der Freisprechmodus aktiviert. Die Angaben in der Dokumentation des SIP-Telefons sind zu beachten, da für die einwandfreie Nutzung des Leistungsmerkmals eventuell zusätzliche Einstellungen am SIP-Telefon notwendig sind. Bei deaktiviertem Flag erfolgt der Gesprächsaufbau erst nach Abnehmen des Hörers. Standardwert: Aktiviert
Handsfree Mikrofon sperren	Ist das Flag aktiviert, so ist die Nutzung des Freisprechmikrofons nicht möglich. Das Flag wird ausschließlich durch OpenStage-Telefone unterstützt. Standardwert: Deaktiviert
Nummer Anzeige Erzwingen	Bei aktiviertem Flag wird anstelle des Namens die Rufnummer des rufenden Teilnehmers im Display des gerufenen Teilnehmers angezeigt. Standardwert: Deaktiviert
Nutzung (nur für bestimmte Länder)	Mit dieser Dropdown-Liste kann der Ausgangsstrom der Schnittstellen einer Analogkarte konfiguriert werden (in mA, z. B. 27 mA für China).
Allgemeiner Betriebszustand	In dieser Klappliste kann eine Betriebsart des Teilnehmeranschlusses ausgewählt werden.

Parameter	Beschreibung
Anruferliste ausgeben	Bei aktiviertem Flag wird für den Teilnehmer die Anruferliste in seinem Telefon aktiviert (nur Telefone mit Display). Anrufe, die nicht vom Teilnehmer entgegengenommen wurden, werden mit einem Zeitstempel (Uhrzeit und Datum) versehen und in eine chronologisch sortierte Liste übernommen. Es werden nur Anrufe aufgezeichnet, die auch eine Rufnummer oder einen Namen enthalten. Ruft ein Teilnehmer wiederholt an, so wird nur der Zeitstempel des Eintrages aktualisiert und ein Anrufzähler für diesen Anrufer inkrementiert.
Zentrale Besetztsignalisierung	Für Teilnehmer, die Besetztsignalisierung auf ein zentralisiertes Kommunikationssystem haben, muss dieses Flag gesetzt werden (siehe auch QSIG-Leistungsmerkmale). Gilt nicht in USA. Die Realisierung der zentralen Besetztsignalisierung sieht eine maximale Anzahl von 100 Teilnehmern pro Knoten vor.
Anzeige Notbetrieb-Text	Ist dieses Flag aktiviert, wird im Notbetrieb ein konfigurierbarer Notbetriebs-Text im Display des Telefons angezeigt.
Call Supervison	Bei aktiviertem Flag kann der Teilnehmer das Gespräch eines beliebigen internen Teilnehmers mithören. Das Mikrofon des mithörenden Teilnehmers wird automatisch stummgeschaltet. Eine Information der überwachten Teilnehmer mittels Signalton oder Displayanzeige erfolgt nicht. Beim Beginn und beim Beenden der Call Supervision können Gesprächsaussetzer von bis zu zwei Sekunden auftreten. Standardwert: Deaktiviert
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die **Suche**-Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.
<	Springt einen Teilnehmer zurück.

Parameterbeschreibung der Registerkarten:

- **Workpointclient Daten ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Parameter	
Status Message	Nur für System-Clients: Dieses Flag aktiviert den “keep-alive”-Mechanismus für Systemtelefone. Fällt ein Systemtelefon z. B. aus, so wird nach vier Minuten dieses Systemtelefon als inaktiv gekennzeichnet. Beim Einrichten eines Systemtelefons als Heimarbeitsplatz sowie bei der Nutzung des Leistungsmerkmals “Short Hold” darf das Flag nicht aktiviert sein. Wenn dieses Flag nicht aktiviert ist, wird der Meldungsverkehrs zwischen dem Kommunikationssystem und den Systemtelefonen reduziert.

Parameter	Beschreibung
Authentifizierung aktiv	Soll sich der IP-Client am Kommunikationssystem mit einem Kennwort identifizieren, muss die Authentifizierung aktiviert und ein Kennwort vergeben werden. Dies ist insbesondere bei Clients von Vorteil, die nicht im internen LAN liegen, sondern sich von außen einwählen. Nur für SIP-Clients: Sie müssen ein Kennwort eingeben. Dasselbe Kennwort muss im Gerät verwendet werden.
Neues Kennwort	Kennwort für die Authentifizierung. Nur für SIP-Clients: Wenn das Gerätekennwort noch nicht eingestellt ist, muss dasselbe Kennwort bei „Übernehmen“ verwendet werden, um die Geräteregistrierung zu behalten.
Passwort bestätigen	Kennwort für die Authentifizierung wiederholen.
SIP User ID / Benutzername	Nur für SIP-Clients: Frei wählbarer Benutzernamen für die Authentifizierung des SIP-Teilnehmers, z. B. "SIP-120". Der hier definierte Wert muss auch am SIP-Telefon eingegeben werden.
Realm	Nur für SIP-Clients: frei wählbarer Namen für die zugehörige Zone, z. B. "OSBIZ-SIP". Dieser Wert muss für alle SIP-Clients gleich sein. Der hier definierte Wert muss auch am SIP-Telefon eingegeben werden.
Feste IP Adresse verwenden	Nur für SIP-Clients: Die Eingabe einer festen IP Adresse stellt sicher, dass sich nur ein SIP-Client mit dieser IP Adresse am System anmelden kann. Wenn dieses Flag aktiviert wird, werden die IP Adresse und die Rufnummer überprüft. Ist das Flag nicht aktiviert, wird nur die Rufnummer überprüft.
IP-Adresse	Nur für SIP-Clients: IP-Adresse des SIP-Clients (z.B. die IP-Adresse des SIP-Telefons)
Typ	Nur für System-Clients: Ein mobiler IP Client (Option Mobil) ist keinem IP Telefon fest zugeordnet. Mit der Rufnummer eines mobilen IP Clients kann sich ein Teilnehmer über die Anmeldeprozedur (*9419) an jedem IP-Endgerät anmelden, das dieses erlaubt (Option Mobil blockiert ist nicht aktiviert).
Typ: **Mobile Rufnummer**	Nur für System-Clients: Dem Teilnehmer ist kein IP-Endgerät fest zugeordnet. Das Leistungsmerkmal wird erst ab dem dritten Teilnehmerport unterstützt.
Typ: **Nicht mobil**	Nur für System-Clients: Dem IP-Endgerät des Teilnehmers ist die Rufnummer fest zugeordnet. Bei Einsatz eines WLx-Phones muss die Option Nicht mobil gesetzt sein, bevor das WLx- Phone am Kommunikationssystem registriert ist.
Typ: **Nicht mobil und blockiert**	Nur für System-Clients: Ein Teilnehmer kann sich nicht mit einem mobilen System-Client an diesem IP-Endgerät anmelden.
Blockiert für Deskshare-Teilnehmer	Nur für System-Clients: Dieses System-Telefon können sich mehrere Teilnehmer teilen (DeskSharing).
ID des Sekundärsystems	Dieser Parameter hat zwei unterschiedliche Funktionalitäten: 1. Für alle Teilnehmer: Definiert das dem Teilnehmer zugeordnete Multi-Location-Gateway. 2. Nur für System-Clients: Ist bei vernetzten Systemen das Flag "Notbetrieb" gesetzt (unter "Teilnehmer/IP Clients/Sekundäres Gateway"), kann hier die Knoten-ID des Failover-Systems für System-Clients eingetragen werden.

Parameter	Beschreibung
Internet-Registrierung am internen SBC	Aktiviert das Leistungsmerkmal SIP@Home. Damit kann sich ein externes STUN-fähiges SIP-Telefon über das Internet an OpenScape Business registrieren und wie ein internes Telefon genutzt werden.
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die **Suche**-Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.
<	Springt einen Teilnehmer zurück.

Parameterbeschreibung der Registerkarten:

- **Gruppen/RWS ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Anrufumleitung	
Ziel Tag	Anzeige der Rufweiterschaltungsziele für kommende externe Rufe am Tag (siehe Wizard User-Telefonie/Rufweiterschaltung)
Ziel Nacht	Anzeige der Rufweiterschaltungsziele für kommende externe Rufe in der Nacht (siehe Wizard User-Telefonie/Rufweiterschaltung).
Ziel Intern	Anzeige der Rufweiterschaltungsziele für kommende interne Rufe (siehe Wizard User-Telefonie/Rufweiterschaltung).
Berechtigung	
Tag	Jedem Teilnehmer kann eine Berechtigungsklasse für den Tag zugeordnet werden. Es kann zwischen 15 Berechtigungsklassen gewählt werden (siehe Telefonie/Berechtigungen).
Nacht	Jedem Teilnehmer kann eine Berechtigungsklasse für die Nacht zugeordnet werden. Es kann zwischen 15 Berechtigungsklassen gewählt werden (siehe Telefonie/Berechtigungen).
Anrufübernahme	
Gruppe	Jeder Teilnehmer kann einer Anrufübernahmegruppe zugeordnet werden. Sie können zwischen 32 Anrufübernahmegruppen wählen (120 bei OpenScape Business S; siehe auch Eingehende Anrufe / Anrufübernahme).
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die **Suche**-Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.
<	Springt einen Teilnehmer zurück.

28.3.7.10 Teilnehmer > Teilnehmer > UC-Anwendungen

Hier sind die Funktionen der UC-Lösungen UC Smart und UC Suite dargestellt. Es wird empfohlen, die Grundeinstellungen unter "Einrichtung > Grundinstallation > Basisinstallation > Vorkonfigurierte Rufnummern ändern" vorzunehmen.

Abhängig von der verwendeten UC-Lösung werden Ihnen unterschiedliche Funktionen angezeigt.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Rufnummer des Dienstes
Durchwahl	Durchwahlnummer des Dienstes
Vorname	Frei wählbarer Vorname des Dienstes. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Dienstes. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Dienstes. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Type	Abhängig von der UC-Lösung: UC Smart: MeetMe / Konferenz UC Suite Auto-Attendant / Fax / Contact Center Fax / Parken / MeetMe / Konferenz / Fax Gruppe
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA) **Anmerkung:** CLIP wird nicht für UC Fax unterstützt. Dies wird nur für Analog-Fax unterstützt.
Aktiv	Zeigt an, ob der Dienst betriebsbereit ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Suche	Sie können sich auch ausgewählte Dienste anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Dienste werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Dienste aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	

Parameter	Beschreibung
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.11 Teilnehmer > Teilnehmer > Profile/Vorlagen

Hier können Benutzerprofile (Teilnehmer-Parameter, Teilnehmer-Flags, Gruppen/RWS) eingerichtet werden, so dass auf einfache Weise eine Grundeinstellung für viele Benutzer zugleich entsteht.

Parameterbeschreibung der Registerkarten:

- **Alle Profile bearbeiten**

Parameter	Beschreibung
Profile	Anzeige der Profilnummer.
Name	Eingabe eines beliebigen Profilnamens.

Parameterbeschreibung der Registerkarten:

- **Alle Profile Mitglieder anzeigen**

Parameter	Beschreibung
Profile	Anzeige der Profilnummer.
Name	Anzeige des Profilnamens.
Mitglied Rufnr	Anzeige der internen Rufnummer des Profil-Mitglieds.
Mitglied Name	Anzeige des Namens des Profil-Mitglieds.

Parameterbeschreibung der Registerkarten:

- **Profile Mitglied hinzufügen/löschen**

Parameter	Beschreibung
Profile - ...	Anzeige der Profilnummer.
Name	Anzeige des vergebenen Profilnamens.
Profile Mitglieder	
Auswahl	Liste der im System verfügbaren Teilnehmer.
Mitglieder	Liste der dem Profil zugeordneten Teilnehmer.
Schaltflächen	

Parameter	Beschreibung
Hinzufügen	Markierten Teilnehmer aus der Auswahl in die Liste der Profil-Mitglieder übernehmen.
Löschen	Markiertes Mitglied aus der Liste der Profil-Mitglieder löschen.

Parameterbeschreibung der Registerkarten:

- **Profil importieren/exportieren**

Parameter	Beschreibung
Profil über HTTP laden	
Remote-Dateiname (PC-Dateisystem)	Laden einer bereits vorhandenen Profil-Datei im XML-Format-
Profil über HTTP exportieren	
Dateiname	Anzeige des Dateinamens, unter dem das Profil ausgegeben wird (Format XML)
Maßnahme	Download des Profils
Schaltflächen	
Default-Werte zurücksetzen	Die Profilwerte für alle diesem Profil zugewiesenen Teilnehmer werden auf den Defaultwert zurückgesetzt.

Parameterbeschreibung der Registerkarten:

- **Import/Export alle Profile**

Parameter	Beschreibung
Alle Profile über HTTP laden	
Remote-Dateiname (PC-Dateisystem)	Laden einer bereits vorhandenen Profil-Datei. In dieser Datei können auch mehrere Profile gespeichert sein.
Alle Profile über HTTP exportieren	
Dateiname	Anzeige des Dateinamens, unter dem die Profile abgespeichert werden.
Maßnahme	Download der Profile in eine Profil-Datei.
Schaltflächen	
Default-Werte zurücksetzen	Die Profilwerte für alle Profile und zugewiesene Teilnehmer werden auf den Defaultwert zurückgesetzt.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer-Parameter ändern: siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter**
- **Teilnehmer-Flags ändern: siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter**
- **Gruppen/RWS ändern: siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter**

28.3.7.12 Teilnehmer > Teilnehmer > Durchwahl Rufnummern

Hier wird eine Übersicht der konfigurierten Durchwahl-Rufnummern mit den zugehörigen Teilnehmern angezeigt.

Parameterbeschreibung der Registerkarten:

- **Durchwahl Rufnummern anzeigen**

Parameter	Beschreibung
Rufnr	Rufnummernanzeige des Teilnehmers.
Name	Namensanzeige des Teilnehmers.
Durchwahl	Durchwahlnummernanzeige des Teilnehmers.
(weitere Felder können angezeigt werden)	

28.3.7.13 Teilnehmer > Teilnehmer > Mobility Entry

Es wird empfohlen, mobile Teilnehmer über den Wizard "User Telefonie > Mobiltelefon Integration" einzurichten.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Eingabe der internen Rufnummer des Mobility-Teilnehmers (z.B. 777). Diese interne Rufnummer darf noch nicht vergeben sein.
Durchwahl	Eingabe der internen Durchwahlnummer des Mobility-Teilnehmers. Diese interne Durchwahlnummer darf noch nicht vergeben sein.
Vorname	Frei wählbarer Vorname des Mobility-Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Mobility-Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Mobility-Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Type	Anzeige des Typs des Mobility-Teilnehmers.
Device-Typ	Anzeige des Systemtelefontyps, der zur Image-Datei gehört.
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA). Wertebereich: max. 16 Ziffern.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.

Parameter	Beschreibung
Mobile Rufnr	Eingabe der Rufnummer des Mobiltelefons. Eingabe mit führender Amtskennziffer, z.B. 0016012345678.
Web Feature ID	Die Web Feature ID legt fest, wie sich der Teilnehmer am mobilen web Client einloggen soll (Benutzername). Auswahl zwischen "keine" (Mobility Entry-Teilnehmer ohne myPortal to go) und "automatisch" (interne Rufnummer des Teilnehmers oder MULAP) oder Auswahl der Rufnummer des Clients bzw. des Telefons aus der Klappliste.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **Sekundäres Gateway**

  Nur für vernetzte Systeme (Multi-Location)

Parameter	Beschreibung
Rufnummer	Interne Rufnummer des Mobility-Teilnehmers.
Name	Name des Mobility-Teilnehmers.
Knoten ID	Eintrag der Knoten-ID, über die der mobile Teilnehmer extern erreichbar ist.

28.3.7.14 Station > Station > SfB-Benutzer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr.	Eingabe der internen Rufnummer des Skype for Business Client Mobility-Teilnehmers (z. B. 777). Diese interne Rufnummer darf noch nicht vergeben sein.
DURCHWAHL	Durchwahlnummer für Skype for Business.

Parameter	Beschreibung
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Darstellung	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Typ	Zeigt den Typ des Mobility-Benutzers an, der in diesem Fall immer SfB Station ist.
SfB Rufnummer	Rufnummer des Skype for Business Clients.
Suchen	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in der Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.15 Teilnehmer > Teilnehmer > Übersicht Teilnehmer

Listet alle Teilnehmer des Kommunikationssystems auf sortiert nach der Rufnummer (Standard). Ein Klick auf einen anderen Spaltentitel sortiert die Liste nach der gewählten Spalte aufsteigend, ein weiterer Klick absteigend.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.

Parameter	Beschreibung
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Gerätetyp	Anzeige des Typs des Teilnehmers.
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/ RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

28.3.7.16 Teilnehmer > Tastenprogrammierung

Parameterbeschreibung der Registerkarten:

- **Tasten programmieren**

  Die Tastenprogrammierung wird nur für UP0-Telefone und HFA-Clients unterstützt. Die Suchfunktion (nach Rufnr., Durchwahl, Vorname, Nachname, Anzeige und Gerätetyp) ist verfügbar.

Parameter	Beschreibung
Auswahlliste	Auswahl Telefons der Teilnehmers.
Ebenenumschaltung	Wenn eine Taste mit der Funktion "Ebenenumschaltung" eingerichtet wurde, kann hier die zweite Ebene programmiert werden
Telefon	Ein Klick auf den Tastenbereich des Telefons öffnet die aktuelle Tastenbelegung.

Parameter	Beschreibung
Tastenfeld	Anzeige der Tastenfunktion (Tastenbeschriftung)
Tastenschaltfläche	Auswahl der gewünschten Funktion

Parameterbeschreibung der Registerkarten:

- **Tastenlayout übernehmen**

Parameter	Beschreibung
Übernehme die Tastenkonfiguration vom Teilnehmer	Auswahl des Teilnehmers, dessen Tastenkonfiguration für ausgewählte Teilnehmer übernommen werden soll.
Alle Teilnehmer	Tastenkonfiguration für alle Teilnehmer übernehmen.
Auswahlfeld	Übernahme der Tastenkonfiguration nur für die ausgewählten Teilnehmer
Teilnehmer	Anzeige der internen Rufnummer und des Namens des Teilnehmers.
Device-Typ	Anzeige des Telefontyp des Teilnehmers. Device-Typ kann für bereits aktive Teilnehmer nicht geändert werden.
Gerätetyp vom Teilnehmer übernehmen	Auswahl des Teilnehmers, dessen Device-Typ für ausgewählte Teilnehmer übernommen werden soll.
für folgende(n) ausgewählte(n) Teilnehmer	Auswahl des Teilnehmers, dessen Device-Typ übernommen werden soll. Filtern nach verfügbaren Device-Typen der Teilnehmer.

28.3.8 Cordless

Unter **Cordless** sind die Funktionen für die integrierte Cordless-Lösung zum Betrieb von Cordless-Telefonen (DECT-Telefonen) über das Kommunikationssystem zusammengefasst. Hier werden die Basisstationen und die DECT-Telefone (interne Teilnehmer mit HFA-Leistungsmerkmalen) konfiguriert.

28.3.8.1 Cordless > Systemweit

Parameterbeschreibung der Registerkarten:

- **Systemweite Daten ändern**

Parameter	Beschreibung
CMI Daten	

Parameter	Beschreibung
Systemkennung	Eingabe der 8-stelligen, hexadezimalen DECT-Systemkennung. Diese wird beim Erwerb des DECT-Systems mit ausgeliefert. Sie setzt sich folgendermaßen zusammen: 1. Ziffer: E/ARC (Access Right Class) 2.-5. Ziffer: EIC (Equipment Installer's Code) 6.-7. Ziffer: FPN (Fixed Part Number) 8. Ziffer: (FPS Fixed Part Subscriber)
Frequenzband	Auswahl des länderabhängigen Frequenzbandes. Es wird standardmäßig das dem eingetragenen Länderkennzeichen zugeordnete Frequenzband angezeigt.
Speech Coding	Anzeige des systemweiten Sprach-Codecs (a-law, µ-law).
Verschlüsselung	Encryption ist die Verschlüsselung der Daten auf der Luft-Schnittstelle und kann ein- oder ausgeschaltet werden. Standard: Aktiv
Anmeldefenster	Öffnungszeit des Anmeldefensters für die Anmeldung der DECT-Telefone. Das Anmeldefenster wird geöffnet, indem an einem Systemtelefon die Kennzahl *94 2 19970707 und das Passwort eingegeben wird. Anschließend werden im Anmeldefenster die Rufnummern der anzumeldenden DECT-Telefone eingegeben. Standard: 10 Minuten
Echo Handling Diese Parameter können die unter **Leitungen** > **Parameters/Allgemeine Flags** eingestellten Echo-Behandlungen für Mobilteilnehmer knotenweit außer Kraft setzen. Die Einstellung erfolgt nach der Leitungseinstellung der Gespräche. Eine Verbesserung durch generelle Deaktivierung oder leitungsspezifische Aktivierung muss im Einzelfall ausgetestet werden.	
Echo Suppressor	Der Echo Suppressor (ES) schaltet abhängig vom Sendepegel des DECT-Telefons eine Dämpfung in Empfangsrichtung des DECT-Telefons. Wenn der Echo Suppressor eingeschaltet ist, kann es bei lauten Nebengeräuschen vorkommen, dass das Empfangssignal zusätzlich bedämpft wird. Dadurch wird die Verständigung zusätzlich erschwert. Im Modus **Deaktiv** wird die Empfangsrichtung des DECT-Telefons bei lautem Sendepegel des DECT-Telefons nicht gedämpft. Diese Einstellung kann bei analoger Amtsanschaltung und lauter Umgebung bessere Verständlichkeit des Amtsteilnehmers am DECT-Telefons bieten. Standard: Automatisch
Echokompensationsglied	Der Echo Canceller (EC) beseitigt unerwünschte Signalrückflüsse, die durch eine 4/2-Draht- Umsetzung (Gabel) im Festnetz verursacht werden. Bei aktiviertem Echo Canceller ohne Echo kann es zu Fehlern kommen, da der Echo Canceller versucht sich auf ein nicht vorhandenes Echo zu adaptieren. Im Modus **Deaktiv** wird das Schalten dieses Parameters verhindert und der Echo Canceller ist immer aus. Standard: Automatisch

Parameter	Beschreibung
Artificial Echo	Über den Artificial Echo-Weg (AE) wird ein Sprachsignal aus dem Festnetz zum fernen Teilnehmer um 24dB bedämpft zurückgeleitet. Dies kann notwendig sein, um ggf. (z.B. Internationale Verbindung) einem eingefügten Echo Canceller eine gewisse Vorlast zu geben. Im Modus **Deaktiv** wird das Schalten dieses Parameters verhindert und der Artificial Echo ist immer aus. Standard: Automatisch
PP Deviation Control	Bei VoIP-Verbindungen über DECT-Telefone treten oft Echos auf. Zum Unterdrücken/Minimieren dieser Echos kann die Funktion „PP Deviation Control“ aktiviert werden. Diese Funktion wirkt auf alle an das Kommunikationssystem angeschlossenen DECT-Mobilteile. Für ein Mobilteil wird die Aktivierung oder Deaktivierung erst wirksam, wenn es aus- und wieder eingeschaltet wird. Im Modus **Deaktiv** wirkt die Echounterdrückung nicht und es können bei VoIP-Verbindungen über DECT-Mobilteile Echos auftreten. Standard: Deaktiv
Economic Mode	
Economic Mode	Der ECO Mode kann für alle DECT-Telefone systemweit aktiviert werden. Dabei wird die Sendeleistung der DECT-Telefone entweder um einen fest eingestellten Wert gesenkt (statisch) oder jedes DECT-Telefon passt seine Sendeleistung selbstständig an die empfangene Signalstärke an (adaptiv). Standard: Deaktiv
Economic Mode: **Aus**	Der ECO Mode ist systemweit deaktiviert.
Economic Mode: **ein**	Der ECO Mode (statisch) ist systemweit aktiviert. Die Sendeleistung der DECT-Telefone wird um einen festen Wert gesenkt.
Economic Mode: **Adaptiv**	Der ECO Mode (adaptiv) ist systemweit aktiviert. Jedes einzelne DECT-Telefone passt seine Sendeleistung selbstständig an die empfangene Signalstärke an. Bei Handover wird zuerst auf die hohe Sendeleistung geschaltet und anschließend abhängig vom Empfang die Sendeleistung reduziert.

28.3.8.2 Cordless > SLC

Parameterbeschreibung der Registerkarten:

- **DECT Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Rufnummer des DECT-Telefons.
Durchwahl	Durchwahlnummer des DECT-Telefons.
Name	Namens des DECT-Telefons.

Parameter	Beschreibung
Aktiv	Anmeldestatus des DECT-Telefons: Grün: DECT-Telefon ist aktiv. Rot: Baugruppen-Sperrschalter bei angemeldetem DECT-Telefon gesetzt. Gelb: DECT-Telefon wurde durch Änderung der PIN automatisch wieder abgemeldet. Grau: An diesem Port wurde noch nie ein DECT-Telefon angemeldet.
Mobilcode	PIN-Code zur Anmeldung des DECT-Telefons. Der Mobilcode muss systemweit eindeutig sein.
Zugang	Name, Nummer und Einbauplatz der S_0-Verlängerungsleitung.
Slot	Anzeige des Slots der gesteckten SLC-Baugruppe.
Schaltflächen	
Löschen	Das DECT-Telefon wird im System ausgetragen. Dabei werden Rufnummer, Durchwahl und Name gelöscht und die zugehörige TDM User Lizenz freigegeben.

Parameterbeschreibung der Registerkarten:

- **DECT-Teilnehmer hinzufügen**

Parameter	Beschreibung
Systemkennung	Gehört das Kommunikationssystem nicht zu einem Netzverbund (Knoten-ID = 0), wird die Systemkennung mit 1 vorbelegt. Gehört das Kommunikationssystem zu einem Netzverbund (Knoten-ID > 0), muss die Systemkennung mit der Knoten-ID übereinstimmen (**Cordless** > **Multi SLC** > **Systemkennung**).
Slot	Slot der gesteckten SLC-Baugruppe.
SLC-Nr.	Systemweit eindeutige ID-Nummer der SLC- Baugruppe. Wertebereich: 1-15,17-31,33-47,...,127. Vielfache von 16 sind nicht erlaubt.
Anzahl DECT-Telefone	Anzahl der bereits konfigurierten DECT-Telefone diese SLC-Baugruppe.
SLC Rufnummer	Systemweit eindeutige Rufnummer der S_0-Verlängerungsleitung.
Zugang	Name, Nummer und Einbauplatz der S_0-Verlängerungsleitung.
DECT-Teilnehmer hinzufügen	
Anzahl DECT-Telefone	Ist die Anzahl der DECT-Telefone kleiner als die im System zulässige Größe (Versionsabhängig), lässt sich hier eine zusätzliche Anzahl von DECT-Telefonen für diese SLC-Baugruppe hinzufügen. Die neu hinzugefügten DECT-Telefone werden unter der Registerkarte **DECT Teilnehmer ändern** angezeigt.

28.3.8.3 Cordless > Multi-SLC

Parameterbeschreibung der Registerkarten:

- **Multi-SLC ändern**

Parameter	Beschreibung
SLC-Nr.	Systemweit eindeutige ID-Nummer der SLC- Baugruppe. Wertebereich: 1-15,17-31,33-47,...,127. Vielfache von 16 sind nicht erlaubt.
Knoten ID	Anzeige der Knoten-ID (falls konfiguriert). Gehört das Kommunikationssystem zu einem Netzverbund, werden hier alle konfigurierten SLC-Baugruppen des Netzverbundes angezeigt.
SLC Rufnummer	Systemweit eindeutige Rufnummer der S_0-Durchwahlleitung der SLC-Baugruppe.

28.3.8.4 Cordless > Basisstationen

Parameterbeschreibung der Registerkarten:

- **Basisstation ändern**

Parameter	Beschreibung
Slot	Anzeige des Slots, in dem die SLC-Baugruppe der Basisstation gesteckt ist. Für das Mainboard (SLUC) wird Slot 2 angezeigt.
Type	Typ der Basisstation. Bei einer SLC-Baugruppe wird der Typ nur angezeigt, bei SLUC kann der Typ ausgewählt werden. Wenn der Typ von **Kein Port** auf **Basisstation** geändert wird, werden automatisch 16 DECT-Telefone vorkonfiguriert und eine SLC-Vernetzungsleitung eingerichtet.
Typ: **Basistation**	Basisstation angeschaltet.
Typ: **Frei**	keine Basisstation angeschaltet.
Name	Name der Basisstation.
Level	Pegel der Basisstation. Wertebereich: 50 % und 100 %; Standardwert: 100%
Status	Status der Basisstation.
Masterport	Bei einer SLC-Baugruppe werden die Ports angezeigt, an denen die Basisstationen angeschaltet sind. Bei SLUC werden alle Ports mit den angeschlossenen Endgeräten angezeigt.

28.3.9 Kommende Rufe

Unter **Kommende Rufe** sind die Funktionen für das sogenannte Call Management (CM) zusammengefasst. Dazu gehören z.B. Einstellungen für Gruppen und die Rufweiterschaltung.

28.3.9.1 Eingehende Anrufe > Gruppen/Huntgruppen

Für die Erstkonfiguration von Gruppenanrufen und Huntgruppen wird empfohlen, den Assistenten für **Gruppenanruf/Huntgruppen** zu verwenden.

Parameterbeschreibung der Registerkarten:

- **Gruppenrufnummern bearbeiten**
- **Verwendete Gruppen anzeigen**
- **Alle Gruppenmitglieder anzeigen**
- **Gruppe hinzufügen**
- **Gruppe löschen**
- **Gruppenparameter bearbeiten**
- **Mitglieder anzeigen**
- **Mitglied hinzufügen**
- **Mitgliederreihenfolge bearbeiten**
- **Grundlegende MULAPs überprüfen**
- **MULAP-Einstellungen überprüfen**

Parameter	Beschreibung
Index	Fortlaufende Nummer, die vom Kommunikationssystem zugewiesen wird.
Rufnummer	Telefonnummer der Gruppenruf-, Huntgruppe, grundlegenden MULAP, Executive-MULAP oder Voicemail-Gruppe
DID	DID-Nummer der Gruppenruf-, Huntgruppe, Basis-MULAP, Executive-MULAP oder Voicemail-Gruppe
Vorname	Frei wählbarer Vorname für die Gruppenruf-, Huntgruppe, Basis-MULAP, Executive-MULAP oder Voicemail-Gruppe. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Nachname	Frei wählbarer Nachname für den Gruppenruf, die Huntgruppe, das Basis-MULAP, das Executive-MULAP oder die Voicemail-Gruppe. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Display	Name des Gruppenrufs, der Huntgruppe, des Basis-MULAP, des Executive-MULAP oder der Voicemail-Gruppe. Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt.
Typ	Definition des Gruppentyps Standardwert: Gruppe Weitere Informationen siehe Tabelle: Typenoptionen
Rufart	Definiert die akustische Signalisierung eingehender externer Anrufe an die Gruppe. Standardwert: 1 Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.
Klingeltyp: **1**	Zwei Klingelzeichen
Klingeltyp: **2**	Dreifach-Rufton
Klingeltyp 3	Kurz/Lang/Kurz-Rufton

Parameter	Beschreibung
Telefonverzeichnis	Wenn dieses Kontrollkästchen aktiviert ist (Anzeige Ja), wird die Rufnummer der Gruppe im internen Verzeichnis angezeigt. Standardwert: Aktiviert
Mulap als Gruppenmitglied	Wenn dieses Kontrollkästchen aktiviert ist, kann die MULAP-Gruppe als Mitglied in Gruppen hinzugefügt werden.
Gruppenmitglied	
Gruppe	Nummer (Index) der Gruppe
Mitglied	Nummer (Index) des Mitglieds innerhalb der Gruppe
Rufnummer	Rufnummer des Gruppenmitglieds
Name	Name des Gruppenmitglieds
Parameter	Aktivierte Parameter des Gruppenmitglieds
Parameter: M	Master (M): Basis-MULAP: Das Mitglied ist für das Basis-MULAP zuständig. Executive MULAP: Das Mitglied verfügt über exekutive Funktionen.
Parameter: R	Akustischer Anruf (R): Basis-MULAP und Executive MULAP: Die eingehenden Anrufe werden akustisch signalisiert.
Parameter: A	Automatische Freigabe, ausgehend (A): Basis-MULAP: Die Basis-MULAP-Leitung wird automatisch für einen Anruf ausgewählt, wenn Sie den Hörer abheben. Executive MULAP: Die Executive MULAP Leitung wird automatisch für einen Anruf ausgewählt, wenn Sie den Hörer abheben.
Parameter: K	Keine automatische Annahme eingehender Anrufe (K): Basis-MULAP und Executive MULAP: Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.
Parameter: P	Automatische Freigabe der Privatsphäre (P): Basis-MULAP und Executive MULAP: Sie können die belegte MULAP-Leitung für eine Konferenz freigeben, indem Sie die MULAP-Taste drücken.
MULAP-Taste eingerichtet	Zeigt an, ob eine MULAP-Taste für das Gruppenmitglied konfiguriert wurde.
Richtung	Für ein externes Mitglied der Gruppe wird die Route angezeigt.
Gruppe	
Konsistenzprüfung	Mögliche Kollisionen aufgrund von Überschneidungen von Mastern von Basis-MULAPs oder bei der automatischen Ausgangsbelegung von Basis-MULAPs werden angezeigt.

Tabelle 63: Typenoptionen

Parameter	Beschreibung
Alle Gruppentypkonvertierungen sind ohne Löschen von Gruppenmitgliedern zulässig, mit Ausnahme von MULAP-Gruppentypen. **Anmerkung:** Wenn eine Gruppe vom Typ *Gruppe*, *Lineare Huntgruppe*, *Zyklische Huntgruppe* oder *Voicemail* eine MULAP-Gruppe als Mitglied hat, ist eine Umwandlung in den Typ *RNA-Gruppe* oder *Anklopfergruppe* nicht zulässig. **Anmerkung:** Wenn ein Gruppenmitglied die Anrufweiterleitung (*1) zu einer anderen *Huntgruppe*, *Anklopfergruppe* und *RNA Group* einstellt, wird der Anruf nicht weitergeleitet. Dies ist nicht zulässig, um Anrufschleifen zu vermeiden. Für Direktanrufe an die Station ist die Weiterleitung gültig. Für Mitglieder von *zyklischen* und *linearen (Hunt-)Gruppen* ist dies erlaubt, *1 zu jedem Ziel funktioniert – außer zu Voicemail.	
Typ: Lineare Huntgruppe	Ein eingehender Anruf wird immer zuerst beim ersten Mitglied eines Sammelanschlusses signalisiert. Die weitere Signalisierung erfolgt anhand der Reihenfolge, in der die Mitglieder in die Gruppentabelle eingetragen werden.
Typ: Zyklische Huntgruppe	Ein eingehender Anruf wird immer zuerst bei dem Mitglied signalisiert, das dem Abonnent, der den letzten Anruf angenommen hat, folgt. Die weitere Signalisierung erfolgt anhand der Reihenfolge, in der die Mitglieder in die Gruppentabelle eingetragen werden.
Typ: Gruppe	Gruppenruf vom Typ Gruppe: Ankommende Anrufe werden gleichzeitig bei allen verfügbaren Gruppenmitgliedern signalisiert. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Sind alle Gruppenmitglieder besetzt, wird ein Anruf durch einen Anklopfton signalisiert. Legt ein Teilnehmer auf, wird der Anruf weiterhin bei allen Gruppenmitgliedern signalisiert (Anklopfton bei besetzten Gruppenmitgliedern).
Typ: RNA	Gruppenruf vom Typ RNA: Ankommende Anrufe werden gleichzeitig bei allen Gruppenmitgliedern signalisiert. Ist ein Gruppenmitglied besetzt, wird der gesamte Gruppenruf als besetzt gekennzeichnet (nur die besetzten Mitglieder werden für den eingehenden Anruf signalisiert). Anrufer der Gruppe erhalten das Besetztzeichen.
Typ: Basis-MULAP	Eingehende Anrufe werden an allen mit dem Basis-MULAP (Multiple Line Appearance) verbundenen Telefonen optisch angezeigt. Der Abonnent kann auch einstellen, ob eingehende Anrufe auch für jedes einzelne Mitglied akustisch signalisiert werden sollen. Der Status der Basis-MULAP ändert sich in besetzt und andere Anrufer hören das besetzt Signal, wenn ein Anruf angenommen wird. Bei ausgehenden Anrufen über den MULAP-Basistrunk wird die MULAP-Basistelefonnummer auf dem Display des Angerufenen angezeigt.

Parameter	Beschreibung
Typ: Executive MULAP	Sie können Executive MULAPs konfigurieren, wenn Sie eingeschränkte Executive- und Sekretariatsfunktionen nutzen möchten. Wenn ein Anrufer die Executive MULAP Telefonnummer anruft, wird der Anruf an allen Telefonen, die zum Executive MULAP gehören, optisch signalisiert. Eingehende Anrufe werden für Mitglieder mit Sekretariatsfunktionen auch akustisch signalisiert.
Typ: Anklopfen	Gruppenruf vom Typ Anklopfen: Ankommende Anrufe werden gleichzeitig bei allen verfügbaren Gruppenmitgliedern signalisiert. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Bei besetzten Gruppenmitgliedern wird ein anstehender Anruf sofort durch einen Anklopfton signalisiert.
Typ: Voicemail	Voicemail-Gruppe: Eine Voicemail-Gruppe ermöglicht einer bestimmten Gruppe von Teilnehmern den Zugriff auf Voicemails. Wenn ein Anruf an die Rufnummer einer Voicemail-Gruppe getätigt wird, wird der Anruf direkt an die Voicemailbox (d. h. die Voicemail) der Gruppe und nicht an die Gruppenmitglieder weitergeleitet. Nachdem eine Voicemail in der Voicemailbox der Gruppe hinterlassen wurde, wird sie an die Voicemailboxen aller Mitglieder weitergeleitet. Alle Mitglieder erhalten die Voicemail gleichzeitig. Wenn ein Mitglied eine Voicemail löscht, wird diese Voicemail auch aus den Voicemailboxen aller Mitglieder und aus der Voicemailbox der Gruppe gelöscht. Die persönlichen Voicemails aller Mitglieder sind davon nicht betroffen.

28.3.9.2 Kommende Rufe > Gruppen-Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Mitglied bearbeiten**
- **Mitglied löschen**

Parameter	Beschreibung
Gruppe	Nummer (Index) der Gruppe
Gruppenmitglied	Nummer (Index) des Gruppenmitglieds
Rufnummer	Rufnummer des Gruppenmitglieds
Vorname	Frei wählbarer Vorname des Gruppenmitglieds. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Nachname	Frei wählbarer Nachname des Gruppenmitglieds. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Name	Name des Gruppenmitglieds Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt.
MULAP-Name	Name der MULAP (Multiple Line Appearance)-Gruppe. Dies ist der MULAP-Name, der auf dem Display angezeigt wird, wenn diese Teamgruppe aufgerufen wird. Der MULAP-Name ist allen Teamgruppenmitgliedern gemeinsam, die den gleichen Typ haben.

Parameter	Beschreibung
MULAP-Ruf-Nr.	Rufnummer der MULAP-Gruppe
Master (M)	Basic-MULAP: Durch Aktivierung dieses Flags wird ein Mitglied zu einem Master der Basic-MULAP. Aktiviert ein Master eine Anrufumleitung, gilt diese für alle Mitglieder (Telefone) der Basic-MULAP. Chef-MULAP: Durch Aktivierung dieses Flags werden einem Mitglied Chef-Funktionen zugewiesen. Beim Abheben des Hörers wird automatisch über die Chef-MULAP-Leitung gerufen. Ankommende Anrufe über Chef-MULAP-Rufnummer werden ausschließlich optisch signalisiert.
Akustischer Ruf(R)	Basic-MULAP und Chef-MULAP: Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert. Standardwert: Aktiviert für alle Master einer Basic-MULAP. Aktiviert für alle Mitglieder mit Sekretär-Funktion einer Chef-MULAP.
Automatische Belegung gehend (A)	Basic-MULAP: Bei aktiviertem Flag wird beim Abheben des Hörers automatisch die Basic-MULAP-Leitung gerufen. Chef-MULAP: Ist dieses Flag gesetzt, wird beim Abheben des Hörers automatisch über die Chef-MULAP-Leitung gerufen. Standardwert: Aktiviert für alle Master einer Basic-MULAP. Aktiviert für alle Mitglieder mit Sekretär-Funktion einer Chef-MULAP.
Keine automatische Rufannahme kommend (K)	Basic-MULAP und Chef-MULAP: Ist dieses Flag gesetzt, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Die Annahme eines ankommenden Rufs ist ausschließlich durch Betätigen der MULAP-Taste möglich. Standardwert: Deaktiviert
Automatische Konferenz Freigabe (P)	Basic-MULAP und Chef-MULAP: Ist dieses Flag gesetzt, wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen. Standardwert: Deaktiviert
MULAP-Taste eingerichtet	Basic-MULAP: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die Basic-MULAP-Leitung. Dem Angerufenen wird die Basic-MULAP-Rufnummer im Display angezeigt. Chef-MULAP: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt. Standardwert: Aktiviert
Richtung	Bei einem externen Gruppenmitglied wird die Richtung angezeigt.
Type	Definition des Gruppentyps

28.3.9.3 Kommende Rufe > Team/Top

Für die Erstkonfiguration von Team- und Top-Gruppen wird empfohlen, die Assistenten **Teamschaltung** und **Chef/Sekretär** zu verwenden.

Parameterbeschreibung der Registerkarten:

- **Alle Team/Top Gruppen anzeigen**
- **Verwendete Team/Top Gruppen anzeigen**
- **Team/Top Gruppe hinzufügen**
- **Team/Top Gruppe ändern**
- **Team/Top Gruppe löschen**
- **Team/Top Gruppe ändern**
- **Alle Team/Top Gruppen-Mitglieder anzeigen**
- **Team/Top Mitglied hinzufügen**
- **Team/Top Mitglied ändern**
- **Team/Top Mitglied löschen**
- **Fax Boxen anzeigen**
- **Fax Box hinzufügen**

Parameter	Beschreibung
Index	Fortlaufende Nummer, die vom Kommunikationssystem vergeben wird.
Vorname	Frei wählbarer Vorname der Team-/Top-Gruppe. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Nachname	Frei wählbarer Nachname der Team-/Top-Gruppe. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Name	Name der Team-/Top-Gruppe Wird je nach dem für den Anzeigename verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt.
Type	Definition des Gruppentyps
Typ: **Team**	Eine Team-Gruppe bietet komfortable Teamfunktionen. Die Teilnehmerrufnummern aller Teammitglieder werden auf MULAP-Tasten (Leitungstasten) programmiert. Damit hat jedes Teammitglied Zugriff auf alle Leitungen (zum Beispiel zur Anrufübernahme) und kann auch gleichzeitig über mehrere Leitungen telefonieren.
Typ: **Top**	Eine Top-Gruppe bietet komfortable Chef- und Sekretär-Funktionen (Top-Funktion) für bis zu drei Chefs und bis zu drei Sekretäre.
Team als Gruppenmitglied	Dieses Flag ist nur konfigurierbar, wenn die Team-Gruppe Mitglieder mit demselben Teilnehmertyp hat, was zu einer einzelnen MULAP-Gruppe unterhalb dieser Team-Gruppe führt. Wenn dieses Flag aktiviert ist, kann die MULAP-Gruppe als Mitglied unter Gruppen hinzugefügt werden.
Tastenvergabe auf Team	Definition für die Einrichtung der MULAP-Tasten für Mitglieder der Team-Gruppe
Tastenvergabe auf Team: **auf erste/zweite Konsole**	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf dem ersten oder zweiten Beistellgerät (Key- oder BLF-Modul) des Team-Telefons.

Parameter	Beschreibung
Tastenvergabe auf Team: **auf erste freie Tasten**	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf der ersten freien Taste des Team-Telefons.
Tastenvergabe auf Top	Definition für die Einrichtung der MULAP-Tasten für Mitglieder der Top-Gruppe
Tastenvergabe auf Top: **auf erste/zweite Konsole**	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf dem ersten oder zweiten Beistellgerät (Key- oder BLF-Modul) des Top-Telefons.
Tastenvergabe auf Top: **auf erste freie Tasten**	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf der ersten freien Taste des Top-Telefons.
Gruppenmitglied	
Gruppe	Nummer (Index) der Gruppe
Mitglieder	Nummer (Index) des Mitglieds innerhalb der Gruppe
Type	Definition des Mitgliedstyps
Ruf-Nr.	Rufnummer des Gruppenmitglieds (ändert sich in einer MULAP-Gruppe in **Ruf-Nr. und ist intern unter dieser **Ruf-Nr. erreichbar.)
Name	Name des Gruppenmitglieds
MULAP-Ruf-Nr.	Rufnummer der MULAP-Gruppe
MULAP-Duwa	Durchwahlnummer der MULAP-Gruppe
MULAP-Name	Name der MULAP-Gruppe. Dies ist der MULAP-Name, der auf dem Display angezeigt wird, wenn diese Teamgruppe aufgerufen wird. Der MULAP-Name ist allen Teamgruppenmitgliedern gemeinsam, die den gleichen Typ haben.
Rufart	Definition der akustischen Signalisierung kommender externer Anrufe der Gruppe Standardwert: 1 Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.
Rufart: **1**	Doppel-Rufton
Rufart: **2**	Dreifach-Rufton
Rufart: 3	Kurz/Lang/Kurz-Rufton
Tel.-Buch	Bei aktiviertem Flag (Anzeige Ja) erscheint die Rufnummer der Gruppe im internen Verzeichnis. Standardwert: Aktiviert

Parameter	Beschreibung
Master (M)	Team-Gruppe: Durch Aktivierung dieses Parameters wird ein Mitglied zu einem Master der Team-Gruppe. Aktiviert ein Master eine Anrufumleitung, gilt diese für alle Mitglieder (Telefone) der Team-Gruppe. Top-Gruppe: Durch Aktivierung dieses Flags werden einem Mitglied Chef-Funktionen zugewiesen. Beim Abheben des Hörers wird automatisch die Chef-MULAP-Leitung für einen Ruf ausgewählt. Kommende Rufe über die zugehörige Chef-MULAP-Rufnummer werden standardmäßig ausschließlich optisch signalisiert.
Akustischer Ruf(R)	Team-Gruppe und Top-Gruppe: Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert. Standardwert: Aktiviert für alle Mitglieder einer Team-Gruppe. Aktiviert für alle Mitglieder mit Sekretär-Funktion einer Top-Gruppe.
Automatische Belegung gehend (A)	Team-Gruppe und Top-Gruppe: Ist dieser Flag gesetzt, wird beim Abheben des Hörers automatisch über die MULAP-Leitung dieses Mitglieds gerufen. Standardwert: Aktiviert
Keine automatische Rufannahme kommend (K)	Team-Gruppe und Top-Gruppe: Ist dieses Flag gesetzt, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Die Annahme eines ankommenden Rufs ist ausschließlich durch Betätigen der MULAP-Taste möglich. Standardwert: Deaktiviert
Automatische Konferenz Freigabe (P)	Team-Gruppe und Top-Gruppe: Ist dieses Flag gesetzt, wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen. Standardwert: Deaktiviert
MULAP-Taste eingerichtet	Team-Gruppe: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf über die MULAP-Leitung des Masters. Dem Angerufenen wird die MULAP-Teilnehmernummer des Masters im Display angezeigt. Top-Gruppe: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt. Standardwert: Deaktiviert für alle Mitglieder einer Team-Gruppe. Aktiviert für alle Mitglieder einer Top-Gruppe.
MULAP-Typ	Definition des MULAP-Typs
MULAP-Typ: **Basic-MULAP**	Kommende Rufe werden bei allen zur Basic-MULAP gehörenden Telefonen optisch signalisiert. Für jedes Mitglied kann zusätzlich angegeben werden, ob ankommende Anrufe auch akustisch signalisiert werden sollen. Nach Annahme des Anrufs ist die Basic-MULAP besetzt und weitere Anrufer erhalten den Besetztton. Bei gehenden Anrufen über die Basic-MULAP-Leitung wird den Angerufenen die Basic-MULAP-Rufnummer im Display angezeigt.

Parameter	Beschreibung
MULAP-Typ: **Chef-MULAP**	Alle Mitglieder einer Chef-MULAP sind unter der Chef-MULAP-Rufnummer sowie unter ihren eigenen Teilnehmerrufnummern erreichbar.
Fax Rufnr	Rufnummer der Faxbox des Gruppenmitglieds
Fax DID	Durchwahlnummer der Faxbox des Gruppenmitglieds

28.3.9.4 Kommende Rufe > Anrufübernahme

Parameterbeschreibung der Registerkarten:

- **Namen Anrufübernahmegruppen ändern**
- **Teilnehmer der Gruppe anzeigen**
- **Teilnehmer der Gruppe zuordnen**

Parameter	Beschreibung
Gruppe	
Gruppe	Nummer (Index) der Anrufübernahmegruppe Wertebereich: 1 bis 32 (120 bei OpenScape Business S)
Name	Name der Anrufübernahmegruppe
Teilnehmer	
Ruf-Nr.	Rufnummer des internen Teilnehmers
Name	Name des internen Teilnehmers
Zuordnung Gruppe X	Bei aktiviertem Flag ist der Teilnehmer der Anrufübernahmegruppe X zugeordnet.
Gruppe	Anrufübernahmegruppe, der dieser Teilnehmer zugeordnet ist.

28.3.9.5 Kommende Rufe > UCD

Parameterbeschreibung der Registerkarte:

- **UCD Parameter ändern**

Parameter	Beschreibung
UCD-Flags	
UCD-Applikation freigeben	Bei aktiviertem Flag ist das Leistungsmerkmal Anrufverteilung (Uniform Call Distribution UCD) systemweit freigegeben. Standardwert: Aktiviert

Parameter	Beschreibung
Agenten dauerverfügbar	Bei aktiviertem Flag sind alle UCD-Agenten dauerverfügbare Agenten. Ein dauerverfügbarer Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat. Standardwert: Deaktiviert
Automatische Nachbearbeitungszeit	
Nachbearbeitungszeit (Zyklen)	Systemweite Definition der automatischen Nachbearbeitungszeit für alle UCD-Agenten in Rufzyklen, das heißt in 5-Sekunden-Schritten. Während der Nachbearbeitungszeit wird ein Agent kurzzeitig von der Anrufverteilung ausgenommen, um Nacharbeiten für den soeben beendeten Anruf durchführen zu können. Standardwert: 0
Priorität bei internen Rufen	
Priorität intern	Systemweite Definition der Priorität für interne Anrufe anhand von 10 Prioritätsebenen (1 = hoch, 10 = niedrig). Standardwert: 10
Priorität bei externen Rufen	
Slot/Leitung	Anzeige der Baugruppe, des Einbauplatzes (Slot) und der Nummer der Leitung (des B-Kanals). Für externe Anrufe erfolgt die Prioritätsvergabe leitungsbezogen (pro B-Kanal), unabhängig davon, ob es sich um IP- oder TDM-Leitungen handelt.
Priorität	Definition der Priorität für externe Anrufe, die über die betreffende Leitung (B-Kanal) eingehen. Die Definition erfolgt anhand von 10 Prioritätsebenen (1 = hoch, 10 = niedrig). Standardwert: 1

Parameterbeschreibung der Registerkarten:

- **UCD Gruppen anzeigen**
- **UCD Gruppe ändern**

Parameter	Beschreibung
Rufnummer	Rufnummer der UCD-Gruppe
MSN	Durchwahlnummer der UCD-Gruppe
Name	Name der UCD-Gruppe
Prim. Rufzykl.	Definition des primären Rufzyklus: Die Angabe erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Eingestellt wird die Zeit, die ein Anruf in der Warteschlange verbleibt, falls er nicht von dem am längsten im Zustand verfügbar befindlichen Agenten angenommen wird. Anschließend wird der Anruf zum nächsten verfügbaren Agenten weitergegeben. Standardwert: 3 Zyklen

Parameter	Beschreibung
Sek. Rufzykl.	Definition des sekundären Rufzyklus: Die Angabe erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Eingestellt wird die Zeit, die ein Anruf in der Warteschlange verbleibt, falls er nicht von dem nächsten verfügbaren Agenten angenommen wird. Standardwert: 3 Zyklen
Wartende Anrufe	Definition der maximalen Anzahl wartender Anrufe: Wird die maximale Anzahl der wartenden Anrufe überschritten, können die weiteren Anrufe an ein Überlaufziel (ein externes Ziel, eine andere UCD-Gruppe, ein interner Teilnehmer oder eine Gruppe) geleitet werden. Standardwert: 10 (Standardwert letzte UCD-Gruppe: 72)
AICC	Definition der Automatic Incoming Call Connection AICC. Die Einstellung gilt für alle Agenten einer UCD-Gruppe, unabhängig davon, ob das Telefon eines Agenten mit Headset ausgestattet ist oder nicht. Standardwert: Nein
AICC: ja	Die Agenten dieser UCD-Gruppe können kommende Anrufe ohne zusätzliche Bedienschritte annehmen. Der Agent wird durch einen Hörton im Headset auf das Eintreffen eines Anrufes aufmerksam gemacht, der anschließend automatisch durchgeschaltet wird.
AICC: Nein	Die Agenten dieser UCD-Gruppe können kommende Anrufe nicht ohne die herkömmlichen Bedienschritte (zum Beispiel durch das Abnehmen des Hörers) annehmen.
Ansagewechsel	Definition möglicher Ansagewechsel Standardwert: Einmalig
Ansagewechsel: einzeln	Die in der Warteschlange befindlichen Anrufer erhalten eine einmalige Ansage.
Ansagewechsel: zyklisch	Die letzte und die vorletzte Ansage in der Konfiguration werden zyklisch wiederholt.
Overflow-Zeit	Definition der Overflow-Zeit in Sekunden: Wird ein wartender Anruf nicht innerhalb der Overflow-Zeit durch die UCD-Applikation angenommen, wird der Anruf anhand der Angaben im Call Management durch das Kommunikationssystem weiterverarbeitet. Diese Einstellung ist ausschließlich relevant, wenn eine externe UCD-Applikation angeschlossen ist. Standardwert: 600
Ansageverzögerung	Definition der Ansageverzögerung in Sekunden: Nach Ablauf dieser Zeit erhält ein Anrufer in der Warteschlange eine Ansage. Standardwert: 0

Parameterbeschreibung der Registerkarte:

- **UCD Gruppen Parameter ändern**

Parameter	Beschreibung
Ziel-Index	Für jede UCD-Gruppe können bis zu sieben Ziele (Index 1 bis 7) für Ansagen definiert werden. Die Ansagen der Ziele werden dem Anrufer in der Warteschlange nacheinander abgespielt.
Ansageeinrichtungen	Ansage für den betreffenden Ziel-Index.
Wartezeit	Die Ansage kann entweder zyklisch (max. 9 Zyklen mit jeweils 5 sec = 45 sec) oder endlos abgespielt werden. Nach Ablauf dieser Zeit wird dem Anrufer in der Warteschlange die Ansage des nächsten Index vorgespielt (nicht bei **endlos**). Standardwert: endlos

Parameterbeschreibung der Registerkarte:

- **UCD Gruppen Mitglied hinzufügen/löschen**

Parameter	Beschreibung
Auswahl	Liste aller UCD-Agenten-IDs. Die UCD-Agenten-IDs entsprechen nicht den Rufnummern im Kommunikationssystem.
Mitglieder	Liste der UCD-Agenten-IDs der gewählten UCD-Gruppe
Schaltflächen	
Hinzufügen	Fügt die markierten UCD-Agenten-IDs der UCD-Gruppe hinzu.
Löschen	Löscht die markierten UCD-Agenten-IDs aus der UCD-Gruppe.

Parameterbeschreibung der Registerkarte:

- **Teilnehmer zuweisen**

Parameter	Beschreibung
Agenten-ID	Liste der UCD-Agenten-IDs der gewählten UCD-Gruppe.
Teilnehmer	Liste der Teilnehmer, die den UCD-Agenten-IDs der UCD-Gruppe zugeordnet werden können.

28.3.9.6 Kommende Rufe > Rufweiterschaltungen

Parameterbeschreibung der Registerkarten:

- **Rufzielliste - Definition**

Parameter	Beschreibung
Rufzielliste	Auswahl der zu bearbeitenden Rufzielliste. Wertebereich: 1 bis 740

Parameter	Beschreibung
Rufweiterschaltung ändern Um ein Rufziel schneller zu finden, können Sie in den Feldern **1. - 4. Ziel** auch eine oder mehrere Ziffern eingeben. Dann wird direkt zum Listeneintrag gesprungen, der mit der eingegebenen Ziffernfolge beginnt. Die Eingabe einer Buchstabenfolge ist ebenfalls möglich.	
Ziel 1 - 4: **Kein Eintrag**	Rufziel wird übersprungen.
Ziel 1 - 4: **Externes Ziel**	Richtung und externe Rufnummer mit Amtskennzahl.
Ziel 1 - 4: *** Angewählter Teilnehmer**	Angerufener Teilnehmer.
Ziel 1 - 4: **** Benutzer definiert**	Ziel der Anrufumleitung nach Zeit (falls eingerichtet).
Ziel 1 - 4: **#9 Systemsuchlauf**	Nächster verfügbarer Teilnehmer (außer Chef-Nebenstelle).
Ziel 1 - 4: **#201 - #260**	Anrufverteilung (UCD-Gruppe).
Ziel 1 - 4: **#801 - #817**	Ansagegerät.
Ziel 1 - 4: 100, 101, ...	Rufnummer eines Teilnehmers oder einer Gruppe (z. B. Sprachbox)
Die Rufweiterschaltung erfolgt immer nach	Zeit, nach der ein Anruf an das nächste Rufziel weitergeschaltet wird. Bei UCD-Gruppen folgt die Weiterschaltung den Mechanismen der primären und sekundären Rufzyklen (siehe UCD-Gruppen). Wertebereich: 5/10/15/...75 s, Standardwert: 15 s
Anrufumleitung	Anruf wird im Besetztfall sofort an das nächste Rufziel weitergeleitet. Standardwert: Aktiviert
Zweitwecker	
Zweitwecker Ziel	Zusätzlicher interner Teilnehmer, bei dem der Anruf ebenfalls signalisiert wird oder ein Aktor (Relais) einer Aktoren/Sensoren-Baugruppe für einen zentralen Wecker.
Zweitwecker-Art	Der Anruf kann sofort oder nach der gesamten Rufweiterschaltungszeit beim Teilnehmer signalisiert werden. Standardwert: Sofort

Parameterbeschreibung der Registerkarten:

- **Rufzielliste - Zuordnung**

Parameter	Beschreibung
Rufnr	Rufnummer des Teilnehmers bzw. der Gruppe.
Name	Name des Teilnehmers bzw. der Gruppe.
Typ	Teilnehmer-Typ, z. B. U_{P0}, System-Client, AB, ISDN, SIP.

Parameter	Beschreibung
Tag	Nummer der Rufzielliste, für kommende externe Anrufe während der Arbeitszeiten (Tagschaltung) Standardwert: 14
Nacht	Nummer der Rufzielliste für kommende externe Anrufe bei aktivierter Nachtschaltung Standardwert: 15
Intern	Nummer der Rufzielliste für kommende interne Anrufe Standardwert: 16
Suche	Wird in die Suchfelder **Rufnr** oder **Name** ein Suchbegriff eingegeben und anschließend die Return-Taste gedrückt, werden alle Treffer angezeigt, die den Suchbegriff enthalten. Mit der Eingabe von `521` als Rufnummer werden z. B. die Treffer `+495213535` und `+498967521` angezeigt oder mit `co` als Name die Treffer `Collins`, `Mcoin` und `Branco`. Alle Einträge werden angezeigt, wenn in allen Suchfeldern nichts eingetragen ist und anschließend die Return-Taste gedrückt wird.

Parameterbeschreibung der Registerkarten:

- **Rufziellisten-Teilnehmer**

Parameter	Beschreibung
Alle Teilnehmer in Rufzielliste anzeigen	Für die ausgewählte Rufzielliste werden alle Teilnehmer bzw. Gruppen angezeigt, die diese Rufzielliste nutzen.

Parameterbeschreibung der Registerkarten:

- **Rufziellisten zuweisen**

Parameter	Beschreibung
Rufzielliste	Auswahl der Rufzielliste, der Teilnehmer zugewiesen werden sollen. Wertebereich: 1 bis 740
Tag	Rufzielliste ist für kommende externe Anrufe während der Arbeitszeiten (Tagschaltung)
Nacht	Rufzielliste ist für kommende externe Anrufe bei aktivierter Nachtschaltung
Intern	Rufzielliste ist für kommende interne Anrufe
Rufziellisten	
Auswahl	Liste aller Teilnehmer.
Mitglieder	Liste der Teilnehmer, denen die Rufzielliste zugeordnet ist.
Schaltflächen	
Hinzufügen	Markierte Teilnehmer werden aus dem Auswahl-Fenster in das Mitglieder-Fenster übernommen.
Löschen	Markierte Teilnehmer werden aus dem Mitglieder-Fenster gelöscht.

28.3.10 Leitungen/Vernetzung

Unter **Leitungen/Vernetzung** sind die Funktionen für die Amtsleitungen und die Richtungen zusammengefasst.

28.3.10.1 Leitungen/Vernetzung > Leitungen

Parameterbeschreibung der Registerkarten:

- **Alle Leitungen anzeigen**
- **Richtung ändern**

Parameter	Beschreibung
Leitung	Anzeige der an das Kommunikationssystem angeschlossenen physikalischen Amtsleitung.
Box-Sl-Pt-Le oder Box/Slot/ Port/Leitung	Anzeige des Baugruppentyps sowie die Einbauplatz- und Port-Nummer (physikalischen Port) für den Anschluss der Leitung an das Kommunikationssystem.
Kennz.	Anzeige oder Einrichtung der Richtungskennzahl. Bei Eingabe dieser Nummer wird vom Kommunikationssystem die zugeordnete Leitung belegt. Diese dient zum Prüfen einer Leitung oder zur Programmierung einer Leitungstaste. Wenn CSTA-Anwendungen verwendet werden, sollte der Wert für diesen Parameter festgelegt werden.
Richtung	Anzeige oder Auswahl der Richtung, die der Leitung zugeordnet ist (keine oder Ltg. Grp 1 bis Ltg. Grp 12). Wird für eine aktive Leitung die Auswahl „keine“ eingestellt, verhält sich das System unstabil. Außerdem kann das System zwar auf dieser Leitung einen Anruf empfangen, aber der Anruf kann nicht weitergeleitet werden.
Status	Anzeige des Leitungszustands. Eine inaktive Leitung wird durch einen Stern gekennzeichnet.
Type	Anzeige des Leitungstyps. Inaktive Leitungen erhalten die Bezeichnung "No Port".

Parameterbeschreibung der Registerkarten:

- **Rufzuordnung aller Leitungen anzeigen**

Parameter	Beschreibung
Leitung	Anzeige der an das Kommunikationssystem angeschlossenen physikalischen Amtsleitung.
Box-Sl-Pt-Le oder Box/Slot/ Port/Leitung	Anzeige des Baugruppentyps sowie die Einbauplatz- und Port-Nummer (physikalischen Port) für den Anschluss der Leitung an das Kommunikationssystem.
Tag Ruf-Nr.	Anzeige der zugewiesene Rufnummer für Tagbetrieb
Tag Name	Anzeige des Namens der zugewiesenen Rufnummer für Tagbetrieb
Nacht Ruf-Nr.	Anzeige der zugewiesene Rufnummer für Nachtbetrieb

Parameter	Beschreibung
Nacht Name	Anzeige des Namens der zugewiesenen Rufnummer für Nachtbetrieb

Parameterbeschreibung der Registerkarten:

- **Leitung hinzufügen**

Parameter	Beschreibung
Nummer	Anzahl der hinzuzufügenden Leitungen.

Parameterbeschreibung der Registerkarten:

- **Rufrichtung ändern**

Parameter	Beschreibung
Ltg.	Anzeige der Leitungsnummer.
gehend	Ausgehende Anrufe können in der Leitung getätigt werden. **Anmerkung:** Das Absetzen von Notrufen ist möglich, auch wenn das Flag deaktiviert ist.
kommend	Eingehende Anrufe können auf der Leitung entgegengenommen werden.

Parameterbeschreibung der Registerkarten:

- **Leitung ändern**
- **Leitung löschen**

Parameter	Beschreibung
Leitung	Anzeige der Leitungsnummer.
Box/Slot/Port/Leitung	Anzeige des physikalischen Ports der Leitung (Box/Slot/Port/Leitung).
Kennz.	Anzeige oder Eingabe der Richtungskennzahl
Richtung	Anzeige oder Auswahl der Richtung, die der Leitung zugeordnet ist (keine oder Ltg. Grp 1 bis Ltg. Grp 12).
Rufzuordnung Leitung	
Tag Ruf-Nr.	Rufnummer für nicht durchwahlfähige kommende Verbindung am Tag
Nacht Ruf-Nr.	Rufnummer für nicht durchwahlfähige, eingehende Verbindung am Nachtbetrieb.

Parameterbeschreibung der Registerkarten:

- **ISDN-Flags ädern**

Parameter	Beschreibung
Protokoll: Beschreibung	Jeder Eintrag für ein Protokoll-Template setzt sich zusammen aus Interface, Protokoll und Zusatzinfo: S0 Basisanschluss 2B+D über S0 -Interface, BRI Basisanschluss 2B+D über U2B1Q -Interface (USA), S2 Primärmultiplexanschluss 30B+D, T1 Primärmultiplexanschluss 23B+D (USA)

Parameter	Beschreibung
Logical/Physical	logische oder physikalische Zählweise der Kanäle
Slave B-channel neg: Master	Festlegung Master/Slave innerhalb des Layer 3. Bei Verbindungen ist eine Seite als Slave - die andere Seite als Master einzustellen.
Up B-channel alloc: Unten	Festlegung der B-Kanalzählweise (muss in beiden Systemen gleich sein)
S0 CHI-Format: S2M	Protokollformat CHI, festzulegen als S0 (kurzes Format) oder S2M (langes Format)
Unsymmetric/Symmetric	Symmetrische bzw. nicht symmetrische Verwendung von L3-Protokollelementen
Automatic/Fixed	Automatische Aushandlung bzw. Feste Zuordnung der Symmetrie
1 CR-Länge: 2	Protokollformat Call Referenzlänge
Alarm signalling	Verwendung von Alarm-signalisierungen im Schicht 3 Protokoll
Protocol timers	Verwendung der Schicht 3 Timer
PRI quickstart	Verwendung der PRI-Quickstart Prozedur
IE_TNS	Verwendung des Informationselements Transit Network Selection
IE_OSA	Verwendung des Informationselementes Open Service Access
CIDL	Verwendung der Call and Link ID-Signalisierung in der Vernetzung
Userside/Networkside	Protokollfestlegung Layer 2. Auf der Gegenseite gespiegelte Einstellung notwendig
Network/Subscriber	Protokollfestlegung Layer 2. Auf der Gegenseite gespiegelte Einstellung notwendig
PP/PMP	Festlegung Punkt zu Punkt oder Punkt zu Mehrpunkt, nur bei S0 relevant
Permanent active	Schicht 2 Daueraktiv
Active TEI verify	TEI Überprüfung aktivieren
Userside/Networkside	Protokollfestlegung Layer 1. Auf der Gegenseite gespiegelte Einstellung notwendig
PP/PMP	Protokollfestlegung Layer 1. Gleiche Einstellungen auf beiden Seiten notwendig
S Bus type: L	kurzer/langer Bus (Reichweiten)
Permanent active	Protokollfestlegung Layer 1. Gleiche Einstellungen auf beiden Seiten notwendig
CRC4 check	Protokollfestlegung Layer 1., nur bei S2M relevant, beide Seiten gleiche Einstellung
CRC4 reporting	Protokollfestlegung Layer 1., nur bei S2M relevant, beide Seiten gleiche Einstellung

Parameterbeschreibung der Registerkarten:

- **B-Kanal ändern**

Parameter	Beschreibung
B-Kanal	Anzeige der B-Kanalnummer.
Gehend	Auf dem B-Kanal darf gehend telefoniert werden.
Kommend	Auf dem B-Kanal darf kommend telefoniert werden.

Parameterbeschreibung der Registerkarten:

- **Rufrichtung ändern**

Parameter	Beschreibung
Ltg.	Anzeige der Leitungsnummer.
Gehend	Ausgehende Anrufe können in der Leitung getätigt werden.
Kommend	Eingehende Anrufe können auf der Leitung entgegengenommen werden.

28.3.10.2 Trunks/Routing > Trunkgruppe

Parameterbeschreibung der Registerkarten:

- **Route ändern**

Parameter	Beschreibung
Routenbezeichnung	Bezeichnung der Route. Der eingegebene Name ersetzt die Standard-Routennummer in der Routenliste.
Belegungcodes	Hier werden die Belegungcodes für die einzelnen Routen eingegeben. Die eingegebenen Routingcodes müssen sowohl untereinander als auch innerhalb des gesamten Rufnummernplans des Kommunikationssystems kollisionsfrei sein. Verwenden Sie die Schaltfläche „Prüfen“, um diese auf Kollisionen zu testen. Der Belegungscode ist der Code, der das Vermittlungssystem veranlasst, eine Leitung zu der Station bereitzustellen, die den Code gewählt hat. Belegungscodes funktionieren nur, wenn LCR nicht aktiviert ist.
CO-Code (2. Trunk-Code)	Ein zweiter Trunk-Code (CO-Code) wird definiert, wenn das Kommunikationssystem ein Subsystem eines anderen Kommunikationssystems ist oder mit mehreren anderen Kommunikationssystemen vernetzt ist. Er ist nur für Netzverbindungen (Verbindungstyp = PABX) relevant. In diesem Fall ist der zweite Trunk-Code der Belegungscode für das Hauptsystem. Innerhalb eines Netzess müssen die Codes für die Trunk-Belegung, die Route-Belegungscodes und der zweite CO-Code einheitlich konfiguriert werden. Die Standardeinstellung in Deutschland ist 0.
Standort des Gateways	
Ländercode	Zeigt den Ländercode des Standorts des eigenen Gateways an. Einstellung über Grundeinstellungen/Gateway/Standorte des Gateways
Ortsnetzkennzahl	Zeigt die Ortsvorwahl des Standorts des eigenen Gateways an. Einstellung über Grundeinstellungen/Gateway/Standorte des Gateways

Parameter	Beschreibung
PABX-Nummer	Zeigt die PABX-Nummer des Standorts des eigenen Gateways an. Einstellung über Grundeinstellungen/Gateway/Standorte des Gateways
Systemstationennummer – eingehend	
Ländercode	Wird für die Ziffernanalyse bei eingehenden Anrufen verwendet. Ländercode ohne vorangestellte Nullen (z. B. 1 in den USA, 49 in Deutschland)
Ortsnetzkennzahl	Wird für die Ziffernanalyse bei eingehenden Anrufen verwendet. Ortsvorwahl ohne vorangestellte Nullen (z. B. 89 für München)
PABX-Nummer	Wird für die Ziffernanalyse bei eingehenden Anrufen verwendet. PABX-Nummer (zentrale Unternehmensrufnummer, z. B. 777)
Standortnummer	Wird für die Ziffernanalyse von öffentlichen Telefonnummern für ausgehende Verbindungen verwendet. Überprüft die Wählinformationen, um festzustellen, ob sich die angerufene Zielnummer im eigenen System befindet.
Systemstationennummer – ausgehend Info: Änderungen an ausgehenden PABX-Nummern müssen mit den Netzbetreibern abgestimmt werden. (Begrenzen ohne Überprüfung)	
Ländercode	Wird zur Anruferidentifizierung bei ausgehenden Anrufen verwendet. Die Ländervorwahl ohne vorangestellte Nullen (z. B. 1 in den USA, 49 in Deutschland) wird an das Netz übertragen. Wenn keine „PABX-Nummer, ausgehend” eingegeben ist, wird automatisch die „PABX-Nummer, eingehend” verwendet.
Ortsnetzkennzahl	Wird zur Anruferidentifizierung bei ausgehenden Anrufen verwendet. Die hier angegebene Ortsvorwahl (ohne vorangestellte Nullen, z. B. 89 für München) wird an das Netz übertragen. Wenn keine „PABX-Nummer, ausgehend” eingegeben ist, wird automatisch die „PABX-Nummer, eingehend” verwendet.
PABX-Nummer	Wird zur Anruferidentifizierung bei ausgehenden Anrufen verwendet. Die hier angegebene PABX-Nummer (zentrale Telefonnummer des Unternehmens, z. B. 777) wird an das Netz übertragen. Wenn keine „PABX-Nummer, ausgehend” eingegeben ist, wird automatisch die „PABX-Nummer, eingehend” verwendet.
Station unterdrücken. Rufnummer	Durch Aktivieren dieses Flags wird die DID-Nummer in der Anrufer-ID unterdrückt.
Überlaufroute	
Überlaufroute	Wenn alle Leitungen der konfigurierten Route belegt sind, kann ein Überlauf zu einer anderen Route eingerichtet werden. Die Überlaufroute gilt nur, wenn LCR deaktiviert ist.
Ziffernübertragung	
Ziffernübertragung	Die Art der Ziffernübertragung wird hier für die ausgewählte Route festgelegt und als statischer Text (z. B. Routentabelle 6: En-bloc-Versand) unter Einstellungen | Least Cost Routing | Wählplan nach Auswahl der Routentabelle (siehe Dropdown-Liste Routentabelle) angezeigt.
Ziffernübertragung: Ziffer für Ziffer	Die Ziffern werden synchron zum Wählvorgang übertragen.

Parameter	Beschreibung
Ziffernübertragung: En-bloc-Versand	Bei der En-bloc-Ziffernübertragung (Blockanwahl pro Route) werden die gewählten Ziffern vom Kommunikationssystem gepuffert. Die Anwahl erfolgt erst, wenn nach der letzten Ziffer ein Timer abgelaufen ist, wenn der Wahlschlusscode # eingegeben wurde oder wenn eine exakte Übereinstimmung in der Wählregel gefunden wurde. Bei PRI in den USA ist die Blockanwahl zur Vermittlungsstelle obligatorisch. LCR muss aktiviert sein, um die En-bloc-Ziffernübertragung auswählen zu können. Die Art der Ziffernübertragung wird in der Routingtabelle automatisch auf En-bloc-Ziffernübertragung gesetzt, wenn mindestens eine Route der LCR-Routingtabelle mit En-bloc-Ziffernübertragung konfiguriert ist.
Mobile Nebenstellennummer (Mobile Extension Number, MEX)	
MEX-Nummer	Wenn der verwendete ITSP die Funktion „Mobile Nebenstelle (MEX)" unterstützt, muss die vom ITSP bereitgestellte MEX-Nummer (8 Stellen, nur Ziffern) hier eingegeben werden. Diese Funktion kann nur mit einer Internet-Telefonie-DID-Verbindung (SIP wie ISDN) genutzt werden. Sie dient dazu, Mobiltelefone/Smartphones in das Kommunikationssystem zu integrieren. Der Nutzer des Mobiltelefons ist über den One Number Service unter einer einzigen Telefonnummer erreichbar, die auch dem Gesprächspartner mitgeteilt wird. Wenn ein Teilnehmer mit seinem Mobiltelefon telefoniert, wird dem Gesprächspartner die Büronummer des Teilnehmers angezeigt, sodass die Nummer des Mobiltelefons des Teilnehmers unbekannt bleibt. Darüber hinaus können andere interne Teilnehmer den Präsenzstatus solcher Teilnehmer überprüfen, auch wenn diese gerade mit ihrem Mobiltelefon telefonieren.
Vertrauenswürdiger externer Benutzer	
Vertrauenswürdiger externer Benutzer	Benutzer, der einer externen Kollaborationsplattform wie MS Teams zugewiesen werden kann, um Telefonanrufe zu tätigen.

Parameterbeschreibung der Registerkarten:

- **Routing-Parameter ändern**

Parameter	Beschreibung
Routing-Flags	
Ziffernwiederholung an	Wenn eine ausgehende Leitung mit aktivierter Ziffernwiederholung belegt ist, wird der Routing-Code vor der Rufnummer gesendet. Dies gilt nur, wenn LCR deaktiviert ist (siehe Einstellungen | Kostengünstigste Route).
Analyse des zweiten Wähltons / Trunk-Überwachung	Die Analyse des zweiten Wähltons alarmiert das Kommunikationssystem, um einen zusätzlichen Wählton zu erkennen. Diese Funktion wird bei Tandem-Kommunikationssystemanwendungen verwendet. Diese Auswertung ist länderabhängig, z B. in Belgien nach 00 und in Frankreich nach 16 oder 19. Für Deutschland ist dies nicht relevant. Dies gilt nur für Netzbetreiber, die bei Auslandsgesprächen einen zweiten Wählton senden.

Parameter	Beschreibung
Abfang pro Richtung	Dieses Flag ist für die QSIG-Vernetzung erforderlich. Wenn dieses Flag gesetzt ist, überprüft das Kommunikationssystem, ob eine Umleitungsanforderung von der Gegenstelle empfangen wurde oder ob das Kommunikationssystem eine Weiterleitung an die zentrale Abhörposition durchgeführt hat. Die Gegenstelle empfängt eine Nachricht, die angibt, ob für diesen Anruf eine Umleitung durchgeführt werden soll oder nicht. Wenn für eine Route die Anrufüberwachung aktiviert ist, werden alle an diese Route weitergeleiteten Anrufe an dieser Überwachungsposition abgefangen. Um diese Funktion zu implementieren, müssen für jede Route Tag- und Nachtnummern konfiguriert werden (siehe Klingelzuordnung pro Leitung). Darüber hinaus sollte für den Tag-/Nachtdienst keine Überwachungsposition eingegeben werden (siehe Anrufüberwachung/Vermittlung).
Über. Dienst 3,1 kHz Audio	Für alle ausgehenden Anrufe über ISDN ist „Über. Dienst 3,1 kHz Audio" die Standardeinstellung. Dies ist der Standardübertragungstyp für ausgehende Anrufe über eine ISDN-Leitung (Integrated Services Digital Network). Eine Verbindung vom Kommunikationssystem zu einer digitalen Vermittlungsstelle mit einem analogen Modem muss als Datendienst identifiziert werden. Dieses Flag sollte gesetzt werden, um Probleme beim Faxbetrieb zu vermeiden. In einigen Fällen unterstützt ein Netzbetreiber möglicherweise den 3,1-kHz-Audio-Bearer-Dienst nicht. Dies kann dazu führen, dass die Faxübertragung an bestimmte externe Telefonnummern fehlschlägt. Eine mögliche Lösung besteht darin, das Flag **Over. service 3.1 kHz Audio** zu deaktivieren.
Richtungsvorwahl hinzufügen – eingehend	Wenn diese Option auf Systemtelefonen mit eingehender Anrufbelegung aktiviert ist, wird die Rufnummernanzeige um den Routencode ergänzt.
Richtungsvorwahl hinzufügen – ausgehend	Wenn diese Option bei ausgehender Anrufbelegung aktiviert ist, wird die Rufnummernanzeige um den Zugangscode ergänzt. Hinweis: Die Änderung dieses Parameters wirkt sich auf die Anruferidentifikation aus und muss daher mit den Netzbetreibern abgestimmt werden. (Begrenzen ohne Überprüfung)
Rufnummer mit Landes-/ Ortsvorwahl	Wenn dieses Flag gesetzt ist, muss die Landes-/Ortsvorwahl der Rufnummer (z B. 02302…., 00492302...) als Vorwahl für den ITSP hinzugefügt werden. Standard: Aktiviert
Rückrufton an der CO	Wenn dieses Flag gesetzt ist, wird bei einem eingehenden Anruf ein „Rückrufton" an die ISDN-Vermittlungsstelle gesendet. Dies ist eine spezielle Protokollbehandlung, die für die Anbieter Global One und Sovintel erforderlich ist.
Segmentierung	Dieser Bereich definiert das Systemverhalten beim Senden von ISDN-Nachrichten, bei denen die maximale Länge der Schicht-2-Benutzerdaten (260 Byte) überschritten wird.
Segmentierung: ja	Die zu sendende Nachricht wird in Segmente von 260 Byte aufgeteilt und einzeln gesendet. Das empfangende Kommunikationssystem muss die Segmentierung unterstützen und die einzelnen Segmente sammeln und zu einer Nachricht zusammenfügen.
Segmentierungnein	Eine Segmentierung ist nicht erforderlich, da die zugrunde liegende Schicht 2 Nachrichten beliebiger Länge transportieren kann.

Parameter	Beschreibung
Segmentierung: Nachricht kürzen	Die zu sendende Nachricht wird durch Entfernen weniger wichtiger Teile (z. B. Namen) auf weniger als 260 Byte gekürzt und dann gesendet.
UUS pro Route deaktivieren	Mit diesem Flag kann das User-to-User Signaling (UUS) deaktiviert werden. Dadurch wird die Übertragung des Namens und der Telefonnummer der A-Station im UUI-Element (User-to-User Information) für die externe Anrufweiterleitung (auch FWD ext. Für External Call Forwarding) unterdrückt. Dieses Flag muss für Telefonica manuell deaktiviert werden.
Immer DSP verwenden	Wenn dieses Flag gesetzt ist, ist eine Verbindung zum Internet-Telefonieanbieter nur über einen DSP (Digital Signal Processor) möglich. Wenn dieses Flag nicht gesetzt ist, besteht eine Direct Payload Verbindung zum Internet-Telefonieanbieter. Dieses Flag muss für die Route des OpenScape Voice Netzwerks gesetzt werden. Dieses Flag darf nicht bei Faxübertragungen (T.38) über ein externes Gerät (z. B. Mediatrix 4102) gesetzt werden.
Name im CO	Dieses Flag wird für COs konfiguriert, die den Namen des Anrufers unterstützen.
Analoge Trunkbelegung	Hier können verschiedene Zeiten ausgewählt werden, die bestimmen, wann die Wahl bei Verwendung analoger Einwahlleitungen (MSI) beginnt. Wenn keine Pause eingestellt ist, wartet das Kommunikationssystem, bis es ein Freizeichen erkennt. Hinweis für Brasilien: Bei Verwendung von DTMF-Signalisierung von analogen Endgeräten in Verbindung mit analogen Trunks und Ziffernauswahl nach Erkennung des Freizeichens kann es zu Problemen mit der Ferngesprächsbeschränkung kommen, wenn die Ländervorwahl auf Brasilien eingestellt ist. In diesem Fall werden die DTMF-Signale von den analogen Endgeräten direkt an die analogen Trunks weitergeleitet (das „1A-Verfahren” wird nicht verwendet). Aus diesem Grund gehen die DTMF-Signale, die vor dem Empfang des Wähltons gewählt werden, verloren. Folglich muss in solchen Fällen die Least-Cost-Routing-Funktion (LCR) für die Wählmethode aktiviert werden, damit die Ferngesprächsbeschränkung auf dem Gerät ordnungsgemäß funktioniert.
Ferngesprächspause	Die CO-Anrufpause bestimmt die Zeitspanne, die verstreicht, bevor ein Anruf als beendet erkannt wird, nachdem der Benutzer aufgelegt hat. Diese Option gilt nur für MSI-Leitungen. Für einen Ferngespräch mit beispielsweise 1 Sekunde Ein- und 4 Sekunden Aus-Zeit sollte eine Ferngesprächspause von 6 Sekunden konfiguriert werden. In einigen COs gilt jedoch eine Klingelpause von 10 Sekunden. In solchen Fällen muss eine Ferngesprächspause von 13 Sekunden programmiert werden. Andernfalls kann keine Anrufumleitung implementiert werden. In den Vereinigten Staaten beträgt dieser Zyklus zwei Sekunden ein, zwei Sekunden aus, insgesamt also sechs Sekunden. Die Option „Sechs Sekunden“ ist die Standardeinstellung, sodass Sie hier keine Änderungen vornehmen müssen. Einstellbereich: 2 bis 13 Sekunden.
Art der Belegung	In diesem Feld werden die Kriterien festgelegt, die gelten, wenn das Kommunikationssystem eine ausgehende Leitung belegen muss.
Art der Belegung: zyklisch	Das Kommunikationssystem beginnt seine zyklische Suche nach einer freien Leitung mit der nächsten Leitungsnummer, basierend auf der letzten in dieser Route belegten ausgehenden Leitung.
Art der Belegung: linear	Das Kommunikationssystem beginnt seine Suche stets mit der niedrigsten dieser Route zugewiesenen Leitungsnummer.

Parameter	Beschreibung
Routentyp	Für den Routentyp stehen zwei Optionen zur Verfügung. Der Routentyp kann entweder als CO (Central Office) oder als PABX (Private Automatic Branch Exchange) festgelegt werden.
Routentyp: CO	Die dieser Route zugewiesenen Leitungen unterliegen einer Gebührenbeschränkung. Wenn LCR aktiv ist, wird die Gebührenbeschränkung durch den Wählplan (Spalte COS) geregelt.
Routentyp: PABX	Die Gebührenbeschränkung wird nur durchgeführt, wenn dieser Route ein zweiter CO-Code zugewiesen ist. Wenn LCR aktiv ist, wird die Gebührenbeschränkung durch den Wählplan (Spalte COS) geregelt. Der Routentyp hat auch Einfluss auf den Standardtext des Routennamens (siehe Routen) sowie auf das Verfahren zur Erkennung des Wähltons auf MSI-Leitungen.
Nr. und Typ – ausgehend	Der Administrator kann die „PABX-Nummer, eingehend” und „PABX-Nummer, ausgehend” separat konfigurieren, unterteilt in die Teile Ländercode, Ortsvorwahl und PABX-Nummer (= Anschlussnummer im lokalen Netz). Dies ist für die Implementierung der Funktion „Beschränken ohne Überprüfung” erforderlich. Wenn keine „PABX-Nummer, ausgehend” konfiguriert wurde, verwendet das Kommunikationssystem immer die Daten der Einstellung „PABX-Nummer, eingehend”. Bei einem eingehenden Anruf über eine ISDN-Leitung kürzt das Kommunikationssystem die PABX-Nummer (linksbündig) aus der empfangenen Telefonnummer und interpretiert den verbleibenden Teil als Direktwahlnummer. Für die Rufnummerninformationen zum PSTN fügt das Kommunikationssystem automatisch die PABX-Nummer (oder den in der Konfiguration definierten Teil) als vorangestellten Teil der Rufnummer ein. Dies gilt nicht für Wählinformationen (Zieladresse). Die Rufnummern interner Stationen, die an die Fernstation gesendet werden, können wie folgt gewählt werden:
Nr. und Typ – ausgehend: Unbekannt	Nur DID-Nummer (Standardeinstellung)
Nr. und Typ – ausgehend: PABX-Nummer	PABX-Nummer + DID-Nummer
Nr. und Typ – ausgehend: Ortsnetzkennzahl	+ Ortsvorwahl + PABX-Nummer + DID-Nummer
Nr. und Typ – ausgehend: Ländercode	Ländervorwahl + Ortsvorwahl + PABX-Nummer + DID-Nummer
Nr. und Typ – ausgehend: Intern	Nur für vernetzte Systeme: Bei geschlossenen Rufnummernplänen dürfen keine Vorwahlen hinzugefügt werden. Hier werden Vorwahlen unterdrückt.
Rufnummerntyp	Die Einstellungen im Bereich „Nr. und Typ – ausgehend” wirken sich auch auf Anrufe aus, die von einer Nebenstelle in einem Partnersystem (einem vernetzten Knoten) kommen. Aufgrund dieser Einstellung wird die Rufnummer des Anrufers, die vom vernetzten Knoten empfangen und an die Vermittlungsstelle weitergeleitet wird, für die abgehende Route erweitert.

Parameter	Beschreibung
Rufnummerntyp: Intern	In diesem Fall wird nur die interne Rufnummer übertragen. Wenn es sich bei dem Ziel um eine externe Sprechstelle handelt, wird entweder keine Nummer übertragen oder nur die der Vermittlungskonsole. Die interne Rufnummer kann angezeigt werden, wenn das Ziel eine interne Sprechstelle auf einem anderen Knoten ist.
Rufnummerntyp: Durchwahl	In diesem Fall wird nur die DID-Nummer übertragen. Die interne Rufnummer wird nicht zur Anzeige an internen Zielen in anderen Knoten bereitgestellt. Die Rufnummerninformationen sind für externe Ziele ausreichend.
Rufnummerntyp: Intern / DID	Diese Einstellung ist für Netzzwecke nützlich. Sowohl die interne Rufnummer als auch die DID-Rufnummer werden an die Gegenstelle übertragen. Wird eine interne Sprechstelle innerhalb des Netzes angerufen, kann für diese Sprechstell die interne Rufnummer des Anrufers angezeigt werden. Hat die interne Gegenstelle die Rufumleitung zu einer externen Gegenstelle aktiviert, kann in diesem Fall auch eine DID-Nummer übertragen werden.
Umleitung	
Route ändern	Wenn dieses Flag aktiviert ist, ist es auch möglich, D-Kanal-Informationen über andere Routen zu leiten. Diese Option ermöglicht eine alternative Weiterleitung über andere Routen. Die Option kann nur aktiviert werden, wenn der Rufnummernplan eindeutig ist. (Geschlossener Nummernplan oder eindeutige Rufnummern in einem Netz. Das anfragende System muss dies ebenfalls unterstützen.) Wenn die Umleitung implementiert ist, muss für die entsprechende Route auch die Umleitung mit aktiver Routenänderung eingestellt werden. Diese Option ist nur für CorNet NQ-Vernetzungen verfügbar und muss in beiden vernetzten Kommunikationssystemen auf die gleiche Weise aktiviert werden.
Routenoptimierung aktiv	Um die Nutzung des B-Kanals zu optimieren, kann die Anrufweiterleitung auf der Grundlage des Protokolls gemäß der Spezifikation „Anrufweiterleitung/ Teilumleitung“ durchgeführt werden. Wird die Teilumleitung abgelehnt, wird die Weitervermittlung verwendet.
Routenoptimierung aktiv: Nein	Wenn Sie diese Option auswählen, wird die Umleitung deaktiviert. Bei der Rufumleitung wird die Verbindung immer über zwei B-Kanäle hergestellt.
Umleitung aktiv: Wenn die Route unbekannt ist	Wenn Sie diese Option auswählen, ist die Umleitung nur aktiv, wenn die Route bekannt ist und ein erfolgreicher „Handshake” zwischen den beiden vernetzten Kommunikationssystemen stattfindet.
Routenoptimierung aktiv: Immer	Wenn die Einrichtung für den eingehenden Anruf über dieselbe Route wie die Anrufweiterleitungszielroute erfolgt, wird der Anruf vom Kommunikationssystem abgelehnt (Anrufumleitungsfunktion), wenn diese Option aktiviert ist. Bei vernetzten Systemen muss diese Option „Immer” in beiden vernetzten Kommunikationssystemen auf die gleiche Weise aktiviert werden.

Parameterbeschreibung der Registerkarten:

- **Spezielle Parameter ändern**

Parameter	Beschreibung
Nummernplan Definiert den Parameter „Nummernplan“ in ausgehenden Nachrichten	
Nummer des angerufenen Teilnehmers	Systemprüfung = vom System definiert; ISDN-Nummernplan, privater Nummernplan, unbekannter Nummernplan = manuell voreingestellt
Alle anderen	z. B. Nummer des anrufenden Teilnehmers, Weiterleitungsnummer usw. Systemprüfung = vom System definiert.. ISDN-Nummernplan, privater Nummernplan, unbekannter Nummernplan = manuell voreingestellt
Site	Der Parameter „Site“ (Standort) bestimmt, wie der Standort-Parameter im Q931-Infoelement CAUSE und Progress Indicator gesetzt wird. Systemprüfung = vom System definiert; alternativ kann die Einstellung „Privates Netz und Sprechstelle“ oder „Immer Sprechstelle“ manuell vorgenommen werden.
COLP	Wenn dieses Flag gesetzt ist, wird dem Anrufer bei einem externen eingehenden CO-Anschluss die Nummer des Angerufenen angezeigt. Der Anrufer kann sehen, ob der Anruf weitergeleitet oder von jemand anderem angenommen wurde. Diese Funktion muss ebenfalls von der Vermittlungsstelle aktiviert werden. Wenn das Flag gesetzt ist und ein externer eingehender Anruf weitergeleitet oder abgefangen wird, wird die aktualisierte Rufnummer in der vom Kommunikationssystem ausgegebenen Verbindungsmeldung an die Vermittlungsstelle gemeldet. Wenn die COLP-Funktion in der Vermittlungsstelle aktiviert ist, wird die aktualisierte Rufnummer auch für den Anrufer angezeigt. Info: Dieses Flag hat keinen Einfluss auf die Anzeige der Rufnummer bei externen ausgehenden Verbindungen.
Benachrichtigung senden	Diese Nachricht wird für die Übertragung von Statusinformationen über die aktuelle Verbindung verwendet. Die Nachricht kann sowohl vom Netz als auch von der Teilnehmerseite gesendet werden, um die andere Partei (Netz oder Teilnehmer) beispielsweise über eine unterbrochene Verbindung oder eine aktive Anrufweiterleitung zu informieren. Wenn die Benachrichtigungsfunktion von der Vermittlungsstelle nicht unterstützt wird, kann die Benachrichtigungsmeldung durch Zurücksetzen dieses Flags unterdrückt werden. Wenn diese Option aktiviert ist, wird beispielsweise bei einem gehaltenen oder geparkten Anruf eine „Benachrichtigungsmeldung” übertragen. Diese wird nur in den Protokollen DSS1, NI1 und MCI ausgewertet. In den Protokollen SIP-Q, CorNet-NQ und QSIG wird die Benachrichtigung immer gesendet.
Ohne CLIP	Wenn dieses Flag gesetzt ist, werden die Informationen zum Anrufer für das öffentliche Netz bei ausgehenden Anrufen über eine BRI- oder PRI-Leitung unterdrückt. Dieses Flag kann für jede Route einzeln aktiviert oder deaktiviert werden. Darüber hinaus hat die Sprechstell die Möglichkeit, die Informationen zum Angerufenen für jeden Anruf einzeln über einen Zugangscode oder das Systemtelefonmenü zu unterdrücken.
Kein SETUP ACK.	Wenn dieses Flag gesetzt ist, wird die Setup-Bestätigungsmeldung vom Kommunikationssystem an die Vermittlungsstelle unterdrückt. Relevant für spezielle Vermittlungsstellen. Beispiel: Fujitsu's Fetex150 COs.

Parameter	Beschreibung
Keine DIV.LEG-Info	Wenn dieses Flag gesetzt ist, wird das standardmäßige LEG-Informationssignal (Rufnummer des umleitenden Teilnehmers) nicht an die Vermittlungsstelle gesendet. Die DIV. LEG-Info sollte unterdrückt werden, wenn Probleme bei der externen Anrufweiterleitung (CF ext.) auftreten.
Bei Sendeabschluss	Wenn dieses Flag gesetzt ist, wird die optionale Information „Alle Ziffern gesendet" vom System ausgegeben, sobald alle gewählten Ziffern übertragen wurden.
Interner Anruf wie externer	Wenn dieses Flag gesetzt ist, werden netzinterne Anrufe akustisch genauso signalisiert wie externe Anrufe.
Ohne CCNR	Wenn dieses Flag gesetzt ist, wird ein eingehender ISDN-Anruf mit CCNR (Call Completion on No Reply) signalisiert, damit das System eine Rückrufaufforderung annehmen kann. Das bedeutet, dass der Anrufer einen Rückruf initiieren kann, wenn die Sprechstelle nicht antwortet. In einigen Fällen wird die Meldung vom ISDN-Anbieter nicht unterstützt. In diesem Fall muss der Schalter aktiviert werden, um zu verhindern, dass das System CCNR sendet.

28.3.10.3 Leitungen/Vernetzung > QSIG-Leistungsmerkmale

In einem aus mehreren Kommunikationssystemen bestehenden Netzverbund werden in den Teilanlagen anfallende Verbindungsinformationen (GEZ-Daten) an ein festgelegtes Kommunikationssystem des Verbunds gesendet. Zu diesem Zweck wird in jedem Kommunikationssystem die Rufnummer des Zielsystems (Rufnummer der zentralen Erfassungsstelle) konfiguriert, an das die Verbindungsdaten gesendet werden.

Parameterbeschreibung der Registerkarten:

- **QSIG-Leistungsmerkmale ändern**

Parameter	Beschreibung
Daten der eigenen Anlage	
Anlagennummer	Mit diesen Daten wird das eigene Kommunikationssystem im Netzverbund identifiziert. Diese Daten sind sowohl für die zentrale Besetztsignalisierung als auch für das Verbindungsdaten-Routing gültig. In einem aus mehreren Kommunikationssystemen bestehenden Netzverbund hat jedes Kommunikationssystem eine eindeutige Anlagennummer. Wenn das Kommunikationssystem mit solchen Kommunikationssystemen vernetzt ist, und man möchte die QSIG-Leistungsmerkmale benutzen, dann muss aus Kompatibilitätsgründen auch hier die Anlagennummer administriert werden. Wertebereich: 1 bis 255
Gruppennummer	In den Kommunikationssystemen können die Teilnehmer in Gruppen eingeteilt werden, die dann eine eindeutige Gruppennummer erhalten. Im Kommunikationssystem existiert eine solche Gruppierung nicht. Trotzdem soll aus Kompatibilitätsgründen auch hier die Gruppennummer administriert werden. Wertebereich: 1 bis 40

Parameter	Beschreibung
Anlagenübergreifende Besetztsignalisierung	
Anlagen-Nr. Zielsystem	Mit diesen Daten wird ein Kommunikationssystem definiert, das die zentrale Besetztsignalisierung realisiert. Dies kann sowohl die Hauptanlage als auch eine Unteranlage sein. Anlagennummer des Kommunikationssystems, das für die zentrale Besetztsignisierung eingerichtet ist. Wertebereich: 1 bis 255
Rufnr. Zielsystem	Rufnummer des Kommunikationssystems, das für die zentrale Besetztsignisierung eingerichtet ist. Hier ist nur die Anlagenrufnummer und keine Teilnehmerrufnummer einzutragen. Im LCR-Wahlplan ist zu berücksichtigen, dass beim Eintrag für diese Anlagenrufnummer keine Nachwahl eingetragen wird! Beispiel: Die Rufnummer des Zielsystems sei: 999 Der Wahlplaneintrag muss dann sein: -999 (und nicht -999XXX und nicht -999Z).
Verbindungsdaten-Routing	
Rufnr. Zielsystem	Mit diesen Daten wird ein Kommunikationssystem definiert, das die zentrale Verbindungsdatenerfassung realisiert. Dies kann sowohl die Hauptanlage als auch eine Unteranlage sein. Rufnummer des Kommunikationssystems, das als zentrale Erfassungsstelle eingerichtet ist (siehe auch den Hinweis zu Ruf-Nr. Zielsystem, weiter oben).

28.3.10.4 Leitungen/Routing > MSN zuweisen

Parameterbeschreibung der Registerkarten:

- **MSN anzeigen**
- **MSN ändern**

Parameter	Beschreibung
MSN	Anzeige oder Eingabe der MSN (Mehrgeräteanschluss Rufnummer).
Leitung	Anzeige der Zuordnung der Leitung, auf der die MSN aktiv ist.

28.3.10.5 Leitungen/Vernetzung > ISDN-Parameter

Durch den Referenztakt (ISDN Clock) werden Abläufe auf Amtsleitungen innerhalb eines bestimmten Netzes oder innerhalb des Amts synchronisiert. Normalerweise sucht sich das Kommunikationssystem automatisch die Leitung aus, die als Referenztaktgeber für sämtliche Kommunikationssysteme innerhalb eines Netzes oder im Amt fungiert. Sollte die Referenztaktleitung jedoch einmal ausfallen, müssen eine oder mehrere andere Leitungen als Referenztaktgeber eingerichtet werden.

Das Kommunikationssystem wählt die Leitung nach folgender Rangfolge aus:

1) Erlaubnisliste

2) S_{2M}-Amtsleitung
3) S_0-Amtsleitung
4) S_{2M}-Querleitung (nur Slave-Konfiguration)
5) S_0-Querleitung

Parameterbeschreibung der Registerkarten:

- **ISDN-Takt**

Parameter	Beschreibung
Index	Die Positionen spiegeln die Prioritäten 1-4 (für Erlaubnisliste) bzw. 1-16 (für Verbotsliste) wider.
Erlaubnislisten	Beinhaltet die Erlaubnisliste Einträge, wird die automatische Leitungsauswahl des Kommunikationssystems außer Kraft gesetzt. Die in der Erlaubnisliste eingetragenen ISDN-Ports (max 4 möglich) werden bei der Suche nach der Referenztaktleitung als Erstes verwendet.
Verbotslisten	Die in der Verbotsliste eingetragenen ISDN-Ports (max 16 möglich) werden bei der Suche nach der Referenztaktleitung übergangen.

28.3.11 Berechtigungen (Classes of Service)

Unter **Berechtigungen** sind die Funktionen für die Berechtigungen der Amtsleitungen zusammengefasst. Sie regeln den Zugang der Teilnehmer zu möglicherweise kostenpflichtigen externen Verbindungen.

28.3.11.1 Berechtigungen > Teilnehmer

Parameterbeschreibung der Registerkarte:

- **Alle Teilnehmer anzeigen**

Parameter	Beschreibung
Rufnr., **Rufnummer**	Rufnummer des Teilnehmers.
Name	Namen des Teilnehmers.
Tag	Ausgewählte Berechtigungsgruppe für den Tag.
Nacht	Ausgewählte Berechtigungsgruppe für die Nacht.
Berechtigungsgruppe Tag	Auswahl der Berechtigungsgruppe für den Tag. Die vorgenommene Auswahl verweist auf die Tabelle **Berechtigungen Tag**, über die die Berechtigungsgruppe mit der tatsächlichen Berechtigung verknüpft wird.
Berechtigungsgruppe Nacht	Auswahl der Berechtigungsgruppe für die Nacht. Die vorgenommene Auswahl verweist auf die Tabelle **Berechtigungen Nacht**, über die die Berechtigungsgruppe mit der tatsächlichen Berechtigung verknüpft wird.

Anmerkung: Die Texte der Dienstklassengruppen werden gemäß dem **Assistenten für die Grundkonfiguration** > **Systemländercode**generiert.

28.3.11.2 Berechtigungen > Tag: Berechtigungsgruppen

Parameterbeschreibung der Registerkarten:

- **Namen ändern**
- **Berechtigungsgruppe ändern**
- **Tag: Gruppenmitglieder anzeigen**

Parameter	Beschreibung
Berechtigungsgruppe	Selbstgewählter Name für die Berechtungsgruppen 1 bis 15. Zuweisung von Amtsberechtigungen pro Richtung (Leitungsbündel) jeweils für Tag und Nacht. Bei der Konfiguration der Teilnehmer kann der Zugriff auf externe Rufnummern durch Zuweisung von Berechtigungsgruppen eingeschränkt werden.
Berechtigung	Zuweisen der Berechtigungen zu den einzelnen Berechtigungsgruppen für Tagbetrieb. Alle Einschränkungen werden nur wirksam an Leitungen einer Richtung des Typs Amt.
Berechtigungsgruppe: Intern	Der Teilnehmer darf nur intern telefonieren. Standardwert: Default in Berechtigungsgruppe 1
Berechtigungsgruppe: Halbamt	Der Teilnehmer darf externe Gespräche nur annehmen. Standardwert: Default in Berechtigungsgruppe 2
Berechtigungsgruppe: Erlaubnisliste	Der Teilnehmer darf nur die in der Erlaubnisliste definierten externen Rufnummern wählen. Ist keine Rufnummer eingetragen gilt Halbamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 4
Berechtigungsgruppe: Verbotsliste	Der Teilnehmer darf die in der Verbotsliste definierten externen Rufnummern nicht wählen. Ist keine Rufnummer eingetragen gilt Vollamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 3, 5, 6
Berechtigungsgruppe: Uneingeschränkt	Der Teilnehmer darf ohne Einschränkung kommende und gehende externe Gespräche annehmen und aufbauen. Standardwert: Default in Berechtigungsgruppe 7 bis 15
Gruppenmitglieder anzeigen	Anzeige von Rufnummer und Name der Mitglieder in der ausgewählten Berechtigungsgruppe.

28.3.11.3 Berechtigungen > Nacht: Berechtigungsgruppen

Parameterbeschreibung der Registerkarten:

- **Namen ändern**
- **Berechtigungsgruppe ändern**
- **Nacht: Gruppenmitglieder anzeigen**

Parameter	Beschreibung
Berechtigungsgruppe	Selbstgewählter Name für die Berechtungsgruppen 1 bis 15. Zuweisung von Amtsberechtigungen pro Richtung (Leitungsbündel) jeweils für Tag und Nacht. Bei der Konfiguration der Teilnehmer kann der Zugriff auf externe Rufnummern durch Zuweisung von Berechtigungsgruppen eingeschränkt werden.
Berechtigung	Zuweisen der Berechtigungen zu den einzelnen Berechtigungsgruppen für Nachtbetrieb. Alle Einschränkungen werden nur wirksam an Leitungen einer Richtung des Typs Amt.
Berechtigungsgruppe: Intern	Der Teilnehmer darf nur intern telefonieren. Standardwert: Default in Berechtigungsgruppe 1
Berechtigungsgruppe: Halbamt	Der Teilnehmer darf externe Gespräche nur annehmen. Standardwert: Default in Berechtigungsgruppe 2
Berechtigungsgruppe: Erlaubnisliste	Der Teilnehmer darf nur die in der Erlaubnisliste definierten externen Rufnummern wählen. Ist keine Rufnummer eingetragen gilt Halbamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 4
Berechtigungsgruppe: Verbotsliste	Der Teilnehmer darf die in der Verbotsliste definierten externen Rufnummern nicht wählen. Ist keine Rufnummer eingetragen gilt Vollamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 3, 5, 6
Berechtigungsgruppe: Uneingeschränkt	Der Teilnehmer darf ohne Einschränkung kommende und gehende externe Gespräche annehmen und aufbauen. Standardwert: Default in Berechtigungsgruppe 7 bis 15
Gruppenmitglieder anzeigen	Anzeige von Rufnummer und Name der Mitglieder in der ausgewählten Berechtigungsgruppe.

28.3.11.4 Berechtigung > Erlaubnislisten

Parameterbeschreibung der Registerkarten:

- **Kurzwahlziele anzeigen**
- **Rufnummer hinzufügen**

Parameter	Beschreibung
Liste 1-6	Anzeigen/Hinzufügen/Ändern/Löschen einer erlaubten Rufnummer. Die Erlaubnisliste enthält die Rufnummern, die der Teilnehmer anrufen darf. Es können bis zu 6 Erlaubnislisten erstellt werden. Die 1. Erlaubnisliste kann 100 Einträge enthalten, die übrigen 5 Listen jeweils bis zu 10 Einträge.
Rufnummer	Die einzelnen Rufnummern können bis zu 26 Stellen (Ziffern 0 bis 9 sowie die Zeichen * und #) umfassen. Es muss dabei nicht die vollständige Rufnummer aufgeführt werden. Um Teilnehmer beispielsweise zur Anwahl aller (kostenlosen) 0800xxxer-Nummern zu berechtigen, muss hier lediglich die 0800 eingeben werden. Da sich die Listen nur auf gehende Externgespräche beziehen, muss die Amtsbelegungs-Kennziffer bei den eingetragenen Rufnummern nicht mit angegeben werden.

28.3.11.5 Berechtigungen > Verbotslisten

Parameterbeschreibung der Registerkarten:

- **Kurzwahlziele anzeigen**
- **Rufnummer hinzufügen**
- **Auswertungsfilter ändern**

Parameter	Beschreibung
Liste 1-6	Anzeigen/Hinzufügen/Ändern/Löschen einer verbotenen Rufnummer. Die Verbotsliste enthält die Rufnummern, die der Teilnehmer nicht anrufen kann. Es können bis zu 6 Verbotslisten erstellt werden. Die 1. Verbotsliste kann dabei 50 Einträge enthalten, die übrigen 5 Listen jeweils bis zu 10 Einträge.
Rufnummer	Die einzelnen Rufnummern können bis zu 26 Stellen (Ziffern 0 bis 9 sowie die Zeichen * und #) umfassen. Es muss dabei nicht die vollständige Rufnummer aufgeführt werden. Um beispielweise die Anwahl von (kostenpflichtigen) 0900xxxer-Nummern durch die Teilnehmer zu verhindern, muss hier lediglich die 0900 eingeben werden. Der Eintrag des Zeichens # an erster Stelle einer verbotenen Rufnummer verhindert eine Umgehung der Wahlkontrolle für Systemtelefone, die eine analoge Amtsleitung mit MFV-Wahlverfahren belegen und während der Wahl auf MFV umschalten wollen. Da sich die Listen nur auf gehende Externgespräche beziehen, muss die Amtskennzahl bei den eingetragenen Rufnummern nicht mit angegeben werden.
Auswertungsfilter ändern Über die Auswertungsfilter können Sie zu einer beliebigen Verbotsliste festlegen, welche Ziffern nicht mit der entsprechenden Verbotsliste verglichen werden sollen. Das Kommunikationssystem blendet den eingestellten Ziffernbereich vor der Wahlbewertung aus.	
Ab Ziffer ... **bis Ziffer**	In diesem Ziffernbereich (1-25) innerhalb der Rufnummer ist der Auswertungsfilter aktiv.
Zeichen	Durch ein Verbot der Zeichen * und # wird erreicht, dass ein Teilnehmer bei der Eingabe dieser Zeichen die Wahlkontrolle umgehen kann.

28.3.11.6 Berechtigungen > Blacklist

Parameterbeschreibung der Registerkarten:

- **Liste Anzeigen**
- **Rufnummer hinzufügen**

Parameter	Beschreibung
Rufnummer	Rufnummern können bis zu 25 Stellen (Ziffern 0 bis 9 sowie das Zeichen „+“) umfassen. Das Zeichen „+“ bezieht sich auf das internationale Präfix, das im System konfiguriert ist, und muss an erster Stelle eingegeben werden. Das erste Zeichen kann das Pluszeichen („+“) oder eine beliebige Ziffer sein. Die Telefonnummern werden in der Blacklist numerische sortiert. Blacklist-Einträge müssen im internationalen (z.B. 004989) oder im kanonischen internationalen Format (z.B. +4989) eingegeben werden.
Anonyme Anrufe blockieren	Wenn Sie dieses Flag aktivieren, werden Anrufe ohne Anrufer-Nummer oder mit Anrufer-Nummer, aber eingeschränkter Darstellung blockiert.

Parameter	Beschreibung
Blacklist Funktion	Durch Aktivieren dieses Flags werden die hinzugefügten Rufnummern blockiert. Die Blacklist-Funktion basiert ausschließlich auf der vom Anbieter angegebenen Rufnummer des Anrufers.

28.3.11.7 Berechtigungen > Nachtschaltung

Parameterbeschreibung der Registerkarte:

- **Nachtschaltung ändern**

Parameter	Beschreibung
Berechtigte Teilnehmer für Nachtschaltung	Sollen bestimmte Teilnehmer die Möglichkeit haben, das Kommunikationssystem in den Nachtmodus zu schalten, müssen diese Teilnehmer in die Liste Berechtigte Teilnehmer für Nachtschaltung eingetragen werden. Es können max. 5 Teilnehmer eingetragen werden. Standardwert: 100
Teilnehmer	Liste aller im Kommunikationssystem vorhandenen Teilnehmer.
Berechtigte Teilnehmer	Liste der berechtigten Teilnehmer, die den Nachtmodus aktivieren können.
Hinzufügen >>	Fügt den ausgewählten Teilnehmer zu den berechtigten Teilnehmern hinzu.

28.3.11.8 Berechtigungen > VBZ Gruppenzuordnung

Parameterbeschreibung der Registerkarten:

- **Zuweisung Teilnehmer zu Berechtigungsgruppe ändern**
- **Zuweisung Leitung zu VBZ-Gruppe**
- **Zuweisung KWZ-Bereich zu VBZ-Gruppe**

Parameter	Beschreibung
VBZ Gruppenzuordnung	Zuweisen einer VBZ-Gruppe (1-64) zu einem Teilnehmer. Über VBZ-Gruppenzuordnung weisen Sie den einzelnen Teilnehmern des Kommunikationssystems eine VBZ-Gruppe zu. Beim Kodieren der Verbindungsmatrix können Sie dann auf diese Gruppen zurückgreifen und festlegen, welche Teilnehmer welche anderen Teilnehmer erreichen können. Standardmäßig sind alle Teilnehmer der VBZ-Gruppe 1 zugeordnet. Damit haben alle Teilnehmer uneingeschränkten Zugang zu anderen Teilnehmern. Wertebereich: 1 - 64

Parameter	Beschreibung
Zuweisung Leitung zu VBZ-Gruppe	Zuweisen einer Leitung zur VBZ-Gruppe. Über VBZ-Gruppenzuordnung weisen Sie den einzelnen Leitungen des Kommunikationssystems eine VBZ-Gruppe zu. Be im Kodieren der Verbindungsmatrix können Sie dann auf diese Gruppen zurückgreifen und festlegen, welche Teilnehmer auf welche Leitungen zugreifen können. Standardmäßig sind alle Amtsleitungen der VBZ-Gruppe 1 zugeordnet. Damit haben alle Teilnehmer uneingeschränkten Zugang zu Leitungen, sowohl kommend als auch gehend. Wertebereich: 1 - 64
Zuweisung KWZ-Bereich zu VBZ-Gruppe	Jeder VBZ-Gruppe wird ein Bereich von Kurzwahlen (KWZ) zugeordnet. Wählt ein beliebiger Teilnehmer eine KWZ aus, wird durch Bestimmen der dazugehörigen VBZ-Gruppe ermittelt, ob dieser Teilnehmer berechtigt ist, diese KWZ auszuwählen. Liegt diese KWZ im Bereich der zugeordneten KWZ für die entsprechende VBZ-Gruppe, so erfolgt die Wahl. Entspricht die KWZ nicht dem zugeordneten Bereich erfolgt eine Fehlermeldung. Die KWZ-Bereiche können sich in der VBZ-Gruppe überschneiden. Es ist jedoch nicht zulässig, einzelne KWZ in den VBZ-Gruppen und mehrere KWZ-Bereiche in einer VBZ-Gruppe einzutragen. Beispielsweise ist Folgendes zulässig: CON 1: 0-99; CON 2: 50-150; CON 3: 200-500. Und Folgendes ist nicht zulässig: CON 1: 0, 5, 10; CON 2: 50-100, 300-500. Wertebereich: 0-7999

28.3.11.9 Berechtigungen > CON Matrix

Parameterbeschreibung der Registerkarten:

- **VBZ-Matrix ändern**

Parameter	Beschreibung
VBZ-Matrix	Wenn Sie eine Verbindungsmöglichkeit zwischen zwei VBZ-Gruppen gezielt bearbeiten möchten, klicken Sie in das Feld am Kreuzungspunkt dieser VBZ-Gruppen in der VBZ-Matrix. Klicken Sie wiederholt in das Feld, um Verbindungsmöglichkeiten in die eine Richtung, in die andere Richtung oder in beide Richtungen freizugeben oder zu sperren. Um die Verbindungsmatrix nutzen zu können, müssen Sie zunächst jeden Teilnehmer über VBZ-Gruppenzuordnung einer Gruppe zuweisen. Bei der Standardeinstellung sind sämtliche Teilnehmer und Leitungen der Gruppe 1 zugeordnet. Nachdem für die Gruppe 1 uneingeschränkter Zugang festgelegt ist, kann bei der Standardeinstellung jeder Teilnehmer auf sämtliche anderen Teilnehmer und Leitungen zugreifen.
Raster	In der Matrix wird eine Liste von Gruppen horizontal am oberen Rand und eine andere Liste vertikal am linken Rand eingeblendet. An den Berührungspunkten befindet sich jeweils ein Kästchen. Der Pfeil in dem betreffenden Kästchen gibt die Beziehung der beiden Gruppen zueinander an. Ein leeres Feld besagt, dass keine Verbindung möglich ist. Eine Verbindungsmatrix, bei der keine Pfeile eingetragen sind, hat eine völlige Blockade des Kommunikationssystems zur Folge.
Alles sperren	Die VBZ-Matrix unterdrückt den Verkehr zwischen Teilnehmern/Leitungen innerhalb einer Gruppe (Teilanlage) und zwischen den Gruppen.

Parameter	Beschreibung
Alles freigeben	Die VBZ-Matrix erlaubt den Verkehr zwischen Teilnehmern/Leitungen innerhalb einer Gruppe (Teilanlage) und zwischen den Gruppen.
Nur guppenintern	Die VBZ-Matrix erlaubt den Verkehr nur zwischen Teilnehmern/Leitungen innerhalb einer Gruppe (Teilanlage).

28.3.11.10 Berechtigungen > Automatische Nachtschaltung

Parameterbeschreibung der Registerkarten:

- **Alle Tage anzeigen**
- **Tag ändern**

Parameter	Beschreibung
Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Sondertag	Tag, der über den Zeitplan eingerichtet wird. Der Zeitplan umfasst die gesamte Woche (Montag bis Sonntag) sowie Sondertage. Sondertage sind Feiertage oder besondere Tage wie beispielsweise Betriebsferien.
Zone	Der Zeitplan eines Tages kann in bis zu 4 Zonen (Zeitintervalle) unterteilt werden. Die Zonen können lückenlos aufeinander aufsetzen, so kann beispielsweise die Endezeit des ersten Intervalls identisch sein mit der Anfangszeit des zweiten Intervalls. Ein Intervall kann nicht dieselbe Anfangs- und Endezeit haben. Die minimale Länge eines Intervalls beträgt 15 Minuten. Wertebereich: 1-4
Beginn	Anfangszeit für die Zone. Beginnt das erste Intervall eines Tages um 0.00 Uhr, muss die Startzeit als 00:00 eingegeben werden.
Ende	Endezeit für die Zone. Endet das letzte Intervall eines Tages um 24.00 Uhr (12 pm), muss die Endezeit als 23:59 (11:59) eingegeben werden.
Nacht Ruf-Nr.	Nacht-Rufnummer für die Zone. Wird für die Nacht-Rufnummer keine Rufnummer eingetragen, dann greift im System die Nachtschaltung pro Leitung. Die Ziele dafür werden unter **Leitungen/Vernetzung** > **Leitung ändern** > **Rufzuordnung Ltg** eingestellt. Die Zeiten, die über die automatische Nachtschaltung eingetragen werden, gelten für alle Leitungen.
OK	Die Zone wird eingerichtet.
Löschen	Die definierte Zone wird gelöscht.
Kopierdienst	Sie können die eingerichteten Zonen auf einen oder mehrere andere Tage kopieren, indem Sie den gewünschten Tag markieren, auf den Sondertag, indem Sie die entsprechende Flagge markieren, auf alle, indem Sie **Alle markieren**. Wenn Sie auf **Übernehmen** klicken, werden die Zoneneinstellungen der ausgewählten Tage mit den Zonen des aktuellen Tages überschrieben.

28.3.11.11 Berechtigungen > Sondertage

Parameterbeschreibung der Registerkarte:

- **Sondertage ändern**

Parameter	Beschreibung
Tag	Bei Auswahl eines Datums im Kalender, wird dieses automatisch hier eingeschrieben.
Name	Name für diesen Sondertag (z.B. Pfingstmontag)

28.3.12 Hilfsausrüstung

Die Funktionen für Hilfsausrüstung wie Wartemusik (MoH), das Einrichten von Ansagen oder das Anschließen einer Türsprechstelle als Türöffner an den Systemanschlüssen (Trunks) sind unter **Hilfsausrüstung** zusammengefasst.

28.3.12.1 Hilfsausrüstung > Wartemusik

Parameterbeschreibung der Registerkarten:

- **Wartemusik bearbeiten**

Parameter	Beschreibung
Typ der Wartemusik	Mit dem Parameter Typ der Wartemusik können Sie zwischen drei möglichen Optionen wählen. Die Musik für diese Funktion kann intern oder extern geliefert werden.
Typ der Wartemusik: Keine Wartemusik	Wenn diese Option ausgewählt ist, wird die Wartemusik komplett deaktiviert. Dies gilt nicht, wenn ein externer Anruf durch eine Übergabe vor der Annahme vermittelt wird; der Anrufer hört dann den Klingelton.
Typ der Wartemusik: Wartemusik ohne Rufton	Wenn diese Option ausgewählt ist, hört der Anrufer bei einer unmaskierten Vermittlung Wartemusik, während der Vermittlung sowie während das Gespräch vom vermittelnden Teilnehmer vermittelt wird und der externe Anschluss am vermittelten Ziel läutet.
Typ der Wartemusik: Wartemusik mit Rufton	Wenn diese Option ausgewählt ist, hört der Anrufer bei einer unmaskierten Vermittlung Wartemusik, während der Vermittlung. Sobald der Anruf vom vermittelnden Teilnehmer durchgestellt wird und der externe Anschluss am vermittelten Ziel läutet, hört der Anrufer einen Rufton. Die Option Wartemusik mit Rufton sollte in einer Netzanlage immer eingestellt sein, um dem Kunden eine einheitliche Umgebung zu bieten. |Wenn der Anrufer das System über einen Internet-Telefonie-Dienst-Anbieter (ITSP) erreicht, gilt diese Option nicht und der Anrufer hört Wartemusik während der Vermittlung.

Zugang und Typaktivierung über Manager E.

Das Eingabeformat für Wartemusik ist eine Wave-Datei mit PCM und 16 Bit. Unterstützte Abtastraten sind 8, 22,05, 24, 32, 40, 44,1 und 48 kHz in Mono oder Stereo. Das bevorzugte Format ist PCM, 16 Bit, 8 kHz, Mono. Es wird empfohlen, das bevorzugte Eingangsformat zu verwenden und die Länge der Wave-Dateien auf etwa 2 Minuten zu begrenzen. Die Wartemusik kann für den Tag und für die Nacht eingestellt werden. Ein Zurücksetzen ist erforderlich.

28.3.12.2 Hilfsausrüstung > PhoneMail

Parameterbeschreibung der Registerkarten:

- **PhoneMail bearbeiten**

Parameter	Beschreibung
Rückruf Zugriff auf Phonemail	Stellen Sie die **Rufnummer** und den **Namen** des Geräts ein.
Live-Aufnahmegerät	Stellen Sie die **Rufnummer** des Geräts ein.

28.3.12.3 Hilfsausrüstung > Ansagen

Parameterbeschreibung der Registerkarten:

- **Ansagen bearbeiten**

Parameter	Beschreibung
WAVE-Datei	Hier können Sie die WAVE-Datei (.wav) für eine bestimmte Ansage auswählen (siehe Konfiguration > Ansagen > Auf Gateway laden).

Parameter	Beschreibung
Zugang	Der Anschluss wird über Zugang definiert. Hier können Sie den Port (SLA analog oder EVM) auswählen, an dem dieses Gerät angeschlossen ist. **Tipp:** Analoge Ports, die als Ansageports eingerichtet sind, müssen unter **Expertenmodus** > **Telefonieserver** > **Station** > **Analoge Stationen** > **Erweiterungstyp** > **bearbeiten** den Wert „Anrufbeantworter“ erhalten, wie unter Station-Parameter beschrieben. Über externe Ziele können Ansagegeräte in einem anderen Systemknoten angesprochen werden. Dazu wird das Ansagegerät als extern gekennzeichnet. Hier wird die Anrufnummer eines Ansageports in einem anderen Systemknoten eingetragen. **Tipp:** Diese Geräteliste bezieht sich auf die Einstellung **Ansage** im **Expertenmodus** > **Telefonieserver** > **Eingehende Anrufe** > **UCD** > **UCD-Gruppenparameter bearbeiten** wie unter Eingehende Anrufe > UCD beschrieben. Wenn Sie **Externes Ziel** wählen, erscheinen die folgenden beiden Felder: • **Route** (Leitungsgruppen) • **Anrufnummer** (Gerät)

Parameter	Beschreibung
Typ	Sie können eine der folgenden Arten von Ansagen aus dem Dropdown-Menü auswählen: • **Keine**: Ansagegerät ist nicht angeschlossen. • **Ansage**: Ermöglicht den Anschluss von nur einem externen Ansagegerät über SLA-Ports oder EVM-Karten. Die von dem aktivierten Ansagegerät gelieferte Ansage muss einen festen Anfang und ein festes Ende haben. Dieses Gerät sollte den Anruf nach dem Ende der Ansage nicht weiterleiten (es sollte kein Vermittlungsziel eingegeben werden). Der entsprechende Ansagegeräte-Port wird unter **Zugang** eingetragen). Äquivalent zu **Start/Stopp** für externe Zielgeräte. • **Wartemusik**: Eine Ansage oder Musik wird kontinuierlich wiederholt. Während die Musik oder die Ansage abgespielt wird, können auch Anrufe in der Warteschlange verbunden werden. Der Anschluss ist entweder über SLA-Ports oder EVM-Karten möglich. Der entsprechende Ansagegeräte-Port wird unter **Zugang** eingetragen. Äquivalent zu **kontinuierlich** für externe Zielgeräte. • **Interne Musik**: Aktiviert die systeminterne Wartemusik im Kommunikationssystem. Für diese Option sollte der Wert **Keine** unter **Zugang** eingegeben werden. Externe Wartemusik (Konfiguration Manager E) wird gehört, wenn sie im Kommunikationssystem als Ziel definiert ist. Eingaben unter **Zugang** haben bei beiden Varianten keine Auswirkung. • **Medien-PC**: Diese Einstellung ist vordefiniert. Der Medien-PC oder die steuernde Anwendung steuert, ob der Anrufer die Ansage von Anfang an hört oder mit einer laufenden Ansage verbunden wird. • **Ansage-Player**: Der Ansage-Player ist ein internes Softwareprogramm, das zusammen mit der UC Booster-Funktionalität (UC Booster Card oder UC Booster Server) verfügbar ist. **Anmerkung:** Die Ansage-Player-Funktionalität ist nur im UC Suite-Modus verfügbar.
Modus	Sie können eine der zwei folgenden Optionen wählen: • **Start/Stopp**: Einzelwiedergabe • **kontinuierlich**: kontinuierliche Wiedergabe

Anmerkung: Der Assistent für **Wartemusik / Ansagen** kann auch zur Konfiguration von **Ansagen** verwendet werden. Weitere Informationen finden Sie unter So konfigurieren Sie Ansagen.

28.3.12.4 Hilfsausrüstung > Türöffner

Parameterbeschreibung der Registerkarten:

- **Türöffner bearbeiten**

Parameter	Beschreibung
Teilnehmer	Auswahl der Rufnummer / des Anschlussports der Türsprechstelle. Der Port-Typ der Teilnehmer muss P.O.T. oder Kein Port sein.
Ziel	Auswahl der Rufnummer / des Anschlusses des Klingelziels der Türsprechanlage. Als Klingelziel kann eine Rufnummer oder eine Gruppennummer angegeben werden, bei der beim Drücken der Türklingeltaste ein Sonderruf signalisiert wird. Die Signalisierung des Anrufs erfolgt gemäß den unter „Einstellungen - Eingehende Anrufe“ definierten Rufumleitungsalgorithmen.
Türöffner	Aktiviert die Türöffner-Funktion. Durch Setzen dieses Flags kann ein an der TFE-S angeschlossener Türöffner für die Teilnehmer aktiviert werden.
DTMF	Durch Setzen dieses Flags kann der Türöffner mit einem MFV-Sender aus der Ferne aktiviert werden.
FWD	Das Setzen dieses Flags ermöglicht die externe Weiterleitung des Rufziels der Türsprechanlage.

28.3.12.5 Hilfsausrüstung > SmartVM

Parameterbeschreibung der Registerkarten:

- **SmartVM-Mailboxen bearbeiten**

Parameter	Beschreibung
Mailbox-Rufnummer	Eingabe der Mailbox-Rufnummern. Eine Mailbox wird anhand der Mailbox-Rufnummer identifiziert. Wenn eine Mailbox einem Teilnehmer zugeordnet werden soll, ist es zwingend erforderlich, dass die Mailbox dieselbe Rufnummer hat wie der Teilnehmer.
Name	Anzeige des Mailbox-Namens. Der Name entspricht dem Namen des Teilnehmers (falls vorhanden). Bei einer Gruppe wird der Gruppenname angezeigt.
Begrüßung	Auswahl der Begrüßung. Die Nutzbarkeit der angebotenen Einträge ist abhängig vom gewählten Telefonmenü (TUI). Mit der OSO TUI wird für Standardmailboxen nur die Begrüßung 1 unterstützt.
Begrüßung: **Begrüßung 1-4**	Die Auswahl der Begrüßungen 1-4 ist abhängig vom Typ der Mailbox: Standard-Mailbox: Begrüßung 1 oder 2 (mit OSO TUI nur Begrüßung 1) Vermittlungs-Mailbox: Begrüßung 1, 2, 3 oder 4
Begrüßung: **Tag/Nacht**	Begrüßung ist abhängig vom Tag-/Nachtbetrieb: Tag - Begrüßung 1 / Nacht - Begrüßung 2
Begrüßung: **Art des Anrufs**	Nur für Standard Mailbox: Die Begrüßung hängt vom Status des Teilnehmers ab: Anruf nicht angenommen - Begrüßung 1 / Besetzt - Begrüßung 2
Begrüßung: **Keine**	Es wird keine Begrüßung abgespielt. Die Mailbox bleibt aber aktiv, z.B. für eine Weiterleitung des Anrufs zum Abwurfplatz.

Parameter	Beschreibung
Aufzeichnung	Ist dieses Flag aktiviert, ist die Mailbox eine Standard-Mailbox. Sie kann dann keine Vermittlungs-Mailbox mehr sein. Ist das Flag deaktiviert (Standard), hat die Mailbox nicht die Möglichkeit, eine Nachricht aufzusprechen. Der Teilnehmer kann beim ersten Abfragen seiner Mailbox die Aufnahme aktivieren. Dadurch ist gewährleistet, dass vor der Erstinbetriebnahme durch den Teilnehmer keine Nachrichten aufgezeichnet werden können. Standard: Aktiviert
AutoAttendant	Ist dieses Flag aktiviert, ist die Mailbox eine Vermittlungs-Mailbox (AutoAttendant). Sie kann dann keine Standard-Mailbox mehr sein. Es können maximal 100 Mailboxen als Vermittlungs-Mailboxen eingerichtet werden. Beim Wechseln einer Standard-Mailbox auf eine Vermittlungs-Mailbox werden alle Nachrichten der Mailbox gelöscht. Standard: deaktiviert
Passwort Reset	Ist dieses Flag aktiviert, wird das Passwort der Mailbox auf `123456` zurückgesetzt. Der Teilnehmer muss das Passwort beim nächsten Zugriff auf seine Mailbox ändern. Standard: deaktiviert

Parameterbeschreibung der Registerkarten:

- **SmartVM-Parameter bearbeiten**

Parameter	Beschreibung
Allgemeine Parameter	
Maximale Mailbox-Nummernlänge	Maximale Länge der Mailbox-Rufnummer. Wertebereich: 2 - 16 Stellen; Standardwert: 3 Positionen
Max. Nachrichtenlänge (Min.)	Maximale Länge der Aufnahmedauer einer Nachricht. Wertebereich: 1 oder 2 Minuten; Standardwert: 2 Minuten
Rufnummernlängenbegrenzung	Bei gehenden Verbindungen, die von der SmartVM eingeleitet werden (AutoAttendant Nachwahl und AutoAttendant Kurzwahl) können nur Rufnummern bis zur angegebenen Länge gewählt werden. Bei eingerichteten längeren Rufnummern unterbleibt der Verbindungsaufbau. Im Standard entspricht die Rufnummernlängenbegrenzung der Mailbox-Rufnummernlänge (interne Rufnummernlänge), so dass nur eine Internwahl erlaubt ist. Wertebereich: 2 bis 30, Standardwert: 3
Allgemeines Fax-Abwurfziel	Eingabe des Fax-Abwurfziels, auf das die SmartVM normalerweise ankommende Faxe schicken soll. Ist kein Fax-Abwurfziel angegeben, werden ankommende Faxe abgewiesen. Wertebereich: max. 16 Ziffern
Standardsprache	Auswahl der Sprache der Benutzerführung. Gilt für alle Mailboxen. Ist die Benutzerführung in der gewünschten Sprache nicht vorhanden, wird die Sprache auf UK-Englisch (enuk) gesetzt.
Telephone User Interface (TUI)	Auswahl der Telefonmenüstruktur der Sprachbox (Telefone User Interface, TUI). Die Auswahl gilt für alle Mailboxen.

Parameter	Beschreibung
Telephone User Interface (TUI): **SmartVM**	SmartVM TUI, EVM TUI (Standard).
Telephone User Interface (TUI): **OSO**	OSO TUI, ähnlich zur UC Suite TUI.
Reihenfolge der Datumsansage	Nur sichtbar mit SmartVM TUI: Einstellung der Ansagenreihenfolge für Nachricht, Aufnahmedatum und Rufnummer des Anrufer (falls bekannt).
Reihenfolge der Terminankündigung: **Datum nach Nachricht**	Nur sichtbar mit SmartVM TUI: Nachricht -- Aufnahmedatum -- Rufnummer des Anrufers (falls bekannt).
Reihenfolge der Terminankündigung: **Datum vor Nachricht**	Nur sichtbar mit SmartVM TUI: Aufnahmedatum -- Rufnummer des Anrufer (falls bekannt) -- Nachricht. Für Nachrichten von internen Teilnehmern gilt: Name des internen Teilnehmers (falls vorhanden) -- Aufnahmedatum -- Rufnummer des Anrufers (falls bekannt) -- Nachricht.
Anzahl der Nachrichten pro Mailbox	Maximale Anzahl der Nachrichten für eine Mailbox. Wertebereich: 0 bis 100, Standardwert: 30
EVM deaktivieren	Ist dieses Flag aktiviert, ist die SmartVM deaktiviert. Standard: deaktiviert
Rückruf von VM nur an bekannte Nummer zulassen	Wenn ein externer BenutzerA einen BenutzerB anruft, BenutzerB eine Anrufweiterleitung an seine Voicemail eingerichtet hat und der externe BenutzerA eine Sprachnachricht hinterlässt, ruft BenutzerB die SmartVM an, gibt sein Passwort ein und wählt während er sich die Nachricht anhört die „8“. Durch die Wahl dieser Ziffer erfolgt ein Rückruf an BenutzerB. Bei aktiviertem Flag erfolgt der Rückruf, wenn die Nummer von BenutzerB zu den bekannten Rufnummern gehört. Bekannte Rufnummern sind die Mobilrufnummer und die private/externe Rufnummer der Profildetails der Benutzerverwaltung (Applications-UC Smart-User Management). Standard: Aktiviert
AA-VP-Verhalten Einstellung, ob der AutoAttendant für bestimmte Fälle automatisch Ansagen abspielen soll.	
VP vor Übergabe	Ist dieses Flag aktiviert, wird im Fall "VP vor Übergabe" folgende Ansage abgespielt: „Bitte warten, Sie werden verbunden...“ Standard: deaktiviert

Parameter	Beschreibung
VP-Übergabe-Ergebnis	Ist dieses Flag aktiviert, wird im Fall "VP-Übergabe-Ergebnis" eine der folgenden Ansagen abgespielt: „Die Teilnehmernummer existiert nicht.“ „Der Teilnehmer ist besetzt.“ „Der Teilnehmer antwortet nicht.“ Standard: Aktiviert
VP-Abwurf	Ist dieses Flag aktiviert, wird im Fall "VP-Abwurf" eine der folgenden Ansagen abgespielt: „Sie werden mit dem Operator verbunden. Bitte warten Sie.“ „Sie werden mit der Mailbox des Teilnehmers verbunden.“ „Bitte warten, Sie werden verbunden...“ Standard: Aktiviert
VP vor Trennen	Ist dieses Flag aktiviert, wird im Fall "VP vor Trennen" eine der folgenden Ansagen abgespielt: „Bitte rufen Sie später an.“ „Vielen Dank. Auf Wiedersehen.“ „Die Mailboxnummer ist ungültig.“ Standard: Aktiviert

Parameterbeschreibung der Registerkarten:

- **AutoAttendant-Parameter bearbeiten**

Parameter	Beschreibung
Rufnummer	Rufnummer des AutoAttendants (Standard 352).
Abwurf nach Ansage	Ist dieses Flag aktiviert, erfolgt nach der Begrüßungsansage der Abwurf des Anrufs zum Abwurfplatz (z.B. Vermittlungsplatz). Während der Begrüßungsansage ist es nicht möglich ein Kurzwahlziel anzuwählen. Standard: deaktiviert
Keine Nachwahl	Ist dieses Flag aktiviert, kann der Anrufer nur über die Wahl der Kurzwahlziele zu anderen Zielen weitergeleitet werden. Der Anrufer kann keine mehrstellige Rufnummer wählen. Standard: deaktiviert

Parameterbeschreibung der Registerkarten:

- **Kurzwahl-/Abwurfziel bearbeiten Tag**
- **Kurzwahl-/Abwurfziel bearbeiten Nacht**
- **Kurzwahl-/Abwurfziel bearbeiten 3**
- **Kurzwahl-/Abwurfziel bearbeiten 4**

Parameter	Beschreibung
Wählen Sie	Auswahl eines internen Teilnehmers (1. Hälfte der Liste) oder einer Sprachbox (2. Hälfte der Liste) als Kurzwahlziel oder Abwurfplatz.
Maßnahme	Anzeige der 10 möglichen Kurzwahlziele und des Abwurfplatzes.
Rufnummer	Rufnummer des ausgewählten Teilnehmers oder der ausgewählten Sprachbox.
Name	Name des ausgewählten Teilnehmers oder der ausgewählten Sprachbox.
Typ	Auswahl des Typs der Rufnummer.
Typ: **Rufnummer**	Hier wird mit der zugeordneten Kurzwahlziffer der ausgewählte Teilnehmer angerufen.
Typ: **Mailbox**	Hier wird mit der zugeordneten Kurzwahlziffer die ausgewählte Sprachbox angerufen.

28.3.13 Payload

Unter **Payload** sind die Funktionen für Anzeige und Konfiguration von Anschlusstypen und Protokollen zusammengefasst.

28.3.13.1 Payload > Devices

Parameterbeschreibung der Registerkarten:

- **Globale Device-Einstellungen anzeigen**
- **Device-Einstellungen auf Lieferzustand zurücksetzen**

Parameter	Beschreibung
Globales Gateway vom Typ G.711	Devices ist der Sammelbegriff für Teilnehmer, Leistungsmerkmale und Funktionen, die Kanäle benötigen. Es werden der Codec-Typ des globalen Gateways, die maximale Anzahl verfügbarer und lizenzierter B-Kanäle, sowie die maximale Anzahl von LAN-Clients an einem Kanal für Music on Hold (überzählige Anrufe werden nicht durchgeschaltet) angezeigt.
Max. Anz. von B-Kanälen der HW	
Anz. LAN-Clients an einem MoH-Kanal	

Das Rücksetzen der Device-Einstellungen erfordert einen Restart des Kommunikationssystems.

28.3.13.2 Payload > Media Stream Control (MSC)

Parameterbeschreibung der Registerkarten:

- **MSC-Jitter-Parameter ändern**

Parameter	Beschreibung
	Die Medienstromsteuerung (MSC) überwacht und verwaltet die Medienströme, die durch das Kommunikationssystem geleitet werden. Sie sorgt für die Übermittlung von Mediendaten zwischen Netzen über Gateways (TDM/IP).
Verkehrsstatistik (nur SNMP)	Erforderlich für Zugang zu den Daten der Per-Call-Statistik des Systems über SNMP.
Intervall für Generierung von RTCP-Paketen (sec.)	Reportintervall in Sekunden für RTCP-Pakete (Real-time Transport Control Protocol). Das RealTime Control Protocol (RTCP) dient der Aushandlung und Einhaltung von Quality of Service (QoS) Parametern durch den periodischen Austausch von Steuernachrichten zwischen Sender und Empfänger. Wertebereich: 5 bis 10, Standardwert: 5

Parameterbeschreibung der Registerkarten:

- **MSC-Einstellungen auf Lieferzustand zurücksetzen**

Parameter	Beschreibung
MSC-Einstellungen auf Lieferzustand zurücksetzen	Wiederherstellen aller ursprünglichen MSC-Einstellungen.

28.3.13.3 Payload > HW-Module

Verwaltung der DSP-Module des Kommunikationssystems

Parameterbeschreibung der Registerkarten:

- **Alle HW-Module anzeigen**
- **DSP-Einstellungen ändern**
- **DSP Jitter-Einstellungen ändern**

Parameter	Beschreibung
HW-Typ	Anzeige der im Kommunikationssystem verwendeten DSPs (Digital Signal Processor). Möglich sind: • **Onboard** = Integrierter DSP des Mainboards • **OCCB X-1** = DSP eines OCCB-Submoduls (OCCB1 oder OCCB3)
Firmware-Version	Aktuelle Firmware-Version jedes einzelnen DSPs
API-Version	Aktuelle API (Application Programming Interface)-Version jedes einzelnen DSPs
Allgemeines	
IP-Adresse	IP-Adresse des DSP-Moduls (kann geändert werden, falls die IP-Adresse bereits vergeben ist). ***Hinweis:*** Das letzte Oktett der IP-Adresse kann nicht .1 sein (xxx.xxx.xxx.1)
Port	Portnummer des DSP-Moduls
Statusanzeige	Dient zur Erkennung der Verfügbarkeit der DSPs Standardwert: Statusmeldungen

Parameter	Beschreibung
Echokompensationsglied	Bei aktiviertem Flag wird die Audio-Rückkopplung (Echo-Effekt) bei Sprachübertragungen unterdrückt. Standardwert: Aktiviert
MFV-Außerband-Signalisierung	Bei aktiviertem Flag werden MFV-Signale im separaten Signalisierungskanal (Outband) übertragen. Standardwert: Deaktiviert
Fax-Parameter	
Anzahl redundanter Pakete	Definition der Anzahl der Redundanz-Pakete: Je größer dieser Wert ist, desto robuster ist die Faxübertragung gegenüber Paketverlusten. Nachteil bei größeren Werten ist der Anstieg der benötigten Bandbreite. Standardwert: 2
Maximaler Netzwerk-Jitter (hex ms)	Definition des maximalen Netzwerk-Jitters in Millisekunden: Je größer der Wert ist, desto größer ist die mögliche Laufzeit-Varianz von Datenpaketen in Netzwerken. Erlaubt sind ausschließlich hexadezimale Werte, bestehend aus den Ziffern 0 bis 9 und A bis F. An diesem Parameter sollten möglichst keine Änderungen vorgenommen werden. Standardwert: 00C8
Timeout für Fax/Modem-Ton-Erkennung (s)	Definition der Zeit in Sekunden für die Erkennung von Faxtönen während einer Verbindung: Hierdurch ist eine Umschaltung auf das Faxprotokoll T.38 gewährleistet. Nach Ablauf der hier eingestellten Zeit werden keine Faxtöne mehr erkannt. Der Wert 0 bedeutet, dass die Tonerkennung für die gesamte Dauer der Verbindung aktiviert ist. Standardwert: 0
DSP Jitter	
Jitter-Buffer-Typ	Definition des Jitter-Buffer-Typs Standardwert: Adaptiv
Jitter-Buffer-Typ: **statisch**	Die Durchschnittsverzögerung des Jitter-Buffers bleibt stets gleich.
Jitter-Buffer-Typ: **Adaptiv**	Der Jitter-Buffer passt die Durchschnittsverzögerung an die Situation beim Datenempfang an. Dabei wird versucht, die Verzögerung so gering wie möglich zu halten und zugleich so wenige Datenpakete wie möglich zu verlieren.
Durchschnittl. Verzögerung für Sprache (ms)	Definition der Zeit in Millisekunden, die ein Paket bei IP-basierten Sprachübertragungen durchschnittlich im Jitter-Buffer gehalten werden soll. ***INFO:*** Beim **Jitter-Buffer-Typ Adaptiv** stellt der hier definierte Wert lediglich einen Anfangswert dar. Standardwert: 40

Parameter	Beschreibung
Max. Verzögerung für Sprache (ms)	Definition der maximalen Zeit in Millisekunden für die Verzögerung für Sprache **Jitter-Buffer-Typ Statisch:** Anzugeben ist, wie viele Millisekunden eine tatsächlich gemessene Verzögerung beim Eintreffen von IP-Paketen bei Sprachübertragung betragen darf, bevor der Jitter-Buffer regulierend in den Datenstrom eingreift. Bei statischem Jitter-Buffer ist 80 ein für die meisten Umgebungen empfehlenswerter Wert. **Jitter Buffer-Typ Adaptiv**: Anzugeben ist, wie viele Millisekunden die Durchschnittsverzögerung für Sprache maximal betragen darf. Ist die tatsächlich gemessene Verzögerung größer, gehen ausgehende Pakete verloren. Bei adaptivem Jitter-Buffer ist 120 ein für die meisten Umgebungen empfehlenswerter Wert. ***Hinweis:*** Der Wert muss in jedem Fall größer sein als der im Feld „Durchschnittliche Verzögerung für Sprache (ms)“ eingetragene Wert. Standardwert: 120
Min. Verzögerung für Sprache (ms)	Definition der minimalen Zeit in Millisekunden für die Verzögerung für Sprache **Jitter Buffer-Typ Adaptiv**: Anzugeben ist, wie viele Millisekunden die Durchschnittsverzögerung für Sprache minimal betragen darf. Die Durchschnittsverzögerung wird in jedem Fall größer oder gleich sein als dieser Wert. Standardwert: 20
Paket-Verlust / Verzögerungpräferenz	Definiert wird das Verhältnis Paketverlust zu Laufzeitverzögerungen von Datenpaketen **Jitter Buffer-Typ Adaptiv**: Anzugeben ist ein Wert zwischen 0 und 8. Der Wert ist abhängig davon, ob im Fall von großen Laufzeitverzögerungen eher der Verlust von Paketen in Kauf genommen werden kann oder eher eine noch größere Verzögerung. Der Wert 0 bedeutet minimalen Paketverlust mit dem Nachteil von Laufzeitverzögerungen. Der Wert 8 bedeutet minimale Laufzeitverzögerung mit dem Nachteil von möglichen Paketverlusten. Ein für die meisten Umgebungen empfehlenswerter Wert ist 4. Standardwert: 4
Durchschnittl. Verzögerung für Daten (ms)	Definition der durchschnittlichen Verzögerung für Daten in Millisekunden Anzugeben ist, wie viele Millisekunden ein Datenpaket bei Datenübertragungen durchschnittlich im Jitter-Buffer gehalten werden soll. Ein für die meisten Umgebungen empfehlenswerter Wert ist 60. Standardwert: 60

Parameter	Beschreibung
Max. Verzögerung für Daten (ms)	Definition der maximalen Verzögerung für Daten in Millisekunden Anzugeben ist, wie viele Millisekunden eine tatsächlich gemessene Verzögerung beim Eintreffen von IP-Paketen betragen darf, bevor der Jitter-Buffer regulierend eingreift. Ein für die meisten Umgebungen empfehlenswerter Wert ist 200. ***INFO:*** Größere Werte (ab ca. 2000) haben keinen Einfluss. Sobald ein Paket im Puffer komplett empfangen wurde, verlässt dieses Paket den Puffer auch wieder. Werte unter 100 ms sind zwar möglich, aber in der Praxis auf keinen Fall zu empfehlen. Standardwert: 200

28.3.14 Statistiken

Unter **Statistiken** sind die Funktionen für die Anzeige von Statistiken zusammengefasst.

28.3.14.1 Statistik > Gateway-Statistik > Mainboard > Device-Statistik

Parameterbeschreibung der Registerkarten:

- **SCN-Statistik anzeigen**
- **LAN-Statistik anzeigen**

Parameter	Beschreibung
Device-Typ	Zeigt die vorhandenen LAN- und SCN-Komponenten (SCN, Switched Circuit Network) an.
Aktuell belegte Ressourcen	Zeigt die aktuell belegten Ressourcen einer Komponente (konfigurierte und verwendete Channels) an.
Summe	Zeigt die Summe der aktuell belegten Ressourcen an.
Autom. Aktualisierung	Die Anzeige wird alle 60 Sekunden automatisch aktualisiert.
Sekunden bis zur nächsten Aktualisierung	Zeigt einen rückläufigen Timer an, beginnend bei 60 Sekunden.
DSS1-Teilnehmer	Sobald ein Mobiltelefon sich im Bereich einer anderen Funkvermittlungsstelle aufhält („Aufenthalts-Cordless-Baugruppe“), wird mittels einer von der Cordless-Baugruppe initiierten DSS1-Verbindung eine Verlängerungsverbindung geschaltet. Der DSS1-Teilnehmer bezieht sich also auf die im Switch eingerichtete Anzahl von Mobiltelefonen oder DSS1-Verbindungen.
HFA / IP-Networking-Sprache	Diese SCN-Komponente zeigt die Anzahl der DSP-Channels an, die besetzt sind, wenn Gateway-Anrufe eingerichtet werden.

Parameter	Beschreibung
Wartemusik	Bei einer IP-Vernetzung mit aktiviertem Leistungsmerkmal DMC Interworking werden Gateway-Verbindungen über sogenannte DMC-Channels realisiert. Aus Anwendersicht handelt es sich beim DMC-Channel um einen Gateway-Channel, der eine Gateway-Verbindung bereitstellt.
SIU	Die Signalling Unit (SIU) reserviert einen DSP-Channel, der zum Erkennen oder Erzeugen von Systemtönen (z.B. DTMF-Töne) verwendet wird.
DMC	Zeigt einen rückläufigen Timer an, beginnend bei 60 Sekunden.
H.323 (RTP)	Zeigt im Falle eines Sprachanrufs die verwendeten Ressourcen an.
T.38-Fax	Zeigt im Falle einer Fax-Verbindung die verwendeten Ressourcen an.
PPP	Zeigt im Falle eines Anlagenanschlusses die verwendeten Ressourcen an.

28.3.14.2 Statistiken > Gateway-Statistiken > Mainboard > MSC-Statistiken

Parameterbeschreibung der Registerkarten:

- **Gesamt-Statistik anzeigen**

  MSC-Statistiken sind Statistiken des Medienstroms, der über digitale Signalprozessoren zwischen IP und TDM umgesetzt wird (Media Stream Control). Die MSC-Gesamt-Statistik bietet einen Überblick über die statistischen Daten für alle registrierten Gespräche. Sie gibt Aufschluss über gesendete und nicht gesendete RTP/TCP-Pakete, über empfangene und nicht empfangene Pakete und über die Anzahl gesendeter und empfangener Bytes.

Parameterbeschreibung der Registerkarten:

- **Einzelruf-Statistik anzeigen**

  Die MSC-Einzelruf-Statistik listet tabellarisch für jede Verbindung mit Umsetzung über digitale Signalprozessoren die Verbindungsdaten und verwendete Parameter auf. Sie dient Experten zur Fehleranalyse.

28.3.14.3 Statistiken > SNMP-Statistiken

Parameterbeschreibung der Registerkarten:

- **Statistik-Tabelle anzeigen**
- **Statistik anzeigen**

Parameter	Beschreibung
if-Tabellen-Statistik	In SNMP erfasste Details zu einzelnen Schnittstellen (if = Interface) im Kommunikationssystem, wie zum Beispiel Ethernet-Schnittstellen.
IP-Statistik	Details und Fehler zum IP-Routing
TCP-Statistik	Details und Fehler zum TCP-Protokoll
UDP-Statistik	Details und Fehler zum UDP-Protokoll

28.3.14.4 Statistiken > Telephonie Statistiken > System Texte

Parameterbeschreibung der Registerkarten:

- **Systemtexte anzeigen**

Parameter	Beschreibung
Verfügbare Sprachen	Anzeige der im Kommunikationssystem verfügbaren Sprachen für die Telefon-Displays

28.3.14.5 Statistiken > Telephonie Statistiken > UCD Agenten

Parameterbeschreibung der Registerkarten:

- **UCD Agenten anzeigen**

Parameter	Beschreibung
Anzahl UCD Agenten	
Summe	Gesamtzahl der im Kommunikationssystem angemeldeten UCD-Agenten
Verfügbar	Anzahl der verfügbaren UCD-Agenten
UCD Agenten Status	
Rufnummer	Rufnummer des UCD-Agenten
Name	Name des UCD-Agenten
ID	ID des UCD-Agenten
UCD-Gruppe	UCD-Gruppe, der der UCD-Agent zugeordnet ist.
Status	Status des UCD-Agenten

28.3.14.6 Statistiken > Telephonie Statistiken > TZustand Leitung

Parameterbeschreibung der Registerkarten:

- **Leitungsstatus anzeigen**

Parameter	Beschreibung
Datum	Datum der Statusabfrage bzw. der letzten Statusänderung der Leitung
Uhrzeit	Uhrzeit der Statusabfrage bzw. der letzten Statusänderung der Leitung
Slot/Port	Anzeige der Baugruppe, des Einbauplatzes (Slot) und der Schnittstelle (Port) bzw. der LAN-Schnittstelle
Richtung	Zeigt den Routennamen an, um einen besseren Hinweis darauf zu erhalten, zu welchem ITSP eine Leitung gehört.
Trunk Number	Leitungskennzahl

Parameter	Beschreibung
Kommentar	Status der Leitung (Angezeigt wird der letzte Zustand der Leitung.) Möglich sind folgende Leitungszustände: • **Idle** (Leitung im Ruhezustand) • **Alerting** (Ruf steht an) • **Connected to:** (Verbindung zur angezeigten Rufnummer) • **Leitung gesperrt** • **Leitung ausgefallen**

28.3.14.7 Statistiken > Telephonie Statistiken > Weiterleitung

Parameterbeschreibung der Registerkarten:

- **Weiterleitungen anzeigen**

Parameter	Beschreibung
Anrufumleitung	
Status	Status der Anrufumleitung: • **Aus** (keine Anrufumleitung aktiv) • Bei aktiver Anrufumleitung werden Art der Anrufumleitung und Umleitungsziel angezeigt.
Umleitungsziel von	Anzeige, ob der Teilnehmer das Umleitungsziel der Anrufumleitung eines anderen Teilnehmers ist. Angezeigt werden Rufnummer und Name des umleitenden Teilnehmers.
Rufzuschaltung	
Zugeschaltete Teilnehmer	Rufnummer und Name von zugeschalteten Teilnehmern
Zuschaltung von	Anzeige, ob der Teilnehmer das Rufzuschaltungsziel eines anderen Teilnehmers ist. Angezeigt werden Rufnummer und Name des rufzuschaltenden Teilnehmers.

28.3.14.8 Statistiken > Telephonie Statistiken > Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer Parameter anzeigen**
- **Aktivierte Merkmale anzeigen**

Parameter	Beschreibung
Rufnummer	Rufnummer
Name	Name des Teilnehmers
Durchwahl	Durchwahlnummer des Teilnehmers
Gerätetyp	Typ des Telefons, wie zum Beispiel OpenStage 60

Parameter	Beschreibung
Clip/Lin	Location Identification Number LIN Nur für USA, Kanada: Durch den erweiterten Notrufdienst E911 werden neben der Rufnummer auch Informationen über den geographischen Standort des Anrufers beim Absetzen eines Notrufs übermittelt. Dazu wird jedem Teilnehmeranschluss mit gültiger Durchwahlnummer eine LIN zugeordnet.
Zugang	Bei analogen und $U_{P0/E}$-Telefonen Anzeige der Baugruppe, des Einbauplatzes und der Nummer des Anschlusses. Zusätzliche Anzeige bei $U_{P0/E}$-Telefonen, ob Master oder Slave. Bei IP-Telefonen Anzeige der LAN-Schnittstelle, des Typs und der Nummer
Parameter	
Stationstyp	Stationstyp, wie zum Beispiel Standard oder Fax Standardwert: Standard
Sprache	Spracheinstellung des Telefons
Rufsignalisierung intern	Rufart für die Signalisierung interner Anrufe Standardwert: Rufart 1
Rufsignalisierung extern	Rufart für die Signalisierung externer Anrufe Standardwert: Rufart 1
Berechtigung (LCR)	Berechtigungsklasse des Teilnehmers für Least Cost Routing Standardwert: 15
Lizenz Typ	Lizenztyp des Teilnehmers
Leistungsmerkmale	
Anrufschutz	Status des Leistungsmerkmals Anrufschutz Standardwert: Aus
Antworttext	Status des Leistungsmerkmals Antworttext Standardwert: Aus
Codeschloss	Status des Leistungsmerkmals Codeschloss Standardwert: Aus
Rufnummerunterdrückung ein	Status des Leistungsmerkmals Rufnummerunterdrückung Standardwert: Aus
Rufzuschaltung	Status des Leistungsmerkmals Rufzuschaltung Standardwert: Aus
Ruhe schalten	Status des Leistungsmerkmals Stiller Ruf/Ruhe Standardwert: Aus
Sammelanschluss/Gruppe	Status des Leistungsmerkmals Sammelanschluss/Gruppenruf Standardwert: Aus

Parameter	Beschreibung
Stilles Anklopfen	Status des Leistungsmerkmals Stilles Anklopfen Standardwert: Aus
Direktantworten	Status des Leistungsmerkmals Direktantworten Standardwert: Aus
Freigeben zum Anklopfen	Status des Leistungsmerkmals Freigeben zum Anklopfen Standardwert: Aus
Anrufumleitung nach Zeit	Status des Leistungsmerkmals Umleitung nach Zeit Standardwert: Aus
AUL	Status des Leistungsmerkmals Anrufumleitung (AUL) Standardwert: Aus

28.4 Applikationen

Unter **Applikationen** sind Funktionen für die Konfiguration des Application Servers für Unified Communications un der Web Services zusammengefasst.

28.4.1 Applikationsauswahl

Unter **Applikationsauswahl** sind Funktionen für die Auswahl der verwendeten Lösung für Unified Communications zusammengefasst.

28.4.1.1 Applikationsauswahl

Parameterbeschreibung der Registerkarten:

- **Applikationsauswahl**

Parameter	Beschreibung
Applikationspakete auswählen	Auswahl der Applikationspakete mit UC Smart oder mit UC Suite. Bei dem Applikationspaket mit UC Suite auf dem OpenScape Business UC Booster Server wird zusätzlich die IP-Adresse des UC Booster Servers (IP-Adresse des Linux-Servers) benötigt.
Applikationsauswahl	Anzeige der unterstützten Komponenten je nach ausgewähltem Applikationspaket inkl. der IP-Adresse des verwendeten Servers.

28.4.2 Active Directory Integration Service

Die relevanten Funktionen für die Integration von Active Directory sind unter **Active Directory Integration Service** gruppiert.

28.4.2.1 Active Directory Integration Service

Parameterbeschreibung der Registerkarten:

- **Active Directory Integration Service**

Parameter	Beschreibung
Synchronisierungstyp	Dieser Synchronisierungstyp kann die folgenden Werte haben: • **Frei** Es erfolgt keine Synchronisierung des Teilnehmers mit dem Active Directory Service. • **Durchwahl** Automatische Synchronisierung des Teilnehmers mit Active Directory. Die Durchwahlnummer wird als Synchronisierungsschlüssel verwendet. • **erzwungen** Manuelle Synchronisierung des Teilnehmers mit einem Active Directory Teilnehmer. Bei erzwungener Synchronisierung ist es möglich, einen Active Directory-Benutzer mit mehreren OpenScape Business Teilnehmern zu synchronisieren. • **mulap_member** Der automatisch synchronisierte Benutzer ist ein Mitglied einer MULAP Gruppe.
Suche	Die leeren Felder oben auf dem Bildschirm können für das Suchen nach einem bestimmten Benutzer verwendet werden, wenn die Zahl der Benutzer so groß ist, dass sie nicht auf einen Bildschirm passen. In den Feldern **Vorname**, **Nachname**, **Anzeigename** und **DID**, wird eine Suche „beginnt mit“ durchgeführt. Im Feld **Active Directory-Benutzer** wird eine Suche „enthält“ durchgeführt. Die Suche beginnt nach Drücken der Schaltfläche **Suchen**.
Ändern	Sie können diese Schaltfläche verwenden, um die Synchronisierung des angegebenen Benutzers zu konfigurieren. Die verfügbaren Aktionen bei Auswahl von **Ändern** bestehen aus den folgenden Schaltflächen, die angezeigt werden.
Daten speichern	Sie können einen spezifischen AD-Benutzer auswählen und die Synchronisierung mit dem spezifischen OpenScape Business Teilnehmer erzwingen. Sie können auf diese Weise unterschiedliche Durchwahlnummern mit demselben AD-Benutzer synchronisieren.
Reset	Versuchen Sie, den OpenScape Business Teilnehmer mit irgendeinem Active Directory-Benutzer zu synchronisieren. Diese Aktion kann zum Beispiel verwendet werden, wenn die Benutzersynchronisierung gestoppt wird.
Nicht synchronisieren	Stoppen Sie die Synchronisierung des angegebenen OpenScape Business Teilnehmers. Bereits synchronisierte Daten für den Benutzer werden nicht entfernt, aber die weitere Synchronisierung mit AD wird abgebrochen.

28.4.3 UC Smart

Unter **UC Smart** sind Funktionen von Unified Communications zusammengefasst.

28.4.3.1 UC Smart > Grundeinstellungen

Parameterbeschreibung der Registerkarten:

- **Grundeinstellungen**

Parameter	Beschreibung
UC Smart Aktivieren/Deaktivieren	
Aktiv	UC Smart und UC Suite können nicht gleichzeitig aktiv sein. (Nach Aktivieren werden weitere Parameter angezeigt)
CloudService aktivieren / deaktivieren	
Aktiv	Dieses Flag steuert den Status der CloudService-Funktionalität. Beachten Sie, dass die Aktivierung der CloudService-Funktion einen Neustart der WebServices verursacht.
Zugangseinstellungen	
HTTP	UC Smart Clients können grundsätzlich über HTTPS verschlüsselt (empfohlen) oder HTTP unverschlüsselt (nicht empfohlen) auf das System zugreifen. Die Auswahl wird in der Applikation selbst getroffen. Hier wird die Berechtigung für eines oder beide Protokolle erteilt.
HTTPS	
Passwort-Policy	
Benutzer muss sicheres Passwort eingeben	Kennwort-Richtlinie für UC Smart Clients. Das standardmäßige Kennwort muss bei der ersten Anmeldung geändert werden und dabei der hier gewählten Richtlinie entsprechen (siehe Ausrufezeichen-Schaltfläche). Das Kennwort wird im Client gespeichert, ansonsten wird es bei jedem beim Start des Clients abgefragt.
Anmeldedaten im Endgerät speichern	Die Anmeldedaten werden zusätzlich im Telefon gespeichert.
Systemweites initiales UC Smart Passwort	Ein systemweites initiales Passwort wirkt sich auf alle konfigurierten UC Smart User aus, die sich noch nie in UC Smart eingeloggt haben bzw. die noch nicht ihr initiales Passwort geändert haben. Jeder betroffene User muss anschließend ein individuelles Passwort vergeben. ***INFO***: Die Vergabe eines systemweiten initialen UC Smart Passwortes stellt ein Sicherheitsrisiko dar, insbesondere wenn einzelne User nicht zeitnah ein persönliches Passwort vergeben. Alternativ empfiehlt sich die Vergabe individueller initialer Passwörter für jeden User.
Bürozeiten	
Startzeit	Sie können die Bürozeiten konfigurieren, indem Sie zwei Werte aus den Aufklapplisten Startzeit und Endezeit auswählen. Die üblichen Bürozeiten liegen zwischen 08:00 Uhr und 20:00 Uhr.
Endezeit	
Anwesenheit	

Parameter	Beschreibung
Status "Krank" ausblenden	Sie können die Option für den Anwesenheitsstatus "Krank" für UC Client-Benutzer ausblenden.

28.4.3.2 UC Smart > Benutzerverwaltung

Parameterbeschreibung der Registerkarten:

- **Benutzerverwaltung**

Parameter	Beschreibung
Benutzer	Liste aller vorhandenen Teilnehmer, der ausgewählte Teilnehmer muss eine UC User-Lizenz erhalten
Einstellungen	
Benutzer	Anzeige der internen Telefonnummer des Benutzers.
Name	Anzeige des Namens des Benutzers.
Kennwort	Kennwort des Benutzers des UC Smart Clients kann hier festgelegt werden.
Sprache	Sprache von UC Smart Assistant
Anwender muss neues Passwort vergeben	(nur Anzeige)
Zugriff auf UC Smart Assistant	Berechtigung für Zugriff auf UC Smart Assistant durch den Benutzer
Konfiguriert als Mobility-Teilnehmer	(nur Anzeige)
Voicemail-Lizenz	(nur Anzeige)
Assoziierte Dienste	(nur Anzeige)
Profildetails	
Mobile Rufnummer	Mobile Rufnummer des Teilnehmers im kanonischen Format (z.B. `+ 49 173 1234567`).
Private/Externe Rufnummer	Zusätzliche Rufnummer des Teilnehmers im kanonischen Format (z.B. `+ 49 89 987654321`).
Email-Adresse	E-Mail-Adresse des Teilnehmers.
Voicemail an E-Mail	Aktivierung/Deaktivierung der Email-Benachrichtigung beim Eingang einer neuen Sprachnachricht.
Sichtbarkeit des Anwesenheitsstatus	Einstellung, ob der Anwesenheitsstatus für interne und externe Teilnehmer sichtbar sein soll oder nur für interne Teilnehmer oder ob er überhaupt nicht sichtbar sein soll.
Lizenzierungsinformationen	Anzeige der im System vorhandenen Lizenzen für die jeweilige Applikation

28.4.3.3 UC Smart > -Status

Parameterbeschreibung der Registerkarten:

- **Status**

Parameter	Beschreibung
Applikationsserver	Anzeige des Status des integrierten UC Smart Applikationsservers.
Aktive Verbindungen	Anzeige der Anzahl der aktiven Verbindungen pro UC Smart Client.

28.4.4 OpenScape Business, UC Suite

Unter **OpenScape Business UC Suite** sind Funktionen von Unified Communications zusammengefasst, wie z.B. Konferenzschaltung, Abteilungen und Gruppen, Konfiguration des externen Verzeichnisses, Urlaubs- und Zeitpläne, das Contact Center und die Server-Einstellungen für UC Suite.

28.4.4.1 OpenScape Business, UC Suite

Parameter	Beschreibung
OpenScape Business UC Suite	Konfiguration von UC Suite, inkl. der Clients myPortal, myAgent, myAttendant und myReports, Sprach- und Faxnachrichten sowie Konferenzen.

28.4.4.2 OpenScape Business, UC Suite > Benutzerverzeichnis

Wenn Sie Ihren Vor- und Nachnamen ändern möchten, müssen Sie dies von Ihrem Administrator durchführen lassen. Andernfalls bleiben die Änderungen nach einer Synchronisation nicht erhalten. Synchronisierungen erfolgen beim Neustart des Systems oder bei Änderungen an Einstellungen durch den Administrator.

Ein Teilnehmer, der Mitglied einer MULAP-Gruppe ist, wird nicht im Benutzerverzeichnis angezeigt. Ein Teilnehmer, der Mitglied eines Sammelanschlusses ist, wird im Benutzerverzeichnis angezeigt.

Parameter	Beschreibung
Suche	Suchen Sie nach einem UC Suite-Benutzer.

Parameter	Beschreibung
Symbol für Anwesenheitsstatus	Der Administrator kann den Anwesenheitsstatus für jeden Benutzer ändern und dessen Rückgabedatum und -uhrzeit im Tag-Monat-Jahr-Format (TT/MM/JJ) bzw. im 24-Stunden-Format (HH: MM) festlegen. Eine graue Figur ist momentan nicht an UC Suite angemeldet. **Anmerkung:** Jedes Mitglied eines Sammelanschlusses wird als Nutzer des Systemverzeichnisses angesehen und wird ausgegraut dargestellt.
Bearbeiten	Einstellungen des ausgewählten UC Suite Benutzers bearbeiten **Anmerkung:** Aufgrund eines bekannten Kompatibilitätsproblems mit einem Browser kann das Layout des Fensters **Benutzer bearbeiten** bei Verwendung von Firefox variieren. Das Layout passt zu IE/Chrome/Edge.
Benutzer zurücksetzen	Die Einstellungen eines Benutzers werden auf Standardwerte zurückgesetzt. Dabei werden seine Sprachnachrichten, persönliche Ansagen der Sprachbox, Journaleinträge, geplante Konferenzen, E-Mails und Faxnachrichten gelöscht. **Anmerkung:** In diesem Fall ist das Standardpasswort auf 4 Zeichen (1234) festgelegt.
Benutzer entsperren	Gesperrte Benutzer (z.B. nach mehrfach falscher Passworteingabe) können hier entsperrt werden, Anzeige Schloss-Symbol. Der Administrator kann vom System via Email über die Sperrung informiert werden.
Persönliche Daten	Persönliche Daten des Benutzers
Persönliche Daten: **Eigene persönliche Daten**	Anmeldename, Passwort, Nachname, Durchwahl, Vorname, VoiceMail-Nummer, Faxnummer, Assistentennummer, E-Mail, Abteilung, Handynummer, externe Nummer 1/2, Privatnummer (im kanonischen Format, z. B. +49 89 700798765). Das Kennwort gilt für UC Suite Clients.
Persönliche Daten: **Eigenes Bild**	Wird automatisch skaliert Unterstützte Dateiformate: BMP, JPG/JPEG/JFIFI, PNG. Max. Dateigröße: 10 MB
Persönliche Daten: **Benutzerebene**	Nur vom Administrator für Contact Center einstellbar: Wenn der Agent dauerverfügbar sein soll, aktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat. Bei der Konfiguration eines Teilnehmers als Agent werden die Rechte des Agenten durch Auswahl des Berechtigungslevels (Agent, Supervisor oder Administrator) aus der Aufklappliste **Level** definiert. Ein Agent mit dem Berechtigungs-Level Supervisor oder ein Administrator verfügt über erweiterte Berechtigungen.

Parameter	Beschreibung
Meine Einstellungen	Benutzerspezifische Einstellungen des Clients.
Meine Einstellungen: **Darstellung**	Skin-Farben der Benutzeroberfläche; Sprache der Benutzeroberfläche; Verwendung oder Nichtverwendung der klassischen Ansicht für Pop-up-Fenster.
Meine Einstellungen: **Benachrichtigungen**	Einstellungen für Pop-up-Fenster.
Meine Einstellungen: **Anwesenheit**	Einstellungen für den Anwesenheitsstatus.
Meine Einstellungen: **Outlook-Anbindung**	Kalendertermine generieren: Übernahme des Anwesenheitsstatus in den Outlook-Kalender Kalenderintegration: Steuerung des Anwesenheitsstatus durch Outlook-/iCal-Termine (erstes Schlüsselwort in der Betreffzeile steuert Anwesenheitsstatus)
Meine Einstellungen: **Abkürzungstasten**	Definition von Tastenkombinationen für Anruffunktionen
Meine Einstellungen: **Verschiedenes**	Automatisches Zurücksetzen des Anwesenheitsstatus nach Terminende, Aufzeichnung von Client-Logs aktivieren, Festlegung der Übergabe-Methode, Aufbewahrungsdauer für Journaleinträge (Maximalwert: 30 Tage), Programmierung von Funktionstasten des Telefons, Aktivierung von Live Search und Einbeziehen von LDAP-Kontakten in die Live Search der Verzeichnisse, Festlegen einer Antwortnachricht.
Anrufregeln	Regeln für kommende Rufe
Anrufregeln: **Weiterleitungsziele**	Festlegung der Weiterleitungsziele für jeden Anwesenheitsstatus (statusbezogene Anrufumleitung)
Anrufregeln: **Regelmodul**	Festlegung komplexer Anrufregeln in Abhängigkeit vom Anwesenheitsstatus (regelbasierte Anrufumleitung)
Kommunikation	Behandlung der benutzerspezifischen Nachrichten
Kommunikation: **Einstellungen für Sprachnachrichten**	Aufzeichnung von Sprachnachrichten im jeweiligen Anwesenheitsstatus ist möglich; Einstellung der Voicemail-Sprache Standardwert: Deaktiviert
Kommunikation: **Sprachnachricht-Benachrichtigung**	Benachrichtigungsservice für neue Voicemail - siehe Informationen zur E-Mail Adresse unter „Eigene persönlichen Daten“. Voraussetzung: Der Mailserver und die eigene E-Mail-Adresse sind unter Service Center > E-Mail-Weiterleitung konfiguriert. „Gehend“ erzeugt einen Benutzeranruf an die angegebene Telefonnummer (im kanonischen Format). Die SMS-Rufnummer finden Sie unter Meine persönlichen Daten. Informationen zu SMS-Vorlagen finden Sie im Abschnitt in Vorlagen.

Parameter	Beschreibung
Kommunikation: **Fax-Benachrichtigung**	Benachrichtigungsservice für neue Faxnachrichten – siehe Informationen zur E-Mail Adresse unter „Eigene persönlichen Daten“. Voraussetzung: Der Mailserver und die eigene E-Mail-Adresse sind unter Service Center > E-Mail-Weiterleitung konfiguriert. „Gehend“ erzeugt einen Benutzeranruf an die angegebene Telefonnummer (im kanonischen Format), entweder nur innerhalb der Geschäftszeiten oder 24 Stunden am Tag. Die SMS-Rufnummer finden Sie unter Meine persönlichen Daten. Informationen zu SMS-Vorlagen finden Sie im Abschnitt in Vorlagen.
Kommunikation: **Benachrichtigungen über entgangene Anrufe**	Benachrichtigungsservice für neue entgangene Anrufe – siehe Informationen zur E-Mail Adresse unter „Eigene persönlichen Daten“. Voraussetzung: Der Mailserver und die eigene E-Mail-Adresse sind unter Service Center > E-Mail-Weiterleitung konfiguriert.
Profile	Profil für persönlichen AutoAttendant
Besetzt, Nicht angenommen, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zu Hause	Ein Anrufer kann durch Nachwahl einer Ziffer von 0 bis 9 auf ein Weiterleitungsziel geführt werden oder eine Nachricht aufsprechen. Voraussetzung ist eine Ansage je Anwesenheitsstatus.
Profile: Dynamische Ansage überspringen	Die automatische Ansage des Anwesenheitsstatus wird übersprungen, statt dessen hört ein Anrufer nur die Ansage des Namens und dann des persönlichen AutoAttendant
Sensibilität	Einstellungen zur Wahrung der Vertraulichkeit
Sensibilität: Sicherheit und Zugriff	Freigabe der Sprachnachrichten für myAttendant; Abfrage der Sprachbox vom eigenen Telefon ohne Kennwort; andere Benutzer können sehen, mit wem Sie sprechen und Ihr BLF-Layout kopieren.
Sensibilität: Sichtbarkeit des Anwesenheitsstatus	Festlegung der Sichtbarkeit des eigenen Anwesenheitsstatus für die internen Benutzer
Sensibilität: **VoiceMail-Anwesenheitsstatus**	Ansage Ihres Anwesenheitsstatus für externe Anrufer. Eingabe von zu sperrenden internen Telefonnummern, es können Wildcards verwendet werden.
myAttendant	Anzeige nur bei Teilnehmern, die für myAttendant lizensiert sind
myAttendant: LAN-Nachrichten	Textbausteine für Sofortnachrichten von myAttendant, freie Eingabe, Auswahl im Chat Fenster des Clients
myAttendant: DuWas	Eingabe von Durchwahlnummern; falls myAttendant für mehrere Firmen verwendet werden soll, kann ein "Für"-Fenster eingeblendet werden
myAttendant: Kommunikation	Eingabe einer internen Nummer für Anrufweiterleitungen im Notfall oder bei Nichtannahme (Anrufweiterleitung bei Nichtannahme) durch myAttendant (für USA)

28.4.4.3 OpenScape Business, UC Suite > Abteilungen

Parameterbeschreibung der Registerkarten:

- **Abteilungen**

Parameter	Beschreibung
Name der Abteilung	Abteilungen gruppieren Teilnehmer im internen Verzeichnis nach ihrer organisatorischen Zugehörigkeit. Damit kann z.B. in myAttendant eine automatische Zuordnung der Benutzer zu den Abteilungen erfolgen.
Gruppennummer	(interne Nummerierung ohne weitere Bedeutung)
Hinzufügen	Fügen Sie eine neue Abteilung hinzu.
Bearbeiten	Bearbeiten Sie eine ausgewählte Abteilung.
Entfernen	Entfernen Sie die ausgewählten Abteilungen.

28.4.4.4 OpenScape Business, UC Suite > Gruppen

Durch eine Sprachbox-Gruppe (Anrufbeantworter-Gruppe) kann einer bestimmten Gruppe von Teilnehmern der Zugriff auf Sprachnachrichten ermöglicht werden. Über die Rufnummer der Voicemail-Gruppe werden nicht die Mitglieder dieser Gruppe gerufen, sondern wird direkt die Voicemail (die Sprachbox) der Gruppe erreicht.

Durch eine Fax-Gruppe (Faxbox-Gruppe) kann einer Teilnehmergruppe der Zugriff auf Faxnachrichten ermöglicht werden. Über die Rufnummer der Fax-Gruppe wird direkt die Faxbox der Gruppe erreicht.

Mit den Favoritengruppen können Sie Gruppen mit Kontakten erstellen und sie den Benutzern zuweisen.

Parameterbeschreibung der Registerkarten:

- **VoiceMail-Gruppen**
- **Fax-Gruppe**
- **Favoritengruppen**

Tabelle 64:

Parameter	Beschreibung
VoiceMail-Gruppen	
Bearbeiten	Bearbeiten Sie die ausgewählte VoiceMail-Gruppe
Entfernen	Entfernen Sie die ausgewählten VoiceMail-Gruppen
VoiceMail-Gruppen	Name der Voicemail-Gruppe
Pilot	Rufnummer der Voicemail-Gruppe
Typ	Typ der Voicemail-Gruppe
Anzahl Benutzer	Anzahl der Mitglieder der Voicemail-Gruppe

Parameter	Beschreibung
Anzahl Nachrichten	Anzahl der neuen Sprachnachrichten für die Voicemail-Gruppe
Benutzer	Mitglieder der Voicemail-Gruppe
Fax-Gruppe	
Bearbeiten	Bearbeiten Sie die ausgewählte Fax-Gruppe
Fax-Gruppe	Name der Fax-Gruppe
Pilot	Rufnummer der Fax-Gruppe
Anzahl Benutzer	Anzahl der Mitglieder in der Fax-Gruppe
Anzahl Faxnachrichten	Anzahl der neuen Faxnachrichten für die Fax-Gruppe
Mehrere Benutzer	Wenn es sich um eine Fax-Gruppe handelt, wird **Ja** angezeigt. Andernfalls wird **Nein** angezeigt.
Favoritengruppen	
Hinzufügen	Fügen Sie eine neue Favoritengruppe hinzu
Bearbeiten	Bearbeiten Sie die ausgewählte Favoritengruppe
Entfernen	Entfernen Sie die ausgewählten Favoritengruppen
Gruppenname	Name der Favoritengruppe
Anzahl der Kontakte	Anzahl der Kontakte, die der Gruppe hinzugefügt wurden
Editierbar	Wählen Sie, ob der Benutzer die Favoritengruppe bearbeiten kann oder nicht.

28.4.4.5 OpenScape Business UC Suite > Templates

Parameterbeschreibung der Registerkarten:

- **SMS-Dienstanbieter**

Parameter	Beschreibung
Hinzufügen	Fügen Sie eine neue Vorlage hinzu. Geben Sie den Namen der Vorlage und den Namen des Autors ein. Im Feld Empfänger, Betreff oder Text können Platzhalter eingefügt werden, die man jeweils unter "VSL-Felder" auswählt.

Parameter	Beschreibung
Bearbeiten	Bearbeiten Sie die ausgewählte Vorlage. Ändern Sie den Namen der Vorlage und den Namen des Autors. Bearbeiten Sie auch die Felder Empfänger, Betreff und Text. Im Feld Empfänger, Betreff oder Text können Platzhalter eingefügt werden, die man jeweils unter "VSL-Felder" auswählt.
Entfernen	Entfernen Sie die ausgewählte Vorlage.
Als Standardeinstellung übernehmen	Legen Sie die ausgewählte Vorlage als Standard fest.

28.4.4.6 OpenScape Business UC Suite > Externes Verzeichnis

Parameterbeschreibung der Registerkarten:

- **Externes Verzeichnis**

Parameter	Beschreibung
Hinzufügen	Manuelles Hinzufügen einzelner Kontakte zum externen Verzeichnis. Die Zeichen müssen dem UTF-8-Format entsprechen
Bearbeiten	Bearbeitung eines ausgewählten Kontakts aus dem externen Verzeichnis.
Entfernen	Entfernung der ausgewählten Kontakte aus dem externen Verzeichnis.

Parameterbeschreibung der Registerkarten:

- **Externes Verzeichnis importieren**

Parameter	Beschreibung
Importieren aus	Wählen Sie, ob der Import der Kontaktdaten aus einer lokalen Datei oder aus einem öffentlichen Windows-Ordner erfolgen soll.
Datei-Upload	Klicken Sie auf **Datei auswählen**, um die Datei auszuwählen, die in das System hochgeladen werden soll.
Öffentlicher Windows-Ordner	Geben Sie den **Dateinamen**, den **Benutzernamen**, die **Domäne** und das **Kennwort** des öffentlichen Windows-Ordners ein, der in das System hochgeladen werden soll, und klicken Sie zum Testen auf **Testen**.
Optionen	Dieser Bereich bietet verschiedene Optionen für die Formatierung der zu importierenden csv-Datei. Zusätzlich gibt es eine Option, die die vorhandenen Daten vor der Ausführung des Imports löscht. Eine weitere Option schließlich legt fest, wie Duplikate während eines Imports behandelt werden sollen.

Parameterbeschreibung der Registerkarten:

- **Externes Verzeichnis exportieren**

Parameter	Beschreibung
Exportieren nach	Wählen Sie, wo die exportierte Datei gespeichert werden soll, lokal oder in einem öffentlichen Windows-Ordner.
Öffentlicher Windows-Ordner	Geben Sie den **Dateinamen**, den **Benutzernamen**, die **Domäne** und das **Kennwort** des öffentlichen Windows-Ordners ein, der in das System hochgeladen werden soll, und klicken Sie zum Testen auf **Testen**.

28.4.4.7 OpenScape Business UC Suite > Externer Anbieter

Parameterbeschreibung der Registerkarten:

- **LDAP-Provider**

Parameter	Beschreibung
Hinzufügen / Bearbeiten / Entfernen	Hinzufügen, Bearbeiten oder Entfernen der Zugangsdaten des LDAP-Servers.
Name	Name für dieses externe Offline-Verzeichnis
Server / Server-Adresse	DNS-Name oder IP-Adresse des LDAP-Servers.
Port	Portnummer des externen LDAP-Servers
Benutzername	Benutzername für den Zugriff auf den externen LDAP-Server.
Kennwort	Kennwort für den Zugriff auf den externen Exchange-Server.
LDAP Basis-DN	LDAP Base Distinguished Name ein, z.B. dc=example-for-a-domain, dc=net.
TLS	Aktivieren Sie die Verwendung von nur sicheren Verbindungen zum LDAP-Server.
Anrede, **Vorname**, **Nachname**, **Geschäftlich 1**, **Geschäftlich 2**, **Privat**, **Mobil**, **Firma**, **Firmen-Rufnr.**, **Postanschrift**, **Bundesland oder Region**, **Land**, **Postleitzahl**, **E-Mail**, **Pager**, **Faxrufnummer** und **Ort**	Bei der Konfiguration eines externen Offline-Verzeichnisses kann der Administrator das Mapping der Felder an die Namen des verwendeten LDAP-Servers anpassen. Gelöschte Felder werden bei der Suche nach Namen mittels Rufnummer ignoriert. Die Suche erfolgt immer mit den letzten 4 Stellen der Rufnummer mit vorangestellter Wildcard. Sie können die Suche nach Namen mittels Rufnummer bei kommenden Gesprächen deaktivieren. Geben Sie jeweils die entsprechende Feldbezeichnung des LDAP-Servers ein. **Anmerkung:** Die Zuordnung des LDAP-Feldes hängt vom entsprechenden Feldnamen durch die Verwendung eines externen LDAP-Servers ab.

Parameterbeschreibung der Registerkarten:

- **Exchange-PST**

Parameter	Beschreibung
Hinzufügen / Bearbeiten / Entfernen	Hinzufügen, Bearbeiten oder Entfernen der Zugangsdaten des Exchange-Servers. In einer Microsoft-Umgebung ist der Active Directory Server (ADS) bzw. der Exchange Server auch gleichzeitig der LDAP-Server.
Name	Name dieses Externen Offline-Verzeichnisses.
Auth-Methode	Authentifizierungsmethode, die für den Zugriff auf den externen Exchange-Server verwendet werden soll. Sie können zwischen **Einfach** und **OAuth 2.0**wählen.
Server / Server-Adresse	DNS-Name oder IP-Adresse des Exchange-Servers.
Benutzername	Benutzername für den Zugriff auf den externen Exchange-Server.

Parameter	Beschreibung
Kennwort	Kennwort für den Zugriff auf den externen Exchange-Server. Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode **Einfach** ist.
Mandanten-ID, **Anwendungs-ID**, **Passwort der Anwendungs ID**, **Umfang**	**Mandanten-ID**, **Anwendungs-ID** und **Passwort der Anwendungs ID** für die Anwendung, die in Azure AD für die Exchange Directory Integration registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator. **Umfang**, den die Anwendung erfordert (optional). Standardwert: https://outlook.office365.com/.default Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode **OAuth 2.0** ist.

Parameterbeschreibung der Registerkarten:

- **Exchange-Kalender-Integration**

Parameter	Beschreibung
Exchange-Kalender-Integration	Bei Abwesenheit des Nutzers dient die Kalenderintegration der automatischen Erstellung von Outlook-Terminen unter Windows. Wenn die Outlook-Termine nicht in der lokalen PST-Datei des Benutzers, sondern auf dem Exchange-Server gespeichert werden sollen, müssen hier die Zugangsdaten eingegeben werden.
Exchange-Kalender-Integration aktivieren	Aktivieren der Exchange-Kalenderintegration
Auth-Methode	Authentifizierungsmethode, die für den Zugriff auf den externen Exchange-Server verwendet werden soll. Sie können zwischen **Einfach** und **OAuth 2.0**wählen.
Server	Details zur Nutzung der verschiedenen Microsoft Exchange Server-Versionen finden Sie im Unify Experts Wiki unter: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.
Benutzername	Benutzername für den Zugriff auf den externen Exchange-Server.
Kennwort	Kennwort für den Zugriff auf den externen Exchange-Server. Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode **Einfach** ist.
Mandanten-ID, **Anwendungs-ID**, **Passwort der Anwendungs ID**, **Umfang**	**Mandanten-ID**, **Anwendungs-ID** und **Passwort der Anwendungs ID** für die Anwendung, die in Azure AD für die Exchange Calendar Integration registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator. **Umfang**, den die Anwendung erfordert (optional). Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode **OAuth 2.0** ist.

28.4.4.8 OpenScape Business UC Suite > Contact Center

Parameterbeschreibung der Registerkarten:

- **Zeitplan**
- **Warteschlange**
- **Servicegrad**
- **VIP-Anruferprioritäten**

- **VIP-Rufliste**
- **Bevorzugte Agenten**
- **Contact Center Pausen**
- **Einfache Nachbearbeitung**
- **Mehrfache Nachbearbeitung**
- **Warteschlangen-Bindungen**

Zeitplan

Über einen Zeitplan wird definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen. Für jede Warteschlange wird über einen Zeitplan und die darin enthaltenen Regeln (Call Control Vector CCV) definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen. Einem Zeitplan muss mindestens eine Regel (Call Control Vector CCV) zugeordnet werden. Die Regeln bestimmen für den Zeitraum für den ein Zeitplan gilt, wie kommende Anrufe in einer Warteschlange behandelt werden. Regeln gelten ausschließlich für Anrufe und nicht für Faxe und E-Mails.

Ausführliche Informationen zur Konfiguration von Zeitplänen siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Zeitplan	Name des Zeitplans
Warteschlange	Name der Warteschlange, der der Zeitplan zugeordnet ist.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Zeitplan	
Name des Zeitplans	Name des Zeitplans
Standard-CCV	Angezeigt wird die Standard-Regel für diesen Zeitplan, die nach Zuweisung zu einer Warteschlange 24 Stunden am Tag und 365 Tage im Jahr gilt. Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden.
Warteschlangen	
Name der Warteschlange	Name der Warteschlange, der dieser Zeitplan zugeordnet ist.
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Ausnahmen	
CCV	Name der Ausnahme-Regel (Ausnahme-CCV) Ausnahme-Regeln definieren, wie kommende Anrufe zu bestimmten Ausnahmezeiten (Pause, Wochenende, Feiertag, Urlaub usw.) behandelt werden. Urlaubspläne haben Vorrang vor anderen Zeitplänen und Regeln einer Warteschlange.
Beschreibung	Beschreibender Text für die Ausnahme-Regel
Typ	Typ der Ausnahme-Regel

Parameter	Beschreibung
Startdatum	Datum für den Beginn der Ausnahme-Regel
Endedatum	Datum für das Ende der Ausnahme-Regel
Startzeit	Uhrzeit für den Beginn der Ausnahme-Regel
Endezeit	Uhrzeit für das Ende der Ausnahme-Regel
erfolgt	Die Häufigkeit, mit der die Ausnahmeregel eingeplant wird

Warteschlange

Warteschlangen sind die Basis des Contact Centers. Anrufe, Faxe und E-Mails für eine Warteschlange können in Abhängigkeit vom Fähigkeits-Level der Agenten, von der Priorität und der Wartezeit behandelt werden. Anrufern, die sich im Wartezustand befinden, können Ansagen eingespielt werden.

Ausführliche Informationen zur Konfiguration von Warteschlangen siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Allgemeine Einstellungen	
Name der Warteschlange	Name der Warteschlange
Warteschlange aktiv	Definition des Warteschlangenzustands
Warteschlange aktiv: Inaktiv	Die Warteschlange ist nicht aktiv.
Warteschlange aktiv: Aktiv	Die Warteschlange ist aktiv.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Telefonanlage	Angezeigt wird der Eintrag CSP
Zeitplan	Angezeigt wird der zugeordnete Zeitplan
Anzahl Warteschlangen-Alarme	Alarm-Schwellwertanzahl Wird die hier angegebene Anzahl wartender Anrufe in der Warteschlange überschritten, wechselt das Warteschlangensymbol bei den Agenten von grün auf orange. Standardwert: 0 Anrufe
Zeit Warteschlangen-Alarm	Alarm-Schwellwertzeit in Sekunden Wird die hier angegebene Wartezeit eines Anrufs in der Warteschlange überschritten, wechselt der betreffende Eintrag in der Liste der Contact-Center-Anrufe bei den Agenten auf rot. Standardwert: 0 Sekunden

Parameter	Beschreibung
Zeitüberschreitung für entgangene Anrufe	Zeitüberschreitung für entgangene Anrufe in Sekunden Nach Ablauf der hier angegebenen Zeit wird ein nicht angenommener Anruf zum nächsten freien Agenten weitergeleitet. Standardwert: 10 Sekunden
Schwellwert für abgebrochene Anrufe	Schwellwertzeit für abgebrochene Anrufe in Sekunden Die hier angegebene Zeit bestimmt, ob ein abgebrochener Anruf in die Statistik aufgenommen wird. Statistisch erfasst werden Anrufe, die nach Ablauf der angegebenen Zeit abgebrochen werden. Standardwert: 0 Sekunden
Popup-Fenster aktiviert	Bei aktiviertem Flag erscheint in myAgent bei kommenden Anrufen ein PopUp-Fenster zur Anzeige und Eingabe von Kundendaten. PopUp-Fenster sind erforderlich, um Rückrufe anzunehmen und auszuführen und um Faxe und E-Mails anzunehmen. Standardwert: Deaktiviert **Anmerkung:** Benachrichtigungsoption über **myAgent** > **Setup** > **Benachrichtigungen** > **Popup-Anwendung bei eingehenden Anrufen** werden durch die Aktivierung des Bildschirm-Popups über **WBM** > **Expertenmodus** > **OpenScape Business UC Suite** > **Contact Center** > **Warteschlange** > **Allgemeine Einstellungen** > **Bildschirm-Popup aktiviert**außer Kraft gesetzt.
Nachbearbeitungsmodus	Definition des Nachbearbeitungsmodus
Nachbearbeitungsmodus: Keine Nachbearbeitung	Für die Warteschlange können keine Nachbearbeitungsgründe definiert werden.
Nachbearbeitungsmodus: Einfache Nachbearbeitung	Für die Warteschlange können ein oder mehrere Nachbearbeitungsgründe definiert werden.
Nachbearbeitungsmodus: Mehrfache Nachbearbeitung	Für die Warteschlange können ein oder mehrere Nachbearbeitungsgründe definiert und in Gruppen und Untergruppen zusammengefasst werden.
Zeitüberschreitung PopUp-Fenster	Screenpop-Timeout in Sekunden Wenn dieser auf 0 gesetzt ist, fordert myAgent implizit eine Screenpopup-Zeit von 20 Sekunden an. Standardwert: 20 Sekunden
Prioritäten	Ist ein Agent mehreren Warteschlangen zugeordnet, kann über die Warteschlangen-Priorität festgelegt werden, ob die Anrufe für eine Warteschlange mit höherer Priorität an diesen Agenten weitergeleitet werden sollen als die Anrufe für andere Warteschlangen.
Warteschlangentiefe-Modus	Definition des Warteschlangentiefe-Modus
Warteschlangentiefe-Modus: Statisch	Falls der Warteschlangentiefe-Modus auf „Statisch“ gesetzt wurde, können WLS und Warteschlangentiefe konfiguriert werden.

Parameter	Beschreibung
Warteschlangentiefe-Modus: Keine	Falls die Warteschlangentiefe auf „Keine“ gesetzt wurde, können die WLS-Parameter konfiguriert werden. Dies beeinflusst auch die UCD-Konfiguration, aber die Warteschlangentiefe kann nicht eingestellt werden.
Warteschlangen-Pilots	
Pilots für eingehende Faxnachrichten	Rufnummern (Pilots) für eingehende Faxnachrichten Faxe an diese Rufnummern werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
Dienst für eingehende E-Mails	E-Mail-Adressen für eingehende E-Mails E-Mails an diese Adressen werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
Hinzufügen	Einen neuen Dienst für eingehende E-Mails hinzufügen
Bearbeiten	Einen ausgewählten Dienst für eingehende E-Mails bearbeiten
Entfernen	Den ausgewählten Dienst für eingehende E-Mails entfernen
Auth-Methode	Authentifizierungsmethode, die für den Zugriff auf den Dienst für eingehende E-Mails verwendet werden soll Sie können zwischen **Einfach** und **OAuth 2.0**wählen.
Server	DNS-Name oder IP-Adresse des Dienstes für eingehende E-Mails
Port	Portnummer des Dienstes für eingehende E-Mails
Benutzername	Benutzername für den Zugriff auf den Dienst für eingehende E-Mails
Kennwort	Kennwort für den Zugriff auf den Dienst für eingehende E-Mails Nur editierbar, wenn die ausgewählte Authentifizierungsmethode **Einfach** ist.
Verwendet SSL-Verbindungen	Aktivieren oder deaktivieren Sie die Verwendung von SSL-Verbindungen entsprechend der Konfiguration des Dienstes für eingehende E-Mails
Mandanten-ID, **Anwendungs-ID**, **Client Secret**, **Umfang**	**Mandanten-ID**, **Anwendungs-ID** und **Client Secret** für die Anwendung, die in Azure AD für die E-Mail-Warteschlangen registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator. **Umfang**, den die Anwendung erfordert (optional). Standardwert: https://outlook.office365.com/.default Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode **OAuth 2.0** ist.
Verschiedenes	
Absender-E-Mail-Adresse	Absender-E-Mail-Adresse für verschickte E-Mails Die hier angegebene E-Mail-Adresse wird beim Versenden einer E-Mail durch einen Agenten beim Empfänger angezeigt.
Intelligente Anrufweiterleitung	Bei aktiviertem Flag werden kommende Anrufe automatisch an den Agenten weitergeleitet, der zuletzt mit dem Anrufer verbunden war. Voraussetzung ist, dass für den Anrufer keine bevorzugten Agenten festgelegt wurden. Standardwert: Deaktiviert

Servicegrad

Anhand des Servicegrads können Aussagen über die Beantwortungsqualität einer Warteschlange getroffen werden. Ermöglicht wird dies durch den Vergleich der Anruferwartezeiten in einer Warteschlange mit Sollwerten, die hier für jede Warteschlange individuell vorgegeben werden können.

Für jeden Anruf an eine entsprechende Warteschlange wird der Servicegrad nach Beendigung des Anrufs ermittelt und in die Datenbank übernommen. Eine Auswertung des Servicegrads können Agenten mit dem Berechtigungs-Level Supervisor oder Administrator über die Applikation myAgent vornehmen.

Ausführliche Informationen zur Definition von Sollwerten für den Servicegrad siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Servicegrad	Die horizontale Achse zeigt die Wartezeit in der Warteschlange in Intervallen von 10 Sekunden, die vertikale Achse den Sollwert für den Servicegrad in Prozentwerten. Die roten Punkte geben die Sollwerte für die Vermittlungsqualität der Warteschlange vor. Durch den Vergleich der Sollwerte mit den tatsächlichen Anruferwartezeiten können Qualitätsaussagen getroffen werden.

VIP-Anruferprioritäten

Anhand der VIP-Anruferpriorität kann für jede Warteschlange individuell definiert werden, ob die in der VIP-Rufliste enthaltenen Anrufer bevorzugt behandelt werden sollen.

Die Werte für die VIP-Anruferpriorität können in Abhängigkeit von der Anruferwartezeit in einer Warteschlange frei bestimmt werden. Damit wird der Grad der Bevorzugung von VIP-Anrufern gegenüber normalen Anrufern festgelegt.

Aktiviert ein VIP-Anrufer einen Agentenrückruf (Aufnahme einer Sprachnachricht mit Rückrufwunsch) verbleibt der Agentenrückruf anstelle des VIP-Anrufers in der Warteschlange. Die VIP-Anruferpriorität wird dabei nicht übernommen.

Ausführliche Informationen zur Definition der VIP-Anruferpriorität siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.

Parameter	Beschreibung
VIP-Anruferpriorität	Die horizontale Achse zeigt die Wartezeit in der Warteschlange in Intervallen von 30 Sekunden, die vertikale Achse die Priorität normaler Anrufer, die nicht in der VIP-Rufliste verzeichnet sind. Die roten Punkte definieren die Priorität normaler Anrufer gegenüber VIP-Anrufern.

VIP-Rufliste

Bereits im Kommunikationssystem erfasste Anrufer (externes Verzeichnis) können in die VIP-Rufliste übernommen werden. Darüber hinaus ist die Eingabe von Rufnummernmustern möglich. Rufnummernmuster setzen sich aus einer bestimmten Ziffernfolge und einer Wildcard (Platzhalter) zusammen. Damit können beispielsweise alle Mitarbeiter eines Unternehmens in die VIP-Rufliste übernommen werden.

Ausführliche Informationen zur Konfiguration der VIP-Rufliste siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
VIP-Rufliste	Angezeigt werden die in der VIP-Rufliste enthaltenen Anrufer und Rufnummernmuster. Sie können Anrufer und Rufnummernmuster in der VIP-Anrufliste hinzufügen, bearbeiten oder entfernen. Je weiter rechts sich der Scrollbalken bei einem Anrufer oder Rufnummernmuster befindet, desto höher ist die Priorität gegenüber den anderen in der VIP-Rufliste enthaltenen Anrufern oder Rufnummernmustern.

Bevorzugte Agenten

Jedem Anrufer können ein oder mehrere bevorzugte Agenten einer Warteschlange zugeordnet werden. In diesem Fall versucht das Kommunikationssystem, den Anrufer und die Rückrufwünsche dieses Anrufers zunächst an einen bevorzugten Agenten zu vermitteln. Wurden mehrere bevorzugte Agenten festgelegt, kann eine Priorität (Reihenfolge) definiert werden, mit der die bevorzugten Agenten vermittelt werden.

Ist kein bevorzugter Agent verfügbar, wird der Anruf an einen beliebigen verfügbaren Agenten weitergeleitet.

Ausführliche Informationen zur Definition bevorzugter Agenten siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.

Parameter	Beschreibung
Bevorzugte Agenten	Angezeigt werden die bevorzugten Agenten der in der Kundenliste genannten Anrufer. Sie können einen Agenten hinzufügen, entfernen und seine Priorität ändern. Wurden für einen Anrufer mehrere bevorzugte Agenten definiert, zeigt die Listenposition die Priorität gegenüber den anderen bevorzugten Agenten. Je höher ein Agent in der Liste positioniert ist, desto höher ist seine Priorität.
Nur Kunden mit Zuweisung zu Agenten anzeigen	Bei aktiviertem Flag werden in der Kundenliste nur Anrufer angezeigt, für die mindestens ein bevorzugter Agent festgelegt wurde. Standardwert: Deaktiviert

Contact Center Pausen

Um jedem Agenten definierte Pausen zu ermöglichen, können unterschiedlich lange Contact Center-Pausen festgelegt werden. Contact Center-Pausen stehen systemweit zur Verfügung und können bei Bedarf von einem Agenten über myAgent ausgewählt werden.

Ausführliche Informationen zur Definition von Contact Center-Pausen siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Hinzufügen	Eine neue Contanct Center-Pause hinzufügen
Bearbeiten	Eine ausgewählte Contanct Center-Pause bearbeiten
Entfernen	Die ausgewählte Contanct Center-Pause entfernen
Name	Name der Contact Center-Pause
Dauer	Dauer der Contact Center-Pause in Minuten
Aktiv	Zeigt an, ob die Contact Center-Pause aktiv oder inaktiv ist.

Einfache Nachbearbeitung

Für Warteschlangen mit dem Nachbearbeitungsmodus "Einfache Nachbearbeitung" können hier ein oder mehrere Nachbearbeitungsgründe definiert werden.

Anhand von Nachbearbeitungsgründen können kommende Anrufe bestimmten Themen (Bestellung, Reklamation, Service usw.) zugeordnet werden. Die Zuweisung erfolgt durch einen Agenten nach Beendigung des Anrufs (während der Arbeitszeit) durch Eingabe des entsprechenden Nachbearbeitungsgrundes über myAgent.

Ausführliche Informationen zur Definition von Nachbearbeitungsgründen (Nachbearbeitungscodes) siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Hinzufügen	Eine neue einfache Nachbearbeitung hinzufügen
Bearbeiten	Eine ausgewählte einfache Nachbearbeitung bearbeiten
Entfernen	Die ausgewählte einfache Nachbearbeitung entfernen

Parameter	Beschreibung
Warteschlange	Name der Warteschlange, für die Einfache Nachbearbeitung konfiguriert wurde.
Beschreibung	Beschreibender Text für den Nachbearbeitungsgrund

Mehrfache Nachbearbeitung

Für Warteschlangen mit dem Nachbearbeitungsmodus "Mehrfache Nachbearbeitung" können hier ein oder mehrere Nachbearbeitungsgründe definiert und in Gruppen und Untergruppen zusammengefasst werden.

Anhand von Nachbearbeitungsgründen können kommende Anrufe bestimmten Themen (Bestellung, Reklamation, Service usw.) zugeordnet werden. Die Zuweisung erfolgt durch einen Agenten nach Beendigung des Anrufs (während der Arbeitszeit) durch Eingabe des entsprechenden Nachbearbeitungsgrundes über myAgent.

Ausführliche Informationen zur Definition von Nachbearbeitungsgründen (Nachbearbeitungscodes) siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange, für die Mehrfache Nachbearbeitung konfiguriert wurde. Angezeigt werden die für diese Warteschlange bereits definierten Gruppen und Untergruppen.
Beschreibung	Beschreibender Text für den Nachbearbeitungsgrund

Warteschlangen-Bindungen

Über die Warteschlangen-Bindungen können Agenten einer oder mehreren Warteschlangen zuordnet werden.

Ausführliche Informationen zur Zuordnung von Agenten zu Warteschlangen siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Agentenzuweisung	
Nebenstelle	Anzeige der Durchwahlnummer des Benutzers
Name	Anzeige des Namens des Benutzers.
Agent	Agent, der der Warteschlange zugeordnet ist.

Parameter	Beschreibung
Typ	Agententyp Möglich sind folgende Optionen: • Hauptagent: Der Agent erhält Anrufe unabhängig von der Auslastung der Warteschlange. • Agent bei Überlauf: Der Agent erhält Anrufe nur bei Überlauf der Warteschlange.
Fähigkeits-Level	Anzeige des Fähigkeits-Levels in Prozent Das Fähigkeits-Level steuert die Verteilung der Anrufe auf die Agenten in einer Warteschlange. Agenten mit höherem Fähigkeits-Level werden bei der Anrufverteilung bevorzugt. Haben alle Agenten das gleiche Fähigkeits-Level, erhält der am längsten freie Agent den Anruf.
Agentenrückruf aktivieren	Bei aktiviertem Flag erhält der Agent Rückrufwünsche in Form von Sprachnachrichten.
Nachbearbeitung	Automatische Nachbearbeitungszeit in Sekunden
Überlauf nach Sekunden in Warteschlange	Nur für Agent bei Überlauf: Overflow-Zeit in Sekunden Nach Ablauf der Überlaufzeit wird ein Anruf an einen Agenten bei Überlauf weitergeleitet.
Überlauf nach Anrufen in Warteschlange	Nur für Agent bei Überlauf: Anzahl Anrufe Anrufe, die über diese Maximalzahl hinausgehen, werden an einen Agenten bei Überlauf weitergeleitet.

28.4.4.9 OpenScape Business UC Suite > Zeitpläne

Parameterbeschreibung der Registerkarten:

- **Bearbeiten/Hinzufügen**

Parameter	Beschreibung
Automatischer Vermittlungsplatz (VPL)	Konfiguration der AutoAttendant-Funktion der UC Suite (Company AutoAttendant)
Zeitplan	Name des Zeitplans
Warteschlange	Name der Warteschlange, der der Zeitplan zugeordnet ist.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Bearbeiten / Hinzufügen / Entfernen	Bearbeiten oder Entfernen der ausgewählten Regel oder Hinzufügen einer neuen (öffnet den Regel-Editor)
Name des Zeitplans	Der Zeitplan kann unter einem frei definierbaren Namen gespeichert werden. Es wird empfohlen, hier einen sinnvollen Namen einzugeben.

Parameter	Beschreibung
Standard-CCV	Dem Zeitplan muss mindestens eine Regel (Call Control Vector CCV) zugeordnet werden. Regeln bestimmen für den betreffenden Zeitraum, wie kommende Anrufe behandelt werden. Regeln gelten ausschließlich für Anrufe und nicht für Faxe und E-Mails. Regeln werden mit dem graphischen Regel-Editor (CCV-Editor) durch die Verknüpfung von vordefinierten CCV-Objekten erstellt. Es sind mehrere vorbelegte, standardisierte Vorlagen verfügbar, die beliebig verändert und an den speziellen Bedarf angepasst werden können.
Warteschlangen	Es wird empfohlen, nur eine Warteschlange je Zeitplan zu aktivieren (nur ein Häkchen setzen).
Name der Warteschlange	Die Warteschlange kann unter einem frei definierbaren Namen gespeichert werden. Es wird empfohlen, hier einen sinnvollen Namen einzugeben.
Warteschlange aktiv	Die Warteschlange kann aktiviert oder deaktiviert werden.
Zeitplan	Auswahl des zugehöriger Zeitplans
Pilot	Rufnummer des zugehörigen virtuellen Ports im Kommunikationssystem.
Ausnahmen	Ein Zeitplan mit einer Standard-Regel gilt nach Zuweisung zu einer Warteschlange 24 Stunden am Tag und 365 Tage im Jahr. Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden. Damit kann definiert werden, wie kommende Anrufe beispielsweise während der Urlaubszeit behandelt werden sollen. Urlaubspläne haben hierbei Vorrang vor anderen Zeitplänen und Regeln.
CCV	Auswahl der Ausnahme-Regel (Ausnahme-CCV)
Beschreibung	Freie Eingabe einer Beschreibung für den Ausnahme-Zeitplan
Typ	Im Zeitbereich innerhalb eines oder mehrerer Wochentage / Im Zeit-/ Datumsbereich frei definierbar / Urlaubspläne für einen Datumsbereich
Startdatum	Beginn der Ausnahme (Datum)
Endedatum	Ende der Ausnahme (Datum)
Startzeit	Beginn der Ausnahme (Uhrzeit)
Endezeit	Ende der Ausnahme (Uhrzeit)
(Wochentag)	Die Ausnahme soll an einem oder mehreren Wochentagen gelten
erfolgt	Die Häufigkeit, mit der die Ausnahme geplant wird

28.4.4.10 OpenScape Business UC Suite > Datei-Upload

Parameterbeschreibung der Registerkarten:

- **Audiodatei-Manager**

Parameter	Beschreibung
Upload-Ziel	Applikation, für welche die neue Ansage verwendet wird
Upload-Ziel: **Automatischer Vermittlungsplatz (VPL)**	Ansagen für die automatische Vermittlung
Upload-Ziel: **Profile**	Ansagen für alle oder einzelne Benutzer von UC Suite
Upload-Ziel: **VoiceMail-Begrüßung**	Sprachbox-Begrüßungen für alle oder einzelne Benutzer von UC Suite Die Aufzeichnungsdauer für VoiceMail-Begrüßungen ist auf 1 Minute begrenzt.
Upload-Ziel: **VM-Gruppenbegrüßung**	Begrüßung für eine Gruppen-Sprachbox
no key for: uploader	Die Ansage liegt zum Upload als PCM-Datei vor, mit folgenden Eigenschaften: 8 kHz, 16 bit, mono. Die Länge des Audio-Dateinamens beträgt maximal 30 Zeichen.
Aufzeichnungsgerät	Die Ansage wird über das Telefon einer Nebenstelle aufgenommen
WAV-Datei	
Download	Heruntergeladene Ansagen.
Löschen	Heruntergeladene Ansagen löschen.
Umbenennen	Heruntergeladene Ansagen umbenennen.
Aufzeichnungsgerät	
Dateiname	Angabe des Dateinamens der aufzuzeichnenden Ansage.
Nebenstelle	Auswahl des Telefons, mit dem die Ansage aufgezeichnet werden soll.
Anrufen	Ruft das Telefon an, mit dem die Ansage aufgezeichnet werden soll.
Abspielen	Gibt die aufgenommene Ansage wieder.
Aufzeichnen	Startet die Aufzeichnung der Ansage.

Parameterbeschreibung der Registerkarten:

- **Upload des zentralen Fax-Deckblatts**

Parameter	Beschreibung
Upload des zentralen Fax-Deckblatts	
Ocp Datei	Fax-Deckblatt verfügbar als .ocp Datei
Name	Der Name des zentralen Fax-Deckblatts
Beschreibung	Eine Beschreibung für das zentrale Fax-Deckblatt
Upload	Zentrale Fax-Deckblattdatei hochladen
Bearbeiten	Ausgewählte zentrale Fax-Deckblattdatei bearbeiten
Entfernen	Ausgewählte zentrale Fax-Deckblattdatei entfernen
Als Standardeinstellung übernehmen	Ausgewählte zentrale Fax-Deckblattdatei als Standard festlegen

Parameter	Beschreibung
Dateiname	Angabe des Dateinamens der hochzuladenden Ansage
Erstellungsdatum	Erstellungsdatum der zentralen Fax-Deckblattdatei

28.4.4.11 OpenScape Business UC Suite > Konferenzschaltung

Parameterbeschreibung der Registerkarten:

- **Konferenzschaltung**

Parameter	Beschreibung
Name	Name der Konferenz (vom Benutzer vergeben)
Besitzer	Name des Benutzers, der die Konferenz initiiert hat
Als nächste geplant	Nächste geplante Startzeit
Aktiv	
Anzahl Mitglieder	Anzahl der Konferenzmitglieder einschließlich Konferenzleiter
Display	Teilnehmer der ausgewählten Konferenz
Löschen	Die ausgewählten Konferenzen löschen

28.4.4.12 OpenScape Business UC Suite > Standort-Liste

Parameterbeschreibung der Registerkarten:

- **Standort-Liste**

Parameter	Beschreibung
Standort-Name	Standorte im vernetzten Kommunikationssystem (siehe Grundeinstellungen > Gateway-Eigenschaften)
Standort-Adresse	IP-Adresse von UC Booster Card, von UC Booster Server oder des Kommunikationssystems
Standort-Port	Server Port
Standort-IP-Trunks	Standort-IP-Trunks, sofern vorhanden
Online-Status	Verbindungsstatus des Kommunikationssystems am Standort

28.4.4.13 OpenScape Business UC Suite > Server

Parameterbeschreibung der Registerkarten:

- **Allgemeine Einstellungen**
- **Gespräch aufzeichnen**
- **Protokollierung**

- **Benachrichtigungen**
- **Wartung**
- **VoiceMail**
- **Contact Card Mapping**

Parameter	Beschreibung
Bürozeiten	
Startzeit	Beginn der täglichen Bürozeit (Geschäftszeit) Einstellung für den Anwesenheitsstatus der UC Clients Standardwert: 07:00 **Anmerkung:** Der eingegebene Wert muss im 24-Stunden-Format (HH:MM) vorliegen.
Endezeit	Ende der täglichen Bürozeit (Geschäftszeit) Einstellung für den Anwesenheitsstatus der UC Clients Standardwert: 19:00 **Anmerkung:** Der eingegebene Wert muss im 24-Stunden-Format (HH:MM) vorliegen.
Kennwortlänge	
Längen	Länge des Kennworts für die UC Clients. Der Mindestwert ist 6. ***HINWEIS:*** Durch das Ändern der Kennwortlänge werden die Kennwörter aller Benutzer zurückgesetzt. Standardwert: 6
Rufnummer des Abwurfplatzes	
Zielnummer	Rufnummer des Abwurfplatzes ***INFO:*** Einzutragen ist die im Kommunikationssystem konfigurierte Rufnummer des Abwurfplatzes.
Sofortnachricht	
Sofortnachricht versenden deaktivieren	Bei aktiviertem Flag ist kein Versand von Sofortnachrichten möglich. Standardwert: Deaktiviert
Analoge Nebenstellen	
Modus Analoger Teilnehmer	Definition der Anzeige analoger Teilnehmer im internen Verzeichnis Standardwert: Alles anzeigen
Modus Analoger Teilnehmer: Alles anzeigen	Alle analogen Teilnehmer werden im internen Verzeichnis angezeigt

Parameter	Beschreibung
Modus Analoger Teilnehmer: Nur Benannte anzeigen	Ausschließlich analoge Teilnehmer mit einem Namen werden im internen Verzeichnis angezeigt.
Modus Analoger Teilnehmer: Nicht angezeigt	Kein analoger Teilnehmer wird im internen Verzeichnis angezeigt.
Nebenstelle	
Max. interne Länge	Maximale Ziffernanzahl bei internen Rufnummern Zum Schutz vor Gebührenmissbrauch ist die Wahl längerer interner Rufnummern nicht möglich. Standardwert: 4
Min. externe Länge	Minimale Ziffernanzahl bei externen Rufnummern Standardwert: 3
Übergeben	
Normales Vermittlungsplatz-SST	Bei aktiviertem Flag erfolgt die Übergabe eines Anrufs, unabhängig davon, ob das Ziel frei, besetzt oder nicht verfügbar ist. Standardwert: Aktiviert
Journal	
Löschen von Journaleinträgen zulassen	Dieses Flag ermöglicht bzw. verbietet das Löschen von Journaleinträgen durch den Benutzer.
Min. externe Länge	
Faxformat	
Als Faxformat PDF verwenden	Wenn das Flag aktiviert ist, kann das eingegangene Fax im PDF-Format gespeichert werden, andernfalls wird das TIFF-Format verwendet.
Verzeichnisserver	
Langsamer externer Provider	Dieses Flag verbessert die Antwortzeit beim Klicken mit der rechten Maustaste auf eine E-Mail. Auch wenn es aktiviert ist, wird die Suche nach Kontakten nur im übergeordneten Exchange-Verzeichnis und nicht in Unterverzeichnissen durchgeführt.
Länge der Überprüfung	Geben Sie eine 4- bis 8-stellige Ziffer ein, um die Länge der CLI-Nummern für die Suche im LDAP-Verzeichnis von myPortal for Desktop und myPortal for Outlook zu definieren. Die höchste Zahl (8) steht für genauere Suche bzw. bessere Performance des Systems Standardwert: 4
Nach Name wählen – Nur lokale Nebenstelle suchen	Wenn dieses Flag markiert ist, ist die Funktion "Nach Namen wählen" auf den aktiven Knoten beschränkt (lokale Funktion). Wenn dieses Flag nicht markiert ist, bleibt die alte Funktion verfügbar, die alle Benutzer im Netzwerk berücksichtigt, aber die Ansage erst nach der Auswahl eines lokalen Benutzers abspielt.

Parameter	Beschreibung
Der Verzeichnis-Suchcache läuft ab in	Legen Sie die Anzahl der Minuten oder einen Bereich von Minuten fest, in denen der Cache-Speicher bei der Suche nach Kontakten verwendet wird. Sie können einen Minutenbereich von 1-60 Minuten einstellen. Bei einem Wert von "0" ist diese Funktion deaktiviert.
Suchen nach Rufnummer	Wenn dieses Flag aktiviert ist, können Sie in Verzeichnissen nach Telefonnummern suchen.
TLS	
Für Client-Verbindungen TLS verwenden	Aus Netzwerkgründen kann es erforderlich sein, die sichere Client-Server-Verbindung auszuschalten. Das Ändern dieser Einstellung erfordert einen Neustart der UC-Anwendung. Dies sollte auf sehr spezielle Fälle beschränkt bleiben!
Anwesenheit	
Status „Krank“ ausblenden	Wenn dieses Flag aktiviert ist, steht der Anwesenheitsstatus "krank" nicht zur Verfügung. Standardwert: Deaktiviert
Benutzername	
Bearbeitung des Namens deaktivieren	Wenn dieses Flag aktiviert ist, können Benutzer ihren konfigurierten Vor- und Nachnamen nicht ändern. Standardwert: Deaktiviert
Wandanzeige (Wallboard)	
Wandanzeige deaktivieren	Wenn dieses Flag aktiviert ist, steht die Wandanzeige nicht zur Verfügung.
Agentennamen in der Warteschlangen-Bindung von myAgent anzeigen	Ist dieses Flag aktiviert, erscheint gemeinsam mit der Rufnummer eines Agenten auch ein Name, den der Benutzer konfigurieren kann. Ein Benutzer zeigt "Hotdesk" an, wenn er eine andere als seine eigene Nebenstelle verwendet. Standardwert: Deaktiviert.
Gespräch aufzeichnen	
Gespräch aufzeichnen	Bei aktiviertem Flag ist das Aufzeichnen von Anrufen möglich. Standardwert: Aktiviert
Vor der Aufzeichnung eine Ansage wiedergeben	Bei aktiviertem Flag wird vor dem Beginn einer Aufzeichnung eine Ansage wiedergeben. Standardwert: Deaktiviert
Während der Aufzeichnung einen Hinweiston wiedergeben	In OpenScape Business S wird bei aktiviertem Flag während der Aufzeichnung ein Hinweiston eingespielt. Standardwert: Aktiviert
Aufzeichnung von Konferenzen verfügbar	Bei aktiviertem Flag ist das Aufzeichnen von Konferenzen möglich. Standardwert: Deaktiviert
Systemprotokolle	

Parameter	Beschreibung
Trace-Meldungen protokollieren (ausführlich)	Bei aktiviertem Flag werden Trace-Meldungen täglich in einer Protokolldatei aufgezeichnet. Standardwert: Deaktiviert
Client-Logs:	
Client-Log-Pfad	Ablagepfad für Client-Log-Dateien (Protokolldateien der UC Suite)
Protokoll-Upload aktivieren	Bei aktiviertem Flag werden Client-Logs auf der Festplatte der UC Booster Card (OCAB), des UC Booster Servers oder des Kommunikationssystems OpenScape Business S abgelegt. Standardwert: Aktiviert
Client-Protokollierung aktivieren	Bei aktiviertem Flag werden Client-Logs aufgezeichnet. Standardwert: Aktiviert
E-Mail-Benachrichtigungen	
E-Mail-Benachrichtigungen bei Systemfehlern aktivieren	Bei aktiviertem Flag werden E-Mails verschickt, um den oder die eingetragenen Empfänger zum Beispiel vor einem kritischem Füllstand der Festplatte zu warnen oder über Fehler zu informieren. Standardwert: Aktiviert
myPortal Einladungs-E-Mail aktivieren	Wenn dieses Flag aktiviert ist, erhalten UC Suite-Benutzer eine Einladungs-E-Mail zur Installation oder Aktualisierung des myPortal-Clients. Diese E-Mail wird normalerweise bei einer Neuinstallation an alle UC Suite-Benutzer mit einer gültigen E-Mail-Adresse im Benutzerverzeichnis gesendet, wenn eine E-Mail-Adresse für einen UC Suite-Benutzer im Benutzerverzeichnis hinzugefügt oder geändert wird oder nachdem ein OpenScape Business-Softwareupdate durchgeführt wurde und eine neue Version des Clients verfügbar ist. Standardwert: Aktiviert
Empfänger	E-Mail-Adressen, an die E-Mail-Benachrichtigungen verschickt werden.
Bedingungen	
Wichtige Benachrichtigungen senden	Bei aktiviertem Flag erfolgt eine E-Mail-Benachrichtigung bei wichtigen Benachrichtigungen (z. B. bei Systemfehlern) Standardwert: Aktiviert
Benachrichtigungen über Systemabsturz senden	Bei aktiviertem Flag erfolgt eine E-Mail-Benachrichtigung bei Systemabstürzen. Standardwert: Aktiviert
Bei Fehlermeldungen die letzten ... Zeilen der Protokolldatei senden	Definition der Anzahl der Zeilen einer Protokolldatei, die mit einer E-Mail verschickt werden sollen. Standardwert: 100
Wartung	

Parameter	Beschreibung
Systemwartung beginnen um	Definition der Uhrzeit, zu der täglich das Löschen folgender Daten erfolgt, wenn diese jeweils eingestellten Aufbewahrungszeiten überschritten haben: • Nachrichten • Anrufinformationen im Anrufjournal (Anrufhistorie) • Mit myAgent aufgezeichnete Anrufe (Contact Center) • Empfangene und gesendete Faxe und E-Mails für das Contact Center • Log-Dateien Standardwert: 2.00 Stunden
Nachricht	
Nachrichten im Posteingang aufbewahren für	Aufbewahrungsdauer in Tagen für Sprachnachrichten im Posteingang Standardwert: 60
Abgespielte / gelesene Nachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für abgespielte/gelesene Sprachnachrichten Standardwert: 30
Gespeicherte Nachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gespeicherte Sprachnachrichten Standardwert: 365
Gelöschte Nachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gelöschte Sprachnachrichten Standardwert: 30
Fax	
Faxnachrichten im Posteingang aufbewahren für	Aufbewahrungsdauer in Tagen für Faxnachrichten im Posteingang Standardwert: 30
Gelesene Faxnachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gelesene Faxnachrichten Standardwert: 30
Gelöschte Faxnachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gelöschte Faxnachrichten Standardwert: 30
Gesendete Faxnachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gesendete Faxnachrichten Standardwert: 30
Wartung der Anrufinformationen	
Anrufhistorie aufbewahren für	Aufbewahrungsdauer in Tagen für Anrufe im Journal Standardwert: 30

Parameter	Beschreibung
Konversation schließen nach	Aufbewahrungsdauer in Tagen für offene Gespräche im Journal. Alle nicht angenommenen Anrufe vom/zum selben Kontakt während dieses Zeitraums werden der Registerkarte "Offene Anrufe" hinzugefügt, die mit demselben Gespräch verknüpft ist. Nach Ablauf dieser Frist werden alle Anrufe in einem Gespräch als automatisch abgeschlossen markiert und aus der Registerkarte "Offene Anrufe" entfernt. Standardwert: 3 Maximalwert: 30
Contact Center	Aufbewahrungsdauer in Tagen für die mit myAgent aufgezeichneten Anrufe und die empfangenen und gesendeten Faxe und E-Mails für das Contact Center Standardwert: 30
CC-Live-Aufzeichnung/ Rückruf/E-Mail/Fax-Anrufe aufbewahren für	Aufbewahrungsdauer in Tagen für alle Kommunikationsdaten im Zusammenhang mit Anrufen, wie Rückrufnachrichten, live aufgezeichnete Anrufe, Faxanrufe und E-Mails. Standardwert: 30
Wartung der Protokolldateien	
Protokollinformationen aufbewahren für	Aufbewahrungsdauer in Tagen für Protokolldateien Standardwert: 10
Sofortnachricht	
Sofortnachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für Sofortnachrichten Standardwert: 30
Berichte	
Kennwort zurücksetzen	Setzt das Administratorpasswort von myReports auf das Standardpasswort zurück.
Alle Benutzerpasswörter zurücksetzen	
Alle Benutzerpasswörter zurücksetzen	Setzt Passwörter für alle Benutzer zurück, erlaubt Passwörter mit bis zu 6 Zeichen. **Anmerkung:** In diesem Fall ist das Standardkennwort auf 6 Zeichen (123456) festgelegt.
VoiceMail	
VoiceMail-Sprache	Voreinstellung der Sprache für das Menü und die systemeigenen Ansagen der Sprachbox
Wiedergabereihenfolge für Sprachnachrichten	Definition der Wiedergabereihenfolge für Sprachnachrichten Standardwert: Neueste zuerst

Parameter	Beschreibung
Wiedergabereihenfolge für Sprachnachrichten: Neueste zuerst	Die neueste Sprachnachricht wird zuerst angeboten.
Wiedergabereihenfolge für Sprachnachrichten: Älteste zuerst	Die älteste Sprachnachricht wird zuerst angeboten.
Aufzeichnungszeit Sprachnachricht	Definition der maximalen Aufzeichnungsdauer für eine Sprachnachricht in Sekunden Standardwert: 900
VoiceMail-Modus	Definition des Funktionsumfangs der Sprachbox Standardwert: Vollständig
VoiceMail-Modus: Vollständig	Voller Funktionsumfang für die Sprachbox
VoiceMail-Modus: Kurzmenü	Nach der statusbezogenen oder persönlichen Ansage wird das Verbinden zum Empfang angeboten.
VoiceMail-Modus: Kein VoiceMail-Menü	Nach der Begrüßungsansage wird der Anrufer direkt zur Sprachaufzeichnung weitergeleitet.
Rückruf von VM nur an bekannte Nummer zulassen	Bei aktiviertem Flag wird der Zugriff von Anrufern auf die Sprachbox verhindert, deren Rufnummern nicht im UC Client hinterlegt sind. Standardwert: Aktiviert
Aufforderung "Bitte hinterlassen Sie eine Nachricht nach dem Ton" überspringen	Wenn dieses Flag aktiviert ist, wird die Aufforderung "Bitte hinterlassen Sie eine Nachricht nach dem Ton" übersprungen. Standardwert: Deaktiviert
Contact Card Mapping	
Microsoft: Verfügbar (grün)	Der UC-Anwesenheitsstatus dieser Zeile ist dem Outlook-Status Verfügbar (Grün) zugeordnet.
Microsoft: Nicht bei der Arbeit (gelb)	Der UC-Anwesenheitsstatus dieser Zeile ist dem Outlook-Status Nicht bei der Arbeit (Gelb) zugeordnet.
Microsoft: Beschäftigt (rot)	Der UC-Anwesenheitsstatus dieser Zeile ist dem Outlook-Status Beschäftigt (Rot) zugeordnet.
Microsoft: Außer Betrieb (grau)	Der UC-Anwesenheitsstatus dieser Zeile ist dem Outlook-Status Außer Betrieb (Grau) zugeordnet.

28.4.4.14 OpenScape Business, UC Suite > Profile

Parameterbeschreibung der Registerkarten:

- **Hinzufügen / Bearbeiten**

Parameter	Beschreibung
Profile	Benutzer-Profile speichern Einstellungen von Benutzern der UC Suite. Einem Benutzer-Profil können mehrere Benutzer (Mitglieder) zugeordnet werden. Alle Mitglieder dieses Profils haben (zunächst) die gleichen Einstellungen. Es können mehrere Profile erstellt werden, die für verschiedene Benutzergruppen unterschiedliche Voreinstellungen ermöglichen.
Name	Name des Profils (freie Eingabe)
Persönliche Daten	
Eigene persönliche Daten	Ausgewählte persönliche Daten für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Meine Einstellungen	
Darstellung	Skin und Sprache des UC Clients der zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Benachrichtigung	Benachrichtigungen für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Outlook-Anbindung	Kalenderintegration für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Abkürzungstasten	Aktivierung und Einrichtung von Tastaturkombination für den Zugriff auf verschiedene, häufig verwendete Funktionen über die Tastatur. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Verschiedenes	Automatische Rückkehr zum Anwesenheitsstatus "Büro", Übergabemethode und Aufbewahrungsdauer des Anrufjournals für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Anrufregeln	
Anrufweiterleitungsziele	Weiterleitungsziele für kommende Anrufe in Abhängigkeit vom Anwesenheitsstatus für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Kommunikation	
Einstellungen für Sprachnachrichten	Aufzeichnung von Sprachnachrichten in Abhängigkeit vom Anwesenheitsstatus für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Sprachnachricht-Benachrichtigung	Mitteilung bei neuen Sprachnachrichten für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Fax-Benachrichtigung	Mitteilung bei neuen Faxnachrichten für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Benachrichtigungen über entgangene Anrufe	Benachrichtigungsservice für entgangene Anrufe.

Parameter	Beschreibung
Profile	
Profile	Persönlicher AutoAttendant für die zugeordneten Benutzer. Die betreffenden Benutzer müssen eine Ansage zur Auswahl aufzeichnen. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Sensibilität	
Sicherheit und Zugriff	Abhören von Sprachnachrichten mit myAttendant zulassen sowie Abfrage der Sprachbox vom eigenen Telefon ohne Kennwort. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Sichtbarkeit des Anwesenheitsstatus	Interne Teilnehmer, welche den Anwesenheitsstatus sehen dürfen. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
VoiceMail-Anwesenheitsstatus	Interne bzw. externe Anrufer, welche über den Anwesenheitsstatus durch automatische Ansagen der Sprachbox informiert werden sollen. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Favoriten	
Favoriten	Favoritengruppen mit einer Liste von Kontakten, die dem Benutzer zugewiesen werden können.

Parameterbeschreibung der Registerkarten:

- **Benutzer zuordnen**

Parameter	Beschreibung
Zugewiesene Benutzer	Benutzer, für welche das Profil gelten soll
Verfügbare Benutzer	Benutzer, für die das Profil gelten soll

Parameterbeschreibung der Registerkarten:

- **Entfernen**

Parameter	Beschreibung
Name	Name des Profils (freie Eingabe)
Benutzer	Benutzer, für welche das Profil gelten soll

28.4.4.15 OpenScape Business, UC Suite > Faxkopfzeilen

Parameterbeschreibung der Registerkarten:

- **Bearbeiten**
- **Hinzufügen**
- **Entfernen**

Parameter	Beschreibung
Name der Vorlage / Name	Name der Kopfzeile (muss eindeutig sein).
Text	Platzhalter für Datum/Uhrzeit, Firmenname, Benutzername, Firmen-Rufnr., Seitennummer sowie Anzahl der Seiten können eingefügt werden.

28.4.5 Web Services

Unter **Web Services** sind die Funktionen für die Konfiguration der Web-Schnittstellen zusammengefasst, wie z . B. zu Web Collaboration.

28.4.5.1 Web Services > Web Collaboration

Für die Einbindung der Web Collaboration über einen Public Server (Web Collaboration Server als Dienst im Internet) oder über einen Custom Server (Web Collaboration Server im Kundennetz oder bei einem Partner).

Parameterbeschreibung der Registerkarten:

- **Web Collaboration Server**

Parameter	Beschreibung
Server Typ	Auswahl des Web Collaboration Servers.
Server-Typ: **Öffentlicher Server**	Der Web Collaboration Server ist ein Public Server und befindet sich im Internet. Dafür wird eine gesicherte https-Verbindung verwendet. Zusätzlich wird eine Lizenznummer und ein Passwort benötigt. Standardmäßig wird dafür der TCP-Port 5100 verwendet.
Server-Typ: **Öffentlicher Server (Demomodus/ Evaluierungsmodus)**	Die Web Collaboration kann 5 min lang getestet werden. Dafür ist keine Eingabe von IP-Adresse, Lizenznummer und Passwort nötig.
Server-Typ: **Benutzerdefinierter Server**	Der Web Collaboration Server ist ein Custom Server und befindet sich im Kundennetz oder bei einem Partner. Dafür kann eine gesicherte https-Verbindung oder eine ungesicherte http-Verbindung verwendet werden. Bei Verbindung über https wird zusätzlich eine Lizenznummer und ein Passwort benötigt. Standardmäßig wird dafür der TCP-Port 5004 verwendet.
Server-Typ: **Kein Web Collaboration-Server**	Es wird kein Web Collaboration Server verwendet. Die Option zum Starten einer Web Collaboration Sitzung ist in den UC Clients deaktiviert.

URL / IP-Adresse	Eingabe der URL / IP-Adresse des entsprechenden Web Collaboration Servers. Public Server über https und Custom Server über https oder http.
	Beispiel:
	`http://<Webcollaboration Server IP Adresse>:5004/OscInterface`
	`https://<Webcollaboration Server IP Adresse>:5100/XMLRPSecure`

Lizenznummer	Lizenznummer für die gesicherte Verbindung zum Web Collaboration Server.
Kennwort	Passwort für die gesicherte Verbindung zum Web Collaboration Server.

28.4.6 Open Directory Service

Unter **Open Directory Service** sind die Funktionen für die Konfiguration von Open Directory Service zusammengefasst.

28.4.6.1 Open Directory Service > Grundeinstellungen

Parameter	Beschreibung
Aktivieren/Deaktivieren des Open Directory Service	Standardwert: Deaktiviert
LDAP-Server Login-Daten	Login-Daten des externen Datenbankservers. Open Directory Service muss berechtigt sein, auf die externe Datenbank zuzugreifen, ggf. muss in dem Server ein eigener Benutzer hinzugefügt werden.

28.4.6.2 Open Directory Service > Data Sources > OpenScape Business-Benutzer

Parameterbeschreibung der Registerkarten:

- **Übersicht der konfigurierten Datenquellen**

Parameter	Beschreibung
OpenScape Business-Benutzer	Internes Verzeichnis der UC Suite. Das Verzeichnis ist dauerhaft dem Open Directory Service zugeordnet und kann nicht gelöscht oder geändert werden.
UC Suite Externes Verzeichnis	Externe Datenquelle für UC Suite-Systeme. Das Verzeichnis ist dauerhaft dem Open Directory Service zugeordnet und kann nicht gelöscht oder geändert werden.
Globales Verzeichnis	Globale Verzeichnisdatenquelle für Nicht-UC Suite-Systeme. Das Verzeichnis ist dauerhaft dem Open Directory Service zugeordnet und kann nicht gelöscht oder geändert werden.
Kurzwahlliste	Zentrale Kurzwahlnummern. Das Verzeichnis ist dauerhaft dem Open Directory Service zugeordnet und kann nicht gelöscht oder geändert werden.
Hinzufügen/Bearbeiten/ Löschen	Externe Datenquellen für Kontaktinformationen aus Datenbanken mit Lesezugriff über ODBC.

Parameterbeschreibung der Registerkarten::

- **Datenquelle bearbeiten**

Parameter	Beschreibung
Neue Datenquelle	Die Parameter der hinzugefügten Datenquellen können hier geändert werden.

28.4.6.3 Open Directory Service > Datenquellen > LXV3

Parameter	Beschreibung
Kurzwahlliste	Zentrale Kurzwahlnummern. Das Verzeichnis ist Open Directory Service fest zugeordnet und kann nicht gelöscht oder geändert werden.

28.4.6.4 Open Directory Service > Datenquellen > LXV3

Parameter	Beschreibung
Überblick über die konfigurierten Datenquellen	Eine LDAP-Ausgabezuordnung legt fest, welche der Felder des Datenschemas von Open Directory Service via LDAP ausgegeben werden sollen, z.B. für spezifische LDAP-Clients oder für verschiedene Gruppen von Teilnehmern, welche nicht alle Details sehen sollen, sondern nur eine definierte Untermenge. Die LDAP-Ausgabezuordnung web steht standardmäßig zur Verfügung und kann nicht gelöscht oder geändert werden. In ihr sind alle Felder des Datenschemas von Open Directory Service der LDAP-Ausgabe fest zugeordnet. Sie können zudem weitere LDAP-Ausgabezuordnungen konfigurieren.
Hinzufügen	Weitere Ausgabezuordnungen hinzufügen. Über den Parameter dc im LDAP-Login können LDAP-Clients auf eine bestimmte LDAP-Ausgabezuordnung zugreifen, z.B.: dc=web.

28.4.6.5 Open Directory Service > Wartung

Parameterbeschreibung der Registerkarten:

- **Wartung**

Parameter	Beschreibung
Open Directory Service prüfen/neu starten	Statusanzeige des Open Directory Service (grau = deaktiviert, rot = Konfiguration fehlerhaft oder Datenquelle nicht verfügbar, grün = aktiviert)
Neustart	Neustart des Open Directory Service

28.4.7 Application Launcher

Unter **Application Launcher** sind die Funktionen für die Konfiguration von Application Launcher zusammengefasst.

28.4.7.1 Application Launcher

Parameter	Beschreibung
Hochladen der Konfigurationsdatei	Profil mit Konfigurationsdaten von Application Launcher zur schnellen Konfiguration von Application Launcher auf allen Client-PCs. Sobald Application Launcher für einen ersten Benutzer vollständig konfiguriert ist, können Sie als Administrator dessen Profil mit den Konfigurationsdaten von Application Launcher im Kommunikationssystem bereitstellen. Anschließend können alle Benutzer die Konfiguration von Application Launcher durch Importieren dieses Profils durchführen.
Profil	Erlaubter Dateityp .xml

28.5 Middleware

Die Funktionen zur Konfiguration der Middleware sind unter **Middleware** zusammengefasst.

28.5.1 Ansage-Player

Parameterbeschreibung der Registerkarten:

- **Einstellungen für Ansage-Player**
- **Statistiken für Ansage-Player**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung des Abspiel-Gerätes für Ansagen.
Statistiken für Ansage-Player	Hier wird der Status des Ansage-Gerätes angezeigt. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aufgefrischt werden.

28.5.2 Csta Message Dispatcher (CMD)

Parameterbeschreibung der Registerkarten:

- **Einstellungen - CSTA Message Dispatcher (CMD)**
- **Statistiken - CSTA Message Dispatcher (CMD)**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung des CSTA Message Dispatchers (CMD). Der CMD stellt die Verbindung zwischen den OpenScape Business TAPI 120 Clients und dem Kommunikationssystem her und ist für die Funktionalität notwendig.

Parameter	Beschreibung
Autom. Registrierung	
Autom. Registrierung des Clients aktiviert	Aktivierung oder Deaktivierung der automatischen Anmeldung der Clients. Automatische Anmeldung bedeutet, dass neue Einträge in der Liste der CTI-Firewall möglich sind. Dadurch wird die CTI-Firewall automatisch konfiguriert. Haben sich alle berechtigten Clients angemeldet, kann das Häkchen entfernt werden und neue Einträge in die CTI-Firewall werden verhindert. Ein PC kann berechtigt werden, eine bestimmte Nebenstelle zu kontrollieren. Die TAPI/CTI-Lizenzen müssen zusätzlich vergeben werden.
CTI Firewall	
Löschen	Einträge mit einem Häkchen in der Löschen-Spalte werden aus der Liste der berechtigten Clients entfernt, sobald auf die Schaltfläche **Übernehmen** geklickt wird. Eine Anmeldung wird dann abgewiesen, sofern nicht die automatische Registrierung aktiv ist.
Anwendungs-ID	Name des PC, von dem aus eine Nebenstelle kontrolliert werden kann. Durch Verwendung des PC-Namens kann für die OpenScape Business TAPI 120 PCs auch DHCP verwendet werden.
Rufnummer	Interne Rufnummer der Nebenstelle, die kontrolliert werden darf.
Statistiken - CSTA Message Dispatcher (CMD)	Hier wird der Status des CMD dargestellt. Im laufenden Betrieb kann kontrolliert werden, welche OpenScape Business TAPI 120 mit dem CMD verbunden sind, dass evtl. Lizenzen zugewiesen werden müssen. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

28.5.3 Csta Service Provider (CSP)

Parameterbeschreibung der Registerkarten:

- **Einstellungen - CSTA Service Provider (CSP)**
- **Statistiken - CSTA Service Provider (CSP)**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung des CSTA Service Providers (CSP). Der CSP wird für die UC-Suite, für den DSS-Server (Presence Manager, nur in Vernetzung), den OpenScape Business TAPI 170 und für externe CSTA-Applikationen benötigt.
CSTA-Zugang	
CSTA-Benutzer-ID / **CSTA-Benutzerpasswort**	OpenScape Business TAPI 170 und externe CSTA-Applikationen können sich nur mit den hier konfigurierten Benutzerkonto am CSP anmelden. Ist kein CSTA-Benutzer konfiguriert, ist die Verwendung von OpenScape Business TAPI 170 oder externen CSTA Applikationen am CSP nicht möglich.

Parameter	Beschreibung
Statistiken - CSTA Service Provider (CSP)	Hier wird der Status des CSP dargestellt. Man sieht wieviele und welche Applikationen mit dem CSP verbunden sind. Unbekannte Applikationen werden mit 'Default' dargestellt. Der Verbindungsstatus zu den einzelnen Knoten des Netzwerks / dem lokalen Knoten kann eingesehen werden. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

28.5.4 DSS-Server

Parameterbeschreibung der Registerkarten:

- **Einstellungen - DSS-Server**
- **Statistiken - DSS-Server**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung des DSS-Servers.
Statistiken - DSS-Server	Hier wird der Status des DSS-Servers dargestellt. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

28.5.5 Media Extension Bridge (MEB)

Parameterbeschreibung der Registerkarten:

- **Einstellungen - Media Extension Bridge (MEB)**
- **Statistiken - Media Extension Bridge (MEB)**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung der Media Extension Bridge.
Statistiken - Media Extension Bridge (MEB)	Hier wird der Status des MEB dargestellt. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

29 Anhang

Der Anhang enthält Referenzinformationen, wie zum Beispiel die unterstützten Sprachen, Standards, Ausbaugrenzen und Kapazitäten, Euro-ISDN-Leistungsmerkmale, Kennzahlen zur Aktivierung und Deaktivierung von Leistungsmerkmalen, Leistungsmerkmal-Codes über MFV und verwendete IP-Protokolle und Portnummern.

29.1 Unterstützte Standards

Hier erhalten Sie Informationen über die unterstützten Standards.

Ethernet

- RFC 894 Ethernet II Encapsulation
- IEEE 802.1Q Virtual LANs
- IEEE 802.2 Logical Link Control
- IEEE 802.3u 100BASE-T
- IEEE 802.3ab Gigabit Ethernet
- IEEE 802.3X Full Duplex Operation

IP-Routing

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 2822 Internet Message Format
- RFC 826 ARP
- RFC 2131 DHCP
- RFC 1918 IP Addressing
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1618 PPP over ISDN
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1877 PPP Internet Protocol Control Protocol
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC 3544 IP Header Compression over PPP

NAT

- RFC 2663 NAT

IPSec

- RFC 2401 Security Architecture for IP
- RFC 2402 AH - IP Authentication Header
- RFC 2403 IPsec Authentication - MD5
- RFC 2404 IPsec Authentication - SHA-1
- RFC 2405 IPsec Encryption - DES
- RFC 2406 ESP - IPsec encryption

- RFC 2407 IPsec DOI
- RFC 2408 ISAKMP
- RFC 2409 IKE
- RFC 2410 IPsec encryption - NULL
- RFC 2411 IP Security Document Roadmap
- RFC 2412 OAKLEY

SNMP

- RFC 1213 MIB-II

QoS

- IEEE 802.1p Priority Tagging
- RFC 1349 Type of Service in the IP Suite
- RFC 2475 An Architecture for Differentiated Services
- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Dienste

- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Codecs

- G.711
- G.729

VoIP über SIP

- RFC 2198 RTP Payload for Redundant Audio Data
- RFC 2327 SDP Session Description Protocol
- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 3261 SIP Session Initiation Protocol
- RFC 3262 Provisional Response Acknowledgement (PRACK) Early Media
- RFC 3263 SIP Locating Servers
- RFC 3264 An Offer/Answer Model with the Session Description Protocol
- RFC 3310 HTTP Digest Authentication
- RFC 3311 Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3489 STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method
- RFC 3550 RTP: Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing

- RFC 3891 The Session Initiation Protocol (SIP) Replaces Header

Andere

- RFC 959 FTP
- RFC 1305 NTPv3
- RFC 1951 DEFLATE

29.2 Euro-ISDN-Leistungsmerkmale

Die Euro-ISDN-Leistungsmerkmale können an jedem Euro-ISDN-Anschluss genutzt werden, wenn die vorhandene Hardware (z.B. Telefon oder ISDN-Karte) dafür ausgelegt ist. Die Leistungsmerkmale stehen entweder dauerhaft im Amt zur Verfügung oder werden per Kennzahl aktiviert/deaktiviert.

Die Verfügbarkeit der Leistungsmerkmale ist abhängig vom Netzanbieter. Einige der genannten Leistungsmerkmale sind kostenpflichtig.

Thema	Erklärung
Mehrfachrufnummer (MSN = Multiple Subscriber Number)	Jedem Mehrgeräteanschluss können mehrere Rufnummern zugeordnet werden. Die Zuordnung dieser Rufnummern zu den einzelnen Endgeräten kann der Anwender selber an den Endgeräten vornehmen.
Calling Line Identification Presentation (CLIP)	Die eigene Rufnummer wird zum angerufenen Teilnehmer übermittelt und erscheint z.B. im Display des Telefons oder wird bei Nichtabheben in der Anrufliste gespeichert. Falsche Rufnummern können nicht übermittelt werden. Allerdings kann die Durchwahl von TK-Anlagen nicht geprüft werden. Die Übermittlung der eigenen Rufnummer kann ständig oder fallweise unterdrückt werden.
Calling Line Identification Restriction (CLIR)	Die Übermittlung der Rufnummer kann auch dauerhaft oder fallweise abgeschaltet werden. Die Rufnummern-Anzeige beim B-Teilnehmer ist dann nur noch bei speziell dafür vorgesehene Anschlüsse möglich (Notruf, Polizei, Feuerwehr).
Rufnummernidentifikation/ Fangen (MCID = Malicious Call Identification)	Der Angerufene kann den anonymen Anrufer über die Vermittlungsstelle identifizieren lassen, auch wenn die Rufnummernübermittlung abgeschaltet ist. Dieses Leistungsmerkmal ist kostenpflichtig.
Umstecken am Bus (TP = Terminal Portability)	Dieses Leistungsmerkmal ermöglicht es Ihnen während einer bestehenden Verbindung das verwendete ISDN-Endgerät an einer anderen ISDN-Dose anzuschließen und das Gespräch fortzuführen. Das Gespräch muss vor dem Umstecken geparkt werden.
Subadressierung (SUB = Subaddressing)	Diese Funktion kann kostenpflichtig zusätzlich zur normalen Rufnummer genutzt werden. Mit dieser Subadressierung kann abhängig vom Anrufer ein anrufbares Endgerät gesteuert werden (z.B. Programm auf dem PC).

Thema	Erklärung
Teilnehmer zu Teilnehmer Zeichengabe (UUS = User-to-User-Signaling)	Während des Verbindungsauf- und abbaus können über den D-Kanal Informationen ausgetauscht werden. Die Übertragung ist in beide Richtungen möglich.
Geschlossene Benutzergruppe (CUG = Closed User Group)	Ist dieses Leistungsmerkmal aktiviert, sind keine Gespräche außerhalb der Benutzergruppe möglich (außer den Notrufnummern 110 und 112). Allerdings können auch Anrufer von außen gesperrt werden.
Anrufumleitung bei Besetzt (CFB = Call Forwarding Busy)	Diese Anrufweiterschaltung leitet Anrufe bei Besetzt an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufweiterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.
Direkte Anrufumleitung (CFU = Call Forwarding Unconditional)	Diese Anrufweiterschaltung leitet Anrufe sofort an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufweiterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.
Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply)	Diese Anrufweiterschaltung leitet Anrufe nach 20 Sekunden (bei nicht Erreichen) an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufweiterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.
Anklopfen (CW = Call Waiting)	Während einer bestehenden Verbindung wird ein weiterer Anrufer signalisiert. Der Anrufer hört währenddessen das Freizeichen. Die anklopfende Verbindung kann angenommen, abgelehnt oder einfach nur ignoriert werden.
Makeln (Hold = Call Hold)	Während einer bestehenden Verbindung kann durch Rückfrage eine zweite Verbindung aufgebaut werden. Wird zwischen den beiden Verbindungen hin und her geschaltet, spricht man von Makeln. Der wartende Gesprächsteilnehmer kann das andere aktive Gespräch nicht mithören.
Dreierkonferenz (3PTY = Three Party Service)	Zwei bestehende Verbindungen können zusammengeschaltet werden. Dadurch ist eine Telefonkonferenz mit 3 Teilnehmern möglich.
Automatischer Rückruf bei Besetzt (CCBS = Completion of Calls to Busy Subscriber)	Ist ein angerufener Teilnehmer besetzt, so kann dieses Leistungsmerkmal aktiviert werden. Sobald der Anschluss dieses Teilnehmers wieder frei ist, erhält man ein Signal. Bei Abheben des Hörers wird die Verbindung aufgebaut.
Gebührenanzeige am Ende des Gesprächs (AOCE = Advice of Charge (End))	Auf Wunsch lassen sich die Gesprächsgebühren am Ende des Gesprächs anzeigen. Eventuelle Rabatte und Tarife werden dabei nicht berücksichtigt.

Thema	Erklärung
Gebührenanzeige während des Gesprächs (AOCD = Advice of Charge (During))	Auf Wunsch lassen sich die Gesprächsgebühren während des Gesprächs anzeigen. Eventuelle Rabatte und Tarife werden dabei nicht berücksichtigt.

29.3 Verwendete Ports

Die OpenScape Business Systemkomponenten nutzen verschiedene Ports, die bei Bedarf in der Firewall freigeschaltet werden müssen. Für die Ports der Webbased Clients (z.B. myPortal to go) muss ein Port Forwarding im Router eingerichtet werden.

Eine tatsächliche und vollständige Liste aller verwendeten Ports von OpenScape Business finden Sie in der "Interface Management Database" (IFMD), die über das Partnerportal von Unify abgerufen werden kann (https://unify.com/en/partners/partner-portal.

Anmerkung: Die in der folgenden Liste mit "O" identifizierten Ports sind optional, d. h. Sie sind in der Firewall nicht dauerhaft geöffnet.

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Systemkomponenten							
Admin Portal (https)	X		443	X	X	X	X
CAR-Lebendigkeitsprüfungen	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (bis zu V3R3) 7780, 7791 (ab V3R3.1 und höher)	O		O	
Communication Client-Installationsprogramm	X		8101	X	X	X	X
Csta Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
Csta Service Provider (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP Server	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
xNAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
xOpenfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X
OpenScape Business Benutzerportal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (eingebettet)		X	29100-30530	X	X	X	X
RTP (Server)		X	29100-30888	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (Traps)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

Anmerkung: Aus Sicherheitsgründen wird empfohlen für die Webbased Clients ausschließlich https zu verwenden und ein Port Forwarding von extern TCP/443 nach intern TCP/8802 einzurichten.

CLS-Zertifikat

Ab V3R3.1 wird über einen neu eingeführten Port ein neues CLS-Zertifikat mit aktualisiertem Common Name (CN) bereitgestellt. Dies bietet einen verbesserten und stärkeren Digest-Algorithmus sowie aktualisierte juristische Personen an. Die online über den CLS Connect-Modus lizenzierten Systeme erfordern die folgenden zwei Voraussetzungen:

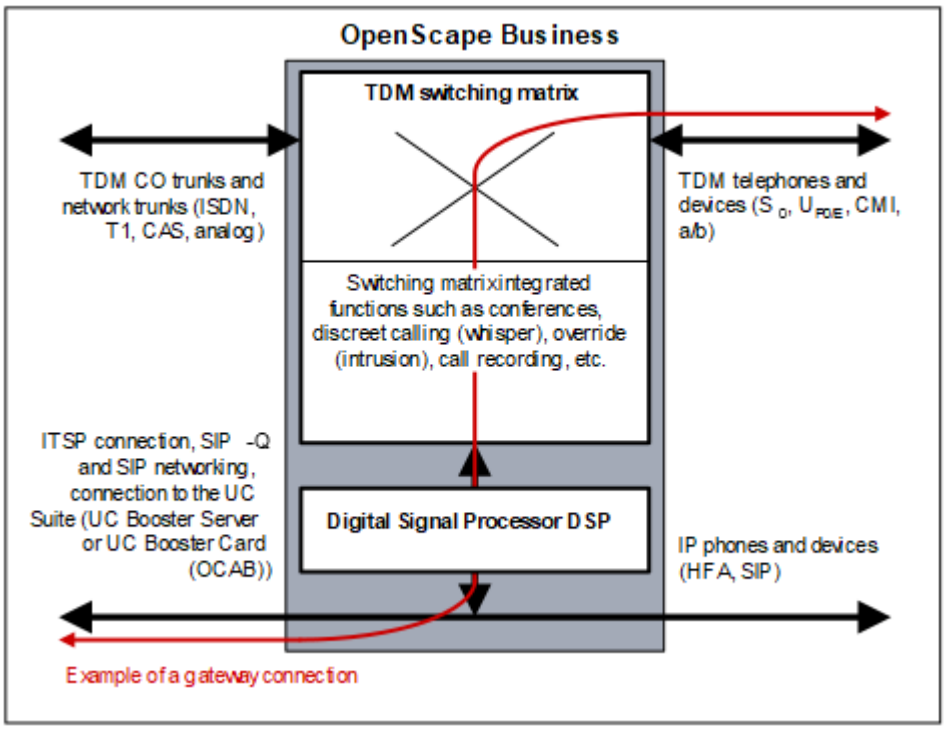
- Die IP-Adresse 188.64.16.4 ist für ausgehenden Datenverkehr in der Firewall aktiviert.
- Die Ports 7780 und 7791 sind für ausgehenden Datenverkehr in der Firewall aktiviert.

Der zuvor verwendete Port 7790 kann nach dem Upgrade auf V3R3.1 aus der Firewall-Konfiguration entfernt werden, um die Sicherheit zu erhöhen.

29.4 Projektierung der DSP-Kanäle für die Kommunikationssysteme OpenScape Business X3/X5/X8

Verbindungen zwischen IP- und TDM-Telefonen/-Leitungen sind sogenannte Gateway-Verbindungen, für die jeweils ein DSP (Digital Signal Processor)-Kanal benötigt wird. Darüber hinaus werden DSP-Kanäle bei Aktivierung des Leistungsmerkmals Signaling And Payload Encryption SPE benötigt.

Keine DSP-Kanäle werden für reine TDM-Verbindungen und für reine IP-Verbindungen benötigt.



Die Mainboards der Kommunikationssysteme OpenScape Business X3/X5/X8 stellen maximal acht DSP-Kanäle zur Verfügung.

Reichen die DSP-Kanäle eines Mainboards nicht aus, können weitere Kanäle durch das Stecken einer Voice Channel Booster Card (Submodul OCCB1 oder OCCB3) bereitgestellt werden:

- OCCB1 stellt bis zu 40 zusätzliche DSP-Kanäle zur Verfügung.
- OCCB3 stellt maximal 120 zusätzliche DSP-Kanäle zur Verfügung.

Die Anzahl der für Gateway-Verbindungen zur Verfügung stehenden DSP-Kanäle verringert sich durch die Verwendung des Codecs G.729 und durch die Nutzung von Signaling And Payload Encryption SPE.

Letztendlich bestimmt die Anzahl der gleichzeitigen Gateway-Verbindungen (der gleichzeitigen Sprachverbindungen mit IP-TDM-Übergang), ob ein OCCB-Submodul und welches OCCB-Submodul einzusetzen ist.

Im Fall von UC-Suite Konferenzen und IP-Telefonen kann ein Kommunikationssystem OpenScape Business X3/X5/X8 bis zu acht DSP-Kanäle umfassen. Standardmäßig werden drei DSP-Kanäle für die 3 Standard-Codecs der Wartemusik zugewiesen . Diese Zahl kann verringert werden, wenn Sie weniger Codecs für die Wartemusik verwenden. Zusätzlich sind zwei DSP-Kanäle für die Konfiguration der Signaling and Payload Encryption (SPE) reserviert. Der Rest der DSP-Kanäle kann den IP-Telefonen zugewiesen werden (ein DSP-Kanal pro IP-Telefon). Wenn die vorhandenen DSP-Kanäle erschöpft sind, kann die Anzahl der DSP-Kanäle durch die Verwendung der entsprechenden OCCB-Karten (OCCB1 oder OCCB3, wie zuvor angegeben) erhöht werden.

Tipp: Weitere Angaben zu den maximal zur Verfügung stehenden DSP-Kanälen der Mainboards und der OCCB-Submodule finden Sie unter Systembedingte Ausbaugrenzen.

Bei einer Unterdimensionierung von DSP-Kanälen kann es zu DSP-Engpässen kommen, die sich beispielsweise durch Besetztzustände beim Verbindungsaufbau äußern (Besetztton beim Verbindungsaufbau, Displayanzeige `Zur Zeit nicht möglich`).

Bei Auftreten eines DSP-Engpasses erfolgt ein Eintrag in der Event-Protokolldatei (Event Log) des Kommunikationssystems.

Folgende Maßnahmen sind bei häufigem Auftreten von DSP-Engpässen zu ergreifen:

Wenn	Dann
Die DSP-Kanäle des Mainboards werden genutzt.	Submodul OCCB1 oder OCCB3 auf dem Mainboard einsetzen.
Die DSP-Kanäle des Mainboards und des Submoduls OCCB1 werden genutzt.	Submodul OCCB3 auf dem Mainboard einsetzen.
Die DSP-Kanäle des Mainboards und des Submoduls OCCB3 werden genutzt.	Zu prüfen ist, ob das Kommunikationssystem ausschließlich mit Codec G.711 betrieben werden kann. Dadurch erhöht sich die Anzahl der DSP-Kanäle auf das Maximum. ***INFO:*** Die Option **Ausschließlich G.711 verwenden** kann durch einen Administrator mit dem Profil **Experte** im **Experten-Modus** (**Telephonie** > **Sprachgateway** > **Codec-Parameter**) aktiviert werden.

Die folgende Tabelle liefert Orientierungswerte, ob und welches OCCB-Submodul einzusetzen ist.

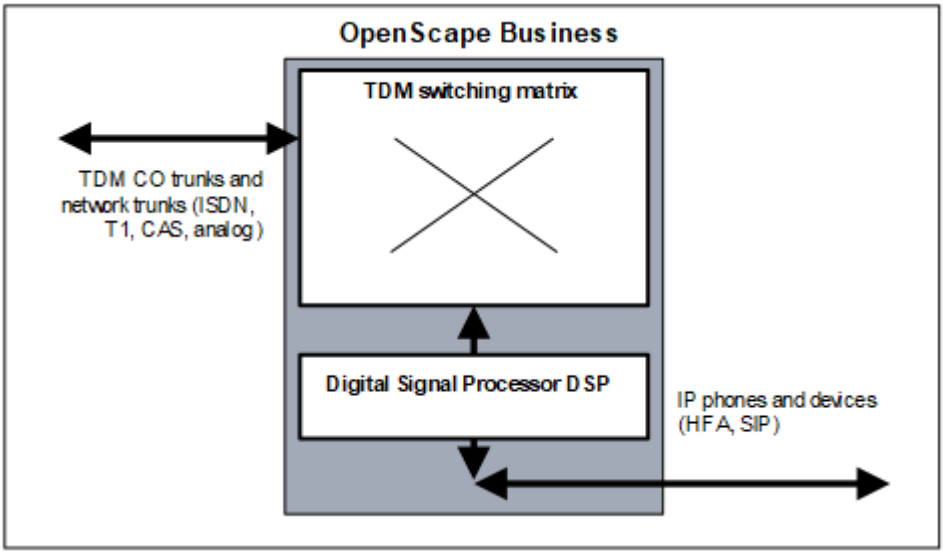
Summe der TDM-Kanäle: Amts- und Vernetzungsleitunge (ISDN, T1, CAS, analog)	Summe der IP-Kanäle: ITSP-Anschaltung, SIP-Q- und SIP-Vernetzung, Verbindung zur UC Suite (UC Booster Server oder UC Booster Card (OCAB))	**Summe der TDM-Telefone und TDM-Geräte (S_0, $U_{P0/E}$, CMI, a/b)**	**Summe der IP-Telefone und IP-Geräte (HFA, SIP)**	**Welches OCCB-Submodul?**	**Bemerkungen**
beliebig viele	Ansagen (bis zu 16) 0	beliebig viele	0	Kein OCCB-Submodul	Smart VM und Systemkonferenzen werden durch das Koppelfeld verarbeitet.

Summe der TDM-Kanäle: Amts- und Vernetzungsleitunge (ISDN, T1, CAS, analog)	Summe der IP-Kanäle: ITSP-Anschaltung, SIP-Q- und SIP-Vernetzung, Verbindung zur UC Suite (UC Booster Server oder UC Booster Card (OCAB))	**Summe der TDM-Telefone und TDM-Geräte (S_0, $U_{P0/E}$, CMI, a/b)**	**Summe der IP-Telefone und IP-Geräte (HFA, SIP)**	**Welches OCCB-Submodul?**	**Bemerkungen**
			bis 8	Kein OCCB-Submodul	Unabhängig von den TDM-Kanälen. Smart VM und Systemkonferenzen in Kombination mit IP-Telefonen und IP-Geräten benötigen DSP-Ressourcen.
			9 bis 100	OCCB1	Unabhängig von den TDM-Kanälen. Smart VM und Systemkonferenzen in Kombination mit IP-Telefonen und IP-Geräten benötigen bis zu 40 DSP-Ressourcen gleichzeitig.
			> 100	OCCB3	Unabhängig von den TDM-Kanälen. Smart VM und Systemkonferenzen in Kombination mit IP-Telefonen und IP-Geräten benötigen bis zu 120 DSP-Ressourcen gleichzeitig.
	> 0	bis 8		Kein OCCB-Submodul	
	> 0	9 bis 100		OCCB1	Bis 40 gleichzeitig
	> 0	> 100		OCCB3	Bis 120 gleichzeitig
> 0	bis 8			Kein OCCB-Submodul	Kombination ist im wesentlichen bei SIP-Q und UC Suite relevant.

Summe der TDM-Kanäle: Amts- und Vernetzungsleitunge (ISDN, T1, CAS, analog)	Summe der IP-Kanäle: ITSP-Anschaltung, SIP-Q- und SIP-Vernetzung, Verbindung zur UC Suite (UC Booster Server oder UC Booster Card (OCAB))	**Summe der TDM-Telefone und TDM-Geräte (S_0, $U_{P0/E}$, CMI, a/b)**	**Summe der IP-Telefone und IP-Geräte (HFA, SIP)**	**Welches OCCB-Submodul?**	**Bemerkungen**
> 0	9 bis 40			OCCB1	Kombination ist im wesentlichen bei SIP-Q und UC Suite relevant.
> 0	> 40			OCCB3	Kombination ist im wesentlichen bei SIP-Q und UC Suite relevant.

Die folgenden Beispiele liefern Orientierungswerte, ob und welches OCCB-Submodul einzusetzen ist.

Beispiel 1: OpenScape Business mit TDM-Amtsleitungen und IP-Telefonen und -Geräten

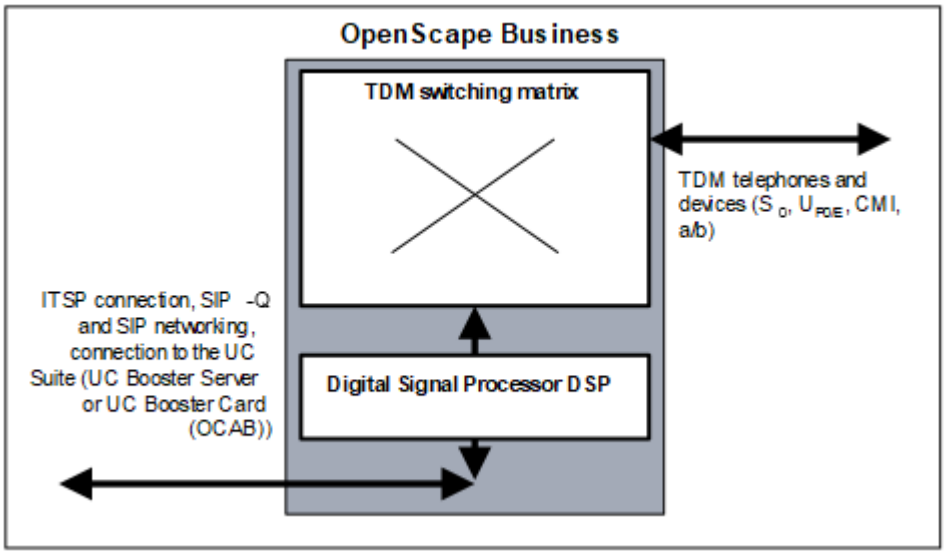


Wenn	Dann
OpenScape Business mit: • 1 x TDM-Amt (ISDN) • 20 x IP-Telefon (HFA, SIP)	Die DSP-Kanäle des Mainboards werden genutzt. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: • 1 x TDM-Amt (ISDN) • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB1 ist erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden.

Wenn	Dann
OpenScape Business mit: • 2 x TDM-Amt (ISDN) • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist erforderlich.
OpenScape Business mit: • 4 x TDM-Amt (ISDN) • 500 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist erforderlich. ***HINWEIS:*** Bei diesem Systemausbau darf ausschließlich der Codec G.711 verwendet werden, um die maximale Anzahl der DSP-Kanäle zu erreichen.

Soll das Kommunikationssystem auch mit TDM-Telefonen und -Geräten (S_0, $U_{P0/E}$, CMI, a/b) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

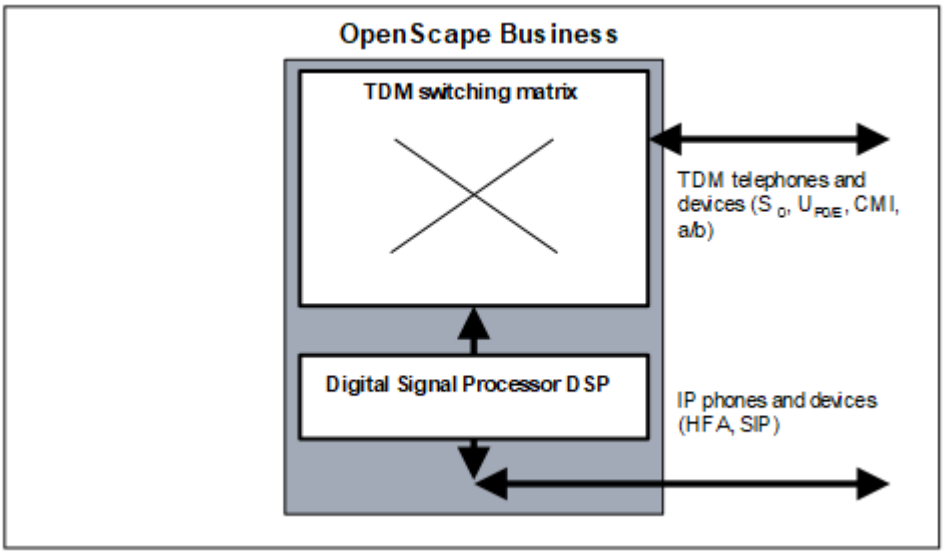
Beispiel 2: OpenScape Business mit ITSP-Verbindungen und TDM-Telefonen und -Geräten



Wenn	Dann
OpenScape Business mit: • 6 x ITSP-Anschaltung (6 B-Kanäle) • 20 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b)	Die DSP-Kanäle des Mainboards werden genutzt. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: • 30 x ITSP-Anschaltung (30 B-Kanäle) • 100 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b)	Submodul OCCB1 ist erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden.

Soll das Kommunikationssystem auch mit IP-Telefonen und -Geräten (HFA, SIP) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

Beispiel 3: OpenScape Business mit TDM-Telefonen und -Geräten und IP-Telefonen und Geräten



Wenn	Dann
OpenScape Business mit: • 6 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b) • 6 x IP-Telefon (HFA, SIP)	Die DSP-Kanäle des Mainboards werden genutzt. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: • 100 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b) • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist erforderlich.

Soll das Kommunikationssystem auch mit TDM-Leitungen oder IP-Leitungen ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

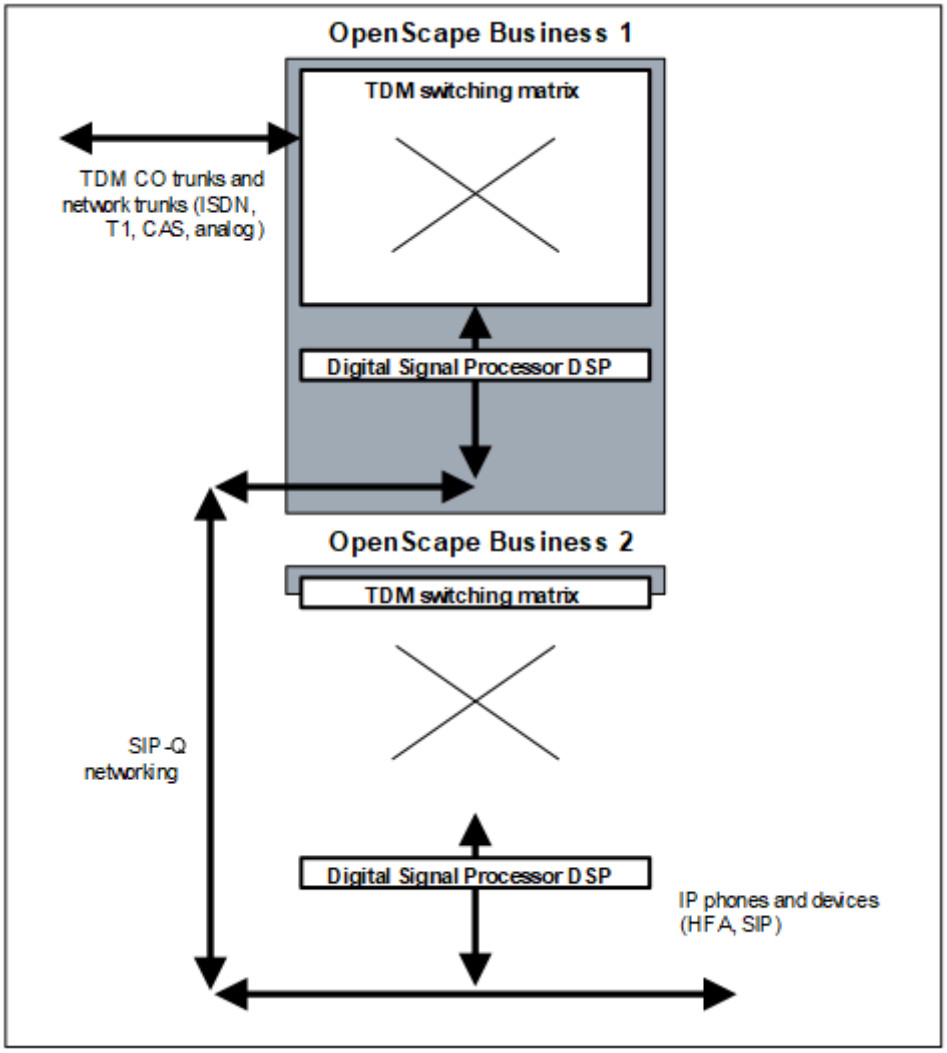
Beispiel 4: SIP-Q-Vernetzung OpenScape Business

Anmerkung: Dieses Beispiel beschreibt die Anforderungen eines vernetzten zweiten OpenScape Business Systems. Verbindungen im ersten System werden hier aus Gründen der Einfachheit nicht dargestellt. Allerdings sind auch die Anforderungen des ersten Systems, wie in den Beispielen 1, 2 und 3 angegeben, zu berücksichtigen.

Kommunikationssystem OpenScape Business 1 fungiert als Gateway zum TDM-Amt.

Ausschließlich am Kommunikationssystem OpenScape Business 2 sind IP-Telefone (HFA, SIP) angeschlossen.

In Abhängigkeit von der Anzahl der IP-Telefone am Kommunikationssystem OpenScape Business 2 sind die DSP-Kanäle für das Kommunikationssystem OpenScape Business 1 zu projektieren. DSP-Kanäle werden ausschließlich im TDM-Gateway benötigt.



Wenn	Dann
OpenScape Business 1 mit: • 1 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB1 ist in OpenScape Business 1 erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden. Kein OCCB-Submodul in OpenScape Business 2 erforderlich.
OpenScape Business 1 mit: • 2 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist in OpenScape Business 1 erforderlich. Kein OCCB-Submodul in OpenScape Business 2 erforderlich.

Wenn	Dann
OpenScape Business 1 mit: • 4 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 500 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist in OpenScape Business 1 erforderlich. ***HINWEIS:*** Bei diesem Systemausbau darf ausschließlich der Codec G.711 verwendet werden, um die maximale Anzahl der DSP-Kanäle zu erreichen. Kein OCCB-Submodul in OpenScape Business 2 erforderlich.

Soll das Kommunikationssystem OpenScape Business 2 auch mit TDM-Leitungen oder TDM-Telefonen und -Geräten (S_0, $U_{P0/E}$, CMI, a/b) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

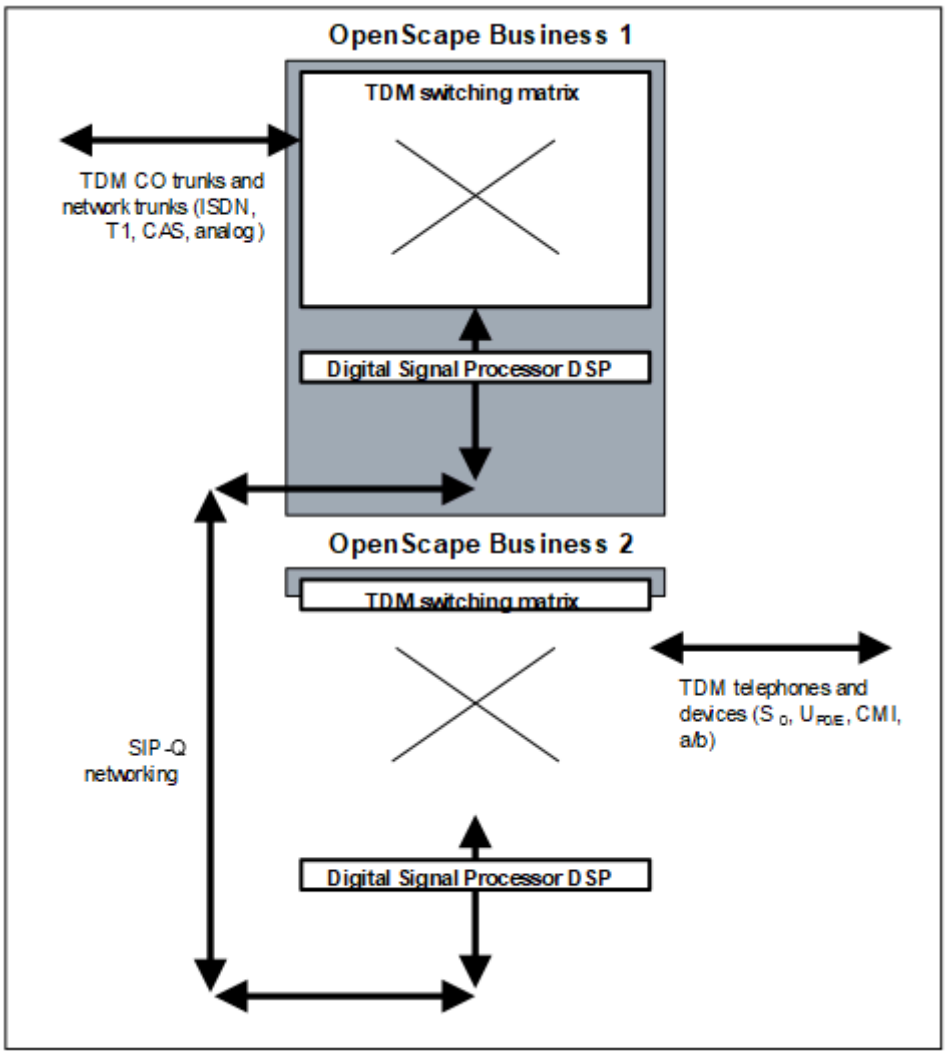
Beispiel 5: SIP-Q-Vernetzung OpenScape Business

Anmerkung: Dieses Beispiel beschreibt die Anforderungen eines vernetzten zweiten OpenScape Business Systems. Verbindungen im ersten System werden hier aus Gründen der Einfachheit nicht dargestellt. Allerdings sind auch die Anforderungen des ersten Systems, wie in den Beispielen 1, 2 und 3 angegeben, zu berücksichtigen.

Kommunikationssystem OpenScape Business 1 fungiert als Gateway zum TDM-Amt.

Ausschließlich am Kommunikationssystem OpenScape Business 2 sind TDM-Telefone (S_0, $U_{P0/E}$, CMI, a / b) angeschlossen.

Da in beiden Kommunikationssystemen Gateway-Verbindungen (OpenScape Business 1: TDM-Amt <-> SIP-Q-Vernetzung, OpenScape Business 2: SIP-Q-Vernetzung <-> TDM-Telefon) erforderlich sind, werden in beiden Systemen DSP-Kanäle benötigt.



Wenn	Dann
OpenScape Business 1 mit: • 1 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 100 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b)	Submodul OCCB1 ist in OpenScape Business 1 und in OpenScape Business 2 erforderlich. Alternativ kann jeweils Submodul OCCB3 eingesetzt werden.
OpenScape Business 1 mit: • 2 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 100 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b)	Submodul OCCB3 ist in OpenScape Business 1 und in OpenScape Business 2 erforderlich.

Soll das Kommunikationssystem OpenScape Business 1 auch mit TDM-Telefonen und -Geräten (S_0, $U_{P0/E}$, CMI, a/b) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

Beispiel 6: OpenScape Business mit IP-Telefonen und -Geräten

Anmerkung: Dieses Beispiel beschreibt die Anforderungen eines vernetzten zweiten OpenScape Business Systems. Verbindungen im ersten System werden hier aus Gründen der Einfachheit nicht dargestellt. Allerdings sind auch die Anforderungen des ersten Systems, wie in den Beispielen 1, 2 und 3 angegeben, zu berücksichtigen.

Wenn	Dann
OpenScape Business X3/X5/ X8 mit: • 7 x IP-Telefon (HFA, SIP)	Die DSP-Kanäle des Mainboards werden genutzt. Kein OCCB-Submodul erforderlich.
OpenScape Business: • 30 x IP-Telefon (HFA, SIP)	Submodul OCCB1 ist erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden.
OpenScape Business mit: • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist erforderlich.

30 Glossar

Das Glossar gibt kurze Erläuterungen zu verwendeten Begriffen (z.B. für Protokolle und Standards).

30.1 Glossar

10BaseT, 100BaseT, 1000BaseT

Hierbei handelt es sich um eine Spezifikation (IEEE 802.3i) für Netzwerke mit 10 MBit/s Basisbandübertragung über ein symmetrisches 100 Ohm Vierdrahtkabel. Dagegen steht 100BaseT für eine Bandbreite von bis zu 100 MBit/s und 1000BaseT für eine Bandbreite von bis zu 1000 MBit/s.

AES (Advanced Encryption Standard)

AES ist ein symmetrisches Kryptosystem, das als Nachfolger für DES bzw. 3DES vom National Institute of Standards and Technology als Standard bekannt gegeben wurde. Wird z.B. bei VPN verwendet.

ADSL mit dynamischer IP-Adresse

ADSL steht für Asymmetric Digital Subscriber Line und bedeutet, dass die Bandbreiten vom Internet (Download, Downstream) und zum Internet (Upload, Upstream) verschieden sind. ADSL entspricht dem klassischen DSL-Anschluss. Eine dynamische IP-Adresse ist ausreichend, wenn Sie die Web- und Email-Dienste vom Internet-Service-Provider bereitgestellt bekommen.

ADSL mit fester IP-Adresse

ADSL steht für Asymmetric Digital Subscriber Line und bedeutet, dass die Bandbreiten vom Internet (Download, Downstream) und zum Internet (Upload, Upstream) verschieden sind. ADSL entspricht dem klassischen DSL-Anschluss. ADSL mit fester IP-Adresse ist erforderlich, falls Sie eigene Web- und Email-Server an ihrem Standort betreiben möchten.

AF-EF (Expedited Forwarding - Assured Forwarding)

Die Codepunkte AF und EF legen die unterschiedlichen Priorisierungen von IP-Paketen bei QOS (Quality of Service) fest.

AF: Garantiert eine minimale Bandbreite für die Daten.

EF: Garantiert eine konstante Bandbreite für die Daten.

ARP (Address Resolution Protocol)

Das Address Resolution Protocol (ARP) ist ein Netzwerkprotokoll, das die Zuordnung von Netzwerkadressen zu Hardwareadressen möglich macht. Obwohl es nicht auf Ethernet- und IP-Protokolle beschränkt ist, wird es fast ausschließlich im Zusammenhang mit IP-Adressierung auf Ethernet-Netzen verwendet.

Authentifizierung

Authentication ist die Überprüfung der Identität einer Person oder eines PCs. Die Überprüfung kann mit einem einfachen Benutzernamen, aber z.B. auch mittels Fingerabdruck durchgeführt werden.

Authorization (Autorisation)

Authorization ist das Gewähren von Rechten, z.B. Zugriffsrechten im Datennetz.

B-Kanal

B-Kanal ist der Übertragungsweg für die Nutzdaten (Sprache, Daten) einer ISDN-Verbindung.

BLF Belegtlampenfeld

myPortal bietet ein sogenanntes Belegtlampenfeld BLF um den Gesprächszustand von hinterlegten Teilnehmern optisch anzuzeigen.

Broadcast

Ein Broadcast ist ein Rundruf in einem PC-Netzwerk. Dabei wird eine Nachricht (ein Datenpaket) von einem Punkt aus an alle Teilnehmer eines Netzes übertragen. Ein Broadcast wird in einem Datennetz verwendet, wenn die Adresse des Empfängers der Nachricht unbekannt ist.

CA (Certification Authority)

CA ist eine Organisation, die Zertifikate mit digitalen Signaturen ausstellt. Digitale Signaturen werden z.B. bei VPN (Virtual Private Network) benötigt.

CAPI-Schnittstelle (Common Application Programming Interface)

CAPI ist eine ISDN-konforme standardisierte Software-Schnittstelle. CAPI ermöglicht die Erstellung von ISDN-Software ohne Kenntnisse der herstellerspezifischen ISDN-Hardware.

Centrex

Centrex (Central Office Exchange) stellt Funktionen einer Telefonanlage via PSTN oder via ITSP bereit. Dies wird auch als virtuelle Telefonanlage, Hosted PBX (Private Branch Exchange) oder NetPBX bezeichnet.

CHAP (Challenge Handshake Authentication Protocol)

CHAP ist ein Authentifizierungsprotokoll, das im Rahmen des Point-to-Point-Protokolls eingesetzt wird.

COS (Class of Service)

QoS ist ein Verfahren, das die Übertragungsqualität von Daten in IP-Netzen gewährleistet.

CLIP (Calling Line Identification Presentation)

Durch die Rufnummernübermittlung wird die Rufnummer des Anrufers dem angerufenen Teilnehmer angezeigt. Der angerufene Teilnehmer kann dadurch vor der Gesprächsannahme den Anrufer identifizieren.

CLIR (Calling Line Identification Restriction)

Der Anrufer unterdrückt die Anzeige seine Rufnummer beim angerufenen Teilnehmer. Der angerufene Teilnehmer kann dadurch den Anrufer vor der Gesprächsannahme nicht identifizieren.

COLP (Connected Line Identification Presentation)

Mit Rufnummernübermittlung des Angerufenen wird dem Anrufer die Rufnummer des angerufenen Teilnehmers angezeigt, wenn die Verbindung zustandegekommen ist.

COLR (Connected Line Identification Restriction)

Mit Rufnummernunterdrückung des Angerufenen wird die Rufnummer vom angerufenen Teilnehmer beim Anrufer unterdrückt, obwohl der Anrufer COLP aktiviert hat.

Comfort User

Comfort User ist der Standart Benutzer des Kommunikationssystems.

Comfort Plus User

Der Comfort Plus User ist der Advanced User (Benutzer) des Kommunikationssystems. Im Gegensatz zum Comfort User kann der Comfort Plus User mehr Leistungsmerkmale (wie Fax, Mobility, Conferencing) nutzen.

CorNet

CorNet ist ein proprietäres Protokoll zur Vernetzung der HiPath- und OpenScape-Kommunikationssysteme. Im Gegensatz zum allgemein unterstützten QSIG sind in CorNet alle herstellerspezifischen Leistungsmerkmale der HiPath- und OpenScape-Kommunikationssysteme integriert.

CorNet-IP

CorNet-IP ist eine Protokollvariante von CorNet, welche eine Quervernetzung von Anlagen oder die Anbindung von Systemtelefonen (z.B. optiPoint) über IP ermöglicht.

CorNet-NQ

Ein proprietäres QSIG-basiertes Signalisierungsprotokoll für die Verbindung von Kommunikationssystemen mit einem oder mehreren QSIG-TK-Anlagen.

CSTA (PC Supported Telecommunications Applications)

CSTA ist eine Protokollschnittstelle für Anwendungen, die den European PC Manufacturers Association (ECMA)-Standard unterstützen. Über CSTA werden die Telekommunikationsaktivitäten über SIP gesteuert und überwacht.

CSV (Character Separated Values)

Eine CSV-Datei ist eine Textdatei zur Speicherung oder zum Austausch einfach strukturierter Daten. CSV steht dabei für Character Separated Values bzw. Comma Separated Values oder Colon Separated Values, weil die einzelnen Werte durch ein spezielles Trennzeichen, beispielsweise ein Komma oder ein Semikolon, getrennt werden. CSV-Dateien müssen im ANSI/ASCII-Format vorliegen.

CRL (Certificate Revocation Lists)

Eine CRL Zertifikatswiderrufliste ist eine Aufstellung sämtlicher widerrufener Zertifikate. CRLs müssen immer von der Zertifizierungsstelle erzeugt werden, von der die Zertifikate stammen.

Delay

Ein Delay hat in der Telekommunikation zwei Bedeutungen:

- Das Zeitintervall, um das ein Ereignis verzögert wird.
- Die Zeit zwischen dem Auftreten eines Ereignisses und dem Auftreten eines erwarteten Folgeereignisses.

Dedicated (dediziertes, fest zugeordnetes) Gateway

Wenn im LCR ein Dedicated Gateway für eine Richtung eingetragen ist, so wird zwingend über dieses Gateway geroutet. Anderslautende Regeln für das Routing sind dann ungültig.

DHCP (Dynamic Host Configuration Protocol)

DHCP ist ein Verfahren um einem PC beim Start bestimmte IP-Konfigurationen (IP-Adresse, Subnetzmaske, usw.) zugewiesen werden.

DS (DiffServ, Differentiated Services)

DS ist ein Verfahren zur Paketverwaltung in Datennetzen. Es wird angegeben, wie ein bestimmtes Datenpaket weitervermittelt werden soll und gibt einen bestimmten Service-Level in Bezug auf Bandbreite, Queueing-Theorie und Paketverwerfungs-Entscheidungen vor.

Diffie-Hellman-Algorithmus

Der Diffie-Hellman-Algorithmus dient dem Schlüsselaustausch bei VPN. Die aus diesem Algorithmus entstehenden Daten werden mit einem bestimmten Satz mathematischer Parameter konfiguriert. Damit der Schlüsselaustausch ordnungsgemäß funktioniert, müssen beide Teilnehmer identische Werte für diese Parameter verwenden.

DLI (Deployment License Service Integrated)

Über DLI kann man IP-Systemtelefone automatisch installieren und hochrüsten.

DMZ (Demilitarized Zone)

Eine DMZ (auch ent- oder demilitarisierte Zone) bezeichnet ein PC-Netzwerk mit sicherheitstechnisch kontrollierten Zugriffmöglichkeiten auf die daran angeschlossenen Netzwerkknoten (PC, Router, etc).

DNS (Domain Name Service)

Namensauflösung im Internet und auch im LAN. Namen von PCs oder Webseiten werden mittels DNS in die zugehörigen IP-Adressen umgesetzt.

DSL (Digital Subscriber Line)

DSL ist eine Technologie, um einen Internetzugang bereitzustellen, der über eine hohe Bandbreite verfügt. Mit der Technik DSL wird dabei die Strecke zwischen der Vermittlungsstelle des Providers und der Telefondose des Kunden überbrückt.

DSS (Direct Station Selection)

Die Funktionstasten eines Telefons oder Beistellgerätes können als Direktruftasten (DSS-Tasten) eingerichtet werden. Dafür werden diese mit der Rufnummer eines internen Teilnehmers oder einer Gruppe programmiert. Durch

Drücken einer DSS-Taste wird ein sofortiger Anruf zum programmierten Ziel ausgeführt.

DTMF (Dual Tone Multifrequency)

Siehe MFV.

EIM (Enterprise Instant Messaging)

EIM ist ein Instant Messaging Dienst, der auf privaten Servern in einem Unternehmen auf Plattformen wie dem Live Communications Server oder Office Communications Server 2007 von Microsoft ausgeführt wird.

Enterasys-Switche

Enterasys-Switche werden von Enterasys Networks als sichere Netzwerklösungen produziert. Die stapelbaren Switche erkennen QoS-Features, klassifizieren und priorisieren Voice-, Video- und Daten-Applikationen.

ESP (Encapsulating Security Payload)

Bei ESP handelt es sich um ein IPSec-Protokoll, durch das die Paketverschlüsselung, Paketintegrität sowie die Paketauthentizität sichergestellt wird. Die Integritäts- sowie Authentizitätsprüfung erstreckt sich hierbei jedoch nicht auf den IP-Header sondern nur auf die eigentlichen Daten (Payload).

FoIP (Fax over IP)

FoIP ist eine Mehtode der Übermittlung von Faxnachrichten über ein IP-Netzwerk.

FTP

Das File Transfer Protocol (Dateiübertragungsverfahren) FTP ist ein im RFC 959 spezifiziertes Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke.

Funktionskennzahlen

Funktionskennzahlen sind Einwahlnummern bzw. Pilotnummern für z.B. Parken, Konferenz und AutoAttendant. Funktionskennzahlen entsprechen dabei virtuellen Teilnehmern. In einem Netzverbund müssen Funktionskennzahlen immer eindeutig sein.

G.711

G.711 ist ein Standard zur Digitalisierung von analogen Audiosignalen. Er wird in der klassischen Festnetz-Telefonie verwendet (PCM-Technik). Auch bei VoIP ist G.711 eine mögliche Sprachcodierung.

G.729AB

G.729 bezeichnet einen Codec zur Komprimierung von Sprache in digitale Signale und wird in der IP-Telephonie eingesetzt. G.729 ist sehr rechenaufwändig. Eine etwas vereinfachte, qualitativ aber geringfügig unterlegene Variante stellt G.729AB dar, die dafür weniger Rechenleistung benötigt.

Gateway / Gatewaymodule

Ein Gateway ist der Ein- bzw. Ausgang zu einem Kommunikationsnetz, es verbindet zwei verschiedene Datenverkehrsströme.

GSM (Global System for Mobile Communications

GSM ist ein Standard für digitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungs- und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Messages) genutzt wird.

Handover

Als Handover bezeichnet man einen Vorgang in einem mobilen Kommunikationsnetz, bei dem das Mobiltelefon während eines Gesprächs oder einer Datenverbindung von einer Funkzelle in eine andere wechselt. Auch bei einem Wechsel zwischen GSM und UMTS mit einem Dual-Mode-Mobiltelefon spricht man von Handover.

Hash-Wert

Hash- bzw. Streuwerte sind meist skalare Werte aus einer Teilmenge der natürlichen Zahlen. Ein Hash-Wert wird auch als Fingerprint bezeichnet. Denn wie ein Fingerabdruck einen Menschen nahezu eindeutig identifiziert, ist ein Hash-Wert eine nahezu eindeutige Kennzeichnung einer Menge.

H.323

H.323 bezeichnet eine Gruppe von Standards, die eine Reihe von Medientypen für Paketnetze definieren. Die Standards decken Sprache, Daten, Fax und Video ab und definieren, wie Signale von analog in digital umgewandelt werden und welche Signalisierung verwendet werden soll.

OpenScape Business Assistant

OpenScape Business Assistant dient der Administration des Kommunikationssystems. Hier finden sie alle Wizards zur schnellen Unterstützung von Administrationsaufgaben.

Hosted Services

Hosted Services oder Gehostete Dienste sind traditionelle IT-Dienste wie E-Mail, Instant Messaging IM und Unified Communications UC, die ein Internet Provider einem Unternehmen von einem Remote-Standort aus bereitstellt; sodass für das Unternehmen die Notwendigkeit entfällt, diese Dienste auf eigenen Servern vor Ort zu verwalten und auszuführen.

ICMP (Internet Control Message Protocol)

ICMP dient in Datennetzen zum Austausch von Informations- und Fehlermeldungen über das Internet-Protokoll IP.

IDS (Intrusion Detection System)

IDS ist ein Sicherheitssystem, das alle ein- und ausgehenden Netzwerkaktivitäten überwacht, um mögliche Sicherheitsverletzungen zu identifizieren. Hierzu gehört sowohl das Eindringen (Angriffe von außerhalb der Organisation) als auch der Missbrauch (Angriffe von innerhalb der Organisation).

IEEE-Standards

IEEE-Standards sind ein Satz von Spezifikationen, die vom Institute of Electrical and Electronic Engineers (IEEE) definiert wurden (zum Beispiel Token Ring, Ethernet), um gemeinsame Netzwerkstandards für Hersteller einzurichten.

IEEE. 802.1p

IEEE. 802.1p ist ein Standard der IEEE, der den Transport von Datenpaketen unterschiedlicher Priorität in Rechnernetzwerken regelt. Die Datenpakete werden in Prioritätsklassen von 1 bis 7 eingeteilt. Der Standard legt nur fest das die Priorität von 1 bis 7 steigt, trifft aber keine weitergehenden Aussagen darüber wie die Datenpakete im einzelnen behandelt werden sollen.

IKE-Protokoll

Das IKE -Protokoll hat zwei verschiedene Aufgaben. Zunächst ist eine ausschließlich vom IKE-Protokoll genutzte SA (Security Association) herzustellen (IKE-SA). Anschließend wird die vorhandene IKE-SA zur sicheren Aushandlung aller weiteren für die Übertragung von Payload-Daten benötigten SAs (Payload-SA) genutzt.

IM (Instant Messaging)

IM ist ein Verfahren zum Echtzeitaustausch von Textnachrichten über das Internet mithilfe von PCs, Pocket-PCs und Mobiletelefonen. Moderne IM-Dienste ermöglichen VoIP und Videokonferenzen, Dateitransfer und Desktop-Application-Sharing.

IP PBX

IP PBX ist eine Kommunikationsanlage, die sowohl VoIP-Verbindungen als auch Sprachverbindungen über herkömmliche Telefonleitungen unterstützt.

IPSec

IPSec ist ein Gerüst offener Standards für die Gewährleistung vertraulicher, sicherer Kommunikationsverbindungen über IP-Netzwerke durch Einsatz verschiedener Sicherheitsdienste und -protokolle.

ISP (Internet-Service-Provider)

Ein ISP ist ein Unternehmen, das Einzelpersonen, Firmen und anderen Organisationen Dienste zur Anbindung an das Internet anbietet. Einige ISPs sind große nationale oder internationale Unternehmen, die den Zugang an einer Vielzahl von Standorten anbieten, während andere ISPs auf einzelne Orte oder Regionen beschränkt sind.

ITSP (Internet-Telefonie-Service-Provider)

Ein ITSP ist ein Unternehmen, das Einzelpersonen, Firmen und anderen Organisationen Telefondienste über das Internet anbietet.

IWV (Impulswahlverfahren)

IWV ist das älteste Signalisierungsverfahren der automatischen Telefonvermittlung. IWV ist heute meistens von MFV abgelöst.

Jitter

Unter Jitter versteht man eine Verzögerung von Datenpaketen bei Sprachübertragungen. Eine zu große Verzögerung zwischen dem Senden von Datenpaketen und ihrem Eingang am empfangenden Ende macht die Sprachkommunikation unregelmäßig und schwer verständlich.

KWI (Kurzwahl individuell)

Mit Hilfe der Kurzwahl individuell KWI können zusätzlich zur Kurzwahl zentral von jedem dazu berechtigtem Telefon 10 externe individuelle Kurzwahlnummern gespeichert werden.

KWZ (Kurzwahl zentral)

Häufig benötigte externe Telefonnummern können im Systemspeicher des Kommunikationssystems hinterlegt werden. Jede Nummer wird durch eine Kurzwahlnummer vertreten, die anstelle der vollständigen Telefonnummer von allen Teilnehmern genutzt werden kann.

Latenz

Unter Latenz versteht man die Zeit, die für den Transport eines Datenpakets von einer Anwendung zur anderen benötigt wird, einschließlich der Zeitdauer für die Übermittlung über das Netzwerk und für die Vorbereitung und Verarbeitung der Daten am sendenden und am empfangenden Gerät.

LCR (Least Cost Routing, Leitweglenkung)

Mit Hilfe von LCR (Least Cost Routing, Leitwenkung) legen Sie fest, über welchen Anbieter z.B. Amts, Handy- oder Auslandsgespräche geführt werden. Sie legen über das Kommunikationssystem den kostengünstigsten Anbieter fest und führen alle entsprechenden Gespräche über diesen definierten Weg.

LIN (Location Identification Number)

LIN ist eine eindeutige max. 16stellige Nummer, die dem 10-stelligen NANP (North American Numbering Plan) entspricht.

LWCA (Leightweight CA)

LWCA ist eine eingeschränkte Zertifizierungsfunktion.

Media Stream Channel

Ein Media Gateway kann leitungsvermittelte B-Kanäle des ISDN terminieren und aus der darin übertragenen Sprachinformation Media Stream Channels für ein IP-basiertes Paket-Netzwerk erzeugen. Media Stream Channels enthalten eine Kombination von Audio-, Video-, und T.120-Medien.

DTMF (Dual Tone Multifrequency)

Das Mehrfrequenzwahlverfahren MFV (auch Tonwahlverfahren) ist das Wahlverfahren in der analogen Telefontechnik und das heute überwiegend in der Vermittlungstechnik genutzte Verfahren zur Übermittlung der Rufnummer an das Telefonnetz.

MIM (Mobile Instant Messaging)

MIM ist ein Presence- und Instant-Messaging-Dienst für mobile Telefone.

Mobility

Mobility bezeichnet die Nutzung von Pocket-PCs und mobilen Telefonen und deren Integration in das Kommunikationssystem einer Firma.

MOH (Music on Hold)

Anrufern kann Wartemusik (MOH, Music on Hold) eingespielt werden, wenn diese nicht sofort vermittelt werden können.

MSN (Multiple Subscriber Number)

Beim Anschluss von ISDN-Telefonen über einen S0-Bus (Mehrgeräteanschluss) wird jedem einzelnen ISDN-Telefon (ISDN-Teilnehmer) eine eindeutige Multiple Subscriber Number MSN zugeordnet. Die ISDN-Teilnehmer sind über ihre MSN erreichbar.

MULAP (Multiple Line Appearance)

MULAPs sind spezielle Gruppen in denen mehrere Telefone zusammengefasst sind. Einem Gruppenmitglied können dabei unter einer Rufnummer mehrere Telefone zugeordnet werden (Basic-MULAP). Außerdem können in einer solchen Gruppe spezielle Leistungsmerkmale, die für die Kommunikation zwischen Chef und Sekretär bzw. in Teams erforderlich sind, realisiert werden (Chef-MULAP, Team-MULAP).

Multi-Gateway

Bei einer Multi-Gateway-Vernetzung werden die Anrufe über mehrere, verschiedene Gateways geroutet.

myAttendant

myAttendant ist der Vermittlungsplatz des Kommunikationssystems.

myPortal

myPortal ist das Java-basierte Benutzerportal für den Zugriff der Teilnehmer auf die Unified Communications Funktionen. Neben Informationen über den Anwesenheitsstatus, komfortablen Wahlhilfen über Favoriten und Verzeichnisse, hat der Teilnehmer auch Zugriff auf Sprachnachrichten und Faxe.

myPortal for Outlook

myPortal for Outlook ist das in Microsoft Outlook integrierte Benutzerportal für den Zugriff der Teilnehmer auf die Unified Communication Funktionen, analog zu myPortal. Zusätzlich bietet myPortal for Outlook eine komfortable Desktop-Wahl.

NAC (Network Admission Control)

NAC ist eine Technologie, die die Abwehr von Viren und Würmern aus dem Netzwerk heraus unterstützt. Mit NAC werden Endgeräte während der Authentisierung auf Richtlinienkonformität geprüft. Ist z.B. der Virenscanner nicht aktuell oder fehlt dem Client-Betriebssystem der neueste Security-Patch, wird das betroffene Endgerät unter Quarantäne gestellt und mit aktuellen Updates versorgt bis es wieder den geltenden Sicherheitsrichtlinien entspricht.

NAT (Network Address Translation)

NAT ist ein Verfahren, um eine IP-Adresse in einem Datenpaket durch eine andere zu ersetzen. Dies wird genutzt, um private IP-Adressen auf öffentliche IP-Adressen abzubilden. Werden auch die Port-Nummern umgeschrieben, spricht man dabei von Maskieren oder PAT (Port Address Translation).

NTBA (Network Termination for ISDN Basic Access)

Ein NTBA (Network Termination for ISDN Basic Acces), oder auch NT (Network Termination) genannt, ist das Netzabschlussgerät für den ISDN-Basisanschluss . Er ist das Bindeglied zwischen dem digitalen Netz des Netzbetreibers und den ISDN-Einrichtungen auf der Teilnehmerseite.

NTPM (Network Termination for Primary Rate Multiplex Access)

Ein NTPM (Network Termination for Primary Rate Multiplex Access) ist das Netzabschlussgerät für den ISDN-Primärmultiplexanschluss. . Er ist das Bindeglied zwischen dem digitalen Netz des Netzbetreibers und den ISDN-Einrichtungen auf der Teilnehmerseite.

OLSR

OLSR ist ein spezielles Ad-hoc-Protokoll, mit dem es ermöglicht wird, die auf OSI-Schicht 2 fehlende Möglichkeit des Routing auf OSI-Schicht 3 nachzurüsten.

ONS (One Number Service)

Rufnummer, die einem Benutzer direkt zugeordnet ist. Einem Benutzer können mehrere Ressourcen (Telefone) zugeordnet werden. Wird er über die ONS-Nummer angerufen, wird der Anruf an das Telefon weitergeleitet, das der Benutzer aktuell nutzt (z.B. das Mobiltelefon).

PAP (Password Authentication Protocol)

PAP ist ein Verfahren zur Authentifizierung über das Point-to-Point-Protocol. Es wird für die Einwahl zu einem ISP verwendet. Bei PAP wird das Passwort für die Authentifizierung im Klartext zusammen mit einer User-ID übertragen.

PBX (Private Branch Exchange)

Eine PBX (Telefonanlage) ist eine Vermittlungseinrichtung, die mehrere Endgeräte wie zum Beispiel Telefon, Fax, Anrufbeantworter sowohl untereinander als auch mit dem öffentlichen Telefonnetz verbindet.

Peer

Als Peer wird der Endpunkt einer Kommunikation in einem Peer-to-Peer-Netzwerk bezeichnet. Jeder Peer bietet dabei seine Dienste an und nutzt die Dienste der anderen Peers.

Peer-to-Peer

In einem Peer-to-Peer-Netz sind alle PCs gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch Dienste zur Verfügung stellen.

Peer-Instanz-Authentifizierung

Die Authentifizierung der Peer-Instanz in einer Verbindung stellt sicher, dass diese den Angaben entspricht.

PKI (Public Key Infrastructure)

Mit PKI bezeichnet man in der Kryptologie und Kryptografie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung computergestützter Kommunikation verwendet.

PPP (Point-to-Point-Protokoll)

PPP ist ein IETF-Standard zur Übertragung von IP-Paketen über serielle Leitungen. PPP wird vor allem für die Einwahl ins Internet genutzt.

PPPoE (Point-to-Point-Protokoll over Ethernet)

Das PPPoE-Protokol (PPP over Ethernet) ist die Verwendung des Netzwerkprotokolls Point-to-Point über eine Ethernet-Verbindung.

Pre-Shared Key

Der Pre-shared Key ist ein Schlüssel, der bei der Tunnelkonfiguration (bei VPN) festgelegt wird. Damit sich die über den Tunnel kommunizierenden VPN-Partner, authentifizieren können, muss für beide Tunnelendpunkte das gleiche Kennwort verwendet werden.

PPTP (Point-to-Point-Tunneling-Protokoll)

PPTP ist eine Technologie, mit der ein Virtuelles Privates Netzwerk (VPN) eingerichtet werden kann. Da das Internet im Grunde ein offenes Netzwerk ist, wird mithilfe von PPTP sichergestellt, dass Nachrichten, die von einem VPN-Knoten zu einem anderen übertragen werden, sicher sind. Mit PPTP können sich Benutzer über das Internet in ihr Firmennetz einwählen.

Präsenz (Presence)

Der Begriff Präsenz oder Anwesenheit steht für die Fähigkeit eines Unified Communication Systems, jederzeit feststellen zu können, wo sich ein Benutzer befindet und welchen Status er hat. Dadurch kann bei der Kommunikation mit diesem Teilnehmer per Telefon, E-Mail, Instant Messaging oder Fax besser auf dessen Wünsche eingegangen werden.

Proxy-Server

Der Proxy-Server ist das Verbindungsglied zwischen Client-Applikation und Web-Server. Seine Aufgabe ist es, die Anforderungen der Client-Applikation zu filtern und den Web-Server zu entlasten.

PSTN (Public Switched Telephone Network)

PSTN bezeichnet das öffentliche, leitungsgebundene Telefonnetz. Öffentliche Netze können in staatlichem oder privatem Besitz sein.

QOS (Quality of Service)

Für Voice over IP ist es wichtig, eine Mindestbandbreite für die Dauer der Übertragung sicherzustellen. Wenn mehrere Applikationen gleichberechtigt über IP arbeiten, so wird die vorhandene Bandbreite einer Übertragungsstrecke aufgeteilt, so dass unter Umständen eine Sprachverbindung von Paketverlusten betroffen ist, woraus eine schlechte Sprachqualität resultieren kann. Es gibt unterschiedliche Verfahren um die höchstmöglich Qualität bei der Übertragung

zu gewährleisten, bei diesen Verfahren spricht man von Quality of Service (QOS).

RAS (Remote Access Service)

Ein RAS- (Remote Access Service) User ist ein IP-Teilnehmer (z.B. ein Teleworker), der sich per Remote am System anmeldet und sich wie ein interner IP-Teilnehmer verhält. Er kann somit den kompletten Leistungsumfang des Kommunikationssystems nutzen.

RJ45 (Registered Jack 45)

RJ45 ist eine achtpolige Steckverbindung, die z.B. für die Verbindung von 10BaseT-Kabel in der Netzwerktechnik eingesetzt wird.

Roaming

Roaming ist die Fähigkeit eines Mobilfunknetz-Teilnehmers, in einem fremden Netzwerk als seinem Heimnetzwerk automatisch zu telefonieren oder Zugriff auf andere Mobilfunknetzdienstleistungen zu haben.

RTCP (Real-Time Control Protocol)

Das RealTime Control Protocol (RTCP) dient der Aushandlung und Einhaltung von Quality of Service (QoS) Parametern durch den periodischen Austausch von Steuernachrichten zwischen Sender und Empfänger.

RTP (Real-Time Transport Protocol)

RTP ist ein IETF-Standard für das Streaming von Echtzeit-Multimediadaten über das Internet-Protokoll. RTP setzt normalerweise auf das UDP-Protokoll auf und verwendet dynamische UDP-Ports, die zwischen dem Sender und dem Empfänger spezieller Medienstreams ausgehandelt werden.

RTT (Round Trip Time)

RTT ist das Zeitintervall, das ein Datenpaket benötigt, um von der Quelle zum Ziel und zurück zu gelangen.

SA (Security Association)

SA ist eine Sicherheitsverbindung zwischen zwei kommunizierenden Einheiten in Rechnernetzen. Sie beschreibt, wie die beiden Parteien Sicherheitsdienste anwenden, um sicher miteinander kommunizieren zu können.

SDSL (Symmetric Digital Subscriber Line)

SDSL eignet sich besonders für Internet-Telefonie, Intranet-Anwendungen in Firmen bei Standortvernetzungen, für Videokonferenzen und ist z.B. prädestiniert für Teleworker, die dadurch Daten mit der gleichen Bandbreite senden und empfangen können. Im Gegensatz zu ADSL sind die Bandbreiten bei SDSL vom und zum Internet gleich hoch.

Secure CLI

Secure CLI ist ein Sicherheitsmerkmal, das mithilfe von SFTP (Secure File Transfer Protocol) sichere Befehlszeilen- und Dateiübertragungs-Schnittstellen bereitstellt.

SFTP (Secure File Transfer Protocol)

SFTP ist ein Sicherheitsprotokoll zur Übermittlung von Verbindungsdatensätzen.

ShrewSoft VPN-Client

Der ShrewSoft VPN-Client ist ein quelloffener und kostenloser VPN-Client mit grafischer Oberfläche. Er beinhaltet unter anderem ISAKMP, Xauth- und RSA-Unterstützung, AES, Blowfish, 3DES-Verschlüsselungsprotokolle.

Single-Gateway

Bei einer Single-Gateway-Vernetzung werden die Anrufe über ein einziges Gateway geroutet.

SIP (Session Initiation Protocol)

SIP ist ein im RFC 3261 spezifiziertes Internet-Standardprotokoll zum Aufbau und Steuerung von Sprachverbindungen und Videokonferenzen über ein IP-Netzwerk.

SNMP (Simple Network Management Protocol)

SNMP ist ein Verfahren um Informationen über den Zustand von Netzwerkkomponenten und PCs zu bekommen.

SPE (Signaling and Payload Encryption)

Signaling & Payload Encryption (SPE) dient der Sicherheit der Übertragung von Sprachdaten. Es werden VoIP-Nutz- und Signalisierungsdatenströme vom und zum Gateway und zwischen IP-Telefonen verschlüsselt.

SRTP (Secure Real-Time Transport Protokoll)

SRTP ist ein verschlüsseltes RTP-Protokoll. Es eignet sich besonders zur Übertragung von Kommunikationsdaten über das Internet, und findet in der IP-Telefonie Verwendung.

SSH (Secure Shell)

SSH ist ein Protokoll, das Unterstützung für sichere Remote-Anmeldung, sicheren Dateitransfer und sichere TCP/IP-Umleitungen bietet. Es kann übertragene Daten automatisch verschlüsseln, authentifizieren und komprimieren.

SSL (Secure Socket Layer)

SSL ist ein Protokoll für die Übertragung von Dokumenten über das Internet. Bei SSL werden Daten mit einem privaten Schlüssel versehen, bevor sie übertragen werden. URLs, die eine SSL-Verbindung erfordern, beginnen immer mit https: statt mit http:.

Status

Der Status gibt (im Zusammenhang mit dem Begriff "Präsenz") an, ob ein Teilnehmer verfügbar, besetzt, offline etc. ist, sodass andere Teilnehmer im Kommunikationssystem wissen, ob dieser Teilnehmer erreichbar ist.

STUN (Simple Traversal of UDP over NAT)

STUN ist ein Netzwerkprotokoll um das Vorhandensein und die Art von Firewalls und NAT-Routern zu erkennen und diese zu umgehen.

Survivability

Survivability ist die Fähigkeit eines Netzverbundes, den Service auch bei vorhandenen Fehlern im Netzwerk aufrechtzuerhalten.

TAE (Telekommunikations-Anschluss-Einheit)

TAE ist eine Steckerart bei analogen Telefonanschlüssen mit a/b-Schnittstelle und bei ISDN-Anschlüssen zum Anstecken des NTBA an die Anschlussleitung. Anschließbar sind analoge Telefone, Faxgeräte und ISDN-Telefonanlagen.

TCP (Transmission Control Protocol)

TCP ist ein Protokoll das regelt, auf welche Art und Weise Daten zwischen PCs ausgetauscht werden sollen. Alle Betriebssysteme moderner PCs beherrschen TCP und nutzen es für den Datenaustausch mit anderen PC.

TFTP (Trivial File Transfer Protocol)

TFTP ist ein Datenübertragungsprotokoll und unterstützt das Lesen und Schreiben von Dateien. Viele Funktionen des übergeordneten FTP-Protokolls sind bei TFTP nicht vorhanden, z.B. Rechtevergabe, Anzeigen der vorhandenen Dateien oder Benutzerauthentifizierung.

Telnet

Ein Protokoll, das zwei PCs miteinander verbindet, um eine Terminalverbindung zum entfernten PC bereitzustellen. Der Benutzer wählt sich nicht in den PC ein, sondern stellt die Verbindung über das Internet per Telnet her. Der Benutzer initiiert eine Telnet-Sitzung, stellt die Verbindung zum Telnet-Host her und meldet sich an. Über die Verbindung kann der Benutzer mit dem entfernten PC arbeiten, und sein eigenes System erscheint auf dem fernen Rechner wie ein lokal angeschlossenes Terminal.

TOS (Type of Service)

TOS ist ein Feld im Header von IP-Datenpaketen und wird für die Priorisierung dieser Pakete gesetzt und ausgewertet (z.B. bei Quality of Service).

Anrufverteilung (UCD Uniform Call Distribution)

UCD ermöglicht eine geichmäßige Verteilung von eingehenden Anrufen im Kommunikationssystem auf eine Gruppe von Teilnehmern (UCD-Gruppe).

UDP (User Datagram Protocol)

UDP ist ein Netzprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. UDP übergibt Daten, die über das Internet übertragen werden, an die jeweilige Anwendung.

UMTS (Universal Mobile Telecommunications System)

UMTS ist ein Mobilfunkstandard der dritten Generation, der deutlich höhere Datenübertragungsraten (384 kbit/s bis 7,2 Mbit/s) ermöglicht als der Mobilfunkstandard der zweiten Generation oder der GSM-Standard.

Unified Communications

Unified Communications ist die Integration unterschiedlicher Kommunikationssysteme, -medien, -geräte und –anwendungen innerhalb einer Umgebung (z.B. IP-Telefonie, ortsgebundene und mobile Telefonie, E-Mail, Instant Messaging, Desktop-Anwendungen, Sprachbox, Fax, Konferenzen und Unified Messaging).

Unified Messaging

Unified Messaging ist die Integration unterschiedlicher Kommunikationsdaten wie E-Mail, SMS, Fax, Telefonie etc. in einen einheitlichen Nachrichtenspeicher. Dieser Nachrichtenspeicher ist über eine Vielzahl unterschiedlicher Geräte erreichbar.

VAD (Voice Activity Detection)

VAD (Voice Activity Detection) bezeichnet eine automatische Sprechpausenerkennung bei der digitalen Übertragung von Audiodaten.

VCAPI-Schnittstelle

VCAPI ist eine virtuelle CAPI-Schnittstelle, die das Vorhandensein einer lokalen ISDN-Karte emuliert. Ist im internen Netz eine ISDN-Karte in einem PC eingebaut, so kann allen Teilnehmern im Netz diese ISDN-Karte über die VCAPI-Schnittstelle zur Verfügung gestellt werden.

VDSL (Very High Speed Digital Subscriber Line)

VDSL kommt überall dort zum Einsatz, wo über kürzere Entfernungen symmetrische oder asymmetrische Datenströme mit hoher Geschwindigkeit zu übertragen sind. VDSL stellt eine Alternative zu ADSL und SDSL dar, aber mit höheren Übertragungsgeschwindigkeiten.

VoIP (Voice over IP)

VoIP ist die Übertragung von Sprachdaten über IP-basierte Netzwerke.

VPN (Virtual Private Network)

VPN nutzt die öffentliche Infrastruktur des Internets für Standortvernetzungen und Zugänge für Teleworker. Durch Verschlüsselungs- und Authentifizierungsmechanismen wird erreicht, dass externe Partner eine sichere Verbindung zum internen Datennetz erhalten.

WAN (Wide Area Network)

WAN ist die Bezeichnung für Weitverkehrsdatennetze, z.B. das Internet.

WBM (Web-Based-Management)

WBM ist eine Bedienoberfläche, die mittels HTML- oder JAVA-Seiten und einem Web-Protokoll, in einem Internet-Browser angezeigt wird.

X.509-Standard (VPN-Zertifikat)

X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur und derzeit der wichtigste Standard für digitale Zertifikate.

XMPP (Extensible Messaging and Presence Protocol)

Internetstandard der primär für Instant Messaging eingesetzt wird. XMPP unterstützt die Interaktion mit Benutzern anderer Netzwerke wie z.B. AIM, ICQ oder Windows Live Messenger (WLM). XMPP und seine Erweiterungen unterstützen unter anderem Konferenzen mit mehreren Benutzern (z.B. Multi-User Chat) und das Anzeigen des Online-Status.

Zweitgradig

Zweitgradig bedeutet, dass ein Teilnehmer telefoniert und zusätzlich steht bei diesem Teilnehmer bereits ein zweiter Ruf an.

Index

Sonderzeichen

<$nopage>Central License Server (siehe Lizenzserver) 342
<$nopage>Medium, Backup (siehe Backup-Medium) 1253
<$nopage>Restore (siehe Wiederherstellen) 1259
<$nopage>UCD (Uniform Call Distribution) (siehe Anrufverteilung) 750

A

Ablauf der Lizenzierung 323
Abteilungen 587
Abteilungen, Experten-Modus 1750
Abwesenheitstexte 676
Abwurf/VPL/Hotline, Experten-Modus 1553
Active Directory Integration Service
  konfigurieren 1201
Active Directory Integration Service, Experten-Modus 1743
Active Directory Service 1200
Ad-hoc-Konferenz 527, 601
Admin-Protokoll 1053
  Admin-Protokoll-Daten, Experten-Modus 1527
  Konfiguration, Experten-Modus 1527
  laden 1053
  Sprache ändern 1007, 1008, 1008, 1008, 1053
Admin-Protokoll-Daten, Experten-Modus 1527
Admin-Protokoll, Experten-Modus 1527
AF/EF-Codepunkte 437
Aktionen
  Automatische Aktionen, Experten-Modus 1530, 1531
  Manuelle Aktionen, Experten-Modus 1528
Aktionen, Experten-Modus 1528
Aktive Dienste, Experten-Modus 1586
Aktive Regeln, Experten-Modus 1594
Aktive Tunnel, Experten-Modus 1588
Aktive Zertifikate, Experten-Modus 1583
Aktivierung, Software (siehe Software-Aktivierung) 1260
Aktualisierungszeit der DNS Namen, Experten-Modus 1563
Alarm-Signalisierungs, Experten-Modus 1523
Alle Leases, Experten-Modus 1614
alternativer Arbeitsplatz 564
Amtsberechtigung 765
  Erlaubnisliste anzeigen 770
  Filter für Verbotsliste ändern 771
  konfigurieren 768, 769, 774, 776, 776
  Rufnummer zur Erlaubnisliste hinzufügen 769
  Rufnummer zur Verbotsliste hinzufügen 770
  Verbotsliste anzeigen 770
Amtszugang
  ISDN-Amtszugang konfigurieren 412
Analoge Teilnehmer, Experten-Modus 1662
Analoges Telefon 449
Anklopfen/Rufeinblendung 673
Announcement Player, Experten-Modus 1570
Anruf
  entgangen 589
  geplant 589
Anrufbeantworter 449
Anrufbeantworter-Gruppe (siehe Sprachbox-Gruppe) 743
Anrufe abweisen 670
Anrufschutz 671
Anrufübernahme von Sprachbox 610
Anrufübernahme, Experten-Modus 1700
Anrufübernahmegruppe 689
  Anrufübernahme außerhalb einer AUN-Gruppe 690
  Anrufübernahme von Wiederanrufen 690
  Anrufübernahme von Wiederanrufen aktivieren 708, 1070
  Anrufübernahme von Wiederanrufen deaktivieren 708, 1070
  Aufmerksamkeitston 690
  Aufmerksamkeitston aktivieren 708
  Aufmerksamkeitston deaktivieren 708
  konfigurieren 699
  Mitglied hinzufügen 700
  Mitglied löschen 700
  Namensanzeige des Anrufers 690
  Namensanzeige des Anrufers aktivieren 708
  Namensanzeige des Anrufers deaktivieren 708
  Rufnummernanzeige des Anrufers 690
  Rufnummernanzeige des Anrufers aktivieren 707
  Rufnummernanzeige des Anrufers deaktivieren 708
  SIP-Telefone 690
Anrufumleitung 665
  regelbasiert 565
  statusbezogen 565
Anrufverteilung 750, 751
  AICC (Automatic Incoming Call Connection) 757
  Ansagen 762
  Ansagen ändern 762
  Konfiguration 751, 752
  Konfiguration einer UCD-Gruppe 752
  Nachbearbeitungszeit 755
  Nachbearbeitungszeit ändern 756
  Nachtschaltung 761
  Priorität externer Anrufe 756
  Priorität externer Anrufe ändern 757
  Priorität interner Anrufe 756
  Priorität interner Anrufe ändern 757
  Teilnehmerzustand 753
  Übergabe an UCD-Gruppe 763
  Übergabe an UCD-Gruppe, Wiederanrufzeit ändern 763
  Überlauf 760
  Überlauf ändern 760
  UCD-Agent 753
  UCD-Agent hinzufügen 755

UCD-Agent löschen 755
UCD-Anrufe automatisch annehmen 757
UCD-Anrufe automatisch annehmen, aktivieren 758
UCD-Anrufe automatisch annehmen, deaktivieren 758
UCD-Anrufe über analoge Leitungen auslösen 763
UCD-Anrufe über analoge Leitungen auslösen, Auslösezeit ändern 764
UCD-Gruppe 751
Wartemusik (Music On Hold MOH) ändern 762
Wartemusik (Music On Hold MOH) 761
Warteschlange 758
Warteschlange ändern 759
Ansage-Player 1780
Ansagen bei Anrufverteilung 762
Ansagen für Sprachbox 610
Anschaltungen, Experten-Modus 1687
Anwendungen, Experten-Modus 1780
Anwendungsfirewall, Expertenmodus 1575
Anwesenheit (UC Smart) 514
Anwesenheitsstatus 542
Anrufumleitung 565
Anwesenheitsstatus (UC Smart) 514
Anwesenheitsstatus (UC Suite) 561
Application Launcher
Profil für Konfigurationsdaten 1204
Application Launcher 1202, 1780
Application Launcher, Experten-Modus 1779
Applikat.-Diagnose, Experten-Modus 1532
Applikationen, Experten-Modus 1743
Applikationsauswahl 1743
Applikationsdiagnose
Entwickler-Einstellungen, Experten-Modus 1532, 1532
Mainboard, Experten-Modus 1532
Applikationsgesteuerte Konferenz 526, 595
ARP-Protokoll, Experten-Modus 1532
Audio-Codec 434
Parameter einem Ziel zuordnen 435
Parameter konfigurieren 435
Audio-Datei 1244
Audiodatei 1247
Auf Gateway laden, Expertenmodus 1495
Aufschalten 675
Aufzeichnen 592
Ausbaugrenzen 1454
Ausnahme
regelbasierte Anrufumleitung 565
Authentifizierung
Konferenzteilnehmer 527
AutoAttendant 610
Automatische Aktion 1287
DLS Notification 1289
DLS Notification ändern 1290
DLS Notification starten 772, 773, 774, 1290, 1293, 1293, 1295
DLS Notification stoppen 1291
Garbage Collection 1287
Garbage Collection ändern 1288
Garbage Collection starten 1289
Garbage Collection stoppen 1289
Automatische Nachtschaltung, Experten-Modus 1725
automatische Updates 551
Automatischer Rückruf 672

B

Backup 1251
Backup-Medium 1251, 1253
bearbeiten 1255
Hinzufügen 1254
löschen 1256
Backup-Set 1251, 1252, 1252
anzeigen 1252, 1253
Backup - zeitgesteuert 1258
Sofortiges Sichern 1257
Wiederherstellen 1259
Backup-Set für Diagnosezwecke 1354, 1355
Backup-sofort 1257
Backup-Verzeichnis 1251
Bandbreiten im LAN 1067
Basic-MULAP
ändern 738
anzeigen 738
Hinzufügen 737, 742
löschen 738
Mitglied ändern 739
Mitglied hinzufügen 739
Mitglied löschen 739
Basis-MULAP 732
Rufart 733
Basisstationen, Experten-Modus 1504, 1504, 1664, 1691
Baugruppen-Zustand, Experten-Modus 1507
Bedingung
regelbasierte Anrufumleitung 565
Benachrichtigung
Faxnachricht 622
Sprachnachricht 539, 622
Benachrichtigungsdienst 539, 622
Benutzer der UC Suite 552
Benutzer von UC Smart
Daten ändern 513, 539
Benutzer von UC Smart
Daten ändern 514
Benutzer von UC Suite
als Agent konfigurieren 555
Anwesenheitsstatus ändern 556
Daten ändern 555
Kennwort ändern 556
Länge des Kennworts ändern 557
zurücksetzen 555
Benutzer-Profile der UC Suite 557
Benutzerschaltflächen 865
Layout 865
Benutzerverzeichnis, Experten-Modus 1747
Berechtigungen, Experten-Modus 1630, 1719

Berechtigungsklassen
Automatische Nachtschaltung, Experten-Modus 1725
Erlaubnislisten, Experten-Modus 1721
Nacht: Berechtigungsgruppen, Experten-Modus 1720
Nachtschaltung, Experten-Modus 1723
Sondertage, Experten-Modus 1725
Tag: Berechtigungsgruppen, Experten-Modus 1720
Teilnehmer, Experten-Modus 1719
VBZ Gruppenzuordnung, Experten-Modus 1723
VBZ Matrix, Experten-Modus 1724
Verbotslisten, Experten-Modus 1722, 1722
Bestimmungsgemäßer Gebrauch der Kommunikationssysteme und Server 82
Betriebsbedingungen (klimatisch, mechanisch)
OpenScape Business S 89
OpenScape Business UC Booster Server 89
OpenScape Business X3, X5, X8 88
Blitzschutzanforderungen 85
Blockwahl 637
Branding, Experten-Modus 1499
Brandschutzanforderungen 85
Breitbandverbindung 372

C

Call Supervision, Experten-Modus 1514
CallMe 564
CallMe-Dienst 564
Carrier Select Override 786
CCV-Objekte 838, 890
CDP (Certificate Distribution Point) 1043
CE-Kennzeichnung 86
CE-Konformität 88
Chef-Funktion (siehe Chef/Sekretär-Konfiguration) 716
Chef-MULAP 734
ändern 740
anzeigen 740
Hinzufügen 740
löschen 741
Mitglied ändern 742
Mitglied hinzufügen 741
Mitglied löschen 741
Rufart 736
SIP-Telefone 736
Chef/Sekretär (siehe Chef/Sekretär-Konfiguration) 716
Chef/Sekretär-Konfiguration 716
ändern 725
Eigenschaften eines Mitglieds ändern 730
Faxbox 719
Faxbox hinzufügen 731
Hinzufügen 724
löschen 726
Mitglied ändern 730
Mitglied hinzufügen 729
Mitglied löschen 729
Rufart 719
SIP-Telefone 719
Client (UC Smart) 495
Client (UC Suite) 541
Client Logs 1364
herunterladen 1367
Clients, Hardware- und Softwarevoraussetzungen 545, 850, 875, 879
CLIP - Rufnummernübermittlung des Anrufers 649
CLIP no screening 652
Clipboard-Wahl 591
CLIR - Rufnummernunterdrückung des Anrufers 650
CMD (CSTA Message Dispatcher) 1780
Codec-Parameter, Experten-Modus 1634
Codeschloss individuell 783
COLP – Connected Line Identification Presentation 651
COLR - Rufnummernunterdrückung des Angerufenen 651
Communities, Experten-Modus 1525
Connected Line Identification Presentation – COLP 651
Contact Center 837, 838, 838, 838, 873, 890, 890, 890, 890
Agent 882
Agent aus der Warteschlange entfernen 949
Agentenrückruf 900
Ansage aufnehmen 924
Ansage laden 925
Anzeige der Warteschlangendetails 900
Bedingungen für den Betrieb 949
Berechtigungs-Level eines Agenten 882, 882
Berichte 953
bevorzugte Agenten 883
Bevorzugte Agenten festlegen 942
bevorzugten Agenten löschen 943
Clients 873
Eine Warteschlange hinzufügen 932
einfache Nachbearbeitung, Nachbearbeitungsgrund ändern 945
einfache Nachbearbeitung, Nachbearbeitungsgrund hinzufügen 944
einfache Nachbearbeitung, Nachbearbeitungsgrund löschen 945
Einsatz von DECT-Telefonen 952
Einschränkungen von System-Leistungsmerkmalen 950
mehrfache Nachbearbeitung, Nachbearbeitungsgrund ändern 947
mehrfache Nachbearbeitung, Nachbearbeitungsgrund löschen 947
Mehrfache Nachbereitung, Nachbereitungsgrund hinzufügen 946
myAgent 874
myReports 877
myReports Benutzerrollen 877
Nachbearbeitung 899
Nachbearbeitungsgründe 899
Pause 884
Pause ändern 944
Pause hinzufügen 943
Pause löschen 944
Regel als PDF-Datei speichern 931

Regel ausdrucken 931, 931, 932
Regel herunterladen 931, 932
Rückfalllösung (Fallback-Lösung) 902
Servicegrad 900
Sollwert für Servicegrad festlegen 940
Teilnehmer als Agent konfigurieren 923
UCD-Gruppe konfigurieren 923
VIP-Anruferpriorität 901
VIP-Anruferpriorität festlegen 940
VIP-Rufliste 901
VIP-Rufliste bearbeiten 941
vordefinierte Berichtsvorlagen 954
Vorgehensweise bei der Konfiguration 922
Wandanzeige/Wallboard 900
Warteschlange 888
Warteschlange aktivieren 939
Warteschlange bearbeiten 936
Warteschlange deaktivieren 939
Warteschlange einen Agenten zuordnen 948
Zeitplan bearbeiten 929
Zeitplan hinzufügen 925
Zeitplan löschen 930
Contact Center, Experten-Modus 1755
Contact Center:Beispiel für eine Contact-Center-Konfiguration 905
Contact Center:Konfiguration 905
Contact Center:Pilot für eingehende Faxnachrichten konfigurieren 940
Cordless
Basisstationen, Experten-Modus 1691
Multi-SLC, Experten-Modus 1690
SLC, Experten-Modus 1689
Systemweit, Experten-Modus 1687
Cordless-Lösung
Systemausbau 975
Corporate Network 795
Cover Page Editor 620
CRL (Certificate Revocation Lists) 1022, 1043
CSP (CSTA Service Provider) 1781
CSTA Message Dispatcher (CMD) 1780
CSTA Service Provider (CSP) 1781
CSTA-Protokoll 1171
CSV-Datei 430

D

Darstellungskonventionen 72
Datei-Upload, Experten-Modus 1765
Datenschutz 86, 954
Datensicherheit 86
Datensicherung (siehe Sichern) 1251
Datum und Uhrzeit, Experten-Modus 1565
Dauerhaft 603
DECT Teilnehmer, Experten-Modus 1665
DECT-Telefone 108
Default Router 365
Konfiguration 366
Default Router, Experten-Modus 1618, 1619
Deployment- und Licensing-Client (DLSC), Experten-Modus 1577
Desk Sharing 971
Desktop-Wahl 543, 591
Device-Statistik, Experten-Modus 1738
Devices, Experten-Modus 1734
DHCP Modus, Experten-Modus 1609
DHCP-Relay-Agent: konfigurieren 357
Diagnose Log 1349
herunterladen 1353
löschen 1353, 1354
öffnen 1353
Diagnose Logs, Experten-Modus 1523, 1528
Diagnose-Protokoll 1319
herunterladen 1321
Diagnosedaten 1319
herunterladen 1321
Dial In Control Server 795
Dienste sperren (nur LX) 1004
Digitale Prüfschleife, Experten-Modus 1510
Digitale Signatur 1020
Digitales Loopback 1324
Direktansprechen 645
Direktansprechen für Gruppen 749
Direktansprechschutz für Teilnehmer 645
aktivieren 646
deaktivieren 646
Direktantworten 645
Direktruftaste 644
DISA, Experten-Modus 1552
Diskretes Ansprechen) 658
Display, Experten-Modus 1548
DLI-Wartung, Experten-Modus 1530
DLS Notification, Experten-Modus 1531
DLSC CA -Zertifikat, Experten-Modus 1579
DLSC Client-Zertifikat, Experten-Modus 1577
DNS (Domain Name Service)
Server definieren 365
DNS-Name 386
DNS-Server 364
DNS-Server, Experten-Modus 1618
Download (siehe Update) 1260
DSL (Digital Subscriber Line) 372
DSP-Kanäle projektieren 1789
DSS-Server 1782
DSS-Taste 644
Dual-Mode-Telefonie 965
Durchsage an Gruppe 749, 749
Gespräch übergeben 750
Durchwahl Rufnummern, Experten-Modus 1683
DynDNS 363
DynDNS (Dynamic Domain Name Service) 386
DynDNS Service, Experten-Modus 1562
DynDNS-Dienst
konfiguration 407

DynDNS-Service 386
Konfiguration 387
konfigurieren 408, 408, 410, 995

E

E-Mail
Benachrichtigung 539, 622
Einladung zu Konferenz 527
E-Mail to SMS 624
E-Mail-Einstellungen 1349
E-Mail-Versand 623
E-Mail, Experten-Modus 1521
E.164-Nummerierung 1069
Editieren der Wahl 638
Eingehende Anrufe
Anrufübernahme, Experten-Modus 1700
Gruppen-Teilnehmer, Experten-Modus 1695
Gruppen/Huntgruppen, Expertenmodus 1691
Team/Top, Experten-Modus 1697
UCD, Experten-Modus 1700
Einladung
Konferenz 527
Einwahlnummer
Konferenz 527
elektrische Umgebung
OpenScape Business S 84
OpenScape Business UC Booster Server 84
Endgerät
Tastenprogrammierung, Experten-Modus 1686
Teilnehmer, Experten-Modus 1662, 1663, 1664, 1665, 1667, 1668, 1681, 1683, 1683
Entsorgung 83
Ereignisse
Diagnose Logs, Experten-Modus 1523
Event-Konfiguration, Experten-Modus 1521
Event-Protokoll, Experten-Modus 1521
Reaktionstabelle, Experten-Modus 1522
Erlaubnislisten
anzeigen 770
Erlaubnislisten, Experten-Modus 1721
ESP-Header 1011
Euro-ISDN-Leistungsmerkmale 1785
Event (Ereignis) 1347, 1348, 1348, 1349, 1349
E-Mail-Einstellungen ändern 1351
Protokoll herunterladen 1350
Protokoll löschen 1350
Protokollierung über LAN ändern 1350
Reaktionseinstellungen eines Events ändern 1351
Reaktionseinstellungen mehrerer Events ändern 1352
Reaktionstabelle anzeigen 1351
Event Viewer 1324
Protokoll ändern 1333
Protokoll anzeigen 1333
Protokoll herunterladen 1334
Protokoll löschen 1334
Protokoll öffnen 1334
Event-Konfiguration, Experten-Modus 1521
Event-Protokoll, Experten-Modus 1521
Events
Alarm-Signalisierung, Experten-Modus 1523
E-Mail, Experten-Modus 1521
Events, Experten-Modus 1520
EVM, Experten-Modus 1667
Experten-Modus, Experten-Modus 1493
Externes Verzeichnis 571
Externes Verzeichnis (LDAP) 576
Externes Verzeichnis, Experten-Modus 1753

F

FastViewer 528, 605, 605
Favoritenliste 588
Sofortnachricht 530
Favoritenliste (UC Smart) 518
Fax 610
T.38 627
Fax Gruppe 3 449
Fax Gruppe 4 446
Fax Printer 543, 619
Faxbox 618
Faxbox-Gruppe 744
ändern 748
anzeigen 748
Konfiguration 747, 748
Mitglied hinzufügen 748
Mitglied löschen 748
Faxgruppe (siehe Faxbox-Gruppe) 744
Faxkopfzeilen, Experten-Modus 1776
Faxnachrichten 610, 866
Fernzugriff auf das Kommunikationssystem 1381
Feste Rufweiterschaltung 661
Firewall 996, 1203
Flex Call 681
Flexible Menüs, Experten-Modus 1558
FTP-Server, Experten-Modus 1608
Funkstörung 86
Funktionen
myPortal 542
myPortal for Outlook 543
myPortal Smart 497
Funktionstasten 451
programmieren 452, 492, 493, 494, 513, 514, 539

G

Garbage Collection, Experten-Modus 1530
Gateway, Experten-Modus 1560
Gebühren Ausgabe, Experten-Modus 1567
Gebühren Faktoren, Experten-Modus 1569
Gebühren Projekt Kennzahlen, Experten-Modus 1570
Geplante Konferenz 527, 601, 601
Gigaset-Telefone 108
Globaler Parameter, Expertenmodus 1609

Grundeinstellungen 1534
Datum und Uhrzeit, Experten-Modus 1565, 1565, 1565
DynDNS, Experten-Modus 1562, 1563
Gateway, Experten-Modus 1559, 1560
Gebühren, Experten-Modus 1567, 1569, 1570
Port-Verwaltung, Experten-Modus 1566
Power Management, Experten-Modus 1574
Quality of Service, Experten-Modus 1564
System, Experten-Modus 1543, 1548, 1552, 1553, 1556, 1557, 1558, 1558, 1559
Telefonparameter-Bereitstellung, Experten-Modus 1571
Wiedergabegerät, Experten-Modus 1570
Grundeinstellungen, Experten-Modus 1534, 1778
Gruppen 689
Gruppen-Teilnehmer, Experten-Modus 1695
Gruppen, Experten-Modus 1751
Gruppen/Huntgruppen, Expertenmodus 1691
Gruppenruf 691
Anklopfschutz für Gruppenmitglied ausschalten 711
Anklopfschutz für Gruppenmitglied einschalten 711
DND für Gruppenmitglied 692
Rufart 694
SIP-Telefone 694
Sprachbox 692
Typ Anklopfen ändern 710
Typ Anklopfen anzeigen 710
Typ Anklopfen hinzufügen 709
Typ Anklopfen löschen 710
Typ Anklopfen, Mitglied hinzufügen 710
Typ Anklopfen, Mitglied löschen 710
Typ Freifall ändern 710
Typ Freifall anzeigen 710
Typ Freifall hinzufügen 709
Typ Freifall löschen 710
Typ Freifall, Mitglied hinzufügen 710
Typ Freifall, Mitglied löschen 711
Typ Gruppe ändern 702
Typ Gruppe hinzufügen 700
Typ Gruppe löschen 703
Typ Gruppe, Mitglied hinzufügen 703
Typ Gruppe, Mitglied löschen 703

H

H.323-Stack-Trace 1326
Konfiguration ändern 1337
Konfiguration anzeigen 1337
Module ändern 1338
Protokoll herunterladen 1338
Protokoll löschen 1338
Protokoll öffnen 1338
H.323-Stack-Trace, Experten-Modus 1513
Halten 653
Handlungsanweisung 71
Hardware-Konfiguration OpenScape Office MX
anzeigen 489
Hardwaretausch 341
Hauptnetzanbieter 794
Hauptplatine, Expertenmodus 1609
Herunterfahren von OpenScape Business X 1277
Hilfsausrüstung
SmartVM, Experten-Modus 1730
Wartemusik, Expertenmodus 1726
Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients 881
Host-Name, Experten-Modus 1601, 1615
Hot Desking 971
Hotline 820
HW-Module, Experten-Modus 1735

I

ICMP (Internet Control Message Protocol) 1303
IKE-SA 1020
Image-Datei 1261
Installation 133, 222, 277
Instant Message 530
Instant Messaging 608, 866
interne Wartemusik 1247
Interne Wartemusik 1244
Internes Verzeichnis (UC Smart) 517
Internes Verzeichnis (UC Suite) 570
Internet-Modem 378
Internet-Router 374
Internet-Telefonie 389
Internet-Telefonie-Service-Provider (ITSP) 181, 247, 389, 391
Internet-Zugang 372
Konfiguration 373
über den Standard-ISP PPPoE konfigurieren 382
über externen Internet-Router 374
über externes Internet-Modem 378
über Standard-ISP PPTP konfigurieren 384
über vorkonfigurierten ISP konfigurieren 379
Internettelefonie-Dienstanbieter, Expertenmodus 1637
Inventar, OpenScape Business S 1285
Inventar, OpenScape Business X 1284
Inventory OpenScape Business S
abfragen 1287
Inventory OpenScape Office LX/HX
abfragen 346, 346
Inventory OpenScape Office MX
abfragen 346
Inventory-Management 1280
Inventory, OpenScape Business X3/X5/X8
prüfen 1285
IP Clients, Experten-Modus 1685
IP Mobility 971
IP-Adressen 1281
Übersicht anzeigen 1283
IP-Adressen-Schema 137, 226
IP-Adresspools, Expertenmodus 1611
IP-Client (siehe IP-Teilnehmer) 440

IP-Clients, Expertenmodus 1659
IP-Diagnose
Mainboard, Experten-Modus 1532, 1533, 1533
IP-Diagnose, Experten-Modus 1532
IP-Gateway-Adresse, Experten-Modus 1499
IP-Teilnehmer 440
IPSec-Tunnel 1019
ISDN Teilnehmer, Experten-Modus 1663
ISDN-Amtsleitung
Gezielte Belegung 795
ISDN-Amtszugang konfigurieren 412
ISDN-Karte 446
ISDN-Modem 446
ISDN-Parameter, Experten-Modus 1718
ISDN-Teilnehmer 446
ISDN-Telefon 446
ITSP (Internet-Telefonie-Service-Provider) 389
ITSP-Status 1281
abfragen 1283

J

Java 1203
Java Runtime Environment (JRE) 135, 223
Journal
Aufbewahrungsdauer 589
Journal (UC Smart) 525
Journal (UC Suite) 589

K

Kabelanschluss 372
kanonisches Rufnummernformat 525
Kapazitäten 1454
Kernel Crash-Datendienst
Anhalten 1344
Starten 1343
Keypad-Wahl 637
Knoten, Experten-Modus 1649
Kommende Rufe
Rufweiterschaltungen, Experten-Modus 1703
Kommende Rufe, Experten-Modus 1691
Kommunikationssystem herunterfahren 1277
Konferenz 527, 594, 603, 603
AdHoc- 601
Applikationsgesteuert 594
Arten von Konferenzen 594
Aufzeichnung 594
Authentifizierung 594
automatische Einladung per E-Mail 594
automatische Einladung per Outlook-Termin 594
Einwahlnummer 594
geplante 601
Konferenzleiter 594
Konferenzteilnehmer 594
Konferenzton 594
Mobility-Entry-Teilnehmer 594, 601, 601, 604
offene 604
Telefongesteuert 594
Verlängerung 594
Virtueller Konferenzraum 594
Konferenz (UC Suite) 594
Konferenz-Management 526, 595
Konferenz, telefongesteuert 526
Konferenzschaltung 603
Konferenzschaltung, Experten-Modus 1767
Konferenzton aktivieren / deaktivieren 666, 667
Konfiguration
Ansagen, Expertenmodus 1495
Branding, Experten-Modus 1499
IP-Gateway-Adresse, Experten-Modus 1499
Port-Konfiguration, Experten-Modus 1495
SmartVM, Experten-Modus 1496, 1496, 1497
Wartemusik (MoH), Experten-Modus 1494
Konfiguration externe Anbieter, Experten-Modus 1754
Konfiguration, Experten-Modus 1494, 1527
Konfigurationsdaten 1251
Konfigurationsdaten für die Diagnose 1354
generieren 1355
Konfigurierte Dienste, Experten-Modus 1587
Konfigurierte Regeln, Experten-Modus 1596
Konfigurierte Tunnel, Experten-Modus 1590
Konfigurierte Zertifikate, Experten-Modus 1585
Konformität
internationale Normen 88
US- und kanadische Normen 88
Kontakt 588
Konzept 71
Kunden-Trace-Protokoll 1325
ändern 1333
anzeigen 1333
herunterladen 1334
löschen 1334
öffnen 1334
Kunden-Trace-Protokoll, Experten-Modus 1511
Kurzwahl individuell (KWI) 644
Kurzwahl zentral (KWZ) 640
Kurzwahlziele, Experten-Modus 1558, 1779

L

Laden zum Gateway, Experten-Modus 1494
LAN 1 (WAN), Expert mode 1602
LAN 1, Experten-Modus 1615
LAN 2, Experten-Modus 1606, 1616
LAN 3 (Admin), Experten-Modus 1608
LAN-Anforderungen 1066
Lautsprecher 449
LCR
Berechtigungen, Experten-Modus 1626
LCR-Flags, Experten-Modus 1625
Mehrere Standorte, Experten-Modus 1630
Plan, Experten-Modus 1626
Wahlregel, Experten-Modus 1628

Wegetabelle, Experten-Modus 1627
LCR (Least Cost Routing) 784
Berechtigung 791
Berechtigung vergeben/ändern 792
Wahlplan 788
Wahlplan bearbeiten 789
Wahlregeln 792
Wahlregeln bearbeiten 794
Wegetabelle 790
Wegetabelle bearbeiten 790
LCR Least Cost Routing
Funktionalität 784, 785
LCR-Flags, Experten-Modus 1625
LDAP-Verbindung 1203
LDAP, Experten-Modus 1556
Leistungsmerkmale
Voice, netzweit 1065
Leitungen 410
Belegungsart 417
Belegungsart konfigurieren 421, 424, 426
Kennzahl ändern 414, 414, 414
MSN zuweisen 415
Protokoll ändern 415, 415, 416
Richtung ändern 419
Leitungen, Experten-Modus 1706
Leitungen/Vernetzung
ISDN-Parameter, Experten-Modus 1718
Leitungen, Experten-Modus 1706
MSN zuweisen, Experten-Modus 1718
QSIG-Leistungsmerkmale, Experten-Modus 1717
Leitungen/Vernetzung, Experten-Modus 1706
Leitungstrennung für einen Notruf 822
Leitungsvormerken 647
Lesende Communities, Experten-Modus 1525
Lightweight CA 1021
Lightweight CA, Experten-Modus 1582
Live Call Recording (Voice Recording; Sprachaufzeichnung) 660
Lizenz 300
aktualisieren 342
Informationen anzeigen 335, 336, 336, 337, 337, 346
über Lizenz-Autorisierungscode aktivieren 316, 1429
über Lizenzdatei aktivieren 316
Lizenz-Autorisierungscode (LAC) 314, 325
Lizenz-Komponenten-Trace 1327
ändern 1339
Lizenz-Komponenten-Trace, Experten-Modus 1516
Lizenzaktivierung 314, 325
Lizenzaktualisierung 341
Lizenzdatei 314, 325
Lizenzserver (CLS) 319, 342
IP-Adresse ändern 210, 263, 322, 330, 333, 338, 339, 339, 340, 343
Log-Datei 1348
Log-Einträge 1348
LXV3, Experten-Modus 1779

M

M5T-Trace-Komponente 1325
ändern 1335
anzeigen 1334
starten 1335
stoppen 1335
M5T-Trace-Komponenten, Experten-Modus 1511
Mail Exchanger 386, 387
definieren 389
Mail-Exchange-Eintrag 386
Mainboard, Experten-Modus 1532
Makeln 655
Manager E 131
Manuelle Aktion 1319
Mapping (Anwesenheitsstatus UC Suite) 561
Maximalwerte
Leistungsmerkmale 1462
MCL Single Stage 795
MCL Two Stage 795
MEB (Media Extension Bridge) 1782
Media Extension Bridge (MEB) 1782
Media Stream Control (MSC), Experten-Modus 1734
Mediatrix 4102S 108
Medienserver-Trace
Anhalten 1345
Starten 1344
Medienserver-Traces, Experten-Modus 1520
Mehrsprachige Textausgabe 1243
Mitteilungstexte 677
mobile anmeldung 971
mobile benutzeranmeldung 971
Mobile Pin 681
Mobilität
Mobiltelefon für GSM konfigurieren 966
Mobility
Teilnehmer löschen 971
Mobility Entry 960
Leistungsmerkmal-Codes 960
Mobility Entry, Experten-Modus 1683
Mobility-Entry-Teilnehmer 603, 603
Konferenz 594, 601, 601, 604
Konferenzschaltung 527
Modem 449
MoH 1244
MSC-Statistiken, Experten-Modus 1739
MSN zuweisen, Experten-Modus 1718
Multi Location 1060
Multi-SLC, Experten-Modus 1690
MX-Record 386
myAgent
Voraussetzungen 875
myPortal
Anwesenheitsstatus 542
Funktionen 542
myPortal for Outlook
Funktionen 543

myPortal Smart
Funktionen 497
myPortal to go
Voraussetzungen 958
myReports
Administrator-Kennwort zurücksetzen 879
Benutzerrollen 877

N

Nachrichten verwalten 865
Nachrichtenübersicht 865
Nacht
Berechtigungsgruppen, Experten-Modus 1720
Nachtschaltung, Experten-Modus 1723
Nachwahl 640
NAT (Network Address Translation) 999
NAT-Regel
konfigurieren 1000
löschen 1001
mit NAT-Tabelleneditor konfigurieren 1000
NAT-Regeln 999
NAT-Tabelleneditor 1000
NAT, Experten-Modus 1619
Nativer SIP-Server-Trunk, Expertenmodus 1651
NCP-Client
aktivieren, deaktivieren 1030
vorbereiten 1030
Netzanbieter 794
Netzwerk
Lizenz 1065
Netzwerkparameter (LAN, WAN) 1066
Netzwerkschnittstellen 1609
Application Board, Experten-Modus 1615, 1615, 1616
Hauptplatine, Expertenmodus 1602, 1611, 1612, 1614
Mainboard, Experten-Modus 1601, 1606, 1608, 1608, 1609, 1614
Netzwerkschnittstellen, Experten-Modus 1601
Netzwerkverbindung prüfen 1302
über Ping 1303
über Traceroute 1303
Neustart von OpenScape Business 1274
Notrufdienst E911 823
Notrufe
Voraussetzungen 819
Nummerierung
offene 1068
verdeckt, geschlossen 1068

O

Offene Konferenz 604
Öffentliche Rufnummern im Netz 1069
Online-Benutzer 1387, 1534
starten 1301, 1388
Online-Benutzer, Experten-Modus 1534
Open Directory Service 1203
Datenquellen, Expertenmodus 1778
Open Directory Service
Datenquellen, Experten Modus 1779, 1779
Grundeinstellungen, Experten-Modus 1778
Wartung, Experten-Modus 1779
Open Directory Service, Experten-Modus 1778, 1779
OpenScape Business Assistant 113, 115
OpenScape Business X3R
Schutzerdung 1424, 1425, 1427
OpenScape Business X5R
Schutzerdung 1424, 1425, 1427
OpenScape Office, Expertenmodus 1778
OpenScape Personal Edition 108
OpenStage 108
OpenStage Attendant 847
OptiPoint 108
Out of Service, Experten-Modus 1507

P

Padding 1011
Parken 654
Path Replacement 1069
Payload
Devices, Experten-Modus 1734
HW-Module, Experten-Modus 1735
Media Stream Control (MSC), Experten-Modus 1734
Payload-SA 1020
Payload, Experten-Modus 1734
PC-Clients 108
PDF-Datei
Benachrichtigung 622
Faxnachricht 618
Peer-Zertifikate, Experten-Modus 1585
Permanente Konferenz 527, 603
PIN zur Aktivierung eines Shutdowns 1277
Ping, Experten-Modus 1533
PKI-Server
anzeigen 1042
hinzufügen 1042
Plattform-Diagnose, Experten-Modus 1531
Port 1203
Port-, Baugruppen-Zustand, Experten-Modus 1506
Port-Konfiguration, Experten-Modus 1495
Port-Verwaltung, Experten-Modus 1566
Ports 997
Portfreigabe konfigurieren 998, 1152
Portverwaltung 998
Power Management, Experten-Modus 1574
PPP-Protokoll, Experten-Modus 1621
Präsenz (UC Suite) 561, 561
Pre-shared Keys 1020
Presence (UC Smart) 514
Primary Rate Interface 795
Priorisierung von Amtsleitungen 427
Priorisierungsklassen 437

Privatleitung 648
Profil für Konfigurationsdaten von Application Launcher 1204
Profile
alle Profile exportieren 484, 993
alle Profile importieren 484, 993
bearbeiten 483
einzelnes Profil exportieren 482
einzelnes Profil importieren 482
Mitglieder anzeigen 481
Mitglieder hinzufügen 481
Mitglieder löschen 482
Neues Profil anlegen 480
Profile anzeigen 481
Teilnehmer 479
Profile, Experten-Modus 1774
Profile:alle Profile exportieren 484, 993
Profile:alle Profile importieren 484, 993
Profile/Vorlagen, Experten-Modus 1681
PSTN-Partner, Experten-Modus 1621
PSTN, Experten-Modus 1620
Public Key Infrastructure (PKI), Experten-Modus 1597

Q

QSIG-Leistungsmerkmale, Experten-Modus 1717
Quality of Service (QoS) 437
Konfiguration 439
Quality of Service, Experten-Modus 1564, 1626

R

R-Gesprächsschutz je Amtsleitung 784
RAS-User 440
Reaktionstabelle 1349
Reaktionstabelle, Experten-Modus 1522
Recycling 83
Regel 565
Regel-Editor 838, 890
Reload der UC Booster Card 1279
Reload von OpenScape Business 1275
Relocate 681
Remote Services 1374
Remote-Zugang 1381
ausschalten 1387
einschalten, über Internet-Zugang mit fester IP-Adresse 211, 213, 264, 265, 1385
einschalten, über Internet-Zugang ohne feste IP-Adresse 1386
einschalten, über ISDN 1382
PC konfigurieren 1382
PC mit Windows 7 konfigurieren 1384
über Internet-Zugang mit fester IP-Adresse einschalten 209, 211, 262, 264
Restart / Reload
Restart / Reload, Experten-Modus 1524
Restart / Reload, Experten-Modus 1523, 1524
Restart von OpenScape Business 1274
Richtungen 410, 416
Anlagenrufnummer eintragen 421
Kennzahl zuweisen 420
Namen zuweisen 420
Nr.-Typ gehend konfigurieren 422
Präfix ergänzen kommend 418, 422
Rufnummerntyp konfigurieren 422
Überlaufrichtung eintragen 420
Zweite Amtskennzahl eintragen 423
Röchelschaltung 820
Route, Expertenmodus 1709
Routing 365
IP Routing, Experten-Modus 1617, 1618, 1618, 1618, 1619
NAT, Experten-Modus 1619
PSTN, Experten-Modus 1620, 1621, 1621
Routing, Experten-Modus 1617, 1649
rpcap Dämon, Experten-Modus 1519
RPCAP-Dämon 1346
aktivieren 1347
deaktivieren 1347
Rückruf 672
Journal 589
Rückruf bei Besetzt 672
Rufeinblendung/Anklopfen 673
Rufnummern
importieren 433
Rufnummernformat 525
Rufnummernplan 136, 227, 428, 788
ändern 432
importieren 433
löschen 431
Rufnummerntausch 681
Rufnummernübermittlung des Anrufers - CLIP 649
Rufnummernumwertung in Namen 653
Rufnummernunterdrückung des Angerufenen - COLR 651
Rufnummernunterdrückung des Anrufers - CLIR 650
Rufsignalisierungen 648
Rufweiterschaltung im Amt 668
Rufweiterschaltung im Besetztfall 662
Rufweiterschaltung konfigurieren 534, 663
Rufweiterschaltung nach Zeit 661
Rufweiterschaltungen, Experten-Modus 1703
Rufzuordnung 668
Rufzuschaltung 669

S

Sammelanschluss 695
ändern 705
Hinzufügen 704
löschen 706
Mitglied hinzufügen 706
Mitglied löschen 707
Rufart 698
SIP-Telefone 698

Sprachnachricht 696
Schnurlose Telefone 108
Schreibende Communities, Experten-Modus 1526
Secure Trace 1325
Passphrase ändern 1336
Passwort ändern 1336
starten 1335
Status abfragen 1336
stoppen 1335, 1336
X.509-Datei importieren 1337
Zertifikat aus X.509-Datei importieren 1337
Secure Trace-Einstellungen, Experten-Modus 1512
Secure Trace-Zertifikat, Experten-Modus 1512
Secure Trace, Experten-Modus 1512
Security Associations SA 1019
Security Checklist 996
Sekretär-Funktion (siehe Chef/Sekretär-Konfiguration) 716
Server-Zertifikate, Experten-Modus 1599
Server, Experten-Modus 1767
Servicekennzahlen, Experten-Modus 1559, 1559
Shutdown
PIN zur Aktivierung 1277
Sicherheit
Anwendungsfirewall, Expertenmodus 1575
Deployment- und Licensing-Client (DLSC), Experten-Modus 1577, 1577, 1579
Signaling- und Payload Encryption, Experten-Modus 1580, 1581, 1581
SQL-Sicherheit, Experten-Modus 1601
SSL, Experten-Modus 1598, 1599, 1599
VPN, Experten-Modus 1581, 1582, 1583, 1583, 1585, 1585, 1586, 1587, 1588, 1590, 1594, 1596, 1597
Web Sicherheit, Experten-Modus 1601
Sicherheit, Experten-Modus 1575
Sicherheitshinweise 72
Sicherheitshinweise für Australien 77
Sicherheitshinweise für Brasilien 77
Sicherheitshinweise für Kanada 80
Sicherheitshinweise für USA. 77
Sichern 1251
sofort 1256
zeitgesteuert 1258
Signaling and Payload Encryption
SPE Unterstützung aktivieren 1007
SPE Unterstützung deaktivieren 1007
Signaling- und Payload Encryption, Experten-Modus 1580
Signaling- und Payload-Encryption (SPE) 1005
Single Location 1060
SIP Interconnection, Experten-Modus 1649
SIP-Client 440
SIP-Parameter, Experten-Modus 1631
SIP-Telefone 108
Site Of Operations, Experten-Modus 1743
SLC, Experten-Modus 1689
SmartVM, Experten-Modus 1496, 1496, 1497, 1730
SMS
Benachrichtigung 622
SMS-Benachrichtigung 624
SMS-Template 624
SNMP
Communities, Experten-Modus 1525, 1525, 1526, 1526
Traps, Experten-Modus 1526
SNMP (Simple Network Management Protocol) 1304
Communities 1304
Communities anzeigen 1316
Community ändern 1317
Community hinzufügen 1317
Community löschen 1318
Management-Informationsdatenbank MIB 1304
Trap-Detaildaten anzeigen 1319
Traps 1305
Traps anzeigen 1318
SNMP Statistik, Experten-Modus 1739
SNMP, Experten-Modus 1525
Sofortnachricht 530, 530, 530, 608, 608, 608
Sofortnachrichten 866
Software-Aktivierung 1260
Software-Image
System Software, Experten-Modus 1500, 1501, 1501
Software-Image, Experten-Modus 1500, 1504
Software-Übertragung 1260
Software-Update (siehe Update) 1260
Software-Updates 1260
Sondertage, Experten-Modus 1725
SPE CA Zertifikate, Experten-Modus 1581
SPE Zertifikat, Experten-Modus 1581
Sprach-Gateway
Internettelefonie-Dienstanbieter, Expertenmodus 1637
SIP-Verbindung, Expertenmodus 1651
Sprachbox 610
Gesprächsübernahme 610
statusbezogene Ansagen 610
Sprachbox (UC Smart) 531
Sprachbox-Gruppe 743
ändern 745
anzeigen 745
Hinzufügen 745
löschen 746
Mitglied ändern 746
Mitglied hinzufügen 746
Mitglied löschen 746
Sprachen 109
Sprachgateway Codec-Parameter, Experten-Modus 1634
Sprachgateway Networking, Experten-Modus 1649, 1649
Sprachgateway SIP Interconnection, Experten-Modus 1649
Sprachgateway SIP-Parameter, Experten-Modus 1631
Sprachgateway Ziel-Codec-Parameter, Experten-Modus 1636
Sprachgateway, Experten-Modus 1631
Sprachnachricht
speichern 610

Sprachnachrichten 610, 866
Sprachnachrichten (UC Smart) 531
SQL-Sicherheit, Experten-Modus 1601
SSDP (Smart Services Delivery Platform) 1375
PIN zur Aktivierung/Deaktivierung des Service-Plugin konfigurieren 1381
Service-Plugin deaktivieren 1380
Service-Plugin konfigurieren für ein Kundennetz mit Proxy 1378
Service-Plugin zurücksetzen 1380
SSL (Secure Socket Layer) 1043
CA-Zertifikat generieren 1045
Importieren eines Serverzertifikats 1051
Selbstsigniertes Zertifikat generieren 1045
Server-Zertifikat wird importiert 1048, 1048
Verlängertes Zertifikat importieren 1050
Zertifikat aktivieren 1050
Zertifikat exportieren 1050
Zertifikat löschen 1049
Zertifikate anzeigen 1003, 1003, 1004, 1049
Zertifikatsanforderung wird generiert 1047
Standards 1783
Standort-Liste, Experten-Modus 1767
Statische IP-Adressen, Expertenmodus 1612
Statische Routen 366
Hinzufügen 366, 370, 370, 371
löschen 367
Statische Routen, Experten-Modus 1617, 1618
Statistiken
Gateway-Statistiken, Experten-Modus 1738, 1739
SNMP Statistik, Experten-Modus 1739
Telefonie-Statistiken, Experten-Modus 1740, 1740, 1740, 1741, 1741
Statistiken, Experten-Modus 1738
Status des Kommunikationssystems 1281
Statusbezogene Sprachbox-Ansagen 610
Störaussendung 86
Stromversorgungsschaltung und Verbindung
OpenScape Business S 84
OpenScape Business UC Booster Server 84
STUN (Simple Traversal of UDP over NAT) 409
System Flags, Experten-Modus 1534
System Texte, Experten-Modus 1740
System-Client 440
System-Flag
A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungsziel / RWS-Ziel 708
Anrufübernahme nach Wiederanruf 709, 1070
Aufmerksamkeitssignalisierung bei AUN-Gruppen 708
SPE Unterstützung 1007
System, Experten-Modus 1534
Systemsprache für Sprachbox 610
Systemtelefonbuch (UC Suite) 578
Systemverbindung 1203
Systemverzeichnis 518
Systemweit, Experten-Modus 1687

T

T.38-Fax 627
Tag
Berechtigungsgruppen, Experten-Modus 1720
Tastenkombination für Desktop-Wahl 591
Tastenprogrammierung 451, 451
Tastenprogrammierung, Experten-Modus 1686
TCP- Dump, Experten-Modus 1518
TCP-Dump 1345
löschen 1346
starten 1345
stoppen 1346
Team (siehe Teamschaltung) 712
Team-Gruppe 712
ändern 722
Eigenschaften eines Mitglieds ändern 728
Faxbox 714
Faxbox hinzufügen 729
Hinzufügen 721
löschen 723
Mitglied ändern 727
Mitglied hinzufügen 727
Mitglied löschen 727
Rufart 714
Telefon-Tastenbelegung ändern 728
Team/Top, Experten-Modus 1697
Teamfunktion (siehe Teamschaltung) 712
Teamschaltung 712
ändern 722
Eigenschaften eines Mitglieds ändern 728
Faxbox 714
Faxbox hinzufügen 729
Hinzufügen 721
löschen 723
Mitglied ändern 727
Mitglied hinzufügen 727
Mitglied löschen 727
Rufart 714
Telefon-Tastenbelegung ändern 728
Teilnehmer 428, 1656
analog 449
IP 440
ISDN 446
Konfiguration über Wizards 454
Stationen, Expertenmodus 1659, 1669
Teilnehmer, Experten-Modus 1680
Teilnehmer Übersicht, Experten-Modus 1685
Teilnehmer-Flag
Anklopfschutz ein 711
Direktansprechschutz aus 646
Teilnehmer-Parameter, Experten-Modus 1669
Teilnehmer-Profile 479
Teilnehmer-Status 1281
abfragen 1282
Teilnehmer, Experten-Modus 1656, 1656, 1719, 1741

Teilnehmerdaten
importieren 433
telearbeit 987
Telefon abschließen 783
Telefon-Image
Laden, Experten-Modus 1502
Verteilen pro Endgerät, Experten-Modus 1503
Telefon-Images
Verteilen, Experten-Modus 1503
Telefon-Logo
Laden, Experten-Modus 1503
Verteilen, Experten-Modus 1504
Telefone 108
Telefongespräche übergeben 655
Telefongesteuerte Konferenz 595
Telefonie, Experten-Modus 1534
Telefonparameter-Bereitstellung, Experten-Modus 1571
Teleworking 564
Templates, Experten-Modus 1752
Termin 684
Terminalserver-/Citrix-Server-Umgebungen 542
Texts, Experten-Modus 1557
Themen, Arten 71
TIFF-Datei
Benachrichtigung 622
Faxnachricht 618
Top-Gruppe 716
ändern 725
Eigenschaften eines Mitglieds ändern 730
Faxbox 719
Faxbox hinzufügen 731
Hinzufügen 724
löschen 726
Mitglied ändern 730
Mitglied hinzufügen 729
Mitglied löschen 729
Rufart 719
SIP-Telefone 719
Trace 1322
Ausgabe-Interfaces ändern 1333
Ausgabe-Interfaces anzeigen 1333
Format-Konfiguration ändern 1332
Format-Konfiguration anzeigen 1332
Protokoll 1324
Protokoll herunterladen 1329
Protokoll löschen 1330, 1330
Trace- Protokoll, Experten-Modus 1510
Trace-Ausgabe-Interfaces, Experten-Modus 1509
Trace-Format-Konfiguration, Experten-Modus 1508
Trace-Komponente 1329
alle Komponenten stoppen 1341
ändern 1342, 1342
anzeigen 1340
Detaildaten anzeigen 1341
starten 1341
stoppen 1341
Trace-Komponenten, Experten-Modus 1517
Trace-Konsolen-Ausgabe, Experten-Modus 1532
Trace-Profil 1327
alle Profile stoppen 1339
anzeigen 1331
Detaildaten anzeigen 1339
hinzufügen 1340
starten 1332
stoppen 1332
Trace-Profile, Experten-Modus 1517
Trace:Ausgabe-Interfaces 1323
Trace:Format-Konfiguration 1322
Traceroute, Experten-Modus 1533
Traces
Call Supervision, Experten-Modus 1514
Digitale Prüfschleife, Experten-Modus 1510
H.323-Stack-Trace, Experten-Modus 1513
Kunden-Trace-Protokoll, Experten-Modus 1511
Lizenz-Komponenten, Experten-Modus 1516
M5T-Trace-Komponenten, Experten-Modus 1511
Medienserver-Traces, Experten-Modus 1520
rpcap Dämon, Experten-Modus 1519
Secure Trace, Experten-Modus 1512, 1512, 1512
TCP- Dump, Experten-Modus 1518
Trace- Protokoll, Experten-Modus 1510
Trace-Ausgabe-Interfaces, Experten-Modus 1509
Trace-Format-Konfiguration, Experten-Modus 1508
Trace-Komponenten, Experten-Modus 1517
Trace-Profile, Experten-Modus 1517
Traces, Experten-Modus 1508
Trap Communities, Experten-Modus 1526
Traps, Experten-Modus 1526
Trunks/Routing
Route, Expertenmodus 1709
Türsprechstelle/Türöffner 1163

U

Übergabe an Gruppe aus Durchsage 750
Überlebensfähigkeit 1153
Übermittlung kundenspezifischer Rufnummerninformation 652
Übernahme des Write Tokens, Experten-Modus 1532
Übertragung, Software (siehe Software-Übertragung) 1260
UC Applications, Experten-Modus 1680
UC Applikation
Neustart 1280, 1280
UC Booster Card
Neustart 1278, 1278
UC Smart
Benutzerverwaltung 1746
Grundeinstellungen 1745
Status 1747
UC Smart
Status 1374
Status abrufen 1374
UC Smart Client 495
UC Smart, Experten-Modus 1745

UC Suite
Ablagepfad für Client-Log-Dateien konfigurieren 1366
Abteilungen, Experten-Modus 1750
Aufbewahrungszeit für Contact-Center-Daten konfigurieren 1374
Aufbewahrungszeit für Protokolldateien konfigurieren 1373
Aufzeichnung der Client-Logs systemweit aktivieren 1365
Aufzeichnung der Client-Logs systemweit deaktivieren 1365
Aufzeichnung der Systemprotokolle aktivieren 1365
Aufzeichnung der Systemprotokolle deaktivieren 1365
Benachrichtigung 1369
Benutzerverzeichnis, Experten-Modus 1747
Client Logs 1364
Contact Center, Experten-Modus 1755
Datei-Upload, Experten-Modus 1765
E-Mail-Benachrichtigung 1368
E-Mail-Benachrichtigungen für Systemfehler konfigurieren 1370
Externes Verzeichnis, Experten-Modus 1753
Faxkopfzeilen, Experten-Modus 1776
Gruppen, Experten-Modus 1751
Konferenzschaltung, Experten-Modus 1767
Konfiguration externe Anbieter, Experten-Modus 1754
Profile, Experten-Modus 1774
Server, Experten-Modus 1767
Speichern der Client-Logs auf der Festplatte aktivieren 1367
Speichern der Client-Logs auf der Festplatte deaktivieren 1367
Systemprotokolle 1364
Systemwartung sofort durchführen 1373
Tageszeit für Wartung konfigurieren 1372
Templates, Experten-Modus 1752
Wartung 1371
Zeitpläne, Experten-Modus 1764
UC Suite 1747
Aufzeichnung der Client-Logs teilnehmerindividuell aktivieren 1366
Aufzeichnung der Client-Logs teilnehmerindividuell deaktivieren 1366
Client Logs herunterladen 1368
Überwachung 1363
Wartung 1363
UC Suite Clients 541
UC Suite Standort-Liste, Experten-Modus 1767
UC Suite, Experten-Modus 1747
UCD Agenten, Experten-Modus 1740
UCD, Experten-Modus 1700
Umfang für Sprachbox 610
Umleiten nach Zeit 667
Unfall melden 82
UP0 Teilnehmer, Experten-Modus 1656
Update 1260
benutzerdefiniert 1269
Update via File Upload, Experten-Modus 1501
Update via Internet, Experten-Modus 1500
Update via USB Stick, Experten-Modus 1501
Update, komplett
mit Fortschrittsanzeige starten 1264, 1273
Update, Software (siehe Software-Updates) 1260
Update, vollständig
im Hintergrund starten 1267
Upgrade 1260
Urlaubsplan 838, 890

V

VBZ Gruppenzuordnung, Experten-Modus 1723
VBZ Matrix, Experten-Modus 1724
VBZ-Gruppen 780, 780
Leitung zuweisen 782
Teilnehmer zuweisen 781
Zuordnung der KWZ-Nummern 781
VBZ-Matrix ändern 782
Verbindung zum lokalen CLA;CLA
lokale Verbindung 333, 334, 344
Verbindung zum zentralen CLA;CLA
zentrale Verbindung 344
Verbindungsaufbau-Status 1281
abfragen 1282
Verbotsliste anzeigen 770
Verbotslisten, Experten-Modus 1722, 1722
Verhalten im Notfall 81, 81
Verkabelung für LAN- und WAN-Anschlüsse 84
Vernetzung
homogen, nativ 1059
inhomogen, hybrid 1059
Knoten aus Netzverbund entfernen 1156
Vernetzungsplan 1059
Verzeichnis
Sofortnachricht 530
Verzeichnisse (UC Smart) 515
Verzeichnisse (UC Suite) 567
Virtuelle Teilnehmer, Experten-Modus 1668
Virtueller Konferenzraum 527
Voice-Mailbox, siehe Sprachbox 610
Voicemail 610
Voraussetzungen für Application Launcher 1203
Voraussetzungen für myAgent 875
Voraussetzungen für myPortal to go 958
Voraussetzungen für myReports 879
VPN
Authentifizierung 1020
Bandbreiten 1010
Clients 1026
Sicherheitsmechanismen 1019
Zertifikate 1021
VPN (Virtual Private Network) 1009
End-to-Site 1009
Site-to-Site 1009
VPN Aktive Dienste
Alle Dienste anzeigen 1032
Speziellen Dienst anzeigen 1032

VPN Aktive Tunnel
anzeigen 1034
Regeln anzeigen 1035
VPN Konfigurierte Dienste
Alle Dienste anzeigen 1033
ändern 1033
löschen 1034
umbenennen 1034
VPN Konfigurierte Tunnel
anzeigen 1035
hinzufügen 1036
Regeln anzeigen 1036
VPN Regeln
alle aktiven Regeln anzeigen 1038
alle konfigurierten Regeln anzeigen 1039
ändern 1040
hinzufügen für Gegenrichtung 1041
konfigurierte Regel hinzufügen 1040
löschen 1041
spezielle aktive Regel anzeigen 1039
VPN-Status 1281
VPN-Zertifikate
anzeigen 1023
importieren 1026
Lightweight-CA-Zertifikat generieren 1023
Trusted CA-Zertifikat importieren 1024
Zertifikatsanforderung generieren 1024, 1025
VPN, Experten-Modus 1581

W

Wahlaussendung 786
auswählen 787
Wählbares Rufnummernformat 525
Wählpause 644
Wahlplan, Experten-Modus 1626
Wahlregel, Experten-Modus 1628
Wahlregeln 792
Wahlwiederholung 639
WAN 386
Warnhinweise 72
Gefahr 73
Hinweis 76
Vorsicht 75
Warnung 74
Wartemusik 1244, 1247, 1247
Wartemusik (Music On Hold MOH) bei Anrufverteilung 762
Wartemusik, Expertenmodus 1726
Wartung, Experten-Modus 1779
Wartungsexpertenmodus 1494
WAV-Datei
Benachrichtigung 539, 622
Wave-Datei 1244, 1247
WBM 113
Startseite 113
Web Collaboration 528, 605, 605, 605
Web Collaboration, Experten-Modus 1777
Web Services 1203
Web Collaboration, Experten-Modus 1777
Web Services Interface 1187
Web Services, Experten-Modus 1777
Web Sicherheit, Experten-Modus 1601
Web-based Management 113
Weckeinrichtung 684
Wegeoptimierung 1069
Wegetabelle 790
Wegetabelle, Experten-Modus 1627
Weiterleitung, Experten-Modus 1741
Wiederanruf 656
Wiederherstellen 1251, 1259
Wizards 122
WLAN-Telefone 108

Z

Zeitparameter
Überwachung eines Übergeben vor Melden an eine UCD-Gruppe 763
Überwachung eines UCD-Rufes auf einer analogen Leitung 764
Zeitparameter, Experten-Modus 1543
Zeitplan 837, 890
Zeitpläne, Experten-Modus 1764
Zeitzonen-Einstellungen, Experten-Modus 1565, 1565
Zertifikatsgenerierung, Experten-Modus 1598
Zertifikatsverwaltung, Experten-Modus 1583, 1599
Ziel-Codec-Parameter, Experten-Modus 1636
Ziffernwahl 637
Zuletzt aktive Leasing, Expertenmodus 1614
Zurückstellen eines Rufes 670
Zustand Leitung, Experten-Modus 1740

© 2025 Mitel Networks Corporation. Alle Rechte vorbehalten. Mitel und das Mitel-Logo sind Marken der Mitel Networks Corporation. Unify und damit verbundene Marken sind Marken der Unify Software and Solutions GmbH & Co. KG. Alle anderen hier genannten Marken sind Eigentum der jeweiligen Inhaber.