A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

OpenScape Business V4

Administrator Documentation
07/2026

A31003-P3040-M100-01-76A9

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 2026, Mitel Networks Corporation

All rights reserved

Contents

1 Historique des modifications..... 38

2 Introduction et remarques importantes..... 40
2.1 À propos de cette documentation..... 40
2.1.1 Documentation et groupes cibles..... 41
2.1.2 Structure de la documentation de l'administrateur..... 42
2.1.3 Types de thèmes..... 44
2.1.4 Conventions de présentation des informations..... 45
2.2 Consignes de sécurité et avertissements..... 45
2.2.1 Indications : Danger..... 46
2.2.2 Avertissements : Avertissement..... 46
2.2.3 Avertissements : Attention..... 47
2.2.4 Avertissements : remarques..... 48
2.2.5 Consignes de sécurité spécifiques du pays..... 49
2.2.5.1 Informations de sécurité pour l'Australie..... 49
2.2.5.2 Informations de sécurité pour le Brésil..... 50
2.2.5.3 Informations de sécurité pour les États-Unis..... 50
2.2.5.4 Informations de sécurité pour le Canada..... 52
2.3 Remarques importantes..... 53
2.3.1 Comportement à adopter en cas d'urgence..... 54
2.3.2 Utilisation conforme..... 54
2.3.3 Mise au rebut et recyclage conformes..... 55
2.3.4 Normes et directives concernant l'installation..... 56
2.3.4.1 Raccordement d'OpenScape Business X au circuit électrique d'alimentation..... 56
2.3.4.2 Raccordement d'OpenScape Business S au circuit d'alimentation..... 56
2.3.4.3 Câblage blindé pour raccordements LAN et WAN de OpenScape Business X..... 57
2.3.4.4 Exigences de protection anti-incendie..... 57
2.3.4.5 Exigences de protection contre la foudre..... 58
2.3.4.6 Identifications pour OpenScape Business X..... 59
2.3.5 Remarques sur les émissions perturbatrices et les perturbations radio de OpenScape Business X..... 59
2.3.6 Protection et sécurité des données..... 59
2.3.7 Prescriptions techniques et conformité de OpenScape Business X..... 60
2.3.7.1 Conformité CE..... 60
2.3.7.2 Conformité aux normes des États-Unis et du Canada..... 60
2.3.7.3 Conformité aux normes internationales..... 61
2.3.8 Conditions de fonctionnement..... 61
2.3.8.1 Conditions d'exploitation d'OpenScape Business X..... 61
2.3.8.2 Conditions d'exploitation pour OpenScape Business S..... 62

3 Vue d'ensemble..... 63
3.1 Points forts..... 63
3.2 Communications unifiées..... 63
3.2.1 Fonctionnalités des communications unifiées (Présentation)..... 64
3.2.2 Accès utilisateur aux fonctionnalités UC (clients UC)..... 71
3.2.3 Intégration dans les applications commerciales..... 73
3.3 Modèles commerciaux d'OpenScape..... 74
3.3.1 Niveaux d'extension disponibles via les ventes..... 74
3.3.2 Modèles matériels UC..... 77
3.3.3 Matériel d'amplification UC..... 78
3.3.4 Modèles UC Logiciel (commutateur logiciel)..... 78
3.3.5 Structure et conditions environnementales..... 78

3.3.6 Téléphones compatibles..... 79
3.4 Autres informations.....81
3.4.1 Langues prises en charge..... 81
3.4.2 Liens Internet.....83

4 Concept d'administration..... 84
4.1 OpenScape Business Assistant (WBM).....84
4.1.1 Conditions nécessaires pour WBM.....84
4.1.2 Page d´accueil des WBM..... 84
4.1.3 Introduction au WBM..... 86
4.1.3.1 Comment se connecter au WBM..... 88
4.1.3.2 Comment se déconnecter de la WBM..... 88
4.1.4 Gestion d'utilisateur du WBM..... 88
4.1.4.1 Comment ajouter un administrateur..... 92
4.1.4.2 Comment modifier un administrateur..... 92
4.1.4.3 Comment modifier le propre mot de passe d'administrateur.....92
4.1.4.4 Comment effacer un administrateur..... 93
4.1.4.5 Comment modifier un mot de passe d'administrateur Manager E..... 93
4.1.5 Assistants..... 93
4.1.5.1 Assistants – Installation de base.....94
4.1.5.2 Assistants – Réseau / Internet.....94
4.1.5.3 Assistants - Téléphones / Abonnés..... 94
4.1.5.4 Assistants – Téléphonie centrale.....95
4.1.5.5 Assistants – Téléphonie utilisateurs..... 96
4.1.5.6 Assistants – Sécurité..... 97
4.1.5.7 Assistants – UC Smart (uniquement avec UC Smart)..... 97
4.1.5.8 Assistants – UC Suite (uniquement avec UC Suite)..... 97
4.1.5.9 Assistants – Unified Directory..... 98
4.1.5.10 Assistants - Services cloud..... 98
4.1.6 Centre de service.....98
4.1.6.1 Centre de service – **Documents**..... 99
4.1.6.2 Centre de service – **Logiciel** 99
4.1.6.3 Centre de service - **Inventory** > **Système**..... 99
4.1.6.4 Centre de service - **Inventory** > **Numéros d'appel**.....99
4.1.6.5 Centre de service - **Inventory** > **Vue d'ensemble du réseau**..... 100
4.1.6.6 Centre de service – **Mise à jour du logiciel**.....100
4.1.6.7 Centre de service – **Renvoi E-Mail**..... 100
4.1.6.8 Centre de service – **Accès distant**..... 100
4.1.6.9 Centre de service – **Redémarrer/Recharger**..... 100
4.1.6.10 Centre de service – **Diagnostic** > **Etat**..... 100
4.1.6.11 Centre de service – **Diagnostic** > **Observateur d'événements** (Event Viewer).....100
4.1.6.12 Centre de service – **Diagnostic** > **Trace**.....100
4.1.6.13 Centre de service – Diagnostic > Journal Service..... 101
4.1.7 Mode Expert.....101
4.1.8 Aide en ligne..... 101
4.1.8.1 Comment appeler l'aide en ligne contextuelle.....101
4.2 Gestionnaire E.....101
4.2.1 Comment charger KDS dans Manager E..... 103
4.2.2 Comment sauvegarder le KDS dans le système.....103

5 Configuration initiale d'OpenScape Business X.....104
5.1 Prérequis pour l'installation initiale.....105
5.2 Composantes.....106
5.3 Plan de numérotation..... 107
5.4 Schéma des adresses IP..... 108
5.5 Démarrage initial..... 110

5.5.1 Comment démarrer le système de communication....110
5.5.2 Comment raccorder le PC Admin au système de communication....111
5.5.3 Comment démarrer WBM....112
5.6 Intégration dans LAN client....114
5.6.1 Comment démarrer l'assistant Lancer la première installation....114
5.6.2 Paramètres système....115
5.6.2.1 Comment déterminer le logo d'écran et la désignation du produit....115
5.6.2.2 Comment spécifier les adresses IP (facultatif)....116
5.6.2.3 Comment spécifier le nom de l'équipement....117
5.6.3 Paramètres DHCP....117
5.6.3.1 Comment désactiver le serveur DHCP interne....118
5.6.3.2 Comment activer et configurer le serveur DHCP interne....118
5.6.3.3 Comment activer DHCP pour les appareils Mitel/Unify uniquement....120
5.6.4 Paramètres de pays et de temps....121
5.6.4.1 Comment sélectionner l'indicatif de pays et la langue du journal des événements....122
5.6.4.2 Comment entrer l'identifiant système DECT....122
5.6.4.3 Comment régler manuellement la date et l'heure....123
5.6.4.4 Comment obtenir la date et l'heure d'un serveur SNTP....124
5.6.5 Solution UC intégrée....124
5.6.5.1 Comment définir la solution UC....125
5.6.6 raccordement du système de communication au LAN client....125
5.6.6.1 Comment connecter le système de communication au réseau local du client....126
5.7 Configuration de base....126
5.7.1 Comment démarrer l'assistant Installation de base....126
5.7.2 Numéros système et mise en réseau....127
5.7.2.1 Comment entrer les numéros de téléphone système pour un raccordement installation....127
5.7.2.2 Comment entrer les numéros de téléphone système pour une connexion point à multipoint....128
5.7.2.3 Comment activer ou désactiver la mise en réseau....129
5.7.3 Données abonnés....130
5.7.3.1 Comment afficher les données d'abonné....132
5.7.3.2 Comment supprimer tous les numéros d'appel....132
5.7.3.3 Adapter les numéros d'appel préconfigurés au plan de numérotation individuel....133
5.7.3.4 Comment importer les données d'abonné via un fichier XML....133
5.7.3.5 Comment afficher les données de masse....134
5.7.4 Configuration RNIS....135
5.7.4.1 Comment configurer la connexion des abonnés RNIS....136
5.7.4.2 Comment configurer l'accès réseau RNIS....136
5.7.4.3 Comment configurer un raccordement multiposte RNIS....137
5.7.4.4 Comment désactiver la configuration RNIS....137
5.7.5 Accès Internet....138
5.7.5.1 Comment configurer l'accès Internet par un routeur Internet externe avec raccordement LAN....141
5.7.5.2 Comment configurer l'accès Internet par un routeur Internet externe par le raccordement WAN....141
5.7.5.3 Comment configurer l'accès Internet via un FAI préconfiguré....142
5.7.5.4 Comment configurer l'accès Internet via le FAI PPPoE par défaut....144
5.7.5.5 Comment configurer l'accès Internet via un FAI PPTP par défaut....147
5.7.5.6 Comment configurer l'accès à Internet via un routeur Internet externe sur le LAN avec un port WAN dédié à l'ITSP....149
5.7.5.7 Comment désactiver l'accès Internet....150
5.7.6 Téléphonie Internet....151
5.7.6.1 Comment configurer un ITSP prédéfini....152
5.7.6.2 Comment désactiver la téléphonie Internet....157
5.7.7 Abonnés....157
5.7.7.1 Comment configurer les abonnés RNIS....158
5.7.7.2 Comment configurer les abonnés analogiques....160
5.7.7.3 Comment configurer les abonnés UP0....163

5.7.7.4 Comment configurer les abonnés DECT....166
5.7.7.5 Comment configurer les abonnés IP et SIP....169
5.7.8 Configuration de UC Suite....172
5.7.8.1 Comment configurer la UC Suite....172
5.7.9 Configuration des boîtes de messagerie vocale de UC Smart....173
5.7.9.1 Comment configurer les boîtes vocales UC Smart....173
5.7.10 Paramètres du serveur de conférence....174
5.7.10.1 Comment modifier la configuration du serveur de conférence....174
5.7.11 Envoi d'e-mails (option)....175
5.7.11.1 Comment configurer l'envoi d'e-mails....175
5.8 Activités finales....178
5.8.1 Comment activer et affecter les licences....179
5.8.2 Comment préparer le clients UC Smart pour l'installation....181
5.8.3 Comment préparer les clients UC Suite pour l'installation....181
5.8.4 Comment réaliser la sauvegarde des données....183
5.9 Mise en service des téléphones IP....183
5.9.1 Comment configurer le téléphone IP....185
5.9.2 Comment configurer un téléphone SIP....186
5.10 Comment collecter les traces de diagnostic pour les incidents de type erreur....188
5.11 Refaire le flashage....189

6 Première configuration de OpenScape Business S....192
6.1 Conditions de la première configuration....192
6.2 Composantes....195
6.3 Schéma des adresses IP....196
6.4 Plan de numérotation....196
6.5 Installation du logiciel de communication....197
6.5.1 Comment installer le logiciel de communication....199
6.6 Mise en service....201
6.6.1 Comment démarrer l'assistant Lancer la première installation....201
6.6.2 Paramètres système....201
6.6.2.1 Comment déterminer le logo d'écran et la désignation du produit....202
6.6.2.2 Comment sélectionner l'indicatif de pays et la langue du journal de trace....203
6.6.2.3 Comment activer un port LAN supplémentaire en tant qu'interface WAN....203
6.6.2.4 Comment modifier le plan de numérotation à 4 chiffres....204
6.6.3 Solution UC....205
6.6.3.1 Comment définir la solution UC....205
6.7 Configuration de base....206
6.7.1 Comment démarrer l'assistant Installation de base....206
6.7.2 Numéros système et mise en réseau....206
6.7.2.1 Comment entrer les numéros de téléphone système pour un raccordement installation....207
6.7.2.2 Comment entrer les numéros de téléphone système pour une connexion point à multipoint....208
6.7.2.3 Comment activer ou désactiver la mise en réseau....209
6.7.2.4 Comment configurer le débit remontant de votre connexion Internet....209
6.7.3 Données abonnés....210
6.7.3.1 Comment afficher les données d'abonné....211
6.7.3.2 Comment supprimer tous les numéros d'appel....212
6.7.3.3 Adapter les numéros d'appel préconfigurés au plan de numérotation individuel....212
6.7.3.4 Comment importer les données d'abonné via un fichier XML....213
6.7.4 Accès Internet....213
6.7.4.1 Comment configurer l'accès à Internet via un routeur Internet externe sur le LAN avec un port WAN dédié à l'ITSP....214
6.7.5 Téléphonie Internet....215
6.7.5.1 Comment configurer un ITSP prédéfini....216
6.7.5.2 Comment désactiver la téléphonie Internet....221
6.7.6 Abonnés....222

6.7.6.1 Comment configurer les abonnés IP et SIP....222
6.7.7 Configuration de UC Suite....225
6.7.7.1 Comment configurer la UC Suite....225
6.7.8 Configuration des boîtes de messagerie vocale de UC Smart....226
6.7.8.1 Comment configurer les boîtes vocales UC Smart....226
6.7.9 Paramètres du serveur de conférence....227
6.7.9.1 Comment modifier la configuration du serveur de conférence....227
6.7.10 Envoi d'e-mails (option)....228
6.7.10.1 Comment configurer l'envoi d'e-mails....228
6.8 Activités finales....231
6.8.1 Comment activer et affecter les licences....232
6.8.2 Comment préparer le clients UC Smart pour l'installation....234
6.8.3 Comment préparer les clients UC Suite pour l'installation....234
6.8.4 Comment réaliser la sauvegarde des données....235
6.9 Mise en service des téléphones IP....236
6.9.1 Comment configurer le téléphone IP....237
6.9.2 Comment configurer un téléphone SIP....239
6.10 Désinstallation du logiciel de communication....240
6.10.1 Comment désinstaller le logiciel de communication....241
6.11 Ports utilisés....241
6.12 Comment collecter les traces de diagnostic pour les incidents de type erreur....243
6.13 Refaire le flashage....244

7 Licences....247
7.1 Procédure d'activation des licences....248
7.2 Licences....250
7.2.1 Licence de base....251
7.2.2 Licences utilisateur....252
7.2.3 Licences orientées utilisateur....253
7.2.4 Licences système....255
7.2.5 Licences d'évaluation....257
7.2.6 Licences de mise à niveau....258
7.2.7 Combinaisons de licences possibles....259
7.3 Procédure de licence d'un système de communication (Standalone)....261
7.3.1 CLS Connect....262
7.3.1.1 Comment activer CLS Connect....262
7.3.1.2 Abandon de CLS Connect....263
7.3.2 Activation des licences (Standalone)....263
7.3.2.1 Comment activer les licences en ligne (standalone)....264
7.3.2.2 Comment activer les licences hors ligne (standalone)....265
7.3.3 Attribution de licences (autonome)....266
7.3.3.1 Comment obtenir des licences d’abonné (autonome)....268
7.3.3.2 Comment effectuer la procédure de licence pour les lignes (standalone)....271
7.4 Procédure de licence de plusieurs systèmes de communication (interconnexion de réseaux)....272
7.4.1 Activation des licences (interconnexion de réseaux)....274
7.4.1.1 Comment activer les licences hors ligne (interconnexion de réseaux)....274
7.4.1.2 Comment regrouper les fichiers de licence dans un fichier de licences réseau....276
7.4.2 Attribution de licences (interconnexion de réseaux)....277
7.4.2.1 Comment effectuer la procédure de licence pour les abonnés (interconnexion de réseaux)....279
7.4.2.2 Comment effectuer la procédure de licence pour les lignes (interconnexion de réseaux)....282
7.4.2.3 Comment affecter des licences système à un noeud....282
7.4.2.4 Comment affecter la licence système "Networking" à un noeud....283
7.5 Information sur la licence....283
7.5.1 Information sur les licences sans interconnexion de réseaux (Standalone)....284
7.5.1.1 Comment afficher des informations sur les licences....284
7.5.2 Information sur la licence dans une interconnexion de réseaux....284

7.5.2.1 Comment afficher toutes les licences de l'interconnexion de réseaux....285
7.5.2.2 Comment afficher les licences liées à un noeud....285
7.5.2.3 Comment afficher toutes les licences utilisées en commun dans une interconnexion de réseaux....286
7.5.2.4 Comment afficher les licences abonnés et les licences orientées utilisateur en fonction du noeud....286
7.6 Affectation des profils de licence 286
7.6.1 Comment ajouter un profil de licence....287
7.6.2 Comment modifier un profil de licence....288
7.6.3 Comment affecter un profil de licence aux abonnés....288
7.6.4 Comment effacer un profil de licence....289
7.7 Ré-hébergement après remplacement du matériel....290
7.7.1 Comment effectuer un ré-hébergement après un remplacement de matériel....291
7.8 Serveur de licences (serveur de licence central, CLS) 291
7.8.1 Comment consulter ou modifier l'adresse IP du serveur de licences....291
7.8.2 Comment vérifier la connexion au Serveur de licence central (CLS)....292
7.9 Agent de licence (Customer License Agent, CLA)....292
7.9.1 Comment configurer la connexion avec l'agent de licence local....293
7.9.2 Comment modifier la connexion à l'agent de licence central....293
7.10 ID de verrouillage (Locking ID et Advanced Locking ID)....293
7.10.1 Comment interroger le Locking ID (identifiant de verrouillage) du système de communication....295
7.10.2 Comment interroger l'ID de verrouillage du commutateur logiciel....295
7.10.3 Comment interroger l'ID Advanced Locking du commutateur logiciel....295
7.11 Comment migrer d'une carte mère V2 vers une carte mère V3 (système autonome)....295
7.12 Comment migrer le nœud maître d'un système en réseau d'une carte mère V2 vers une carte mère V3....298
7.13 Comment migrer le nœud esclave d'un système en réseau d'une carte mère V2 vers une carte mère V3....298
7.14 Migration des systèmes HiPath 3000 vers le logiciel OSBiz V3 avec la carte mère V3....299
7.15 Mise à niveau de V2 vers V3 avec **CLS Connect**....299
7.16 Mise à niveau de V2 vers V3 sans **CLS Connect**....299

8 Intégration au réseau de données interne (LAN)....301
8.1 Interface LAN....301
8.1.1 Adresse IP et masque de sous-réseau de l'interface LAN....301
8.1.1.1 Comment modifier l'adresse IP et le masque réseau de la plate-forme matérielle....302
8.1.1.2 Comment modifier l'adresse IP et le masque réseau du commutateur logiciel....302
8.1.2 Plage d'adresses IP interne de l'interface LAN....303
8.1.2.1 Comment modifier la plage d'adresses IP interne de la plate-forme matérielle....303
8.1.2.2 Comment réinitialiser la plage d'adresses IP interne de la plate-forme matérielle....304
8.2 DHCP....304
8.2.1 Agent relais DHCP....305
8.2.1.1 Comment configurer la plateforme matérielle en tant qu'agent relais DHCP....305
8.2.2 Serveur DHCP 305
8.2.2.1 Comment activer et configurer le serveur DHCP de la plateforme matérielle....307
8.2.2.2 Comment désactiver le serveur DHCP de la plateforme matérielle....309
8.2.2.3 Comment activer et configurer le serveur DHCP du commutateur logiciel....309
8.2.2.4 Comment désactiver le serveur DHCP du commutateur logiciel....310
8.2.2.5 Comment activer DHCP pour les appareils Mitel/Unify uniquement....310
8.3 DNS - Résolution du nom....312
8.3.1 Comment définir un serveur DNS externe....313
8.4 Routage IP....314
8.4.1 Comment activer ou désactiver le routeur par défaut....314
8.4.2 Comment ajouter un itinéraire statique....315
8.4.3 Comment effacer les itinéraires statiques....316
8.5 Deployment Service (DLI et DLS)....316

8.5.1 Comment configurer un serveur DLS externe dans le serveur DHCP interne..... 318
8.5.2 Comment activer DLI interne.....319
8.5.3 Comment configurer le système de communication comme client Deployment et Licensing.....320

9 Connexion à fournisseur de services.....321
9.1 Accès Internet.....321
9.1.1 Accès Internet par routeur Internet externe 323
9.1.1.1 Comment configurer l'accès Internet par un routeur Internet externe avec raccordement LAN.... 324
9.1.1.2 Comment configurer l'accès Internet par un routeur Internet externe par le raccordement WAN.....325
9.1.1.3 Comment configurer l'accès à Internet via un routeur Internet externe sur le LAN avec un port WAN dédié à l'ITSP.....326
9.1.2 Accès Internet par un modem Internet 327
9.1.2.1 Comment configurer l'accès Internet via un FAI préconfiguré.....328
9.1.2.2 Comment configurer l'accès Internet via un FAI PPPoE par défaut.....330
9.1.2.3 Comment configurer l'accès Internet via un FAI PPTP par défaut.....333
9.1.3 Interface WAN.....335
9.1.4 DynDNS.....335
9.1.4.1 Comment configurer le service DynDNS.....336
9.1.4.2 Comment définir l'échangeur de messagerie.....338
9.2 Accès au CO via ITSP.....339
9.2.1 Configuration d'un ITSP.....341
9.2.1.1 Comment configurer un ITSP prédéfini.....342
9.2.1.2 Comment ajouter un nouveau fournisseur de services de téléphonie sur internet (ITSP).....348
9.2.1.3 Comment configurer un multisite via ITSP 355
9.2.1.4 Comment enregistrer un modèle ITSP préconfiguré en tant que nouveau modèle.....356
9.2.1.5 Comment adapter un modèle ITSP préconfiguré.....357
9.2.1.6 Comment actualiser manuellement un modèle ITSP préconfiguré..... 358
9.2.2 STUN (Simple Traversal of UDP through NAT).....358
9.2.2.1 Comment déterminer le mode STUN.....359
9.3 Accès réseau via lignes numériques et analogiques.....360
9.3.1 Lignes.....360
9.3.1.1 Comment configurer l'accès réseau RNIS..... 361
9.3.1.2 Comment configurer l'accès réseau analogique..... 362
9.3.1.3 Comment afficher toutes les lignes..... 363
9.3.1.4 Comment afficher une ligne individuelle.....363
9.3.1.5 Comment modifier l'indicatif de ligne.....364
9.3.1.6 Comment affecter le MSN à une ligne.....364
9.3.1.7 Comment modifier le protocole RNIS.....365
9.3.1.8 Comment modifier le mode de prise du canal B.....365
9.3.1.9 Comment modifier le mode de numérotation.....365
9.3.2 Faisceaux..... 366
9.3.2.1 Comment modifier l'affectation de faisceau.....369
9.3.2.2 Comment modifier le nom du faisceau.....369
9.3.2.3 Comment modifier l'indicatif du faisceau.....370
9.3.2.4 Comment configurer un débordement lorsque LCR est désactivé.....370
9.3.2.5 Comment configurer un débordement lorsque LCR est activé..... 370
9.3.2.6 Comment configurer la prise de ligne..... 371
9.3.2.7 Comment inscrire le numéro d'installation entrant et sortant..... 371
9.3.2.8 Comment configurer le format des numéros de téléphone transmis.....371
9.3.2.9 Comment configurer le type de numéro de téléphone transmis..... 372
9.3.2.10 Comment configurer le préfixe réseau..... 372
9.3.2.11 Comment définir un faisceau pour la mise en réseau et inscrire un second indicatif réseau.....373
9.3.3 Surveillance de la tonalité d'invitation à numéroter..... 373
9.3.3.1 Comment configurer la temporisation de la surveillance de la tonalité d'invitation à numéroter.... 374
9.3.3.2 Comment configurer la durée de surveillance de la tonalité d'invitation à numéroter.....375

9.3.3.3 Comment configurer le délai de composition des chiffres....376
9.3.3.4 Comment activer ou désactiver l'évaluation de la deuxième tonalité d'invitation à numéroter....376
9.4 Priorisation du réseau lorsque LCR est activé....377
9.4.1 Comment définir une priorité pour l'Indicatif réseau....377

10 Abonnés....378
10.1 Plan de numérotation....378
10.1.1 Plan de numérotation par défaut....379
10.1.2 Plan de numérotation individuel....380
10.1.2.1 Comment effacer ou modifier les numéros par défaut....381
10.1.2.2 Comment modifier les numéros par défaut spécifiques....382
10.1.2.3 Comment importer les numéros et données d'abonnés....382
10.2 Exigences pour la téléphonie LAN....383
10.2.1 Codecs audio....384
10.2.1.1 Comment configurer les paramètres du codec audio....385
10.2.1.2 Comment affecter les paramètres d'un codec audio à une destination....385
10.2.2 Transmission de tonalités selon RFC2833....386
10.2.2.1 Comment activer ou désactiver les tonalités fax et modem selon RFC2833....386
10.2.2.2 Comment activer ou désactiver la transmission MF selon RFC2833....387
10.2.3 Qualité de service....387
10.2.3.1 Comment configurer la Qualité de service....389
10.3 Abonnés IP....390
10.4 Stations SIP....391
10.5 Stations UP0....393
10.6 Stations DECT....394
10.7 Stations Mitel SIP DECT....395
10.8 Terminaux RNIS....395
10.8.1 Comment configurer l'interface S_0 pour abonnés RNIS....397
10.8.2 Comment autoriser uniquement les numéros paramétrés pour MSN....398
10.9 Stations analogiques....399
10.10 Abonnés virtuels....400
10.11 Programmation des touches....400
10.11.1 Comment programmer les touches de fonction des téléphones système....401
10.12 Profils d'abonnés....403
10.13 Configuration des abonnés....403
10.13.1 Comment configurer les stations IP....405
10.13.2 Comment configurer les abonnés SIP....409
10.13.3 Comment configurer les stations UP0....413
10.13.4 Comment configurer les abonnés DECT....416
10.13.5 Comment configurer les stations SIP-DECT Mitel via le provisioning....419
10.13.5.1 Comment configurer les stations SIP via le mode Expert....421
10.13.6 Comment configurer les abonnés RNIS....422
10.13.7 Comment configurer les abonnés analogiques....425
10.13.8 Comment modifier les noms des abonnés....428
10.14 Configuration des profils d'abonné....429
10.14.1 Comment créer un nouveau profil d'abonné....430
10.14.2 Comment afficher les profils d'abonné et leurs membres....431
10.14.3 Comment ajouter des membres à un profil d'abonné....431
10.14.4 Comment effacer les membres d'un profil d'abonné....432
10.14.5 Comment exporter ou importer un profil d'abonné....432
10.14.6 Comment modifier les valeurs et paramètres d'un profil....433
10.14.7 Comment exporter ou importer tous les profils d'abonné....434
10.15 Configuration des données d'authentification sur le téléphone SIP....435
10.15.1 Comment configurer les données d'authentification avec la WBM du téléphone SIP....435
10.15.2 Comment configurer les données d'authentification sur l'écran du téléphone SIP....437
10.16 Exporter les données d'abonné....438

10.16.1 Comment exporter les données d'abonné....439

11 UC Smart....440
11.1 Configuration de base pour UC Smart....441
11.1.1 Comment activer UC Smart....441
11.1.2 Comment configurer UC Smart....442
11.1.3 Comment configurer les conférences gérées par une application....443
11.1.4 Comment déterminer les adresses IP des composants du système....444
11.1.5 Comment déterminer l'état de UC Smart....444
11.2 Clients intelligents UC....445
11.2.1 myPortal @work....445
11.2.1.1 Prérequis pour myPortal @work....447
11.2.1.2 Configuration des utilisateurs myPortal @work....449
11.2.1.3 Étapes de configuration pour utiliser myPortal @work via Internet....456
11.2.1.4 Autres conseils de configuration & Paramètres....457
11.2.1.5 Guide de dépannage....459
11.2.1.6 Autres conseils....461
11.3 Utilisateurs de UC Smart....462
11.3.1 Comment configurer un utilisateur de UC Smart....463
11.3.2 Comment changer le mot de passe pour un utilisateur de UC Smart....463
11.4 Statut de présence (Présence)....464
11.5 Répertoires et Journal....465
11.5.1 Répertoires....465
11.5.1.1 Comment configurer les répertoires des téléphones système....466
11.5.2 Répertoire interne....466
11.5.2.1 Comment activer ou désactiver l'affichage d'un abonné dans le répertoire interne....467
11.5.3 Liste des favoris....467
11.5.4 Répertoire système....467
11.5.5 Annuaire unifié....468
11.5.5.1 Caractéristiques....469
11.5.5.2 Règles et Conventions....472
11.5.5.3 Chapitre 11.5.5.3 Limites fonctionnelles....473
11.5.5.4 Annuaire unifié dans les systèmes en réseau....474
11.5.6 Journal....474
11.6 Appels....475
11.6.1 Formats des numéros d'appel....475
11.7 Conférences....476
11.8 Messagerie instantanée....478
11.8.1 Messagerie instantanée....478
11.9 Boîte vocale (SmartVM)....478
11.9.1 Configuration de la boîte vocale (SmartVM) 481
11.9.1.1 Comment désactiver ou activer la boîte vocale....482
11.9.1.2 Comment configurer la boîte vocale (SmartVM)....482
11.9.1.3 Comment ajouter une boîte de messagerie standard pour un abonné....483
11.9.1.4 Comment modifier le groupe de discrimination pour un port de boîte vocale....484
11.9.1.5 Comment modifier la structure du menu téléphone ou de la boîte vocale....484
11.9.1.6 Comment charger, sauvegarder et effacer des messages d'accueils....485
11.9.1.7 Comment sauvegarder et rétablir les messages d'accueil et les messages....485
11.9.2 Service de notification pour les nouveaux messages....486
11.9.2.1 Comment activer ou désactiver la notification par e-mail....487

12 Suite UC....488
12.1 Configuration de base pour UC Suite....488
12.1.1 Comment activer UC Suite....488
12.1.2 Comment limiter la classe de discrimination des appels UC lancés côté système....489
12.2 Clients UC Suite....489

12.2.1 myPortal for Desktop..... 490
12.2.2 myPortal @work..... 490
12.2.3 myPortal for Outlook..... 491
12.2.4 Fax Printer (imprimante Fax)..... 491
12.2.5 myAttendant..... 491
12.2.6 Prérequis pour les clients PC UC Suite..... 492
12.2.7 Installation/Désinstallation silencieuse pour PC client UC Suite..... 496
12.2.7.1 Comment effectuer l'installation silencieuse..... 497
12.2.7.2 Comment effectuer une désinstallation silencieuse..... 497
12.2.8 Mise à jour automatique..... 499
12.3 Utilisateurs et profils utilisateur de UC Suite..... 499
12.3.1 Utilisateurs de UC Suite..... 499
12.3.1.1 Comment configurer un utilisateur de UC Suite..... 502
12.3.1.2 Comment réinitialiser un utilisateur de UC Suite..... 502
12.3.1.3 Comment configurer un utilisateur de la suite UC comme agent..... 503
12.3.1.4 Comment modifier l'état Présence pour un utilisateur de UC Suite..... 503
12.3.1.5 Comment changer le mot de passe pour un utilisateur de UC Suite..... 504
12.3.1.6 Comment modifier la longueur du mot de passe pour un utilisateur de UC Suite..... 504
12.3.2 Profils utilisateur de UC Suite..... 505
12.3.2.1 Comment ajouter un profil utilisateur de UC Suite..... 506
12.3.2.2 Comment modifier un profil utilisateur de UC Suite..... 507
12.3.2.3 Comment afficher les profils utilisateur de UC Suite..... 507
12.3.2.4 Comment ajouter des membres à un profil utilisateur de UC Suite..... 508
12.3.2.5 Comment effacer des membres dans un profil utilisateur de UC Suite..... 508
12.3.2.6 Comment effacer un profil utilisateur de UC Suite..... 508
12.4 Etat Présence et Service CallMe..... 509
12.4.1 État de présence (Présence)..... 509
12.4.2 Service CallMe..... 511
12.4.3 Renvoi d'appel en fonction de l'état..... 512
12.4.4 Renvoi d’appel basé sur une règle..... 513
12.5 Répertoires et Journal..... 514
12.5.1 Répertoires..... 514
12.5.1.1 Comment configurer les répertoires des téléphones système..... 516
12.5.2 Répertoire interne..... 517
12.5.2.1 Comment activer ou désactiver les abonnés du répertoire interne..... 517
12.5.2.2 Comment activer ou désactiver la recherche du répertoire interne uniquement..... 518
12.5.3 Répertoire externe..... 519
12.5.3.1 Comment importer un fichier CSV depuis le système de fichiers local vers le répertoire externe..... 520
12.5.3.2 Comment ajouter l'accès à une base de données externe pour le répertoire externe..... 522
12.5.3.3 Comment exporter un fichier CSV depuis l’annuaire externe..... 522
12.5.4 Répertoire hors ligne externe (LDAP)..... 522
12.5.4.1 Comment ajouter un répertoire hors ligne externe (LDAP) pour les client PC..... 524
12.5.4.2 Comment effacer un répertoire hors ligne externe (LDAP) pour les PC clients..... 524
12.5.4.3 Comment ajouter un répertoire hors ligne externe (LDAP) pour les téléphones système..... 525
12.5.5 Répertoire système..... 525
12.5.6 Annuaire unifié..... 526
12.5.6.1 Caractéristiques..... 527
12.5.6.2 Règles et Conventions..... 530
12.5.6.3 Chapitre 11.5.5.3 Limites fonctionnelles..... 531
12.5.6.4 Annuaire unifié dans les systèmes en réseau..... 532
12.5.6.5 Comment importer des contacts dans Unified Directory..... 532
12.5.6.6 Comment modifier ou ajouter de nouveaux contacts Unified Directory..... 534
12.5.7 Départements..... 534
12.5.7.1 Comment ajouter un département..... 534
12.5.7.2 Comment affecter les abonnés à un département..... 535

12.5.7.3 Comment modifier le département..... 535
12.5.7.4 Comment supprimer un département..... 535
12.5.8 Liste des favoris..... 536
12.5.9 Journal..... 536
12.5.9.1 Comment modifier la durée maximale de conservation d'un journal..... 538
12.6 Appels..... 538
12.6.1 Numérotation via le bureau et numérotation à partir du presse-papiers..... 538
12.6.2 Fenêtres surgissantes..... 539
12.6.3 Enregistrement des appels..... 539
12.6.3.1 Comment activer ou désactiver l'enregistrement des appels..... 540
12.6.3.2 Comment activer ou désactiver l'annonce d'enregistrement..... 540
12.6.3.3 Comment activer ou désactiver la tonalité d'avertissement pour l'enregistrement..... 541
12.7 Conférences..... 541
12.7.1 gestion des conférences..... 541
12.7.1.1 Comment modifier le numéro de sélection pour salle de conférence virtuelle..... 545
12.7.1.2 Autoriser ou interdire plusieurs participants externes à la conférence..... 546
12.7.1.3 Comment activer ou désactiver la tonalité de conférence..... 546
12.7.1.4 Comment modifier l'intervalle de temps pour la fin automatique des conférences..... 546
12.7.1.5 Comment afficher les détails concernant une conférence enregistrée..... 547
12.7.1.6 Comment supprimer la conférence enregistrée..... 547
12.7.1.7 Comment configurer l'enregistrement des conférences..... 547
12.7.2 Conférence Ad-hoc..... 548
12.7.3 Conférence programmée..... 549
12.7.4 Conférence permanente..... 550
12.7.5 Conférence ouverte..... 551
12.8 Messagerie instantanée..... 552
12.8.1 Messagerie instantanée..... 552
12.8.1.1 Comment activer ou désactiver les messages instantanés..... 553
12.9 Standard automatique..... 554
12.9.1 Standard automatique personnel..... 554
12.10 Messages Voix et Fax..... 554
12.10.1 Boîte vocale..... 554
12.10.1.1 Comment configurer le numéro d'appel de la boîte vocale..... 556
12.10.1.2 Comment configurer le renvoi temporisé vers la boîte vocale..... 557
12.10.1.3 Comment configurer les paramètres de la boîte vocale..... 557
12.10.1.4 Comment configurer la durée de conservation pour les messages vocaux..... 558
12.10.1.5 Comment activer ou désactiver la demande de mot de passe de la boîte vocale..... 558
12.10.1.6 Comment configurer les informations relatives aux messages vocaux reçus..... 559
12.10.1.7 Comment configurer la touche Boîte aux lettres pour l'interrogation des messages vocaux..... 559
12.10.2 Annonces de la boîte vocale..... 559
12.10.2.1 Comment importer une annonce pour la boîte vocale..... 561
12.10.2.2 Comment modifier la langue des annonces de la boîte vocale..... 562
12.10.3 Boîte Fax..... 562
12.10.3.1 Comment ajouter une boîte Fax pour des abonnés..... 563
12.10.3.2 Comment configurer le type de fichier pour les messages fax enregistrer (UC Suite)..... 563
12.10.4 Envoi de messages Fax avec Fax Printer..... 563
12.10.4.1 Comment ajouter une page de garde de fax..... 564
12.10.4.2 Comment modifier la page de garde centrale..... 565
12.10.4.3 Comment ajouter la ligne d'en-tête pour Fax Printer..... 565
12.10.4.4 Comment changer la ligne d'en-tête pour Fax Printer..... 566
12.10.4.5 Comment effacer la ligne d'en-tête pour Fax Printer..... 566
12.10.5 Service de notification pour les nouveaux messages (UC Suite)..... 566
12.10.6 Envoi d'e-mails..... 567
12.10.6.1 Comment configurer l'envoi d'e-mails..... 567
12.10.7 Modèle de SMS..... 568
12.10.7.1 Comment ajouter un modèle de SMS..... 569

12.10.7.2 Comment modifier le modèle SMS....570
12.10.7.3 Comment supprimer un modèle de SMS....570
12.10.8 Fax sur IP (T.38 / G.711 Fax)....571
12.10.8.1 Comment activer ou désactiver Fax over IP (Fax T.38)....572
12.11 Présentation de l'intégration Microsoft Office 365....572
12.11.1 Comment connecter le système OpenScape Business à Microsoft Office 365....573
12.11.2 Comment vérifier que les fonctionnalités de l'intégration Microsoft Office 365 sont configurées....576

13 Fonctions du téléphone....578
13.1 Appeler....578
13.1.1 Composition de chiffres....578
13.1.2 Numérotation par blocs....578
13.1.3 Numérotation KEYPAD....578
13.1.4 Détection de la fin de la numérotation....579
13.1.5 Edition numérotation (type GSM)....579
13.1.5.1 Comment activer ou désactiver l'édition de la numérotation....580
13.1.6 Répétition de la numérotation....580
13.1.6.1 Comment activer ou désactiver la répétition automatique....581
13.1.7 Numérotation abrégée centralisée....581
13.1.7.1 Comment ajouter un numéro abrégé....583
13.1.7.2 Comment importer les numéros abrégés d'un fichier XML....583
13.1.7.3 Comment exporter des numéros abrégés dans un fichier XML....584
13.1.7.4 Comment modifier les numéros abrégés....584
13.1.8 Numéro abrégé individuel (KWI)....585
13.1.9 Appel direct....585
13.1.10 Appel interphone/Réponse appel interphone....586
13.1.10.1 Comment activer / désactiver la protection contre les appels interphones pour un abonné....587
13.1.11 Numérotation associée....587
13.1.12 Réservation de ligne....588
13.1.12.1 Comment activer ou désactiver la réservation de ligne....588
13.1.13 Ligne privée....589
13.2 Signalisation d'appel, affichage du numéro....589
13.2.1 Différenciation de la signalisation d'appel....589
13.2.2 Présentation de la ligne appelante (CLIP)....590
13.2.2.1 Comment activer ou désactiver les CLIP configurables....590
13.2.3 Calling Line Identification Restriction CLIR (restriction de présentation du numéro de l'appelant)....591
13.2.3.1 Comment activer ou désactiver le Masquage de l'affichage du numéro, de l'abonné....591
13.2.4 Présentation de l'identification de la ligne connectée (COLP)....592
13.2.4.1 Comment activer ou désactiver la présentation du numéro de la ligne connectée....592
13.2.5 Non-identification de la ligne connectée (COLR)....592
13.2.6 CLIP No Screening (présentation de la ligne appelante avec transmission d'informations client spécifiques, relatives au numéro d'appel)....593
13.2.6.1 Comment configurer CLIP no screening....593
13.2.7 CLIP pour terminaux analogiques....594
13.2.8 Appel sans sonnerie / Coupure sonnerie....594
13.2.9 Conversion des numéros en nom avec la numérotation abrégée centralisée....594
13.3 Fonctions en cours de communication....594
13.3.1 Mise en garde....594
13.3.2 Parcage....595
13.3.3 Double appel....596
13.3.4 Va-et-vient....596
13.3.5 Transférer....596
13.3.6 Retour d'appel....597
13.3.7 Surveillance d'appel....598
13.3.7.1 Comment activer ou désactiver la surveillance d'appel pour un abonné....599
13.3.8 Message discret....599

13.3.9 Enregistrement de l'appel en direct (enregistrement vocal)..... 601
13.4 Gérer la disponibilité.....602
13.4.1 Renvois temporisés 603
13.4.1.1 Comment configurer un renvoi temporisé..... 604
13.4.2 Transfert d'appel (CF - Call Forwarding).....606
13.4.2.1 Comment activer ou désactiver le renvoi d'appel via lignes réseau analogiques.....608
13.4.2.2 Comment activer ou désactiver un renvoi d'appel vers une destination externe.....608
13.4.3 Renvoi d'appel Après tempo.....608
13.4.4 Renvoi temporisé au réseau (pas pour les Etats-Unis).....609
13.4.5 Acheminement.....610
13.4.5.1 Comment configurer l'acheminement..... 610
13.4.6 Pilotage.....610
13.4.7 Refuser les appels..... 611
13.4.8 Mise en réserve d'un appel..... 612
13.4.9 Ne pas déranger..... 612
13.5 Optimisation du déroulement de la communication.....613
13.5.1 Rappel..... 613
13.5.2 Avertissement..... 614
13.5.2.1 Comment activer ou désactiver l'avertissement..... 615
13.5.2.2 Comment activer/désactiver l'avertissement immédiat par le P.O.....615
13.5.3 Entrée en tiers (Intrusion)..... 616
13.5.3.1 Comment autoriser un abonné interne à effectuer des entrées en tiers..... 617
13.5.3.2 Comment autoriser l'entrée en tiers dans le poste de renvoi.....617
13.5.4 Textes d'absence.....618
13.5.4.1 Comment modifier un texte d'absence.....618
13.5.5 Textes messages.....618
13.5.5.1 Comment modifier un texte d'information.....619
13.5.6 Services associés.....619
13.5.6.1 Comment activer ou désactiver des services associés.....620
13.5.7 DISA..... 620
13.5.7.1 Comment activer ou désactiver la classe de discrimination DISA pour un abonné.....621
13.5.7.2 Comment configurer un numéro DISA..... 622
13.5.7.3 Comment configurer le mode sécurisé pour la fonction DISA..... 622
13.5.8 Appel flexible/PIN mobile..... 622
13.5.9 Relocate.....623
13.5.9.1 Comment valider pour l'ensemble du système un relocate/échange de numéro d'appel..... 623
13.5.10 Réinitialisation des fonctionnalités activées.....624
13.5.11 Procédures.....624
13.5.12 Equipement de réveil et rendez-vous..... 626
13.6 Vue d’ensembles des fonctions et des codes..... 626

14 Travailler en équipe (groupes).....631
14.1 Groupe d'interception, appel de groupe et groupe de recherche..... 631
14.1.1 Groupe d'interception 631
14.1.2 Appel de groupe.....633
14.1.3 Groupe de recherche.....637
14.1.4 Configuration des groupes d'interception d'appel, des groupes d'appel collectif et des groupements à l'aide des assistants 640
14.1.4.1 Configurer les groupes d'interception.....641
14.1.4.2 Comment ajouter ou supprimer des membres dans un groupe d'interception.....641
14.1.4.3 Comment ajouter un groupe d'appel collectif.....642
14.1.4.4 Comment modifier un groupe d'appel collectif (groupe).....643
14.1.4.5 Comment effacer un groupe d'appel collectif.....644
14.1.4.6 Comment ajouter ou effacer un membre dans un groupe d'appel collectif..... 645
14.1.4.7 Comment ajouter un groupe de recherche..... 645
14.1.4.8 Comment modifier un groupe de recherche.....647

14.1.4.9 Comment effacer un groupe de recherche..... 648
14.1.4.10 Comment ajouter ou effacer un membre dans un groupe de recherche.....648
14.1.5 Configuration des groupes d'interception d'appel, des groupes d'appel collectif et des groupements à l'aide du mode Expert..... 649
14.1.5.1 Comment activer ou désactiver l'affichage du numéro et du nom de l'appelant.....649
14.1.5.2 Comment activer ou désactiver la tonalité d'avertissement..... 650
14.1.5.3 Comment activer ou désactiver l'interception de retour d'appel.....650
14.1.5.4 Comment ajouter un groupe d'appel collectif (non-réponse ou avertissement).....650
14.1.5.5 Comment afficher ou modifier l'appel collectif (non-réponse ou avertissement).....651
14.1.5.6 Comment effacer l'appel collectif (non-réponse ou avertissement).....652
14.1.5.7 Comment ajouter ou effacer un membre du groupe d'appel collectif (non-réponse ou avertissement)..... 652
14.1.5.8 Comment activer ou désactiver le rejet des appels en instance pour les membres d'un groupe.....653
14.2 Configuration Team / groupe Team et Groupe chef/secrétaire / groupe Top..... 653
14.2.1 La configuration Team / le groupe Team..... 654
14.2.2 Groupe chef/secrétaire / groupe Top..... 658
14.2.3 Configuration des équipes (Team) / groupes Team et fonctions Chef/Secrétaire / groupes Top à l'aide des assistants 662
14.2.3.1 Comment ajouter une configuration Team / un groupe Team..... 662
14.2.3.2 Comment modifier la configuration Team / le groupe Team.....663
14.2.3.3 Comment effacer la configuration Team / le groupe Team.....664
14.2.3.4 Comment ajouter le groupe Chef/Secrétaire / groupe Top.....665
14.2.3.5 Comment modifier le groupe Chef/Secrétaire / groupe Top..... 666
14.2.3.6 Comment effacer un groupe Chef/Secrétaire / Top..... 667
14.2.4 Configuration des équipes (Team) / groupes Team et fonctions Chef/Secrétaire / groupes Top à l'aide du mode Expert.....667
14.2.4.1 Comment ajouter ou effacer un membre à la configuration Team / au groupe Team.....668
14.2.4.2 Comment modifier un membre d'une configuration Team / d'un groupe Team..... 669
14.2.4.3 Comment modifier les propriétés des membres d'une configuration Team / d'un groupe Team.....669
14.2.4.4 Comment modifier la programmation des touches du téléphone pour la configuration Team/le groupe Team..... 670
14.2.4.5 Comment ajouter une boîte Fax à une configuration Team / un groupe Team.....670
14.2.4.6 Comment ajouter ou effacer un membre au groupe Chef/Secrétaire / groupe Top.....671
14.2.4.7 Comment modifier un membre d'un groupe Chef/Secrétaire / groupe Top..... 671
14.2.4.8 Comment modifier les caractéristiques des membres d'un groupe Chef/Secrétaire / groupe Top.....672
14.2.4.9 Comment ajouter une boîte Fax à un groupe Chef/Secrétaire / un groupe Top.....672
14.3 MULAP de base et MULAP chef.....673
14.3.1 MULAP de base.....673
14.3.2 MULAP chef..... 676
14.3.3 Configuration de MULAP de base et MULAP chef..... 678
14.3.3.1 Comment ajouter un MULAP de base..... 679
14.3.3.2 Comment afficher ou modifier le MULAP de base.....679
14.3.3.3 Comment effacer le MULAP de base.....680
14.3.3.4 Comment ajouter ou effacer un membre du MULAP de base..... 680
14.3.3.5 Comment modifier le membre d'un MULAP de base.....681
14.3.3.6 Comment ajouter un MULAP chef.....681
14.3.3.7 Comment afficher ou modifier le MULAP chef.....682
14.3.3.8 Comment effacer le MULAP chef.....682
14.3.3.9 Comment ajouter ou effacer un membre du MULAP chef..... 683
14.3.3.10 Comment modifier un membre d'un MULAP chef.....683
14.3.3.11 Comment ajouter un MULAP de base dans un groupe..... 684
14.4 Groupes Messagerie vocale et Boîte Fax.....685
14.4.1 Groupe Boîte vocale..... 685

14.4.2 Groupe Boîte Fax....685
14.4.3 Configuration des groupes de boîtes vocales et groupes de boîtes Fax....686
14.4.3.1 Comment ajouter un groupe Boîte vocale....686
14.4.3.2 Comment afficher ou modifier le groupe Boîte vocale....687
14.4.3.3 Comment effacer un groupe Boîte vocale....687
14.4.3.4 Comment ajouter ou effacer un membre dans le groupe Boîte vocale....688
14.4.3.5 Comment modifier le membre d'un groupe Boîte vocale....688
14.4.3.6 Comment configurer un groupe Boîte Fax....689
14.4.3.7 Comment afficher ou modifier le groupe Boîte Fax....690
14.4.3.8 Comment effacer un groupe Boîte Fax....690
14.4.3.9 Comment ajouter ou effacer un membre dans le groupe Boîte Fax....690
14.5 Appel interphone pour groupes....691
14.5.1 Diffusion à un groupe....691
14.5.2 Transférer à un groupe à partir d'une diffusion....691
14.6 UCD (Uniform Call Distribution, distribution uniforme des appels)....692
14.6.1 Distribution d'appels / Groupe UCD....693
14.6.1.1 Comment configurer le renvoi d'appel / les groupes UCD....693
14.6.2 Agents UCD....695
14.6.2.1 Comment ajouter ou effacer des agents UCD....696
14.6.3 Post-traitement....697
14.6.3.1 Comment modifier le délai de post-traitement automatique....697
14.6.4 Distribution des appels avec priorité....697
14.6.4.1 Comment modifier la priorité de la file des appels....698
14.6.5 Prendre automatiquement les appels UCD....699
14.6.5.1 Comment modifier la réception automatique des appels UCD....699
14.6.6 File d'attente UCD....699
14.6.6.1 Comment modifier la file d'attente UCD....700
14.6.7 Débordement UCD....701
14.6.7.1 Comment modifier le débordement UCD....701
14.6.8 Renvoi de nuit UCD....702
14.6.9 Annonces/musique d'attente pour UCD....703
14.6.9.1 Comment modifier les annonces/la musique d'attente pour UCD....703
14.6.10 Transfert aux groupes UCD....704
14.6.10.1 Comment modifier le délai de retour d'appel pour les communications transférées aux groupes UCD....704
14.6.11 Libération des appels UCD via lignes analogiques....705
14.6.11.1 Comment modifier l'heure de libération des appels UCD via lignes analogiques....705

15 Routage de l'appel....706
15.1 Discriminations (contrôle de la numérotation)....706
15.1.1 Groupes de discrimination et classes de service....706
15.1.1.1 Comment modifier le nom d'un groupe de discrimination....707
15.1.1.2 Comment modifier les discriminations d'un groupe de discrimination....707
15.1.1.3 Comment afficher tous les membres d'un groupe de discrimination....708
15.1.2 Listes des numéros autorisés et des numéros interdits....708
15.1.2.1 Comment établir une liste des numéros d'urgence....709
15.1.2.2 Comment créer une liste des numéros autorisés et une liste des numéros interdits....710
15.1.2.3 Comment établir d'autres listes de numéros autorisés....710
15.1.2.4 Comment établir des listes de numéros interdits....711
15.1.2.5 Comment afficher tous les numéros de téléphone d'une liste des numéros interdits....711
15.1.2.6 Comment afficher tous les numéros de téléphone d'une liste des numéros autorisés....712
15.1.2.7 Comment modifier le filtre d'analyse pour les numéros interdits....712
15.1.3 Liste noire....713
15.1.3.1 Comment créer une liste noire pour les appels entrants en Mode expert....714
15.1.3.2 Comment modifier/supprimer tous les numéros de téléphone d'une liste noire....714
15.1.3.3 Comment afficher tous les numéros de téléphone d'une liste noire....715

15.1.3.4 Comment créer une liste noire pour les appels entrants dans la configuration....716
15.1.4 Renvoi de nuit....716
15.1.4.1 Comment attribuer les discriminations relatives au renvoi de nuit manuel....717
15.1.4.2 Comment effacer les discriminations pour le renvoi de nuit manuel....718
15.1.4.3 Comment configurer le renvoi de nuit avec programmation temporelle....718
15.1.4.4 Comment configurer un jour spécial pour le renvoi de nuit avec programmation temporelle....719
15.1.4.5 Comment effacer un jour spécial pour le renvoi de nuit avec programmation temporelle....719
15.1.5 Changement de catégorie d'accès automatique en fonction du temps....719
15.1.5.1 Calendrier....720
15.1.6 VBZ (matrice de connexion)....721
15.1.6.1 Groupes de restriction de trafic (groupes de matrices de connexion)....722
15.1.6.2 Affectation des numéros KWZ aux groupes de restriction de trafic....722
15.1.6.3 Comment affecter une ligne à un groupe de restriction de trafic....723
15.1.6.4 Comment affecter une ligne à un groupe de restriction de trafic....723
15.1.6.5 Comment modifier la matrice de connexions....724
15.1.7 Code de verrouillage centralisé, changement de catégorie d'accès....724
15.1.8 Code de verrouillage individuel (verrouiller le téléphone)....725
15.1.8.1 Comment réinitialiser le code de verrouillage individuel....725
15.1.9 Protection appel PCV par ligne réseau (Brésil uniquement)....726
15.1.10 Protection appel PCV par abonné (uniquement pour le Brésil)....726
15.2 LCR (Least Cost Routing)....726
15.2.1 Fonctionnalité LCR....726
15.2.1.1 Comment valider LCR....729
15.2.2 LCR-Plan de numérotation....730
15.2.2.1 Comment modifier le plan de numérotation....731
15.2.3 Table de routage LCR....732
15.2.3.1 Comment modifier les tables de routage....733
15.2.4 Classe de service LCR....733
15.2.4.1 Comment attribuer et modifier une classe de service LCR....734
15.2.5 LCR-Règles de numérotation....734
15.2.5.1 Comment modifier les règles de numérotation....736
15.2.6 Opérateur....737
15.2.7 Prise ciblée des lignes réseau....738
15.2.7.1 Comment configurer l'indicatif pour une prise ciblée de la ligne RNIS....738
15.2.7.2 Comment afficher les indicatifs pour la prise réseau ciblée....739
15.3 Evaluation de la numérotation et routage de l'appel....739
15.3.1 Aperçu du routage d'appel / LCR....740
15.3.2 Organigramme Evaluation de la numérotation....742
15.3.3 Routage d'appel et LCR en interconnexion de réseaux....743
15.3.3.1 Passerelle dédiée....745
15.3.4 Scénarios : évaluation de la numérotation et routage de l'appel....746
15.3.4.1 Abonné A appelle abonnés B via numéro d'appel interne....747
15.3.4.2 Abonné A appelle abonnés B à l'aide d'un numéro public....749
15.3.4.3 Abonnés A appelle abonné externe via le réseau....752
15.3.4.4 Réseau RNIS appelle abonné A....753
15.3.4.5 Configurations spéciales....753
15.3.4.6 Abonné A appelle abonné C via numéro d'appel interne....756
15.3.4.7 Abonné A appelle abonné C via numéro public d'une interconnexion de réseaux....757
15.3.4.8 RNIS appelle abonnés C....760
15.3.4.9 Passerelle 1 résau RNIS appelle abonné D....761
15.3.4.10 Abonnés D appelle abonné externe via le réseau....764
15.4 Appels d'urgence....766
15.4.1 Ligne directe après temporisation / Hotline....767
15.4.1.1 Comment configurer et modifier la destination de ligne directe (Hotline)....768
15.4.1.2 Comment modifier la temporisation du renvoi sur ligne directe....768
15.4.1.3 Comment configurer la temporisation ou la Hotline pour un abonné....769

15.4.2 Coupure de la ligne pour un appel d'urgence....769
15.4.2.1 Comment activer ou désactiver la libération de ligne pour les appels d'urgence....769
15.4.3 Uniquement pour les Etats-Unis, le Canada : Service d'appel d'urgence E911....770
15.4.3.1 Comment modifier le CLIP / LIN....770
15.4.4 Appels d'urgence en combinaison avec Mobile Logon....771
15.4.4.1 Configuration du scénario d'appel d'urgence....771
15.4.5 Service d'appel d'urgence E112 pour l'Europe....774
15.4.5.1 Comment ajouter une urgence SIP à une station....774
15.5 Service de gestion des appels (Call Admission Control)....775
15.5.1 Limitation du nombre de communications simultanées via ITSP....775
15.5.2 Limitation du besoin en bande passante pour les communications passerelle....776
15.5.3 Restriction du nombre de communications dans les scénarios de mise en réseau....776
15.6 Système multisociétés....776
15.6.1 Numérotation abrégée centralisée dans les systèmes multi-sociétés....778

16 Préposés....779
16.1 Standard automatique....779
16.1.1 Company AutoAttendant (UC Smart)....781
16.1.1.1 Comment configurer un standard automatique d'entreprise créé....782
16.1.1.2 Comment créer un nouveau standard automatique d'entreprise....783
16.1.2 Company AutoAttendant (UC Suite)....785
16.1.2.1 Calendriers....785
16.1.2.2 Modèles....794
16.2 Préposé OpenStage....796
16.3 mon assistant....797
16.3.1 Gestion des abonnés....798
16.3.2 Centre de messages 799
16.3.3 Scénario 1 : Comment paramétrer myAttendant sur un système OpenScape Business unique....799
16.3.4 Scénario 2 : Comment paramétrer deux myAttendants ou plus sur un système OpenScape Business unique....800
16.3.5 Scénario 3 : Comment configurer un réseau OpenScape Business avec un myAttendant central....801
16.4 Poste de renvoi....802
16.4.1 Comment configurer le poste de renvoi et les critères de renvoi....804
16.4.2 Comment configurer le poste de renvoi distinct central....805
16.4.3 Comment configurer le renvoi en cas de code de verrouillage....805
16.4.4 Comment configurer le renvoi en cas d'annonce....805

17 Centre de contacts multimédia....807
17.1 Centre d'appels Clients....807
17.1.1 myAgent....808
17.1.2 Prérequis pour myAgent....809
17.1.3 myReports....811
17.1.3.1 Comment réinitialiser le mot de passe pour l'Administrateur myReports....813
17.1.4 Conditions nécessaires pour myReports....813
17.1.5 Remarques sur l'utilisation simultanée de myAgent et des clients UC Suite....815
17.2 Agents....816
17.2.1 Fonctions soumises à autorisation pour les agents....817
17.2.2 Agents préférés....818
17.2.3 Agent figurant dans plusieurs files d'attente....818
17.2.4 Pauses du Centre de contacts....818
17.2.5 Connexion/Déconnexion d'agent via téléphone....818
17.3 Files d'attente et calendriers....822
17.3.1 Files d'attente....822
17.3.2 Planifications....824
17.3.3 Post-traitement....833
17.3.4 Niveau de service....833

17.3.5 Affichage mural (Wallboard)....834
17.3.6 Rappel d'agent....834
17.4 Suivi VIP....834
17.4.1 Priorités des appelants VIP....834
17.4.2 Liste d'appels VIP....835
17.5 Solution de repli (solution Fallback)....835
17.6 Configuration de base du centre d'appels....839
17.6.1 Exemple de configuration d'un centre d'appels....839
17.6.1.1 Comment configurer les groupes UCD dans le centre de contacts qui sert d'exemple....841
17.6.1.2 Comment configurer une solution de repli (fallback) dans l'exemple donné de centre de contacts....842
17.6.1.3 Comment configurer les abonnés en tant qu'agents du centre de contacts dans l'exemple présenté....843
17.6.1.4 Comment enregistrer les annonces pour le centre d'appels exemple....844
17.6.1.5 Comment charger les annonces pour le centre d'appels exemple....844
17.6.1.6 Comment ajouter le calendrier standard XYZ au centre d'appels de l'exemple....845
17.6.1.7 Comment ajouter le calendrier Schedule Hotline par défaut dans le centre de contacts de l'exemple....850
17.6.1.8 Comment ajouter des files d'attente pour le centre de contact d'exemple....852
17.6.1.9 Comment affecter les agents aux files d'attente du centre d'appels exemple....854
17.6.2 Marche à suivre pour la configuration....855
17.6.2.1 Comment configurer les groupes UCD pour le centre de contacts....856
17.6.2.2 Comment configurer un abonné en tant qu'agent....857
17.6.2.3 Comment enregistrer une annonce individuelle pour le centre d'appels....857
17.6.2.4 Comment charger une annonce individuelle pour le centre d'appels....858
17.6.2.5 Comment ajouter un calendrier....858
17.6.2.6 Comment modifier le calendrier....862
17.6.2.7 Comment effacer un calendrier....863
17.6.2.8 Comment enregistrer une règle (CCV) en tant que fichier PDF....864
17.6.2.9 Comment télécharger une règle (CCV) en tant que fichier de sauvegarde....864
17.6.2.10 Comment charger une règle téléchargée (CCV) dans un format de fichier de sauvegarde....865
17.6.2.11 Comment ajouter un calendrier....865
17.6.2.12 Comment modifier le calendrier....869
17.6.2.13 Comment activer ou désactiver la file d'attente....872
17.6.2.14 Comment configurer dans les files d'attente les pilotes des messages fax entrants....872
17.6.2.15 Comment définir les valeurs de consigne pour le degré de service....873
17.6.2.16 Comment définir les priorités des appelants VIP....873
17.6.2.17 Comment modifier la liste d'appels VIP....874
17.6.2.18 Comment définir les agents préférés....875
17.6.2.19 Comment effacer des agents préférés....876
17.6.2.20 Comment ajouter une pause dans un centre d'appels....876
17.6.2.21 Comment modifier la pause du centre de contacts....876
17.6.2.22 Comment effacer une pause d'un centre d'appels....877
17.6.2.23 Comment ajouter un code de post-traitement pour "Post-traitement simple"....877
17.6.2.24 Comment modifier le code de post-traitement pour "Post-traitement simple"....878
17.6.2.25 Comment effacer un code de post-traitement pour "Post-traitement simple"....878
17.6.2.26 Comment ajouter un code de post-traitement pour "Post-traitement multiple"....878
17.6.2.27 Comment modifier le code de post-traitement pour "Post-traitement multiple"....879
17.6.2.28 Comment effacer le code de post-traitement pour "Post-traitement multiple"....880
17.6.2.29 Comment affecter un agent à une file d'attente....880
17.6.2.30 Comment supprimer un agent dans une file d'attente....881
17.7 Remarques sur l'utilisation des centres d'appel....882
17.7.1 Restrictions lors de l'exploitation du centre d'appels....882
17.8 Remarques sur l'utilisation des téléphones DECT....885
17.9 Rapports....886
17.9.1 Modèles de rapport prédéfinis....887

18 Mobilité..... 888
18.1 Solutions mobilité intégrées..... 888
18.2 Sur la route..... 888
18.2.1 Mobility Entry..... 889
18.2.2 Postes de fonctionnalités d'entrée de mobilité..... 890
18.2.3 Dépendances pour l'entrée en mobilité..... 892
18.2.4 One Number Service..... 893
18.2.5 (Voir Téléphonie dual mode)..... 893
18.2.6 Configuration de l'entrée de mobilité..... 894
18.2.6.1 Comment intégrer les téléphones mobiles GSM..... 894
18.2.6.2 Comment intégrer des téléphones bimodes (GSM/WLAN) avec un client HFA ou SIP..... 896
18.2.6.3 Comment activer l'interface Web pour les téléphones mobiles et les clients Web..... 897
18.2.6.4 Comment effacer l'intégration de téléphone mobile..... 898
18.3 Mobilité au bureau..... 899
18.3.1 Desk Sharing..... 899
18.3.2 Solution sans fil intégrée..... 900
18.3.2.1 Présentation du système..... 901
18.3.2.2 Capacité du système..... 902
18.3.2.3 Téléphones cordless/DECT..... 903
18.3.2.4 Signification des résultats obtenus en testant le système radio..... 904
18.3.3 Configuration de la solution cordless intégrée..... 906
18.3.3.1 Comment entrer l'identifiant système DECT et configurer d'autres paramètres cordless (données pour l'ensemble du système)..... 906
18.3.3.2 Comment configurer les stations de base Cordless..... 907
18.3.3.3 Comment configurer pour la première fois les abonnés DECT..... 907
18.3.3.4 Comment connecter un téléphone DECT (combiné OpenStage/Gigaset) sur cordless..... 908
18.3.3.5 Comment ajouter d'autres téléphones DECT..... 910
18.3.3.6 Comment effacer des téléphones DECT..... 910
18.3.3.7 Comment configurer le paramètre Multi-SLC..... 911
18.3.3.8 Comment interroger les données des stations de base..... 911
18.3.3.9 Comment activer Message Waiting Indication (MWI - indication de message en attente) pour les téléphones DECT..... 912
18.3.3.10 Comment interroger l'état de connexion des téléphones DECT..... 912
18.3.4 Téléphones WLAN et points d'accès..... 913
18.3.4.1 Exigences du WLAN..... 913
18.4 Mobilité à domicile..... 913
18.4.1 Configuration pour VPN..... 914
18.4.2 Configuration de SIP Device@Home..... 915
18.4.3 Configuration pour le périphérique système@Home..... 917
18.4.4 Comme activer Equipement@Home..... 919
18.4.5 Comment mettre à jour le logiciel pour l'équipement HFA @Home..... 920
18.4.6 Comment indiquer un serveur STUN pour Equipement@Home..... 921

19 Sécurité..... 923
19.1 Pare-feu..... 923
19.1.1 Porthandling..... 923
19.1.1.1 Validation de port..... 924
19.1.1.2 Comment configurer la validation de port..... 924
19.1.1.3 Gestion des ports..... 925
19.1.1.4 Comment modifier les paramètres de gestionnaire de ports généraux..... 925
19.1.2 NAT..... 926
19.1.2.1 Comment configurer une règle NAT..... 926
19.1.2.2 Comment configurer plusieurs règles NAT avec le tableur NAT..... 927
19.1.2.3 Comment effacer une règle NAT..... 928
19.1.3 Application pare-feu..... 928
19.1.3.1 Comment afficher la configuration de l'application pare-feu..... 929

19.1.3.2 Comment restreindre les services via l'application pare-feu..... 930
19.1.3.3 Comment effacer la configuration de l'application pare-feu..... 930
19.1.4 Administration des services (OpenScape Business S)..... 930
19.1.4.1 Comment ajouter ou verrouiller des services..... 931
19.2 Cryptage de la signalisation et de la charge utile (SPE)..... 931
19.2.1 Comment activer ou désactiver SPE..... 933
19.2.2 Comment modifier les paramètres de sécurité modification..... 933
19.2.3 Comment importer le certificat SPE et la clé privée (PKCS#12)..... 934
19.2.4 Comment importer le certificat CA SPE..... 934
19.2.5 Comment activer ou désactiver SPE pour un abonné..... 935
19.3 Virtual Private Network VPN 935
19.3.1 Exigences pour VPN..... 936
19.3.2 Connexion des télétravailleurs via VPN..... 938
19.3.2.1 Comment configurer la connexion des télétravailleurs via VPN..... 940
19.3.2.2 Comment exporter les données des télétravailleurs..... 941
19.3.3 Mise en réseau de système de communication via VPN..... 942
19.3.3.1 Comment configurer la mise en réseau via un VPN..... 943
19.3.3.2 Comment exporter et importer les données de topologie d'une interconnexion de réseaux VPN..... 945
19.3.4 Mécanismes de sécurité VPN..... 945
19.3.5 Certificats VPN..... 947
19.3.5.1 VPN - Comment générer les certificats Lightweight CA..... 949
19.3.5.2 VPN - Gestion des certificats - Comment afficher le certificat..... 950
19.3.5.3 VPN - Comment importer le certificat CA Trusted (X.509)..... 950
19.3.5.4 VPN - Certificats Peer - Comment générer une demande de certificat (CSR)..... 951
19.3.5.5 VPN - Certificats Peer - Comment générer le certificat (PKCS#12)..... 951
19.3.5.6 VPN - Comment importer le certificat Peer (PKCS#12)..... 952
19.3.6 Clients VPN..... 952
19.3.6.1 Paramètres du client NCP VPN..... 954
19.3.6.2 Comment configurer un client NCP VPN..... 956
19.3.6.3 Comment configurer un client Shrew Soft VPN..... 956
19.3.6.4 Comment configurer un client iOS ou Android VPN..... 957
19.3.6.5 Comment configurer un client Mac OS-X VPN..... 957
19.3.7 VPN - Services..... 958
19.3.7.1 VPN - Services actifs - Comment afficher tous les services IPSec..... 958
19.3.7.2 VPN - Services actifs - Comment afficher le service IPSec spécifique..... 958
19.3.7.3 VPN - Services configurés - Comment afficher tous les services IPSec..... 959
19.3.7.4 VPN - Services configurés - Comment modifier le service IPSec..... 959
19.3.7.5 VPN - Services configurés - Comment renommer le service IPSec..... 960
19.3.7.6 VPN - Services configurés - Comment effacer le service IPSec..... 960
19.3.8 Tunnel VPN..... 960
19.3.8.1 VPN - Tunnels actifs - Comment afficher les données de tunnel générales..... 960
19.3.8.2 VPN - Tunnels actifs - Comment afficher les règles pour tous les tunnels..... 961
19.3.8.3 VPN - Tunnels configurés - Comment afficher les données de tunnel générales..... 961
19.3.8.4 VPN - Tunnels configurés - Comment afficher les règles pour tous les tunnels..... 962
19.3.8.5 VPN - Comment ajouter un tunnel configuré..... 962
19.3.9 Règles VPN..... 964
19.3.9.1 VPN - Règles actives - Comment afficher les règles..... 964
19.3.9.2 VPN - Règles actives - Comment afficher la règle spéciale..... 965
19.3.9.3 VPN - Règles configurées - Comment afficher toutes les règles..... 965
19.3.9.4 VPN - Règles configurées - Comment ajouter une règle..... 966
19.3.9.5 VPN - Comment modifier la règle..... 966
19.3.9.6 VPN - Comment ajouter une règle pour le sens opposé..... 967
19.3.9.7 VPN - Comment effacer la règle..... 967
19.3.10 Serveur PKI..... 968
19.3.10.1 VPN - Comment afficher le serveur PKI..... 968

19.3.10.2 VPN - Comment ajouter un serveur PKI....968
19.4 Gestion du certificat....968
19.4.1 Introduction....969
19.4.2 Comment générer un certificat CA....971
19.4.3 Comment générer le certificat autosigné....971
19.4.4 - Comment générer une demande de certificat (CSR)....972
19.4.5 Comment importer le certificat de serveur (PKCS#12)....973
19.4.6 Comment importer les certificats de serveur (PEM)....974
19.4.7 Comment afficher les certificats....975
19.4.8 Comment supprimer un certificat....975
19.4.9 Comment exporter un certificat (X.509)....975
19.4.10 Comment importer un certificat prolongé (X.509)....976
19.4.11 Comment activer les certificats....976
19.5 Sécurité web....977
19.5.1 Connexions au serveur Web....977
19.5.1.1 Comment configurer les connexions vers le serveur Web (UC Suite)....977
19.5.1.2 Comment configurer les connexions vers le serveur Web (UC Smart)....977
19.5.2 Protocole Admin....978
19.5.2.1 Comment effacer le protocole d'administration....978
19.5.2.2 Comment modifier la langue du protocole d'administration....978
19.6 Sécurité SQL....978
19.6.1 Noeud unique....979
19.6.2 Multinoeud....979
19.6.3 Configurer les mots de passe de la base de données SQL....980
19.7 Protection contre les attaques SIP (SIP Attack Protection)....981

20 Mise en réseau de OpenScape Business....982
20.1 Plan de mise en réseau....983
20.1.1 Réseaux homogènes et hétérogènes....983
20.1.1.1 Comment afficher la présentation de tous les noeuds OpenScape Business....984
20.1.2 Mono-passerelle et multi-passerelle....984
20.2 Fonctionnalités sur l'ensemble du réseau....985
20.2.1 Fonctionnalités à l'échelle du réseau des solutions UC....985
20.2.2 Fonctionnalités Voix sur l'ensemble du réseau....988
20.3 Procédure de licence d'une interconnexion de réseaux....990
20.4 Exigences pour la mise en réseau....990
20.4.1 Exigences pour la mise en réseau LAN....991
20.4.2 Plan de numérotation dans le réseau....992
20.4.2.1 Sélection des numéros de téléphone publics dans le réseau....994
20.5 Optimisation de route (Path Replacement)....994
20.5.1 Comment activer ou désactiver l'optimisation de route (Path Replacement) Activer ou désactiver....995
20.6 Scénarios de mise en réseau....995
20.6.1 Fonctions et restrictions....995
20.6.2 Mise en réseau de plusieurs systèmes OpenScape Business X....996
20.6.2.1 Comment configurer l'installation de base pour noeud 1 (Maître)....1000
20.6.2.2 Comment configurer la mise en réseau pour le noeud 1 (Maître)....1001
20.6.2.3 Comment configurer l'installation de base pour le noeud 2 (Esclave)....1002
20.6.2.4 Comment configurer la mise en réseau pour le noeud 2 (Esclave)....1003
20.6.2.5 Comment contrôler la fonction de mise en réseau pour Maître....1004
20.6.2.6 Comment configurer les faisceaux et les paramètres du faisceau (réseau RNIS pour le maître)....1004
20.6.2.7 Comment configurer les faisceaux et les paramètres de faisceau (faisc. 16) (Maître)....1005
20.6.2.8 Comment configurer LCR pour la mise en réseau (Maître)....1005
20.6.2.9 Comment configurer le faisceau et les paramètres du faisceau (Esclave)....1006
20.6.2.10 Comment configurer LCR pour la mise en réseau (Esclave)....1007
20.6.3 Mise en réseau d'OpenScape Business X et d'OpenScape Business S (passerelle unique)....1008

20.6.3.1 Comment configurer l'installation de base pour noeud 1 (Maître)....1014
20.6.3.2 Comment configurer la mise en réseau pour le noeud 1 (Maître)....1015
20.6.3.3 Comment configurer l'installation de base pour le noeud 2 (Esclave)....1016
20.6.3.4 Comment configurer la mise en réseau pour le noeud 2 (Esclave)....1017
20.6.3.5 Comment configurer l'installation de base pour le noeud 3 (Esclave)....1018
20.6.3.6 Comment contrôler la fonction de mise en réseau pour Maître....1019
20.6.3.7 Configurer la mise en réseau pour le noeud 3 (Esclave)....1019
20.6.3.8 Comment configurer LCR pour la mise en réseau (Noeud 3, Esclave)....1020
20.6.3.9 Comment configurer LCR pour la mise en réseau (Noeud 2)....1021
20.6.3.10 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 1, Maître)....1023
20.6.3.11 Comment configurer les faisceaux et les paramètres de faisceau (Faisc. 16) (Noeud 1)....1023
20.6.3.12 Comment configurer LCR pour la mise en réseau (Noeud 1)....1024
20.6.4 Mise en réseau d'OpenScape Business X et d'OpenScape Business S (Multi-Gateway)....1026
20.6.4.1 Comment configurer l'installation de base pour noeud 4 (OpenScape Business S, maître)....1034
20.6.4.2 Comment configurer la mise en réseau pour le noeud 4 (Maître)....1035
20.6.4.3 Comment configurer l'installation de base pour le noeud 1 (Esclave)....1035
20.6.4.4 Comment configurer la mise en réseau pour le noeud 1 (Esclave)....1036
20.6.4.5 Comment configurer l'installation de base pour le noeud 2 (Esclave)....1037
20.6.4.6 Comment configurer la mise en réseau pour le noeud 2 (Esclave)....1038
20.6.4.7 Comment configurer l'installation de base pour le noeud 3 (Esclave)....1038
20.6.4.8 Comment configurer la mise en réseau pour le noeud 3 (Esclave)....1039
20.6.4.9 Comment contrôler la fonction de mise en réseau pour Maître....1040
20.6.4.10 Comment configurer la multi-passerelle pour noeud 4 (Maître)....1040
20.6.4.11 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 1, Esclave)....1041
20.6.4.12 Comment configurer LCR pour la mise en réseau (Noeud 1, Esclave)....1042
20.6.4.13 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 2, Esclave)....1044
20.6.4.14 Comment configurer LCR pour la mise en réseau (Noeud 2, Esclave)....1045
20.6.4.15 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 3, Esclave)....1047
20.6.4.16 Comment configurer LCR pour la mise en réseau (Noeud 3, Esclave)....1047
20.6.4.17 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 4, Maître)....1049
20.6.4.18 Comment configurer LCR pour la mise en réseau (Noeud 4, Maître)....1050
20.6.5 Mise en réseau de OpenScape Business dans un environnement d'hébergement....1053
20.6.6 Mise en réseau d'OpenScape Business X et d'OpenScape 4000....1056
20.6.7 Mise en réseau de OpenScape Business X et OpenScape Voice....1063
20.6.8 Association de connexions externes à OpenScape Business via interconnexion SIP....1066
20.6.9 Numérotation ouverte dans les réseaux OpenScape Business X....1067
20.6.9.1 Comment configurer la numérotation ouverte....1068
20.6.10 Mise en réseau par RNIS....1070
20.6.11 Interconnexion de réseaux OpenScape Business avec raccordement réseau ITSP central....1071
20.7 Poste de renvoi central dans l'interconnexion de réseaux (pas pour les Etats-Unis)....1073
20.7.1 Comment configurer un poste de renvoi central dans une interconnexion de réseaux multi-passerelle....1074
20.8 Gestionnaire de présence....1076
20.9 État de la synchronisation dans l'interconnexion de réseaux....1076
20.9.1 Synchronisation manuelle dans interconnexion de réseaux....1077
20.9.2 Comment démarrer la synchronisation manuelle....1077
20.10 Survivabilité....1078
20.10.1 Configuration de la survivabilité....1080
20.11 Retirer un noeud de l'interconnexion de réseaux....1080

21 Autres équipements....1082
21.1 Dispositif d'annonce analogique....1082
21.1.1 Comment ajouter un équipement d'annonce analogique....1083
21.1.2 Comment modifier le retard de l'annonce....1084
21.2 Poste de portier et Ouverture de porte....1084
21.2.1 DoorLine a/b T01-T04....1084

21.2.1.1 Comment configurer le port abonné de DoorLine a/b T01-T04....1085
21.2.1.2 Comment configurer le poste pour la Doorline a/b T01-T04....1086
21.2.2 DoorCom Analog....1086
21.2.2.1 Comment configurer le port abonné de DoorCom Analog....1087
21.2.2.2 Comment configurer le poste pour DoorCom Analog....1087
21.2.3 Poste de portier avec amplificateur (TFE-S)....1087
21.2.3.1 Comment configurer le poste de portier....1089
21.2.4 Haut-parleur....1089
21.2.4.1 Comment configurer l'interface abonné analogique pour un haut-parleur....1090
21.2.4.2 Comment configurer l'interface d'abonné analogique pour le raccordement d'un amplificateur au module TFE S....1091
21.3 Relais....1091
21.3.1 Comment configurer un actionneur....1093
21.4 Capteurs....1094

22 Application Connectivity....1096
22.1 CSTA....1096
22.1.1 Comment modifier le numéro de port pour CSTA....1098
22.1.2 Comment activer ou désactiver CMD pour l'utilisation de TAPI 120....1099
22.1.3 Comment activer ou désactiver le serveur DSS pour l'utilisation des touches DSS sur l'ensemble du réseau....1100
22.1.4 Comment activer ou désactiver le CSP....1100
22.1.5 Comment activer ou désactiver Media Extension Bridge....1101
22.2 OpenScape Business TAPI 120/170....1101
22.2.1 OpenScape Business TAPI 120....1102
22.2.2 OpenScape Business TAPI 170....1106
22.3 Interface des services Web....1111
22.4 Open Directory Service....1112
22.4.1 Comment activer ou désactiver Open Directory Service....1117
22.4.2 Comment démarrer de nouveau Open Directory Service....1117
22.4.3 Comment configurer le mot de passe pour l'accès à Open Directory Service....1117
22.4.4 Comment configurer le serveur ODBC en serveur ODBC Bridge....1118
22.4.5 Comment ajouter une source de données externe pour Open Directory Service....1120
22.4.6 Comment réaliser un aperçu des résultats de la recherche LDAP pour Open Directory Service....1123
22.4.7 Comment effacer une source de données externe pour Open Directory Service....1123
22.5 Intégration d'Active Directory Service....1124
22.5.1 Comment configurer Active Directory Service....1125
22.6 Application Launcher....1126
22.6.1 Conditions nécessaires pour Application Launcher....1127
22.6.2 Profil avec les données de configuration de Application Launcher....1128
22.6.2.1 Comment fournir le profil avec les données de configuration de Application Launcher....1128
22.7 Présentation de myPortal for Teams....1128
22.7.1 Comment configurer MyPortal for Teams....1129
22.7.2 Comment importer myPortal for Teams dans le magasin d'applications Teams....1130
22.8 Unify Phone....1130
22.8.1 Comment configurer la connectivité du Unify Phone....1131
22.8.2 Comment configurer l'instance utilisateur de Unify Phone....1132
22.8.3 Comment gérer les utilisateurs Phone Unify....1133
22.8.3.1 Comment créer de nouveaux utilisateurs de téléphone Unify....1133
22.8.3.2 Comment ajouter des utilisateurs existants d'Unify Phone....1134
22.8.3.3 Comment modifier les détails des utilisateurs de Unify Phone....1135
22.8.3.4 Comment retirer ou supprimer des utilisateurs d'Unify Phone....1135
22.8.3.5 Comment préparer un numéro alternatif et un routage des appels pour une interopérabilité des téléphones Unify....1136
22.9 Mitel WX....1136
22.9.1 Comment configurer la connectivité Mitel WX....1137

22.9.2 Migration d’Unify Phone vers Mitel WX....1138
22.9.3 Comment configurer Mitel WX dans le service CloudLink....1139
22.10 Service Let's Encrypt....1140
22.10.1 Comment configurer le service Let's Encrypt....1140
22.11 Service CloudLink....1141
22.11.1 Comment configurer le service CloudLink....1142
22.11.2 Comment ouvrir l'interface web de CloudLink Daemon....1142
22.11.3 Comment configurer l'interface web de CloudLink Daemon....1143
22.11.4 Comment activer/configurer SIP Connector pour se connecter à Workflow Studio....1144
22.12 Numéros de pilote CloudLink....1144
22.12.1 Comment configurer les numéros pilotes CloudLink....1144

23 Taxation....1146
23.1 Données de connexion....1146
23.1.1 Saisie des données de connexion....1146
23.1.1.1 Comment activer ou désactiver la saisie des données de connexion....1147
23.1.1.2 Comment activer ou désactiver l'enregistrement des communications....1147
23.1.1.3 Comment configurer la création de journal pour les montants en devise ou les unités de tarification....1148
23.1.1.4 Comment configurer le facteur de taxation, la devise et la précision....1148
23.1.1.5 Comment activer ou désactiver la consignation des quatre derniers chiffres....1149
23.1.1.6 Comment activer ou désactiver l'enregistrement des appels sortants sans connexion....1149
23.1.1.7 Comment activer ou désactiver l'enregistrement des communications entrantes....1150
23.1.1.8 Comment activer ou désactiver le protocole de communication....1150
23.1.1.9 Comment activer ou désactiver l'édition des MSN....1151
23.1.1.10 Comment activer ou désactiver le format décimal....1151
23.1.2 Codes affaire....1151
23.1.2.1 Comment configurer le code Affaire....1153
23.1.2.2 Comment configurer la procédure de contrôle des codes affaire....1153
23.1.2.3 Comment activer ou désactiver la répétition de la numérotation avec code affaire....1153
23.2 Affichage et tranmission des données de connexion....1154
23.2.1 Transfert des montants (non disponible aux Etats-Unis)....1154
23.2.1.1 Comment configurer la transmission des montants....1155
23.2.2 Affichage des coûts de connexion sur le téléphone....1155
23.2.3 Affichage de la durée de connexion sur le téléphone....1155
23.2.3.1 Comment activer ou désactiver l'affichage de durée de la communication....1156
23.2.4 Transmission des données de connexion....1156
23.2.4.1 Comment sélectionner le format....1164
23.2.4.2 Comment activer ou désactiver la transmission de données de taxation via HTTPS....1164
23.3 Contrôle des coûts....1164
23.3.1 Remarque sur les voies de communication onéreuses....1165
23.3.1.1 Comment configurer l'avertissement relatif à une voie de communication onéreuse....1165
23.3.2 Protection contre les fraudes de taxation....1165
23.3.2.1 Comment activer ou désactiver la Protection contre une falsification des taxes....1166
23.4 Outils de taxation....1166
23.4.1 Accounting Manager....1166
23.4.2 Teledata Office....1167

24 Entretien....1168
24.1 Configuration téléphonique....1168
24.1.1 Date et heure....1168
24.1.1.1 Comment paramétrer manuellement la date et l'heure....1169
24.1.1.2 Comment paramétrer le fuseau horaire....1169
24.1.1.3 Comment configurer le format de la date....1169
24.1.2 SNTP....1170
24.1.2.1 Comment reprendre la date et l'heure d'un serveur SNTP....1170

24.1.3 Logos Téléphone....1170
24.1.3.1 Comment charger un logo téléphone dans le système....1171
24.1.3.2 Comment distribuer un logo téléphone aux téléphones système....1172
24.1.3.3 Comment effacer le logo Téléphone....1172
24.1.4 Affichage spécifique du client....1172
24.1.4.1 Comment modifier l'affichage du client (nom du système)....1173
24.1.5 Texte en plusieurs langues....1173
24.1.6 Menus flexibles....1173
24.1.6.1 Comment modifier les menus flexibles....1174
24.1.7 Musique en attente....1174
24.1.7.1 Comment importer la musique d'attente....1175
24.1.7.2 Comment configurer la fonction Musique d'attente interne....1176
24.1.7.3 Comment modifier la musique d'attente pour chaque groupe de restriction de tarif....1176
24.1.8 Annonces....1177
24.1.8.1 Comment configurer les communications d'interphone (UC Smart)....1178
24.1.8.2 Comment configurer les communications d'interphone (UC Smart)....1179
24.1.9 Signalisation d'abonné à abonné....1180
24.1.10 Protection de la signalisation sur le canal vocal....1180
24.1.11 Temporisations....1180
24.1.12 Gestion des fonctionnalités Centrex....1180
24.1.12.1 Comment activer ou désactiver la gestion des fonctionnalités Centrex....1181
24.2 Sauvegarde et restauration....1181
24.2.1 Jeux de sauvegarde....1182
24.2.1.1 Comment afficher les jeux de sauvegarde....1183
24.2.1.2 Comment effacer les jeux de sauvegarde....1183
24.2.2 Supports de sauvegarde....1183
24.2.2.1 Comment ajouter un moyen de sauvegarde....1184
24.2.2.2 Comment modifier le moyen de sauvegarde....1185
24.2.2.3 Comment effacer le moyen de sauvegarde....1186
24.2.3 Sauvegarde immédiate....1186
24.2.3.1 Comment sauvegarder immédiatement un jeu de sauvegarde....1187
24.2.4 Sauvegarde planifiée....1188
24.2.4.1 Comment sauvegarder un jeu de sauvegarde de façon planifiée....1188
24.2.5 Rétablir....1189
24.2.5.1 Comment rétablir un jeu de sauvegarde....1189
24.3 Mises à jour....1190
24.3.1 Utilisation d'un serveur Web local....1192
24.3.1.1 Comment configurer l'accès au serveur web local....1192
24.3.2 Mise à jour du système de communication....1193
24.3.2.1 Comment actualiser le système à partir d'un serveur Web....1194
24.3.2.2 Comment actualiser le système à partir d'un support USB....1196
24.3.2.3 Comment actualiser le système à partir d'un chargement de fichier....1197
24.3.2.4 Comment actualiser le système à partir d'un support USB sans accès WBM....1198
24.3.3 Mise à jour des téléphones système....1199
24.3.3.1 Comment charger le logiciel de téléphonie dans le système....1199
24.3.3.2 Comment distribuer le logiciel téléphone aux téléphones système....1200
24.3.3.3 Comment effacer le logiciel de téléphonie....1200
24.3.3.4 Comment activer ou désactiver la diffusion automatique du logiciel de téléphonie....1201
24.3.3.5 Comment configurer le reflashing automatique....1201
24.3.4 Etat du logiciel....1203
24.3.4.1 Comment interroger l'état du logiciel....1203
24.4 Redémarrer, recharger, éteindre....1203
24.4.1 Redémarrage d'OpenScape Business....1204
24.4.1.1 Comment lancer un redémarrage d'OpenScape Business....1204
24.4.2 Rechargement d'OpenScape Business....1205
24.4.2.1 Comment lancer un rechargement d'OpenScape Business....1205

24.4.3 Arrêt (shutdown) d'OpenScape Business X..... 1206
24.4.3.1 Comment arrêter OpenScape Business X..... 1206
24.4.4 PIN pour l'arrêt contrôlé (Shutdown) de OpenScape Business X..... 1206
24.4.4.1 Comment configurer un PIN pour l'arrêt contrôlé (Shutdown) d'OpenScape Business X.....1207
24.4.5 Redémarrage (restart) de l'application UC..... 1207
24.4.5.1 Comment lancer le redémarrage (restart) de l'application UC..... 1207
24.5 Gestion Inventory..... 1208
24.5.1 Etat du système 1208
24.5.1.1 Comment consulter l'état de l'abonné..... 1209
24.5.1.2 Comment interroger l'état d'établissement de la liaison..... 1210
24.5.1.3 Comment interroger l'état ITSP..... 1210
24.5.1.4 Comment afficher les adresses IP..... 1210
24.5.2 Inventaire..... 1211
24.5.2.1 Comment interroger Inventory d'OpenScape Business X..... 1212
24.5.2.2 Comment interroger Inventory d'OpenScape Business S..... 1213
24.6 Actions automatiques..... 1213
24.6.1 Action automatique Regroupement des positions non utilisées..... 1214
24.6.1.1 Comment modifier l'action automatique Regroupement des positions non utilisées..... 1214
24.6.1.2 Comment lancer (activer) l'action automatique Regroupement des positions non utilisées..... 1215
24.6.1.3 Comment arrêter (désactiver) l'action automatique Regroupement des positions non utilisées..... 1215
24.6.2 Action automatique Notification DLS..... 1216
24.6.2.1 Comment modifier l'action automatique Notification DLS..... 1216
24.6.2.2 Comment lancer l'action automatique Démarrer la notification DLS (activer)..... 1217
24.6.2.3 Comment arrêter l'action automatique Arrêter la notification DLS (désactiver)..... 1217
24.6.3 Mécanisme d'alerte pour la durée de vie de la carte SDHC..... 1218
24.6.3.1 Comment définir une notification en cas d’erreur sur la carte SDHC..... 1219
24.6.3.2 Comment démarrer le mécanisme d'alerte pour l'action automatique sur la durée de vie de SDHC..... 1220
24.6.3.3 Comment cloner et changer une carte SDHC..... 1220
24.6.3.4 Comment créer un fichier de sauvegarde de données SDHC..... 1222
24.6.3.5 Comment remplacer une carte SDHC..... 1224
24.7 Gestion de l'alimentation..... 1226
24.7.1 Comment activer ou désactiver la gestion de l'alimentation..... 1227
24.7.2 Comment modifier le mode de liaison Ethernet des interfaces LAN..... 1227
24.8 Surveillance et maintenance d'OpenScape Business..... 1228
24.8.1 Contrôler une connexion réseau d'OpenScape Business X..... 1228
24.8.1.1 Comment envoyer un Ping..... 1228
24.8.1.2 Comment tester l'itinéraire de trace..... 1229
24.8.2 SNMP (Simple Network Management Protocol)..... 1229
24.8.2.1 Comment afficher toutes les communautés..... 1241
24.8.2.2 Comment ajouter une communauté..... 1242
24.8.2.3 Comment modifier la communauté..... 1242
24.8.2.4 Comment effacer la communauté..... 1243
24.8.2.5 Comment afficher des traps..... 1243
24.8.2.6 Comment afficher les détails d'un trap..... 1244
24.8.3 Actions manuelles..... 1244
24.8.3.1 Comment Télécharger les données de diagnostic / les journaux de diagnostic..... 1246
24.8.4 Traces..... 1247
24.8.4.1 Comment charger le fichier journal de trace système..... 1254
24.8.4.2 Comment effacer le fichier journal de trace système..... 1255
24.8.4.3 Comment définir les paramètres Trace sur des valeurs par défaut..... 1255
24.8.4.4 Comment afficher tous les profils de trace..... 1256
24.8.4.5 Comment démarrer ou arrêter un profil de trace..... 1256
24.8.4.6 Comment afficher ou modifier la configuration du format Trace..... 1257
24.8.4.7 Comment afficher ou modifier les interfaces d'édition Trace..... 1257

24.8.4.8 Comment afficher ou modifier le journal Observateur d’événements / Journal de trace client.. 1258
24.8.4.9 Comment télécharger et ouvrir le journal Observateur d’événements / le journal Trace client.. 1258
24.8.4.10 Comment effacer le journal Observateur d’événements / le journal Trace client.....1259
24.8.4.11 Comment afficher les composantes de trace M5T.....1259
24.8.4.12 Comment démarrer ou arrêter une composante Trace M5T.....1260
24.8.4.13 Comment modifier la composante de trace M5T.....1260
24.8.4.14 Comment démarrer ou arrêter le chiffrement de la trace.....1260
24.8.4.15 Comment interroger l'état Chiffrement de la trace.....1261
24.8.4.16 Comment modifier le mot de passe pour le chiffrement de la trace.....1261
24.8.4.17 Comment importer le certificat pour le Chiffrement de la trace (Secure Trace) à partir d'un fichier X.509.....1262
24.8.4.18 Comment afficher ou modifier la configuration Trace de la pile H.323.....1262
24.8.4.19 Comment modifier les modules H.323.....1263
24.8.4.20 Comment télécharger ou ouvrir le fichier-journal Trace de la pile H.323.....1263
24.8.4.21 Comment effacer le fichier-journal Trace de la pile H.323.....1263
24.8.4.22 Comment modifier la composante de licence Trace.....1264
24.8.4.23 Comment afficher les détails d'un profil de trace.....1264
24.8.4.24 Comment arrêter tous les profils de trace.....1265
24.8.4.25 Comment ajouter un profil Trace.....1265
24.8.4.26 Comment afficher les composantes de trace.....1265
24.8.4.27 Comment afficher les détails d'une composante de trace.....1266
24.8.4.28 Comment démarrer ou arrêter une composante Trace.....1266
24.8.4.29 Comment arrêter toutes les composantes de trace.....1267
24.8.4.30 Comment définir les paramètres Trace sur des valeurs par défaut.....1267
24.8.4.31 Comment modifier la composante de trace.....1267
24.8.4.32 Comment transférer automatiquement les fichiers journaux système.....1268
24.8.4.33 Comment démarrer le service des données de crash du noyau.....1268
24.8.4.34 Comment arrêter le service des données de crash du noyau.....1269
24.8.4.35 Comment démarrer la trace du serveur média.....1269
24.8.4.36 Comment arrêter la trace du serveur média.....1270
24.9 TCP-Dump.....1270
24.9.1 Comment démarrer TCP-Dump.....1270
24.9.2 Comment arrêter TCP-Dump.....1271
24.9.3 Comment effacer TCP-Dump.....1271
24.10 Démon RPCAP.....1271
24.10.1 Comment activer Démon RPCAP.....1272
24.10.2 Comment désactiver Démon RPCAP.....1272
24.11 Événements (events).....1272
24.11.1 Comment modifier la consignation des événements par LAN.....1274
24.11.2 Comment charger le fichier de journal d'événements.....1275
24.11.3 Comment effacer le fichier de journal d'événements.....1275
24.11.4 Comment modifier les paramètres e-mail des événements.....1276
24.11.5 Comment afficher le tableau de réactions aux événements.....1276
24.11.6 Comment modifier les paramètres de réaction d'un événement.....1276
24.11.7 Comment modifier les paramètres de réaction de plusieurs événements.....1277
24.11.8 Comment télécharger ou ouvrir les journaux de diagnostic.....1278
24.11.9 Comment effacer les journaux de diagnostic.....1279
24.11.10 Comment définir les destinations de la signalisation d'alarme.....1279
24.12 Données de configuration pour les diagnostics.....1279
24.12.1 Comment générer des données de configuration pour les diagnostics.....1280
24.13 Gestionnaire de cartes.....1282
24.13.1 Comment inscrire le logiciel de communication sur le disque SSD M.2 SATA à l’aide de Card Manager.....1282
24.13.2 Comment utiliser le gestionnaire de cartes pour écrire le logiciel de communication sur la carte SDHC.....1284
24.14 Surveillance et Maintenance de la suite UC.....1286

24.14.1 Journalisation....1287
24.14.1.1 Comment activer ou désactiver l'enregistrement de la journalisation système.... 1288
24.14.1.2 Comment activer ou désactiver l'enregistrement de la journalisation client sur l'ensemble du système.... 1288
24.14.1.3 Comment activer ou désactiver l'enregistrement de la journalisation client, individuellement par abonné....1289
24.14.1.4 Comment configurer le chemin d'archivage pour fichiers journal Client....1290
24.14.1.5 Comment activer ou désactiver le stockage centralisé des journaux clients sur le disque dur du système de communication.... 1290
24.14.1.6 Comment télécharger les journaux Client de tous les abonnées internes.... 1291
24.14.2 Notification....1291
24.14.2.1 Comment configurer les notifications par e-mail des erreurs du système....1294
24.14.3 Maintenance....1294
24.14.3.1 Comment configurer la période de la journée pour la maintenance....1296
24.14.3.2 Comment configurer la durée de conservation des fichiers de protocole....1296
24.14.3.3 Comment effectuer une maintenance système instantanée....1296
24.14.3.4 Comment configurer la durée de conservation des données de Centre d'appels.... 1297
24.15 Surveillance de UC Smart.... 1297
24.15.1 Comment appeler l'état actuel de UC Smart....1297
24.16 Services à distance....1298
24.16.1 RSP.servicelink....1298
24.16.1.1 Comment installer, configurer et enregistrer le plugin RSP.servicelink....1301
24.16.1.2 Comment activer le plugin RSP.servicelink.... 1302
24.16.1.3 Comment désactiver le plugin RSP.servicelink.... 1303
24.16.1.4 Comment réinitialiser le plugin Service RSP....1303
24.16.1.5 Comment configurer un PIN pour l'activation et la désactivation du plugin RSP.servicelink....1304
24.16.2 Accès distant....1304
24.16.2.1 Comment activer l'accès distant via RNIS.... 1305
24.16.2.2 Comment configurer les PC avec Microsoft Windows Vista pour l'accès à distance via RNIS.... 1305
24.16.2.3 Comment configurer un PC sous Microsoft Windows 7 pour l'accès à distance via ISDN..... 1307
24.16.2.4 Comment activer l'accès distant par l'accès Internet avec adresse IP fixe.... 1308
24.16.2.5 Comment activer l'accès distant par l'accès Internet sans adresse IP fixe.... 1309
24.16.2.6 Comment désactiver l'accès distant.... 1310
24.16.3 Utilisateur en ligne.... 1310
24.16.3.1 Comment démarrer l'utilisateur en ligne....1311

25 Migration....1312
25.1 Mise à niveau logicielle pour les systèmes OpenScape Business X....1313
25.1.1 Mise à niveau logicielle d'OpenScape Business X V2 vers OpenScape Business X V3....1314
25.1.1.1 Mise à niveau des systèmes sous licence permanente avec CLS Connect.... 1315
25.1.1.2 Mise à niveau des systèmes sous licence permanente sans CLS Connect.... 1315
25.1.1.3 Mise à niveau des systèmes sous licence PayGo....1316
25.1.2 Mise à niveau logicielle d'OpenScape Business X V3 vers OpenScape Business X V4....1316
25.2 Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3....1316
25.2.1 Comment mettre à niveau UC Business Booster Server de V2 vers V3....1317
25.3 Migration matérielle et logicielle des systèmes OpenScape Business X vers V3....1318
25.3.1 Migration d'OpenScape Business X V2 vers OpenScape Business X V3....1320
25.3.1.1 Comment migrer vers des systèmes à licence permanente V3 avec CLS Connect....1321
25.3.1.2 Comment migrer vers des systèmes à licence permanente V3 sans CLS Connect....1322
25.3.1.3 Comment migrer vers les systèmes avec licence V3 PayGo....1323
25.3.2 Migration d'OpenScape Business X V3 avec carte mère V2 vers OpenScape Business X V4 avec carte mère V3....1323
25.3.3 Migration d'OpenScape Business X V2 avec carte mère V2 vers OpenScape Business X V4 avec carte mère V3....1324
25.4 Migration d'un système OpenScape Business X V3 de la carte mère V2 vers la carte mère V3....1324

25.4.1 Comment migrer vers des systèmes à licence permanente de carte mère V3 avec CLS Connect.. 1326
25.4.2 Comment migrer vers des systèmes à licence permanente de carte mère V3 sans CLS Connect.. 1327
25.4.3 Comment migrer vers des systèmes de licence Carte mère V3 PayGo..... 1328
25.5 Mise à niveau logicielle d'OpenScape Business S..... 1329
25.5.1 Mise à niveau logicielle d'OpenScape Business S V3 vers OpenScape Business S V4..... 1330
25.5.2 Mise à niveau logicielle d'OpenScape Business S V2 vers OpenScape Business S V4..... 1330
25.5.3 Mise à niveau logicielle d'OpenScape Business S V2 vers OpenScape Business S V3..... 1331
25.5.3.1 Comment passer à la version V3 des systèmes sous licence permanente avec CLS Connect..... 1332
25.5.3.2 Comment passer à des systèmes sous licence V3 PayGo..... 1332
25.5.4 Mise à niveau logicielle d'OpenScape Business S V2 vers OpenScape Business S V3..... 1333
25.6 Migration/mise à niveau du réseau OpenScape Business V2 vers V3..... 1334
25.6.1 Scénario 1 : Migration matérielle du nœud maître, mise à niveau logicielle des nœuds esclaves.... 1335
25.6.1.1 Migration/mise à niveau avec CLS Connect dans le nœud maître..... 1335
25.6.1.2 Migration/mise à niveau sans CLS Connect dans le nœud maître..... 1336
25.6.2 Scénario 2 : Mise à niveau logicielle de tous les systèmes du réseau vers la version 3..... 1337
25.6.2.1 Mise à jour du logiciel avec CLS Connect dans le nœud maître..... 1337
25.6.2.2 Mise à jour du logiciel sans CLS Connect dans le nœud maître..... 1338
25.6.3 Scénario 3a : Mise à niveau logicielle de tous les nœuds..... 1339
25.6.4 Scénario 3b : Mise à niveau logicielle dans le nœud maître, migration du matériel dans les nœuds esclaves..... 1339
25.6.4.1 Migration / Mise à niveau avec CLS Connect dans le nœud maître..... 1339
25.6.4.2 Migration / Mise à jour sans CLS Connect dans le nœud maître..... 1340
25.7 Migration de HiPath 3000 vers OpenScape Business V4..... 1341
25.7.1 Migration des systèmes HiPath 33xx, 35xx et 3800 vers OpenScape Business X5/X8 V4..... 1343
25.7.1.1 Comment charger KDS à partir de HiPath 3000..... 1347
25.7.1.2 Comment lire les paramètres HG1500..... 1348
25.7.1.3 Comment convertir la KDS HiPath 3000 V9..... 1348
25.7.1.4 Comment remplacer le matériel HiPath 3300/3500..... 1349
25.7.1.5 Comment remplacer le matériel du HiPath 3800..... 1350
25.7.1.6 Comment lancer la première installation..... 1351
25.7.1.7 Comment charger le KDS converti dans le nouveau système..... 1351
25.7.1.8 Comment générer un nouveau fichier de licence..... 1352
25.7.1.9 Comment activer le fichier de licence hors ligne..... 1353
25.7.1.10 Comment affecter les licences..... 1354
25.7.1.11 Comment réinitialiser les entrées LCR..... 1354
25.7.2 Migration d'un système HiPath 3000 avec OpenScape Office V3 HX vers OpenScape Business V3 avec carte mère V3..... 1354
25.7.3 Migration d'un réseau HiPath 3000 vers un réseau OpenScape Business..... 1356
25.7.4 Migration d'une interconnexion de réseaux HiPath 3000 V9 avec HiPath 5000 RSM..... 1358
25.7.5 Fonctionnalités et interfaces modifiées/supprimées du HiPath 3000..... 1361
25.8 Migration au sein d'OpenScape V3 Business..... 1368
25.9 Migration des modules matériels..... 1369
25.9.1 Remplacement de SLMO24N par SLMU..... 1369
25.9.2 Remplacement de SLM8N par SLMU..... 1369
25.9.3 Remplacement de SLCN par SLMUC (SLMU + CMAe)..... 1370

26 Configurations et capacités..... 1371
26.1 Valeurs maximales pour les stations..... 1371
26.2 Valeurs maximales des lignes..... 1373
26.3 Valeurs maximum des ressources..... 1376
26.3.1 Détails sur l'utilisation des canaux DSP..... 1377
26.3.2 Détails sur l'utilisation des canaux proxy RTP..... 1378
26.4 Valeurs maximales des ressources..... 1379
26.4.1 Connexion au fournisseur de services..... 1379
26.4.2 Abonnés..... 1379

26.4.3 Niveaux d'extension UC Smart....1379
26.4.4 Niveaux d'extension de Smart Voicemail....1382
26.4.5 Niveaux d'extension UC Suite....1384
26.4.6 Fonctions sur le téléphone....1392
26.4.7 Travailler en équipe (groupes)....1395
26.4.8 Routage des appels....1399
26.4.9 Centre de contacts multimédia....1400
26.4.10 Limites d'extension Mobility....1401
26.4.11 Sécurité....1402
26.4.12 Mise en réseau de OpenScape Business....1403
26.4.13 Connectivité des applications....1403
26.4.14 Comptabilité....1405

27 Mode Expert....1406
27.1 Conventions de présentation des discriptions de paramètres....1406
27.2 **Maintenance**....1407
27.2.1 **Configuration**....1407
27.2.1.1 **Configuration > Musique d'attente (MoH) > Charger sur la passerelle**....1407
27.2.1.2 **Configuration > Annonces > Charger vers la passerelle**....1408
27.2.1.3 **Configuration > Configuration de port**....1409
27.2.1.4 **Configuration > SmartVM**....1409
27.2.1.5 **Configuration > SmartVM > Opérations boîte de messagerie**....1410
27.2.1.6 **Configuration > SmartVM > Opérations sur les fichiers**....1410
27.2.1.7 **Configuration > Branding**....1412
27.2.1.8 **Configuration > Adresse passerelle IP**....1413
27.2.2 **Image logicielle**....1413
27.2.2.1 **Image logicielle > Logiciel système > Mise à jour via Internet**....1413
27.2.2.2 **Image logicielle > Logiciel système > Mise à jour via chargement de fichier**....1414
27.2.2.3 **Image logicielle > Logiciel système > Mise à jour via chargement de fichier**....1415
27.2.2.4 **Image logicielle > Images du téléphone > Charger**....1415
27.2.2.5 **Image logicielle > Images du téléphone > Distribuer**....1416
27.2.2.6 **Image logiciel > Images téléphone > Déploiement vers le terminal**....1416
27.2.2.7 **Image logicielle > Images du téléphone > Charger**....1417
27.2.2.8 **Image logicielle > Images du téléphone > Distribuer**....1417
27.2.3 **Cordless**....1418
27.2.3.1 **Cordless > Stations de base**....1418
27.2.4 **Etat des ports/modules**....1420
27.2.4.1 **Etat des ports/modules > Etat des modules**....1420
27.2.4.2 **Etat port/modules > Out of Service (hors service)**....1421
27.2.5 **Traces**....1421
27.2.5.1 **Traces > Configuration du format Trace**....1422
27.2.5.2 **Traces > Interfaces d'édition Trace**....1423
27.2.5.3 **Traces > Journal de trace**....1424
27.2.5.4 **Traces > Bouclage numérique**....1424
27.2.5.5 **Traces > Journal Trace client**....1424
27.2.5.6 **Traces > Composante de trace M5T**....1425
27.2.5.7 **Traces > Secure Trace**....1425
27.2.5.8 **Traces > Secure Trace (chiffrement de la trace) > Certificat SecureTrace**....1426
27.2.5.9 **Traces > Secure Trace (chiffrement de la trace) > Paramètres SecureTrace**....1426
27.2.5.10 **Traces > Trace de pile H.323**....1427
27.2.5.11 **Traces > Surveillance d'appel**....1428
27.2.5.12 **Traces > Composante de licence**....1430
27.2.5.13 **Traces > Profils de trace**....1431
27.2.5.14 **Traces > Composants Trace**....1431
27.2.5.15 **Traces > TCP- Dump**....1432
27.2.5.16 **Traces > rpcap Daemon**....1433

27.2.5.17 **Traces** > **Données de crash du noyau**....1433
27.2.5.18 **Traces** > **Trace du serveur média**.... 1434
27.2.6 **Evénements (events)**.... 1435
27.2.6.1 **Evénements** > **Configuration des événements** 1435
27.2.6.2 **Evénements** > **Fichier-journal d'événements** 1435
27.2.6.3 **Evénements** > **E-mail**....1435
27.2.6.4 **Evénements** > **Tableau de réactions** 1436
27.2.6.5 **Evénements** > **Journaux de diagnostic** 1437
27.2.6.6 **Evénements** > **Signalisation d'alarme**.... 1437
27.2.7 **Redémarrer / Recharger**.... 1438
27.2.7.1 **Redémarrer / Recharger** > **Redémarrer / Recharger**....1438
27.2.8 **SNMP**.... 1439
27.2.8.1 **SNMP** > **Communautés** 1439
27.2.8.2 **SNMP** > **Communautés** > **Communautés de lecture** 1439
27.2.8.3 **SNMP** > **Communautés** > **Communautés d'écriture** 1440
27.2.8.4 **SNMP** > **Communautés** > **Trap Communautés** 1440
27.2.8.5 **SNMP** > **Traps** 1440
27.2.9 **Protocole Admin**....1441
27.2.9.1 **Protocole Admin** > **Configuration** 1441
27.2.9.2 **Protocole d'admin** > **Données du protocole d'admin** 1441
27.2.10 **Actions**....1442
27.2.10.1 **Actions** > **Actions manuelles** > **Journaux de diagnostic** 1442
27.2.10.2 **Actions** > **Actions manuelles** > **Maintenance DLI**....1444
27.2.10.3 **Actions** > **Actions automatiques** > **Regroupement des positions non utilisées** 1444
27.2.10.4 **Actions** > **Actions automatiques** > **Notification DLS** 1445
27.2.10.5 **Actions > Actions automatiques > Contrôle d'intégrité SDHC**....1445
27.2.11 **Diagnostic de la plate-forme**....1445
27.2.12 **Diagnostics des applications**....1446
27.2.12.1 **Diagnostics des applications** > **Paramètres développeur** > **Sortie console de trace** 1446
27.2.12.2 **Diagnostics des applications** > **Paramètres développeur** > **Reprendre le jeton écriture** 1446
27.2.12.3 **Diagnostics des applications** > **Carte mère** 1446
27.2.12.4 Diagnostics des applications > Paramètres développeur > Profils de fournisseur SIP....1446
27.2.13 **Diagnostic IP**....1446
27.2.13.1 **Diagnostic IP** > **Carte mère** > **Protocole ARP** 1446
27.2.13.2 **Diagnostic IP** > **Carte mère** > **Demande ICMP** > **Ping** 1447
27.2.13.3 **Diagnostic IP** > **Carte mère** > **Demande ICMP** > **Itinéraire de trace** 1447
27.2.14 **Utilisateur en ligne**....1448
27.2.14.1 **Abonné en ligne** 1448
27.3 **Téléphonie**.... 1448
27.3.1 **Configuration de base**.... 1448
27.3.1.1 **Configuration de base** > **Système** > **Indicateurs système**....1448
27.3.1.2 **Configuration de base** > **Système** > **Temporisations** 1457
27.3.1.3 **Configuration de base** > **Système** > **Écran**.... 1463
27.3.1.4 **Configuration de base** > **Système** > **DISA** 1466
27.3.1.5 **Paramétrage de base** > **Système** > **Renvoi/P.O./Hotline**.... 1467
27.3.1.6 **Configuration de base** > **Système** > **LDAP**.... 1470
27.3.1.7 **Configuration de base** > **Système** > **Textes** 1471
27.3.1.8 **Configuration de base** > **Système** > **Menus flexibles** 1472
27.3.1.9 **Configuration de base** > **Système** > **Numéros abrégés**.... 1472
27.3.1.10 **Paramètres de base** > **Système** > **Indicatifs de service**....1473
27.3.1.11 **Configuration de base** > **Système > Mot de passe d'enregistrement HFA**.... 1473
27.3.1.12 **Configuration de base** > **Passerelle** 1474
27.3.1.13 **Configuration de base** > **DynDNS** > **Service DynDNS** 1476
27.3.1.14 **Configuration de base** > **DynDNS** > **Heure d'actualisation des noms DNS** 1477
27.3.1.15 **Configuration de base** > **Qualité de service** 1478

27.3.1.16 **Configuration de base > Date et heure > Date et heure** 1479
27.3.1.17 **Configuration de base > Date et heure > Paramètres de fuseaux horaires** 1479
27.3.1.18 **Configuration de base > Date et heure > Paramètres SNTP** 1479
27.3.1.19 **Configuration de base > Gestion des ports** 1480
27.3.1.20 **Configuration de base > Taxes > Taxes - Format d'édition** 1481
27.3.1.21 **Configuration de base > Taxes > Facteurs de taxation** 1483
27.3.1.22 **Configuration de base > Taxes > Taxes - Codes affaire** 1484
27.3.1.23 **Configuration de base > Messagerie vocale / Lecteur d'annonces** 1485
27.3.1.24 **Configuration de base > Développement paramètres téléphone**..... 1485
27.3.1.25 **Configuration de base > Gestion de l'alimentation** 1488
27.3.1.26 Installation de base> Données de masse..... 1488
27.3.2 **Sécurité**..... 1490
27.3.2.1 **Sécurité > Pare-feu applicatif**..... 1490
27.3.2.2 **Sécurité > Client de développement et licence (DLSC)** 1492
27.3.2.3 **Sécurité > Client de développement et licence (DLSC) > Certificat client DLSC** 1492
27.3.2.4 **Sécurité > Client de développement et licence (DLSC) > Certificat CA DLSC** 1493
27.3.2.5 **Sécurité > Cryptage de la signalisation et de la charge utile** 1495
27.3.2.6 **Sécurité > Cryptage de la signalisation et de la charge utile > Certificat SPE** 1496
27.3.2.7 **Sécurité > Cryptage de la signalisation et de la charge utile > Certificat CA SPE** 1496
27.3.2.8 **Sécurité > VPN** 1496
27.3.2.9 **Sécurité > VPN > Lightweight CA** 1497
27.3.2.10 **Sécurité > VPN > Gestion des certificats** 1498
27.3.2.11 **Sécurité > VPN > Gestion des certificats > Certificats CA fiables > Certificats actifs** 1498
27.3.2.12 **Sécurité > VPN > Gestion des certificats > Certificats CA fiables > Certificats configurés** 1500
27.3.2.13 **Sécurité > VPN > Certificats Peer** 1500
27.3.2.14 **Sécurité > VPN > Services > Services actifs** 1501
27.3.2.15 **Sécurité > VPN > Services > Services configurés** 1502
27.3.2.16 **Sécurité > VPN > Tunnels > Tunnels actifs** 1502
27.3.2.17 **Sécurité > VPN > Tunnels > Tunnels configurés** 1505
27.3.2.18 **Sécurité > VPN > Règles > Règles actives** 1509
27.3.2.19 **Sécurité > VPN > Règles > Règles configurées** 1511
27.3.2.20 **Sécurité > VPN > Public Key Infrastructure (PKI)** 1512
27.3.2.21 **Sécurité > SSL > Génération de certificats** 1512
27.3.2.22 **Sécurité > SSL > Gestion des certificats** 1514
27.3.2.23 **Sécurité > SSL > Gestion des certificats > Certificats de serveur** 1514
27.3.2.24 **Sécurité > Web**..... 1515
27.3.2.25 **Sécurité > Sécurité SQL** 1516
27.3.3 **Interfaces réseau**..... 1516
27.3.3.1 **Interfaces réseau > Carte mère > Nom d'hôte** 1516
27.3.3.2 **Interfaces réseaux > Carte mère > LAN 1 (WAN)**..... 1516
27.3.3.3 **Interfaces réseau > Carte mère > LAN 2** 1521
27.3.3.4 **Interfaces réseau > Carte mère > LAN 3 (Admin)** 1522
27.3.3.5 **Interfaces réseau > Carte mère > Serveur FTP** 1523
27.3.3.6 **Interfaces réseau > Carte mère > Mode DHCP** 1524
27.3.3.7 **Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Paramètres globaux**... 1524
27.3.3.8 **Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Pools d'adresses IP**....1526
27.3.3.9 **Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Adresses IP statiques**..... 1527
27.3.3.10 **Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Derniers baux actifs**. 1528
27.3.3.11 **Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Toutes les locations** 1529
27.3.3.12 **Interfaces réseau > Carte d'application > Nom d'hôte** 1530
27.3.3.13 **Interfaces réseau > Carte d'application > LAN 1** 1530
27.3.3.14 **Interfaces réseau > Carte d'application > LAN 2** 1531
27.3.4 **Routage**..... 1532

27.3.4.1 **Routing > IP Routing > Mainboard > Static Routes** 1532
27.3.4.2 **Routage > IP Routage > CarteMère > RouteurParDéfaut** 1532
27.3.4.3 **Routage > Routage IP > Carte mère > Serveur DNS** 1533
27.3.4.4 **Routage > IP Routage > Application Board > Itinéraires statiques** 1533
27.3.4.5 **Routage > IP Routage > Application Board > Routeur par défaut** 1534
27.3.4.6 **Routage > NAT** 1534
27.3.4.7 **Routage > RTC** 1535
27.3.4.8 **Routage > RTC > Protocole PPP** 1536
27.3.4.9 **Routage > RTC > Partenaire RTC** 1536
27.3.5 **LCR** 1540
27.3.5.1 **LCR > Flags LCR** 1540
27.3.5.2 **LCR > Classes de service** 1541
27.3.5.3 **Plan de numérotation > LCR** 1541
27.3.5.4 **LCR > Table de routage** 1542
27.3.5.5 **Règle de numérotation > LCR** 1544
27.3.5.6 **LCR > Multisite** 1546
27.3.6 **Passerelle vocale** 1546
27.3.6.1 **Passerelle vocale > Paramètres SIP** 1546
27.3.6.2 Passerelle vocale > Urgence SIP 1548
27.3.6.3 **Paramètres du codec > de la passerelle vocale** 1550
27.3.6.4 **Passerelle vocale > Paramètres du codec de destination** 1552
27.3.6.5 **Passerelle vocale > Fournisseur de services de téléphonie Internet** 1553
27.3.6.6 **Passerelle vocale > Mise en réseau > Noeud** 1565
27.3.6.7 **Passerelle vocale > Mise en réseau > Routage** 1566
27.3.6.8 **Passerelle vocale > SIPQ-Interconnexion** 1566
27.3.6.9 **Passerelle vocale > Ligne réseau du serveur SIP natif** 1568
27.3.7 **Abonnés** 1573
27.3.7.1 **Station > Station > UP0 Stations** 1573
27.3.7.2 **Clients IP > de > la station** 1576
27.3.7.3 **Station > Station > Stations analogiques** 1579
27.3.7.4 **Station > Station > Stations ISDN** 1580
27.3.7.5 **Station > Station > DECT Stations > SLC Numéro d'appel** 1581
27.3.7.6 **Station > Station > DECT Stations > DECT** 1583
27.3.7.7 **Station > Station > Ports IVM/EVM > EVM** 1584
27.3.7.8 **Station > Station > Stations virtuelles** 1585
27.3.7.9 **Paramètres de > la > station** 1586
27.3.7.10 **Applications UC > de > la station** 1598
27.3.7.11 **Abonnés > Abonnés > Profils / Modèles** 1599
27.3.7.12 **Abonnés > Abonnés > Numéros SDA** 1601
27.3.7.13 **Entrée pour les personnes à mobilité réduite > de > la gare** 1601
27.3.7.14 **Abonné > Abonné > Utilisateur SfB** 1603
27.3.7.15 **Abonnés > Abonnés > Vue d'ensemble des abonnés** 1604
27.3.7.16 **Abonné > Programmation des touches** 1605
27.3.8 **Cordless** 1606
27.3.8.1 **Cordless > Dans l'ensemble du système** 1606
27.3.8.2 **Cordless > SLC** 1608
27.3.8.3 **Cordless > Multi-SLC** 1609
27.3.8.4 **Cordless > Station de base** 1609
27.3.9 **Appels entrants** 1610
27.3.9.1 **Appels entrants > Groupes/Groupes de recherche** 1610
27.3.9.2 **Appels entrants > Membres du groupe** 1614
27.3.9.3 **Gestion des appels > Team/Top** 1616
27.3.9.4 **Appels entrants > Interception d'appel** 1619
27.3.9.5 **Appels entrants > UCD** 1619
27.3.9.6 **Appels entrants > Renvois d'appels** 1622
27.3.10 **Lignes/Routage** 1624

27.3.10.1 **Lignes/Routage > Lignes** 1625
27.3.10.2 **Groupe > de troncs/tronçons de routage**..... 1628
27.3.10.3 **Lignes/Routage > Fonctionnalités QSIG** 1636
27.3.10.4 **Lignes/Routage > Affecter le MSN** 1637
27.3.10.5 **Lignes/Routage > Paramètres RNIS** 1638
27.3.11 **Discriminations**..... 1638
27.3.11.1 **Classes de service > Abonnés**..... 1638
27.3.11.2 **Classes de service > Jour : Groupes de discrimination** 1639
27.3.11.3 **Classes de service > Nuit Groupes de discrimination** 1640
27.3.11.4 **Classes de service > Listes des numéros autorisés** 1641
27.3.11.5 **Classes de service > Listes des numéros interdits** 1641
27.3.11.6 **Classes de service > Liste noire** 1642
27.3.11.7 **Classes de service > Renvoi de nuit** 1642
27.3.11.8 **Classes de service > Affectation à un groupe VBZ** 1643
27.3.11.9 **Classes de service > Matrice VBZ** 1643
27.3.11.10 **Classes de service > Renvoi de nuit automatique**..... 1644
27.3.11.11 **Classes de service > Jours spéciaux** 1645
27.3.12 **Connexions**..... 1645
27.3.12.1 **Connexion > Musique d'attente**..... 1645
27.3.12.2 **Connexions > PhoneMail**..... 1646
27.3.12.3 **Annonces > équipements auxiliaires**..... 1647
27.3.12.4 **Connexion > Ouvre-porte**..... 1648
27.3.12.5 **Connexions > SmartVM**..... 1649
27.3.13 **Charge utile**..... 1653
27.3.13.1 **Charge utile > Equipements** 1653
27.3.13.2 **Charge utile > Media Stream Control (MSC)** 1653
27.3.13.3 **Charge utile > Modules matériels** 1654
27.3.14 **Statistiques**..... 1657
27.3.14.1 **Statistiques > Statistiques de la passerelle > Carte mère > Statistiques d'équipements** 1657
27.3.14.2 **Statistiques > Statistiques de la passerelle > Carte mère > Statistiques MSC** 1658
27.3.14.3 **Statistiques > Statistiques SNMP** 1658
27.3.14.4 **Statistiques > Statistiques de téléphonie > Textes système** 1659
27.3.14.5 **Statistiques > Statistiques de téléphonie > Agents UCD** 1659
27.3.14.6 **Statistiques > Statistiques de téléphonie > Etat de la ligne**..... 1659
27.3.14.7 **Statistiques > Statistiques de téléphonie > Renvois** 1660
27.3.14.8 **Statistiques > Statistiques de téléphonie > Abonnés** 1660
27.4 **Applications**..... 1662
27.4.1 **Sélection de l'application**..... 1662
27.4.1.1 **Sélection de l'application**..... 1662
27.4.2 **Intégration d'Active Directory Service**..... 1662
27.4.2.1 **Intégration d'Active Directory Service** 1663
27.4.3 **UC Smart**..... 1663
27.4.3.1 **UC Smart > Configuration de base** 1664
27.4.3.2 **UC Smart > Gestion des utilisateurs**..... 1665
27.4.3.3 **UC Smart > État**..... 1665
27.4.4 **OpenScape Business, UC Suite**..... 1666
27.4.4.1 **OpenScape Business, UC Suite** 1666
27.4.4.2 **OpenScape Business UC Suite > Répertoire utilisateur**..... 1666
27.4.4.3 **OpenScape Business UC Suite > Départements**..... 1669
27.4.4.4 **OpenScape Business UC Suite > Groupes**..... 1669
27.4.4.5 **OpenScape Business UC Suite > Modèles**..... 1671
27.4.4.6 **OpenScape Business UC Suite > Répertoire externe**..... 1671
27.4.4.7 **Configuration des fournisseurs externes > d'OpenScape Business UC Suite**..... 1672
27.4.4.8 **Suite de communications unifiées OpenScape Business > Centre de contact**..... 1674
27.4.4.9 **OpenScape Business UC Suite > Calendriers**..... 1683

27.4.4.10 **OpenScape Business UC Suite** > **Chargement du fichier**....1684
27.4.4.11 **OpenScape Business UC Suite** > **Conférences**.... 1686
27.4.4.12 **Liste des sites** > **OpenScape Business UC Suite**....1686
27.4.4.13 **Serveur** > **OpenScape Business UC Suite**.... 1686
27.4.4.14 **OpenScape Business, UC Suite** > **Profils**....1693
27.4.4.15 **OpenScape Business UC Suite** > **Lignes d'en-tête de fax**.... 1695
27.4.5 **Open Directory Service**.... 1696
27.4.5.1 **Open Directory Service** > **Configuration de base** 1696
27.4.5.2 **Open Directory Service** > **Sources de données** > **Utilisateurs OpenScape Business**.... 1696
27.4.5.3 **Open Directory Service** > **Sources de données** > **LXV3** 1697
27.4.5.4 **Open Directory Service** > **Sources de données** > **LXV3** 1697
27.4.5.5 **Open Directory Service** > **Maintenance**.... 1697
27.4.6 **Application Launcher**.... 1697
27.4.6.1 **Application Launcher** 1698
27.5 **Intergiciel**.... 1698
27.5.1 Lecteur de communication d'interphone.... 1698
27.5.2 CSTA Message Dispatcher (CMD) 1698
27.5.3 Fournisseur de services CSTA (CSP) 1699
27.5.4 Serveur DSS 1700
27.5.5 Media Extension Bridge (MEB) 1700

28 Annexe.... 1701
28.1 Normes supportées.... 1701
28.2 Fonctionnalités Euro-RNIS.... 1703
28.3 Ports utilisés.... 1705
28.4 Planification de projet des canaux DSP pour les systèmes de communication Unify OpenScape Business X5/X8....1707

29 Glossaire....1718
29.1 Glossaire.... 1718

Index.... 1734

1 Historique des modifications

Les modifications mentionnées dans ce chapitre sont cumulatives.

Modifications de la version V4

Chapitres concernés	Description des modifications
Comment configurer les stations IP à la page 405 Comment ajouter une urgence SIP à une station à la page 774 Passerelle vocale > Urgence SIP à la page 1548 Passerelle vocale Fournisseur de services de téléphonie Internet à la page 1553 Configuration de baseSystèmeNuméros abrégés à la page 1472	• ITSP Loc-ID remplacé par SIP Emergency • Mise en œuvre de la gestion des appels d'urgence
Comment configurer les stations SIP-DECT Mitel via le provisioning à la page 419	Améliorations de Mitel SIP-DECT
Groupe de troncs/tronçons de routage à la page 1628 Plan de numérotation LCR à la page 1541	Ajout de l'option d'équilibrage de charge
Mitel WX à la page 1136 Comment configurer Mitel WX dans le service CloudLink à la page 1139 Comment configurer la connectivité Mitel WX à la page 1137 Comment configurer l'instance utilisateur Mitel WX	Ajout de la configuration de Mitel WX
Migration d'Unify Phone vers Mitel WX à la page 1138	Migration des utilisateurs d'Unify Phone vers Mitel WX
Migration à la page 1312 Mise à niveau logicielle d'OpenScape Business X V3 vers OpenScape Business X V4 à la page 1316 Migration d'OpenScape Business X V3 avec carte mère V2 vers OpenScape Business X V4 avec carte mère V3 à la page 1323 Migration d'OpenScape Business X V2 avec carte mère V2 vers OpenScape Business X V4 avec carte mère V3 à la page 1324 Mise à niveau logicielle d'OpenScape Business S V3 vers OpenScape Business S V4 à la page 1330 Mise à niveau logicielle d'OpenScape Business S V2 vers OpenScape Business S V4 à la page 1330 Migration de HiPath 3000 vers OpenScape Business V4 à la page 1341	Scénarios de migration et de mise à niveau pour V4

Chapitres concernés	Description des modifications
Les composants obsolètes ou en fin de vie ont été supprimés de l’ensemble du document	• myPortal to go • OpenScape Business Attendant • OpenScape Business BLF • UC Booster Server • CallBridge • Web Collaboration • OpenScape sans fil DECT IP V2 • myContacts • XMPP • UC Booster Card (OCAB) • X1W, X3R, X3W, X5W

2 Introduction et remarques importantes

L'introduction fournit un aperçu sur la structure de cette documentation. L'introduction doit vous permettre de trouver plus rapidement des informations sur les différents thèmes. Avant de commencer le montage et la mise en service du système de communication, tenez compte des consignes de sécurité et des avertissement ainsi que des remarques importantes.

Conseil : Les consignes de sécurité et avertissements vous informent des consignes et avertissement à respecter. Les remarques importantes contiennent des indications sur le comportement à adopter en cas d'urgence, sur les normes et directives d'installation, sur les caractéristiques de déparasitage du système de communication. De plus, elles fournissent des informations sur la mise au rebut et le recyclage conformes.

Remarque : This document may contain descriptions for features which may still be in beta status. For details see sales info and release notes.

2.1 À propos de cette documentation

Cette documentation décrit l'administration de Unify OpenScape Business.™.

Il comprend les modèles matériels OpenScape Business X1, OpenScape Business X5 et OpenScape Business X8 ainsi que le modèle logiciel OpenScape Business S (softswitch). La solution UC Smart est intégrée à tous les modèles commerciaux d'OpenScape. Dans le cas du commutateur logiciel, un choix peut être fait entre UC Smart et UC Suite.

Remarque : Les modèles matériels OpenScape Business X1/X5/X8 (ou OpenScape Business X en abrégé) et le Softswitch OpenScape Business S sont désignés dans cette documentation comme des systèmes de communication.

UC Suite désigne les fonctions de communications unifiées avancées, notamment le centre de contact multimédia.

Les informations contenues dans ce document présentent des descriptions générales des possibilités techniques, qui ne seront pas toujours disponibles dans certains cas particuliers. Les caractéristiques souhaitées doivent être spécifiées contractuellement pour chaque cas.

Si une fonction n'est pas disponible comme décrit ici, cela peut être dû aux raisons suivantes :

- Le système de communication ne possède pas cette fonctionnalité.
- La licence requise n'est pas disponible ou n'est pas activée.

2.1.1 Documentation et groupes cibles

La documentation d'OpenScape Business est destinée à différents groupes cibles.

Planification des ventes et des projets

La documentation suivante est destinée à la planification des ventes et des projets.

- Description des fonctionnalités

  Cette documentation décrit toutes les fonctionnalités. Ce document est un extrait de la documentation de l'administrateur.

Installation et service

La documentation suivante est destinée aux techniciens de maintenance.

- Guide d'installation d'OpenScape Business X1

  Ce document décrit l'installation du matériel et l'installation initiale d'OpenScape Business X1.
- Guide d'installation d'OpenScape Business X5/X8

  Ce document décrit l'installation du matériel et l'installation initiale d'OpenScape Business X5/X8.
- Guide d'installation d'OpenScape Business S

  Cette documentation décrit l'installation initiale du softswitch OpenScape Business S.
- Documentation de service OpenScape Business X1

  Cette documentation décrit le matériel d'OpenScape Business X1.
- Documentation de service OpenScape Business X5/X8

  Cette documentation décrit le matériel d'OpenScape Business X5/X8.
- OpenScape Business X1R, Guide de service et d'installation Documentation de service

  Ce document décrit l'installation du matériel, l'installation initiale et le service d'OpenScape Business X1R.

Administration

La documentation suivante est destinée aux administrateurs.

- Documentation de l'administrateur

  Cette documentation décrit la configuration des fonctionnalités mises en place à l'aide de l'assistant OpenScape Business Assistant (WBM). La documentation de l'administrateur est disponible dans le système sous forme d'aide en ligne.
- Configuration pour les administrateurs clients, documentation administrateur

  Cette documentation décrit la configuration des fonctionnalités qui peuvent être mises en place à l'aide d'OpenScape Business Assistant (WBM) avec le profil d'administrateur **de base** .
- Gestionnaire E, Documentation de l'administrateur

  Cette documentation décrit la configuration des fonctionnalités mises en place à l'aide de Manager E.

Clients UC / Interfaces utilisateur téléphoniques (TUI)

La documentation suivante est destinée aux utilisateurs de UC.

- myPortal pour ordinateur de bureau, Guide de l'utilisateur

  Cette documentation décrit l'installation, la configuration et le fonctionnement du client UC myPortal pour ordinateur de bureau.
- myPortal pour Outlook, Guide de l'utilisateur

  Cette documentation décrit l'installation, la configuration et le fonctionnement du client UC myPortal pour Outlook.
- myPortal @work, Guide de l'utilisateur

  Cette documentation décrit l'installation, la configuration et le fonctionnement du client UC myPortal @work.
- Imprimante fax, guide d'utilisation

  Cette documentation décrit l'installation, la configuration et le fonctionnement de l'imprimante fax.
- myAgent, Guide de l'utilisateur

  Cette documentation décrit l'installation, la configuration et le fonctionnement du client myAgent pour centres de contact.
- myReports, Guide de l'utilisateur

  Cette documentation décrit l'installation, la configuration et le fonctionnement du client Contact Center myReports.
- Mon assistant, guide de l'utilisateur

  Cette documentation décrit l'installation, la configuration et le fonctionnement de la console opérateur my Attendant.
- Guide de référence rapide de l'interface utilisateur du téléphone intelligent UC (TUI)

  Cette documentation décrit le menu téléphonique de la messagerie vocale de la solution UC Smart.
- Interface utilisateur téléphonique (TUI) UC Suite, Guide de référence rapide

  Cette documentation décrit le menu téléphonique de la messagerie vocale de la solution UC Suite.

2.1.2 Structure de la documentation de l'administrateur

Cette section vous montre comment le contenu de la documentation de l'administrateur est structuré. Le matériel est décrit dans la documentation de service.

Section	Contenu
Introduction et notes importantes	Présentation de la structure de cette documentation et informations importantes/ consignes de sécurité à respecter lors de l'installation et du fonctionnement
Présentation du système	Aperçu du système de communication pour une prise en main rapide
Concept d'administration	Aperçu des programmes d'administration et des rôles des utilisateurs dans le WBM

Section	Contenu
Installation initiale d'OpenScape Business X	Intégration d'OpenScape Business X5/ X8 dans le réseau local du client et configuration de base à l'aide d'assistants
Installation initiale d'OpenScape Business S	Intégration d'OpenScape Business S au réseau local du client et configuration de base à l'aide d'assistants
Installation initiale du module OpenScape Business UC Booster	Intégration d'OpenScape UC Business Booster au réseau local du client et configuration de base à l'aide d'assistants
Licence	Procédures et licences d'octroi de licences
Intégration au réseau de données interne (LAN)	Interface LAN/WAN, résolution de noms, routage des données, DLI et DLS
Connexion au fournisseur de services	Accès Internet, téléphonie IP, accès aux lignes interurbaines
Gare	Plan de numérotation, postes IP, postes UP0 ; postes DECT, postes Mitel SIP-DECT, postes RNIS et analogiques, postes virtuels, utilisateurs de clients UC, profils d’utilisateurs
UC Smart	Clients et fonctionnalités de la solution de communications unifiées UC Smart, y compris la messagerie vocale intelligente. Statut de présence, annuaires et journal, conférences, activités d'équipe, messagerie vocale
Suite UC	Clients et fonctionnalités de la solution de communications unifiées UC Suite : statut de présence et CallMe, annuaires et journal, conférences, messages vocaux et fax, messagerie instantanée
Fonctions du téléphone	Passer des appels, signalisation d'appel, identification de l'appelant, fonctions pendant l'appel, optimisation de la communication
Travailler en équipe (groupes)	groupe de prise d'appel, appel de groupe, groupe de chasse, équipe/meilleure équipe, MULAP, UCD
Routage des appels	Classes de service, restriction de péage, système locataire, LCR, appels d'urgence
Préposés	Répondeurs automatiques, répondeur OpenStage, répondeurs sur PC, position d'interception
Centre de contact multimédia	Clients et fonctions du centre de contact : agents, files d’attente et plannings, service VIP, solution de repli, rapports
Mobilité	Accès mobile, numéro unique, téléphonie bimode, mobilité IP, sans fil/DECT

Section	Contenu
Sécurité	Pare-feu, SPE, VPN, certificats
Réseautage OpenScape Business	Plan de réseau, scénarios de mise en réseau, position d'interception centrale, capacité de survie
Équipement auxiliaire	Dispositifs d'annonce, interphone et ouvre-porte d'entrée, actionneurs et capteurs
Connectivité des applications	CSTA, TAPI, lanceur d'applications
Comptabilité	Enregistrement détaillé des appels, facturation et durée des appels, contrôle des coûts
Entretien	Sauvegarde et restauration, mise à jour, redémarrage, rechargement, arrêt, réinitialisation d'usine, inventaire, actions, services à distance
Migration	Mise à niveau de HiPath 3000 vers OpenScape Business
Limites et capacités de configuration	Valeurs maximales des limites de configuration et des capacités des différents systèmes de communication
Mode expert	Description de référence des fenêtres/ masques en mode Expert
Appendice	Liste des normes prises en charge, des fonctionnalités Euro-ISDN et des protocoles IP et numéros de port utilisés
Glossaire	Brève description des termes couramment utilisés

2.1.3 Types de thèmes

Les thèmes abordés englobent la définition des conceptions et des tâches:

Type du thème	Description
Concept	Explique le "Quoi" et fournit un aperçu des conditions ainsi que des informations d'arrière-plan, par ex. à propos des fonctionnalités.
Tâche (Instructions d'utilisation)	Explique le "Comment", étape par étape, pour les cas d'application orientés tâche et suppose une connaissance des concepts correspondants. Les tâches sont reconnaissables à leur titre **Comment...**.

2.1.4 Conventions de présentation des informations

La présente Documentation utilise différents moyens pour représenter différents types d'informations.

Type d'information	Représentation	Exemple
Eléments de l'interface utilisateur	gras	Cliquez sur **OK**.
Séquence de menu	>	**Fichier** > **Quitter**
Accentuation spéciale	gras	**Ne pas supprimer** le nom
Texte de renvoi	Caractères italiques	Vous trouverez des informations supplémentaires au point *Réseau*.
Edition	Police à espacement fixe, par ex. Courier	`Commande introuvable.`
Entrée	Police à espacement fixe, par ex. Courier	`Entrer` LOCAL comme nom de fichier
Raccourci clavier	Police à espacement fixe, par ex. Courier	`<Ctrl>+<Alt>+<Esc>`

2.2 Consignes de sécurité et avertissements

Les consignes de sécurité et avertissements identifient des situations pouvant provoquer la mort, des blessures graves des dommages matériels et/ou des pertes de données.

Les travaux sur les systèmes de communication et les équipements doivent être exécutés **exclusivement** par des personnes qualifiées.

Dans le contexte des présentes consignes de sécurité et des présents avertissement, des personnes qualifiées sont des personnes autorisées à mettre en service, à mettre à la terre et à identifier les systèmes, appareils et lignes conformément aux consignes et normes de sécurité applicables.

Lire et respecter impérativement les indications consignes de sécurité et avertissements suivants avant de commencer à monter et mettre en service le système de communication.

Lisez soigneusement toutes les consignes de sécurité et tous les avertissements figurant sur le système de communication et les appareils et s'y conformer.

Notez également les numéros d’appel d’urgence.

Types de consignes de sécurité et d'avertissements

Dans la présente documentation les niveaux suivants de consignes de sécurité et d'avertissement sont utilisés.

DANGER : Identifie une situation immédiatement dangereuse pouvant provoquer la mort ou des blessures graves.

Avertissement : Identifie une situation généralement dangereuse pouvant provoquer la mort ou des blessures graves.

ATTENTION : Identifie une situation dangereuse pouvant provoquer des blessures.

Remarque : Identifie des situations pouvant provoquer des dommages matériels et/ou des pertes de données.

Autres symboles identifiant des risques

Le symbole suivant n'est normalement pas utilisé dans la présente documentation, mais il peut figurer sur les appareils ou emballages.

	Composant sensibles aux décharges électrostatiques (ESD)

Concepts associés

Remarques importantes à la page 53

2.2.1 Indications : Danger

Les indications de type Danger identifient une situation directement dangereuse, pouvant provoquer la port ou des blessures graves.

DANGER : Choc électrique en cas de contact avec les lignes sous tension

- Ne pas oublier : les tensions supérieures à 30 V CA (courant alternatif) ou 60 V CC (courant continu) sont dangereuses !
- Les interventions sur le réseau basse tension (<1000 V CA) ne doivent être effectuées que si l'on dispose de la qualification nécessaire ou par des électrotechniciens d'expérience, dans le respect des dispositions nationales/locales applicables aux raccordements électriques.

2.2.2 Avertissements : Avertissement

Les « avertissements » signalent des situations dangereuses universelles pouvant entraîner la mort ou des blessures graves.

Avertissement : Risque de choc électrique par contact avec des fils électriques sous tension

- Utilisez des fils de terre séparés pour assurer la mise à la terre de protection du système de communication OpenScape Business X5R. Avant de mettre le système en marche et de connecter les téléphones et les lignes téléphoniques, raccordez le système de communication à un conducteur de mise à la terre permanent.
- Prévoir une mise à la terre de protection pour chaque boîtier du système de communication OpenScape Business X8 à l'aide d'un fil de terre séparé. Avant de mettre le système en marche et de connecter les téléphones et les lignes téléphoniques, raccordez le système de communication à un conducteur de mise à la terre permanent.
- N’utilisez que des systèmes, des outils et des équipements en parfait état. N’utilisez pas d’équipement présentant des dommages visibles.
- Remplacez immédiatement tout équipement de sécurité endommagé (couvercles, étiquettes et fils de terre).
- Remplacez immédiatement le câble d'alimentation s'il semble endommagé.
- Les systèmes de communication et les serveurs ne doivent être utilisés qu'avec des prises de courant reliées à la terre.
- Pendant un orage, ne branchez ni ne débranchez de lignes et n'installez ni ne retirez de tableaux électriques.
- Débranchez tous les circuits d'alimentation électrique si vous n'avez pas besoin d'électricité pour certaines activités (par exemple, lors du changement de câbles). Débranchez toutes les prises d'alimentation du système de communication et assurez-vous que celui-ci n'est pas alimenté par une autre source d'alimentation (par exemple, un onduleur).

  Avant de commencer tout travail, assurez-vous que le système de communication est hors tension. Ne jamais considérer comme acquis que tous les circuits ont été correctement déconnectés de l'alimentation électrique lorsqu'un fusible ou un interrupteur principal a été mis hors tension.
- Il faut s'attendre à des courants de fuite provenant du réseau de télécommunications. Débranchez toutes les lignes de télécommunication du système de communication avant de débrancher le fil de terre prescrit du système.
- Tant que l'alimentation est allumée, faites toujours preuve de la plus grande prudence lors de la réalisation de mesures sur des composants alimentés et de travaux de maintenance sur des cartes et des boîtiers de circuits imprimés.

  Les surfaces métalliques, comme les miroirs, sont conductrices. Si vous les touchez, vous risquez de recevoir des chocs électriques ou de faire un court-circuit.

2.2.3 Avertissements : Attention

Les indications de type Attention identifient une situation dangereuse pouvant provoquer des blessures.

ATTENTION : Risque d'explosion lors d'un changement non correct des accumulateurs et des batteries

- Utilisez exclusivement des accumulateurs homologués.
- Ne remplacer la batterie lithium que par un modèle identique ou recommandé par le constructeur.

ATTENTION : Risque d'incendie

- N'utilisez que des lignes de communication d'un diamètre d'au moins 0,4 mm (AWG 26) ou supérieur.
- Ne jamais stocker de documents ou d'objets similaires combustibles dans un système de communication.

ATTENTION : Risque général de blessure ou d'accident sur le poste de travail

- Une fois les interventions de test et de maintenance effectuées, réinstallez tous les dispositifs de sécurité au bon endroit, verrouiller les couvercles et les boîtiers.
- Posez les lignes de manière à ce qu'elles ne constituent pas une source de danger (chute de personnes) et ne puissent pas être endommagées.
- Assurez-vous qu'en cas d'intervention sur un système de communication ou serveur ouvert, celui-ci ne reste jamais sans surveillance.
- Utilisez un moyen adapté pour soulever des objets ou des charges lourds.
- Contrôlez régulièrement votre outillage. N'utilisez que des outils en parfait état.
- Lorsque vous intervenez sur une installation, ne portez jamais de vêtements flottants et, si vous avez les cheveux longs, attachez-les afin qu'ils ne retombent pas.
- Ne portez pas de bijoux, de bracelets de montre métalliques ou des boucles et des rivets métalliques sur vos vêtements.
- Lorsque le travail le nécessite, portez toujours une protection oculaire appropriée.
- Lorsqu'il existe un risque de chute d'objets, portez toujours un casque.
- Veillez à disposer d'un éclairage suffisant sur le poste de travail et maintenez-le en bon ordre.

2.2.4 Avertissements : remarques

Les indications de type Remarque identifient des situations qui peuvent se traduire par des dommages matériels et/ou des pertes de données.

Tenez compte des remarques suivantes pour éviter les dommages matériels et/ou les pertes de données.

- Avant la mise en service, vérifiez que la tension nominale du réseau d'alimentation correspond à la tension nominale du système de communication ou du serveur (plaque signalétique).
- Conformez-vous aux mesures ESD suivantes pour assurer la protection des composants sensibles aux décharges électrostatiques.
  - Portez toujours un bracelet de mise à la terre lorsque vous effectuez des travaux sur des composants et modules.
  - Toujours placer les composants et modules sur un support conducteur, relié à la terre.
  - Ne transporter et n'envoyer les composants des systèmes de communication (par exemple les modules) que dans des emballages adaptés.
- Utilisez exclusivement des accessoires originaux. Dans le cas contraire, vous risquez d'endommager l'installation ou d'enfreindre les consignes en matière de sécurité et de compatibilité électromagnétique.
- En cas de variation brusque de la température, l'humidité contenue dans l'air peut se condenser. Par exemple, lorsqu'un système de communication ou un serveur passe d'un environnement froid à un local chauffé, l'humidité peut se condenser. Attendez que la température se soit stabilisée et que le système de communication ou le serveur soit entièrement sec avant de le mettre en service.
- Ne raccordez les lignes qu’aux points de connexion prévus.
- Lorsque aucune alimentation de secours n'est disponible ou bien lorsque il est impossible de commuter sur des téléphones de secours analogiques en cas de panne de courant, il est impossible d'effectuer des appels de secours à l'aide du système de communication lorsque l'alimentation électrique est coupée.
- Avant le début du montage mural, vérifiez que le mur ait une force porteuse suffisante. Utilisez toujours des moyens d'installation et de fixation appropriés pour un montage en toute sécurité des systèmes de communication et appareils.
- N’autorisez jamais le stockage de matières facilement inflammables à proximité immédiate du système de communication.

2.2.5 Consignes de sécurité spécifiques du pays

Vous trouverez ici des informations sur les consignes de sécurité à respecter pour le montage, la mise en service et l'exploitation du système de communication dans certains pays.

2.2.5.1 Informations de sécurité pour l'Australie

Les précautions de sécurité suivantes doivent toujours être respectées lors de l'installation, de la mise en service et de l'utilisation des systèmes de communication OpenScape Business X et OpenScape Business S en Australie :

- Les systèmes de communication OpenScape Business X et OpenScape Business S doivent être installés et entretenus uniquement par du personnel autorisé.
- Les systèmes muraux OpenScape Business doivent être installés à proximité de la prise de courant qui alimente le système de communication

correspondant. La prise murale doit être facilement accessible. L'intégrité de la prise murale doit être assurée.

- Les systèmes de communication OpenScape Business X et OpenScape Business S doivent être configurés pour permettre à tout moment de passer des appels d'urgence (par exemple, le 000).
- Si aucune alimentation de secours n'est disponible ou si aucun basculement vers des téléphones analogiques d'urgence (transfert en cas de panne de ligne) n'est possible en cas de panne de courant, alors aucun appel d'urgence ne peut être passé via le système de communication après une panne de courant).
- Les dispositifs de musique d'attente et de radiomessagerie doivent être connectés au système de communication via une unité d'isolation de ligne approuvée par l'Autorité australienne des communications (ACA).

2.2.5.2 Informations de sécurité pour le Brésil

Les précautions de sécurité suivantes doivent toujours être respectées lors de l'installation, de la mise en service et de l'utilisation des systèmes de communication OpenScape Business X et OpenScape Business S au Brésil :

- L'utilisation de la multiprise avec protection contre les surtensions portant la référence C39334-Z7052-C33 est absolument obligatoire. L'alimentation électrique des systèmes de communication OpenScape Business X et OpenScape Business S doit passer par une multiprise avec protection contre les surtensions.
- L'utilisation de câbles Ethernet blindés pour les interfaces/ports LAN/WAN des cartes mères OCCL, OCCM et OCCMR est absolument obligatoire.

2.2.5.3 Informations de sécurité pour les États-Unis

Les précautions de sécurité suivantes doivent toujours être respectées lors de l'installation, de la mise en service et de l'utilisation des systèmes de communication OpenScape Business X et OpenScape Business S aux États-Unis :

- Perturbation du réseau et T1

  Lorsque les systèmes de communication sont mis en réseau à l'aide de T1 (1,544 Mbit/s), la société de télécommunications (Federal Communications Commission (FCC)) doit être informée chaque fois qu'un système de communication est retiré du réseau.

  Si l'un des systèmes de communication d'Unify Software and Solutions GmbH & Co. KG décrit dans cette documentation perturbe le fonctionnement du réseau public de télécommunications, l'opérateur de télécommunications est en droit de bloquer temporairement l'accès à la ligne extérieure. En général, l'entreprise de télécommunications vous en informera à l'avance. Si cela s'avère impossible, vous en serez informé dans les plus brefs délais. Dans ce contexte, vous serez également informé que vous pouvez déposer une réclamation auprès de l'entreprise de télécommunications.
- Changements dans les installations de la compagnie de téléphone

  L'entreprise de télécommunications est en droit d'adapter ses propres équipements, dispositifs, procédures d'exploitation et processus selon les besoins ; de telles modifications peuvent perturber le fonctionnement

de vos systèmes de communication. Dans des circonstances normales, vous devriez être prévenu à l'avance afin de pouvoir maintenir un service téléphonique ininterrompu.

- Équipement vocal non en direct

  Les équipements vocaux non en direct, tels que les appareils de musique d'attente et les enregistreurs vocaux, doivent être approuvés et mis en circulation par Unify Software and Solutions GmbH & Co. KG et enregistrés conformément aux règles et réglementations de la sous-partie C des règles de la FCC, partie 68.

  Les appareils non commercialisés destinés à la lecture vocale ne peuvent être connectés que par l'intermédiaire de circuits de protection approuvés et commercialisés par Unify Software and Solutions GmbH & Co. KG et enregistrés conformément aux règles et réglementations de la sous-partie C des règles de la FCC, partie 68.
- Numéro d'équivalence de sonnerie REN

  Le numéro d'équivalence de sonnerie (REN) est utilisé pour déterminer le nombre d'appareils pouvant être connectés à une ligne téléphonique afin que tous les appareils sonnent lorsque ce numéro de téléphone est appelé. Dans la plupart des zones, mais pas toutes, la somme des REN de tous les appareils connectés à une ligne ne doit pas dépasser cinq. Contactez votre opérateur de télécommunications local pour connaître le REN maximal applicable à votre zone d'appel.
- Nouveaux codes d'accès locaux et CO

  Le routage au moindre coût (LCR) doit être configuré pour reconnaître et prendre automatiquement en compte les changements de codes régionaux locaux et de codes d'accès CO. Autrement, ces codes ne seront pas utilisables pour les appels lorsque des modifications surviendront.
- Compatibilité avec les appareils auditifs

  Les téléphones d'urgence et les téléphones publics (installés dans les espaces communs tels que les halls d'entrée, les chambres d'hôpital, les ascenseurs et les chambres d'hôtel, par exemple) doivent être équipés de combinés compatibles avec les appareils auditifs à couplage magnétique. Les personnes malentendantes qui ne se trouvent pas dans les espaces communs doivent se voir fournir, si nécessaire, des combinés compatibles avec les appareils auditifs.

  Tous les téléphones numériques de Unify Software and Solutions GmbH & Co. KG fabriqués après le 16 août 1989 sont compatibles avec les appareils auditifs et conformes aux règles de la FCC, partie 68, sections 68.316 et 68.317.
- Fonctionnalités du numéroteur programmé

  Lorsque vous programmez des numéros d'urgence ou effectuez des appels tests vers des numéros d'urgence avec des fonctions de numérotation programmées à l'aide des produits d'Unify Software and Solutions GmbH & Co. KG, restez en ligne et expliquez brièvement au répartiteur la raison de l'appel avant de raccrocher. Ces activités devraient être réalisées en dehors des heures de pointe, par exemple tôt le matin ou tard le soir.
- Raccordement des installations de la gare hors site

  Les clients qui ont l'intention de connecter des installations de station hors site (OPS) doivent informer l'entreprise de télécommunications de la classe OPS pour laquelle l'équipement est enregistré et de la connexion souhaitée.

- Supervision des réponses aux appels entrants directs

  Les clients qui utilisent l'un des systèmes de communication d'Unify Software and Solutions GmbH & Co. KG décrits dans cette documentation sans assurer une supervision adéquate des réponses contreviennent à la partie 68 des règles de la FCC.

  Chaque système de communication d'Unify Software and Solutions GmbH & Co. KG décrit dans cette documentation renvoie une supervision de réponse appropriée au réseau téléphonique public commuté (RTPC) lorsque des appels DID sont :

  – Répondu par la station appelée.
  – Réponse donnée par un employé.
  – redirigé vers une annonce gérée par le client.

  De plus, chaque système de communication d'Unify Software and Solutions GmbH & Co. KG décrit dans cette documentation assure également une supervision de réponse appropriée sur tous les appels DID transférés vers le réseau téléphonique public commuté (RTPC). Les exceptions admissibles sont les suivantes :

  – L'appel reste sans réponse.
  – On reçoit une tonalité d'occupation.
  – Une tonalité de congestion (tonalité de réordonnancement) est reçue.
- Exigences d'égalité d'accès

  Les agrégateurs d'appels connaissant une augmentation du volume de trafic (tels que les hôtels, les hôpitaux, les aéroports, les écoles, etc.) doivent garantir aux utilisateurs finaux un accès égal aux fournisseurs de leur choix. Les codes d'accès égaux actuels (également appelés codes d'accès opérateur, CAC) sont 10xxx et 101xxxx, et 800/888 et 950, où xxx ou xxxx représente le code du fournisseur.

  Pour sélectionner l'opérateur de son choix pour un appel, l'utilisateur compose un code d'accès spécifique à l'opérateur avant de composer le numéro de l'appelé. L'égalité d'accès est également obtenue en composant le code 800/888 ou 950 du fournisseur de votre choix.

  Chaque système de communication d'Unify Software and Solutions GmbH & Co. KG décrit dans cette documentation est capable de fournir un accès utilisateur aux fournisseurs interétatiques grâce à l'utilisation de codes d'accès égaux.

  Les modifications apportées par les agrégateurs pour altérer ces capacités constituent une violation de la loi de 1990 sur l'amélioration des services aux consommateurs des opérateurs téléphoniques et de la partie 68 des règles de la FCC.

2.2.5.4 Informations de sécurité pour le Canada

DANGER : Risque de choc électrique par contact avec des fils électriques sous tension

Seul le personnel dûment qualifié ou les électriciens qualifiés doivent effectuer des travaux sur le réseau basse tension (<1000 VAC) et tous

les travaux doivent être conformes aux exigences nationales/locales en matière de raccordements électriques.

Les précautions de sécurité suivantes doivent toujours être respectées lors de l'installation, de la mise en service et de l'utilisation des systèmes de communication OpenScape Business X et OpenScape Business S au Canada :

- Numéro d'équivalence de sonnerie REN

  Le numéro d'équivalence de sonnerie (REN) définit le nombre d'appareils pouvant être connectés simultanément à une ligne téléphonique. La terminaison d'une interface peut consister en n'importe quelle combinaison de dispositifs, sous réserve uniquement de l'exigence que la somme des REN de tous les dispositifs ne dépasse pas cinq.
- Restrictions relatives à la connexion des appareils

  Le label Innovation, Sciences et Développement économique Canada (ISDE) identifie les équipements certifiés. Cette certification signifie que l'équipement répond à certaines exigences en matière de protection, d'exploitation et de sécurité des réseaux de télécommunications.
  Les exigences sont documentées dans le document « Exigences techniques relatives aux équipements terminaux ». Innovation, Sciences et Développement économique Canada (ISDE) ne fournit aucune garantie que les appareils certifiés fonctionneront toujours à la satisfaction du client.

  Avant d’installer l’équipement et les composants décrits dans cette documentation, il convient de s’assurer que les raccordements aux installations de l’opérateur de télécommunications local sont autorisés. Les systèmes de communication et les serveurs doivent également être installés en utilisant une méthode de connexion acceptable. Le client doit être conscient que le respect de ces conditions peut ne pas empêcher une dégradation des performances dans certaines situations.

  Les réparations des équipements certifiés doivent être coordonnées par un technicien de maintenance désigné par le fabricant ou le fournisseur. Toute réparation ou modification apportée par l'utilisateur à l'un des équipements ou composants décrits dans cette documentation, ou tout dysfonctionnement de l'équipement, peut donner à l'entreprise de télécommunications le motif de demander à l'utilisateur de débrancher l'équipement.

  Pour leur propre sécurité, les utilisateurs doivent vérifier que les connexions de mise à la terre électriques de l'alimentation électrique, des lignes téléphoniques et du système de canalisations d'eau métalliques, le cas échéant, sont interconnectées. Cette précaution peut s'avérer particulièrement importante en milieu rural.

2.3 Remarques importantes

Les remarques importantes vous informent sur le comportement à adopter en cas d’urgence, la mise au rebut conforme et le recyclage adapté ainsi que sur l'utilisation respectueuse de la destination et les conditions d'utilisation des systèmes de communication et serveur. De plus, vous recevez des indications à propos des normes et directives concernant l'installation, les caractéristiques de déparasitage des systèmes de communication et de la protection et sécurité des données.

Concepts associés

Consignes de sécurité et avertissements à la page 45

2.3.1 Comportement à adopter en cas d’urgence

Il figure ici des informations à propose des mesures à prendre en cas d'urgence.

Comportement en cas d’accident

Mesures de premiers secours

Appel d’urgence

Signalisation des accidents

- En cas d’accident, conservez votre calme et réfléchissez bien avant d’agir.
- Avant de toucher la victime d’un accident, coupez toujours la source de courant électrique.
- Si vous n’êtes pas en mesure de couper immédiatement la source de tension, déplacez la victime à l’aide d’un objet non conducteur (manche à balai en bois, par exemple) de manière à supprimer le contact avec la source de tension.
- Familiarisez-vous avec les consignes de premiers secours en cas de choc électrique, en particulier avec les mesures de réanimation en cas d'arrêt respiratoire ou cardiaque, et avec les interventions en cas de brûlure.
- En cas d’arrêt respiratoire, pratiquez immédiatement la respiration artificielle (bouche à bouche ou bouche à nez).
- En cas d’arrêt du coeur, pratiquez immédiatement un massage cardiaque si vous disposez de la formation nécessaire.

Appelez immédiatement une ambulance ou le médecin de service. Lorsque vous appelez, donnez les précisions suivantes :

- Lieu de l’accident
- Nature de l’accident
- Nombre de blessés
- Nature des blessures
- Attendez pour répondre aux questions supplémentaires de votre interlocuteur.
- Signalez immédiatement à votre supérieur hiérarchique tous les accidents, les accidents évités de justesse ainsi que les sources potentielles de risques.
- Signalez tout choc électrique, même s’il a été très faible.

2.3.2 Utilisation conforme

Le système de communication ne doit être utilisé que pour les usages décrits dans la présente Documentation et uniquement sur les connexions des

appareils et composantes recommandés et autorisés par Unify Software and Solutions GmbH & Co. KG.

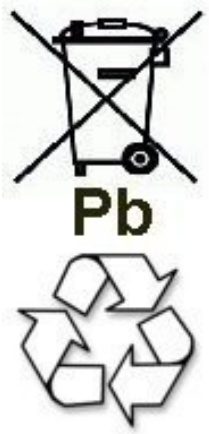
L'utilisation conforme du système de communication suppose un transport conforme, un stockage, un montage et une mise en service conformes ainsi qu'une utilisation et un entretien soigneux.

Remarque : Ne nettoyer le boîtier du système de communication et du serveur qu'avec un chiffon doux, légèrement humide. Ne pas utiliser de produit nettoyant corrosif ou d'éponge abrasive.

2.3.3 Mise au rebut et recyclage conformes

Il est fourni des informations sur la mise au rebut et le recyclage conformes des équipements électriques et électroniques ainsi que des anciennes batteries et anciens accumulateurs.

Tous les équipements électriques et électroniques doivent être éliminés séparément des déchets municipaux, dans les lieux de collecte prévus à cet effet par les dispositions prises à l'échelle nationale. L'élimination appropriée et la collecte sélective de vos appareils usagés servent à prévenir tout dommage potentiel pour l'environnement et la santé humaine. Elles constituent une condition à la réutilisation et au recyclage des équipements électriques et électroniques usagés. Pour avoir des informations détaillées sur le recyclage de vos appareils usagés, renseignez-vous auprès de votre commune, du service responsable de l'élimination des déchets, du commerçant auquel vous avez acheté votre produit ou de votre partenaire commercial. Ces informations s'appliquent uniquement aux équipements installés et vendus dans les pays de l'Union européenne et soumis à la directive européenne 2012/19/UE. Dans les pays hors Union européenne, des dispositions différentes peuvent s'appliquer au recyclage des équipements électriques et électroniques.



Les batteries ou accumulateurs usagés portant cette identification sont des biens économiques récupérables et doivent être soumis à un processus de recyclage. Les batteries ou accumulateurs qui ne peuvent pas être recyclés doivent être mis au rebut en tant que déchets spéciaux, dans le respect de toutes les prescriptions applicables.

2.3.4 Normes et directives concernant l'installation

Tenez compte des informations sur les instructions à respecter pour le raccordement du système de communication au circuit d'alimentation électrique et pour le câblage avec blindage des raccordements LAN et WAN.

2.3.4.1 Raccordement d’OpenScape Business X au circuit électrique d’alimentation

Les systèmes de communication OpenScape Business X sont validés pour le raccordement aux systèmes d’alimentation TN-S. Est également autorisé le raccordement à un système d’alimentation TN-C-S pour lequel le conducteur PEN se subdivise en un conducteur de protection et un conducteur neutre. TN-S et TN-C-S sont conformes à la définition des normes IEC 60364-1 et IEC 60364-5-51.

Si des opérations sont nécessaires sur le réseau basse tension, elles doivent être réalisées par un électrotechnicien qualifié. Ces opérations d'installation pour le raccordement des systèmes de communication doivent se faire conformément à IEC 60364-1 et IEC 60364-4-41 ou aux normes ou directives nationales légales en vigueur.

2.3.4.2 Raccordement d'OpenScape Business S au circuit d'alimentation

Pour plus d'informations concernant le raccordement d'OpenScape Business S au circuit d'alimentation, veuillez vous référer à la documentation du fabricant relative au serveur PC et aux autres composants.

Seuls des électriciens qualifiés devraient effectuer les travaux qui pourraient être nécessaires sur le réseau basse tension. Ces activités d'installation pour connecter OpenScape Business S doivent être réalisées conformément aux normes IEC 60364-1 et IEC 60364-4-41 ou à toute autre norme légale ou réglementation nationale correspondante (par exemple aux États-Unis et au Canada).

2.3.4.3 Câblage blindé pour raccordements LAN et WAN de OpenScape Business X

Le respect des exigences CE concernant la compatibilité électromagnétique des systèmes de communication OpenScape Business X ainsi que leurs raccordements LAN et WAN suppose la prise en compte des conditions ci-après.

- Le fonctionnement du système de communication n'est autorisé qu'avec un câblage de raccordement blindé. Cela signifie qu'il faut utiliser entre les prises blindées de raccordement LAN et WAN du système de communication et le raccordement à l'installation du bâtiment ou le raccordement à des composantes actives externes un câble blindé de catégorie 5 (câble CAT.5) d'une longueur de 3 m au minimum. À l'extrémité du câble appliquée à l'installation du boîtier ou de la composante active, il faut mettre à la terre le blindage du câble (liaison avec le potentiel d'équilibre du bâtiment).
- Pour les liaisons plus courtes avec une composante active externe (commutateur LAN ou similaire), il faut également utiliser un câble blindé de catégorie 5 (câble CAT.5). Toutefois, la composante active doit présenter un raccordement LAN également blindé dont le raccordement blindé est mis à la terre (liaison avec le potentiel d'équilibre du bâtiment).
- Les caractéristiques de blindage des composantes de câblage doivent répondre au moins aux exigences de la norme européenne EN 50173-1[*)] « Technologies de l'information – Systèmes de câblage générique » (et des renvois qui y sont mentionnés).[***)]
- Les installations de bâtiments qui sont équipées de bout en bout d'un câblage en cuivre symétrique blindé conformément aux exigences de la classe D[**)] de l'EN 50173-1 répondent à la condition ci-dessus.[***)]

2.3.4.4 Exigences de protection anti-incendie

Les exigences de protection anti-incendie sont réglementées dans les dispositions sur les bâtiments spécifiquement pour chaque pays. Les directives en vigueur doivent être respectées.

Afin de satisfaire aux exigences de la protection incendie et de la CEM, les systèmes de communication OpenScape Business X ne peuvent être exploités que de manière fermée. L'ouverture n'est autorisée que brièvement, à des fins de montage et de maintenance.

Le comportement au feu des câbles système de OpenScape Business répond aux exigences de la norme internationale IEC 60332-1. Les normes suivantes

---

*) La norme européenne EN 50173-1 est dérivée de la norme mondiale ISO/IEC 11801.

**) La classe D est atteinte notamment lorsque des composantes (câble, prises de raccordement, câbles de raccordement, etc.) de catégorie 5 (CAT.5) sont installées.

***) Sur le marché nord-américain, il est principalement installé du câblage UTP (norme américaine EIA/TIA 568 A/B), par conséquent la règle suivante s'applique pour les raccordements LAN et WAN des systèmes de communication : le fonctionnement du système n'est autorisé qu'avec un câblage de raccordement blindé. Cela signifie qu'il faut utiliser entre les prises blindées de raccordement LAN et WAN du système de communication et le raccordement à l'installation du bâtiment ou le raccordement à des composantes actives externes un câble blindé de catégorie 5 (câble CAT.5) d'une longueur de 3 m au minimum. À l'extrémité du câble appliquée à l'installation du boîtier ou de la composante active, il faut mettre à la terre le blindage du câble (liaison avec le potentiel d'équilibre du bâtiment).

définissent des exigences de même niveau concernant le comportement au feu des câbles.

IEC 60332-1 Remarque : L'IEC 60332-1 correspond au type de contrôle UL VW-1	EN 60332-1-et EN 60332-2-1	DIN EN 60332-1-1 (VDE 0482-332-1-1) et DIN EN 60332-2-1 (VDE 0482-332-2-1)

Il convient de faire contrôler par le service responsable de l'élaboration du projet et de l'assistance technique que la norme IEC 60332-1 est suffisamment conforme aux réglementations sur le bâtiment pertinentes et aux autres réglementations applicables.

2.3.4.5 Exigences de protection contre la foudre

La protection des systèmes de communication contre les surtensions génératrices d'énergie nécessite une mise à la terre basse impédance, conformément aux indications figurant dans le *Guide d'installation OpenScape Business*.

Remarque : Après mise à la terre de protection d'un système de communication, il faut contrôler la liaison à la terre basse impédance du système à l'aide du conducteur de protection du circuit d'alimentation de la tension réseau et la liaison basse impédance du conducteur de terre supplémentaire, raccordé en permanence, avec le rail d'équilibrage de potentiel du bâtiment.

Remarque :

Risque d'incendie en raison de surtension

Les lignes de télécommunications de plus de 500 m de longueur ou les lignes de télécommunications qui quittent le bâtiment doivent être équipées d'une protection contre la foudre externe supplémentaire.

Une protection contre la foudre de ce type est appelée Protection primaire supplémentaire. La protection primaire supplémentaire est assuré par le montage conforme d'un parasurtenseur à gaz sur le répartiteur principale, le panneau de brassage ou au point d'entrée de la ligne dans le bâtiment. Pour cela, il faut monter sur chaque ligne à protéger un parasurtenseur à gaz d'une tension nominale de 230 V par rapport à la terre.

Sans cette protection primaire supplémentaire, l'action de la foudre peut provoquer la destruction de certains modules. Cela peut provoquer la défaillance du système de communication complet et la surchauffe de certains modules (risque d'incendie).

2.3.4.6 Identifications pour OpenScape Business X

La conformité de l’appareil à la directive européenne 1999/5/UE est attestée par le label CE.

2.3.5 Remarques sur les émissions perturbatrices et les perturbations radio de OpenScape Business X

Les systèmes de communication OpenScape Business X sont des équipements de classe B selon l’EN 55032.

2.3.6 Protection et sécurité des données

Tenez compte des informations sur la garantie de confidentialité des données et sur la sécurité des données.

Dans les systémes de communication et les serveurs décrits dans cette documentation, il est notamment traité et utilisé des données personnelles, par exemple lors de la taxation, des affichages écran, la saisie des données client.

En Allemagne, la gestion et l'utilisation de données confidentielles sont réglementées par les dispositions de la loi pour la protection des données (BDSG). Dans ce contexte s’appliquent les dispositions de la loi Informatique et Libertés.

La loi sur la protection des données a pour objet de préserver la vie privée des personnes lors de l’utilisation des informations qui les concernent.

De plus, cette loi protège les données lors des opérations de traitement et empêche ainsi tout préjudice aux intérêts propres ou de tiers.

Conseil : Le client est responsable du respect de la législation en vigueur sur la protection des données, le travail et la protection du travail durant l’installation, lors de l'installation, de l’exploitation et de la maintenance du système de communication et du serveur.

Les collaborateurs de Unify Software and Solutions GmbH & Co. KG sont tenus au secret professionnel et doivent préserver la confidentialité des données.

Afin de respecter strictement les dispositions légales dans le cadre de vos activités (maintenance sur le site ou télémaintenance), tenez compte des règles indiquées ci-après. Vous protégerez ainsi les intérêts de vos et nos clients et vous dégagerez votre responsabilité personnelle.

En agissant de manière responsable, vous assurerez la protection et la confidentialité des données :

- Vérifiez que seules des personnes autorisées puissent accéder aux données des clients.
- Utilisez tous les mots de passe disponibles ; ne communiquez jamais ces mots de passe à des personnes non autorisées ; ne les inscrivez jamais sur un document.
- Veillez à ce qu'aucune personne non autorisée ne puisse traiter (enregistrer, modifier, transmettre, verrouiller, effacer) les données client ou les utiliser.
- Ne permettez pas aux personnes non autorisées d'accéder aux supports de données, par exemple aux CD/DVD de sauvegarde ou aux impressions de protocoles. Cela s'applique en cours d'exploitation, comme lors du stockage ou du transport.
- Veillez à ce que les supports de données qui ne sont plus utilisés soient bien détruits. De manière générale, ne conservez jamais de documents accessibles.
- Coopérez étroitement avec vos partenaires. Vous créerez ainsi un rapport de confiance avec vos clients et pourrez vous décharger de certaines tâches.

2.3.7 Prescriptions techniques et conformité de OpenScape Business X

Vous obtenez ici des informations sur le respect des exigences définies (Conformité) par les systèmes de communication OpenScape Business X.

2.3.7.1 Conformité CE

La certification CE est basée sur : 2014/35/UE - Directive sur la basse tension ; (Journal officiel de l'Union européenne L96, 29/03/2014, p. 357-374) 2014/30/UE - Directive sur la compatibilité électromagnétique (EMC) ; (Journal officiel de l'Union européenne L96, 29/03/2014, p. 79-106) 2011/65/UE - Directive sur la limitation d'utilisation de certaines substances dangereuses (RoHS) ; (Journal officiel de l'Union européenne L174, 01/07/2011, p. 88–110)

	Norme de référence
Sécurité	EN 62368-1
Electromagnetic Compatibility EMC (compatibilité électromagnétique)	EN 55032 (Émission EMC) EN55024 (EMC Immunity Residential)

2.3.7.2 Conformité aux normes des États-Unis et du Canada

	Norme de référence
Sécurité États-Unis et Canada	CSA/UL 62368-1
Émission EMC Canada	ICES-003 Issue 6 Class B
Émission EMC États-Unis	FCC 47 CFR Part 15 Subpart B Class B

N° d'enregistrement FCC et valeur de raccordement

À l'extérieur, au dos du boîtier des systèmes de communication, se trouvent un autocollant avec le numéro d'enregistrement FCC, la valeur de raccordement (Ringer Equivalence Number, REN) et d'autres informations. Sur demande, ces informations peuvent être transmises à la société de télécommunications.

2.3.7.3 Conformité aux normes internationales

	Norme de référence
Sécurité	IEC 60950-1 et IEC 62368-1
Émission EMC	CISPR 32

2.3.8 Conditions de fonctionnement

Notez les conditions environnementales et mécaniques de fonctionnement des systèmes de communication OpenScape Business X et OpenScape Business S.

2.3.8.1 Conditions d'exploitation d'OpenScape Business X

Les conditions environnementales et mécaniques de fonctionnement des systèmes de communication OpenScape Business X sont spécifiées.

Conditions environnementales d'exploitation

Limites de fonctionnement :

- Température ambiante : + 5 à + 40 °C (41 à 104 °F)
- Humidité absolue : 1 à 25 g H_2O/m^3
- Humidité relative : 5 à 80 %

La ventilation des systèmes de communication se fait uniquement par convection.

Remarque : Dommages causés par les hausses de température locales

Évitez d'exposer les systèmes de communication à la lumière directe du soleil et à d'autres sources de chaleur.

Remarque : Dommages causés par la condensation due à l'humidité

Évitez toute condensation d'humidité sur ou dans les systèmes de communication avant ou pendant leur fonctionnement, et ce en toutes circonstances.

Un système de communication doit être complètement sec avant sa mise en service.

Conditions de fonctionnement mécaniques

Les systèmes de communication sont destinés à un usage stationnaire.

2.3.8.2 Conditions d'exploitation pour OpenScape Business S

Pour plus de détails sur les conditions environnementales et mécaniques de fonctionnement d'OpenScape Business S, veuillez également vous référer à la documentation du fabricant des serveurs et des autres composants.

3 Vue d'ensemble

OpenScape Business apporte aux petites et moyennes entreprises une réponse à leurs exigences individuelles et diversifiées en communications, sous forme solution flexible et évolutive. L'architecture de la solution OpenScape Business permet l'utilisation indépendamment de l'infrastructure de téléphonie existante, qu'il s'agisse de téléphonie classique, IP ou DECT. De la téléphonie performante à la solution complète de communications unifiées (UC), OpenScape Business fournit toujours la bonne réponse.

Flexible, évolutif et performant

OpenScape Business regroupe le meilleur de HiPath 3000 et OpenScape Office dans une nouvelle plate-forme.

3.1 Points forts

OpenScape Business est la solution tout-en-un pour les petites et moyennes entreprises et offre les avantages suivants.

Points forts

- Services vocaux intégrés, gestion de la présence (statut de présence), visioconférence par glisser-déposer, messagerie vocale visuelle, standard automatique, centre de contact multimédia, messagerie instantanée, mobilité, accès à l'annuaire avec connexion à une base de données, fax, intégration aux processus métier, et bien plus encore.
- Les clients UC sont personnalisés en fonction de leur lieu de travail et de leur mode de fonctionnement.
- La solution idéale pour les clients possédant un seul site ou une solution à l'échelle d'un réseau avec plusieurs sites.
- OpenScape Business propose une architecture de solution métier unifiée.
- En fonction de l'infrastructure existante, différents modèles commerciaux OpenScape sont disponibles pour des configurations de différentes tailles. Il est également possible d'exécuter le logiciel OpenScape Business sur un serveur standard (Softswitch) - y compris dans des environnements entièrement virtualisés, bien entendu.
- La solution UC Smart est déjà intégrée à la carte mère.
- Toutes les interfaces de communication sont déjà disponibles pour répondre à des exigences diverses et hétérogènes : IP, numérique, analogique et DECT, ainsi que toutes les interfaces de réseau commun pour les communications vocales.

3.2 Communications unifiées

Les communications unifiées (UC) sont une technologie qui améliore la communication au sein des entreprises en intégrant divers supports de communication dans un environnement applicatif unifié. Les communications unifiées simplifient les processus métier dans les entreprises grâce à une gestion intégrée de la présence (par exemple, les appels sont automatiquement redirigés vers le téléphone mobile lorsque l'utilisateur est hors du bureau). Plusieurs autres fonctionnalités telles que la conférence téléphonique, la messagerie vocale personnelle, la boîte de fax personnelle, la messagerie

instantanée, l'utilisation du téléphone mobile comme extension du système de communication, le centre de contact, la vidéo, etc., sont également combinées dans cette solution unifiée.

Grâce à l'approche flexible de communications unifiées d'OpenScape Business, plusieurs solutions UC différentes sont proposées, en fonction des besoins sur le lieu de travail et de l'infrastructure existante. Pour la solution UC, vous pouvez choisir entre UC Smart et UC Suite (les deux ne peuvent pas être utilisés simultanément).

La solution UC Smart déjà intégrée à OpenScape Business peut être migrée à tout moment vers la solution avancée UC Suite via une licence de mise à niveau. En tant que commutateur logiciel pur, OpenScape Business S est disponible comme solution serveur avec les modules UC Smart ou UC Suite en option.

3.2.1 Fonctionnalités des communications unifiées (Présentation)

Selon la solution UC sélectionnée (UC Smart ou UC Suite), différentes fonctions UC sont disponibles.

Les tableaux suivants sont destinés à vous aider à choisir la meilleure solution de communications unifiées pour vos besoins. Les contraintes fonctionnelles détaillées se trouvent dans les sections correspondantes (UC Smart, UC Suite, Attendants) de la description des fonctionnalités et de la documentation de l'administrateur.

Fonctionnalité UC	**UC Smart**	**Suite UC**		**Notes**
	-	**myPortal pour ordinateur/ Outlook**	**myPortal au travail**	
État de présence				
Statut de présence (gestion de la présence)	-	x	x	
Modifier le statut de présence via le client	-	x	x	
Modifier le statut de présence via l'interface utilisateur du terminal (TUI)	-	x	-	

Fonctionnalité UC	UC Smart	Suite UC		Notes
	-	myPortal pour ordinateur/ Outlook	myPortal au travail	
Transfert d'appel basé sur le statut	-	x	x	Avec UC Smart, n'importe quel numéro peut être sélectionné comme destination. Avec UC Suite, seul un numéro de la présélection peut être sélectionné.
Affichage de l'état dans les favoris	-	x	x	
Affichage de l'état dans les répertoires	-	x	x	
Affichage de l'état dans le journal	-	x	-	
Activer le service CallMe	-	x	x	
Intégration du calendrier (Outlook)	-	x	-	
Intégration du calendrier (iCal) (uniquement avec myPortal pour ordinateur)	-	x	-	
Favoris				
Afficher l'état de l'appel	-	x	x	
Créer des groupes	-	x	-	
Affichage compact des favoris	-	x	-	
Annuaires				
Annuaire personnel	-	x	x	
Répertoire interne	-	x	x	
Répertoire externe	-	x	x	
Recherche dans les répertoires	-	x	x	
Accès aux destinations en numérotation abrégée définies dans le système (SSD)	-	-	x	
Importer/Gérer les contacts personnels (CSV/XML)	-	x	-	
Accès aux contacts Outlook	-	x	-	

Fonctionnalité UC	UC Smart	Suite UC		Notes
	-	myPortal pour ordinateur/ Outlook	myPortal au travail	
Importation des contacts personnels (Mac OS) (myPortal pour ordinateur)	-	x	-	
Intégration d'un serveur d'annuaire externe via LDAP	-	x	-	
Journal				
Tous les appels	-	x	-	
Appels à candidatures ouverts	-	x	-	
Appels manqués	-	x	-	
Répondre aux appels	-	x	-	
Appels programmés	-	x	-	
Messagerie vocale	-	x	-	
Journal de télécopie	-	x	-	
Conversations				
Chat	-	-	-	
Journal	-	-	x	
Messagerie vocale	-	-	x	
Appels				
numérotation manuelle	-	x	x	
Composeur de bureau (cliquer pour appeler)	-	x	-	
Expéditeur	-	x	x	
Mettre l'appel en attente	-	x	x	
Enregistrement des appels (enregistrement vocal)	-	x	-	
Envoyer un courriel	-	x	x	
Envoyer un SMS	-	-	-	
Démarrer une conversation	-	x	-	
Fenêtres contextuelles	-	x	-	
Conférences				
Conférence ad hoc	-	x	x	
Conférences programmées	-	x	-	
Conférences permanentes et ouvertes (conférence par glisser-déposer)	-	x	-	

Fonctionnalité UC	UC Smart	Suite UC		Notes
	-	myPortal pour ordinateur/ Outlook	myPortal au travail	
Intégration de la collaboration Web	-	x		
Messages vocaux et fax				
Boîte vocale (messagerie vocale visuelle)	-	x	x	Fonctionnalité de messagerie vocale pour les abonnés (IP, TDM)
Lecture via téléphone	-	x	x	
Lecture via la carte son du PC	-	x	-	
Comment envoyer un message vocal par e-mail	-	x	-	
Fax	-	x	-	
Messagerie instantanée				
Messagerie instantanée (chat)	-	x	-	

Centre de contact

Fonctionnalité UC	UC Smart	Suite UC		Notes
		monAgent	mes rapports	
Agents, files d'attente et horaires	-	x	-	
Fax et courriel	-	x	-	
rapports prédéfinis/ modèles de rapports	-	x	x	
Création programmée de rapports	-	-	x	

La connexion à OpenScape Contact Center est possible en option.

Postes de travail (Consoles de poste de travail)

Fonctionnalité UC	UC Smart	Suite UC	Notes
	-	mon assistant	
Affichage des appels en attente avec type d'appel, nom et numéro de téléphone	-	x	
Afficher l'état de la connexion	-	x	
Commutation rapide des appels	-	x	

Fonctionnalité UC	UC Smart	Suite UC	Notes
	-	mon assistant	
Numérotation abrégée via les touches BLF et les boutons utilisateur. Configuration personnalisée des champs de voyants d'occupation et des boutons utilisateur avec numéro d'appel ou nom	-	x	
Consulter le statut de présence des autres abonnés	-	x	
Modifier le statut de présence des autres abonnés	-	x	
Annuaire personnel	-	x	
Répertoire interne	-	x	
Répertoire externe	-	x	
Contacts Outlook	-	x	
Accès LDAP	-	x	
Journal	-	x	
Conférence ad hoc	-	x	
Conférences programmées, permanentes et ouvertes (conférence par glisser-déposer)	-	x	
Centre de messagerie	-	x	Tous les messages vocaux, fax, messages instantanés, SMS et courriels sont enregistrés et gérés via le Centre de messagerie.
Accès aux messages vocaux et aux fax des autres abonnés	-	x	Doit être publié par chaque abonné respectif
Messagerie instantanée (chat)	-	x	
Service de nuit	-	x	

Le client Attendant recommandé pour UC Suite est mon Attendant.

Messagerie vocale et standard automatique de l'entreprise

Fonctionnalité UC	UC Smart	Suite UC	Note
Fonctionnalités de base de la messagerie vocale intelligente UC et du standard automatique d'entreprise	-	-	
Fonctionnalités de base de la messagerie vocale UC Suite et du standard automatique d'entreprise	-	x	Exige des compétences commerciales
Fonctionnalités UC			

Fonctionnalité UC	UC Smart	Suite UC	Note
Fonctionnement graphique de la messagerie vocale pour les abonnés (interface web ou interface client)	-	x	
Messagerie vocale : instructions pour la fonction de présence	-	x	Différentes annonces, en fonction de la présence UC définie
Règles personnelles pour les salutations par boîte aux lettres	-	x	L'abonné définit des règles détaillées pour la sélection de ses messages de bienvenue personnalisés.
Messagerie vocale par courriel	-	x	Le message vocal est joint à l'e-mail sous forme de fichier WAV.
Fonctions du standard automatique			
Boîtes aux lettres avec standard automatique (standard automatique de base)	-	20	
Répondeur automatique de l'entreprise	-	x	Console centrale d'opérateur et messagerie vocale centralisée avec messages d'accueil alternatifs pour chaque poste
Annonce avant réponse / Signalisation parallèle	-	x	Annonce faite à l'appelant pendant l'appel à l'abonné Pour UC Suite, cela n'est possible qu'en association avec le centre de contact.
Destinations d'appel pour les sections de 4 jours / Calendrier pour standard automatique	-	x	Système automatisé de réponse variable pour différents moments de la journée Fonction calendrier possible avec UC Smart via le service de nuit automatique
Calendrier central pour la boîte aux lettres	-	x	Annonces et gestion des appels pour les événements d'entreprise tels que les jours fériés, les congés d'entreprise, etc.
Profils personnalisés pour la boîte aux lettres et le standard automatique personnel	-	x	Gestion des appels basée sur la présence, configurable individuellement pour chaque abonné.

Fonctionnalité UC	UC Smart	Suite UC	Note
Horaires	-	Planification avec règles (vecteur de contrôle d'appel, CCV)	
Modèles	-	5 modèles personnalisables	
Éditeur de règles graphique (éditeur CCV)	-	x	
Concaténation de boîtes aux lettres / Répondeur automatique à plusieurs étapes	-	-	L'appel est transféré d'une boîte vocale concaténée à l'autre, et à chaque fois, l'annonce correspondante est diffusée.
Composer par nom	-	x	
Composez par extension	-	x	
Fonctionnalités de messagerie vocale			
Messages personnalisés par boîte aux lettres	-	10	Enregistrer et configurer diverses annonces
Transfert des messages vocaux	-	x	Transférer le message à un autre abonné/une autre boîte aux lettres
Rappel depuis la messagerie vocale	-	x	Le rappel de l'appelant du message peut être activé.
Appel de notification	-	x	Lorsqu'un message arrive, un appel est passé vers une destination externe, par exemple un téléphone portable.
Fonction représentative	-	x	Transférer l'appelant à un représentant pour une annonce personnelle
Messagerie vocale basée sur l'appelant / routage CLI	-	x	Gestion des appels en fonction du numéro d'appel, par exemple, un message d'accueil dans la langue de l'appelant.
Boîte aux lettres du groupe central	-	x	Avec des annonces pour les départements / groupes
Enregistrement en direct	-	x	Enregistrement des conversations avec fonctions de sécurité Dans OpenScape Business S, où l'enregistrement en direct depuis UC est utilisé, G.729A n'est pas pris en compte.

Fonctionnalité UC	UC Smart	Suite UC	Note
Enregistrer les messages	-	x	Les abonnés peuvent enregistrer individuellement les messages vocaux pour eux-mêmes
Suppression automatique des messages	-	x	Après une période de conservation, les messages sont supprimés afin de libérer de l'espace de stockage.
Modifier la langue de la messagerie vocale en fonction de l'abonné	-	x	Sélection des annonces automatiques dans une langue spécifique

Concepts associés

UC Smart à la page 440

3.2.2 Accès utilisateur aux fonctionnalités UC (clients UC)

L'accès aux fonctionnalités UC se fait via les clients UC. Le statut de présence (UC Suite) et la messagerie vocale (UC Smart et UC Suite) sont également accessibles via l'interface utilisateur du téléphone (TUI).

Des clients UC sont proposés pour les principaux systèmes d'exploitation. Veuillez également prendre en compte les exigences des clients dans les notes de version respectives.

Clients de communication (clients de bureau et logiciels de travail collaboratif)

Client	Recommandé pour		Description
	UC Smart	Suite UC	
myPortal au travail	x	x	Client UC Desktop pour Microsoft Windows et Mac OS X
myPortal pour ordinateur	-	x	Client de bureau UC avancé pour Microsoft Windows et Apple Mac
myPortail pour Outlook	-	x	Client UC Groupware pour l'intégration de Microsoft Outlook
Téléphone de bureau OpenScape CP 400/600/600E/700/700X/710 HFA (logiciel client intégré au téléphone)	x	x	Contrôle de présence et accès au répertoire téléphonique pour UC Suite et UC Smart

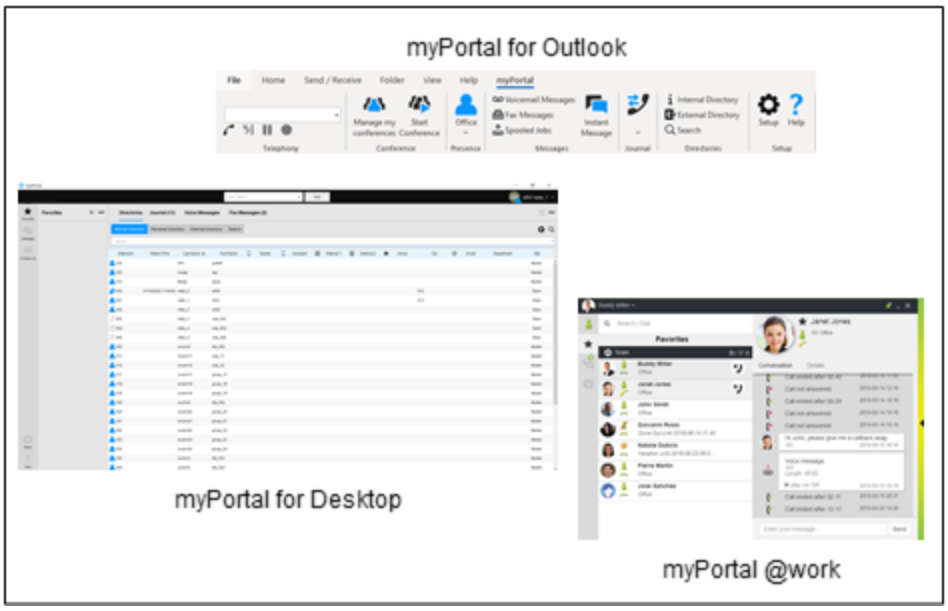


Illustration 1 : myPortal pour ordinateur, myPortal pour Outlook et myPortal @work

Clients du centre de contact

Client	Recommandé pour		Description
	UC Smart	Suite UC	
monAgent	-	x	Client du centre de contact
mes rapports	-	x	Interface de rapports/de reporting pour le centre de contact myReports peut également être utilisé pour les statistiques système indépendamment du centre de contact.

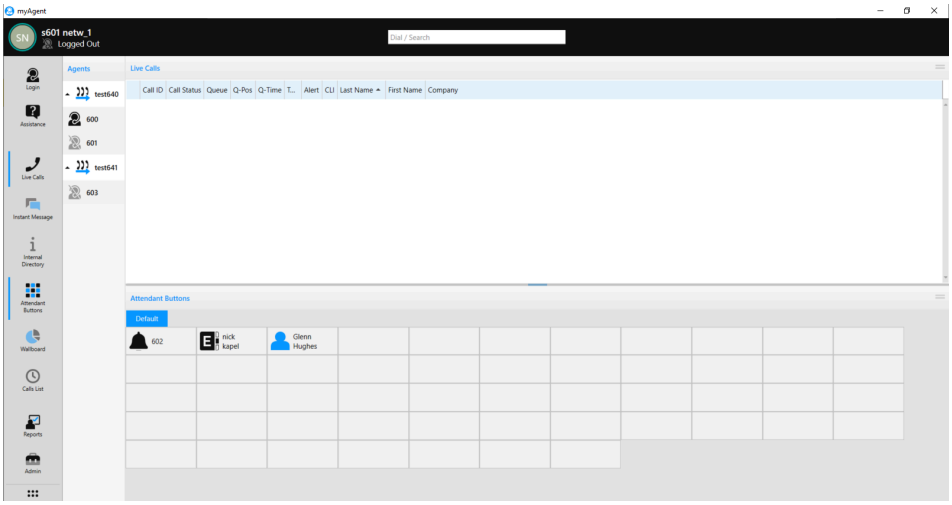


Illustration 2 : monAgent

Postes de travail/Consoles de poste de travail

Client	Recommandé pour		Description
	UC Smart	Suite UC	
mon assistant	-	x	Console avancée d'opérateur UC pour UC Suite

Illustration 3 : mon assistant

3.2.3 Intégration dans les applications commerciales

OpenScape Business peut être intégré dans les infrastructures IT existantes et les applications commerciales.

Applications

- Application Launcher pour une interaction active avec les applications CRM/ERP
- Logiciel de taxation pour l'évaluation des taxes

Service intégrés

- Services de répertoire pour les informations concernant les appelants et pour la recherche dans les répertoires internes et externes
- Gestion de la présence et messagerie instantanée pour les réseaux sociaux
- Services Web pour les interactions avec les applications basées sur le Web avec téléphones mobiles et tablettes PC par ex.

CTI-Middleware

- First- and Third-party TAPI Service Provider (fournisseur de services TAPI) pour la gestion des appels provenant des applications CTI ou CRM/ERP

Interfaces et Journalisation

- CSTA pour la surveillance et la gestion de différentes applications
- SIP pour la connexion aux applications basées sur SIP-Trunking
- LDAP pour la connexion aux répertoires externes ou des clients LDAP externes
- HTTP et HTTPS pour l'accès aux fonctions UC du Web-Server intégré
- TCP/IP comme protocole de base pour toutes les connexion Ethernet
- SQL Connektor pour la connexion des bases de données SQL (Microsoft SQL Server, PostgreSQL, Sybase SQL Server)
- LDAP Konnektor pour serveurs LDAP externes comme Active Directory

3.3 Modèles commerciaux d'OpenScape

Différents modèles sont disponibles pour l'utilisation des fonctionnalités de téléphonie et de communications unifiées. Vous pouvez choisir entre des modèles matériels et des modèles purement logiciels fonctionnant sur des serveurs standard ou dans un environnement virtuel avec VMware vSphere.

La fonctionnalité UC pour UC Smart est déjà intégrée à OpenScape Business X. Le commutateur logiciel OpenScape Business S prend en charge, en option, UC Smart ou UC Suite.

3.3.1 Niveaux d'extension disponibles via les ventes

Les modèles commerciaux d'OpenScape présentent différents niveaux d'expansion.

	X1	X5R	X8	S
Connexion au fournisseur de services				
Canaux ITSP (fournisseurs SIP)	30	60	60	180
Nombre maximal de fournisseurs SIP actifs	8	8	8	8

	X1	X5R	X8	S
ISDN S_0 (BRI)	4	52	128	-
	via la carte mère	X5R : 6* STLSX4R	Limite logicielle, c'est-à-dire indépendamment du nombre de cartes STDM3	
ISDN S_{2M} (PRI)	-	30	120	-
		1* TS2	3 * DIUT3	
Nombre maximal de canaux de jonction (ITSP, SIP-Q, SIP natif, jonctions TDM, MEB)	250	250	250	250
Gares				
ISDN	4	52	128	-
	via la carte mère	X5R : 6* STLSX4R	8* STMD3	
Analogique	4	52/68	384	-
	via la carte mère	X5R : 6* SLAV8R	16* SLMA	
Numérique ($U_{P0/E}$)	8	56	384	-
	via la carte mère	6* SLU8R	16* SLMO2	
Stations IP	20[1]	500	500	2000 (max. 500 stations SIP)
Sans fil/DECT (CMI)	16	32/64	250	-
	1 à 7 stations de base via carte mère	1 à 7 stations de base via la carte mère + 8 à 15 via SLUN	4* SLMUC	
Nombre maximal de stations	30[1]	500	500	2000
Communications unifiées (UC Smart)				
Messagerie vocale intelligente UC (Smart VM)	30	320	320	1500
Nombre maximal de clients UC Smart actifs simultanément (Somme du lanceur d'applications et des clients WSI tiers)	30	50	50	250
Nombre maximal de stations mobiles	30	50	50	250
Nombre de stations d'accès pour les utilisateurs de la mobilité	30	150	150	250

	X1	X5R	X8	S
myPortail pour les équipes	-	-	-	250
Nombre maximal de canaux pour les conférences UC	30	30	30	60
Communications unifiées (suite UC)				
Messagerie vocale UC Suite	-	500	500	1500
Nombre maximal de clients UC Suite actifs simultanément (Somme de myPortal pour ordinateur, myPortal pour Outlook, myAttendant, myAgent)	-	150	150	1500
Nombre maximal d'autres clients actifs simultanément (Somme de myPortal for Teams, d'Application Launcher et des clients WSI tiers)	-	-	-	500
myPortal pour ordinateur	-	150	150	1500
myPortail pour Outlook	-	150	150	1500
mon assistant	-	20	20	20
monAgent	-	192 configurables / 64 actifs simultanément	192 configurables / 64 actifs simultanément	192 configurables / 64 actifs simultanément
Nombre maximal de stations mobiles	-	150	150	250
Nombre de stations d'accès pour les utilisateurs de la mobilité	-	150	150	250
myPortail pour les équipes	-	-	-	250
mes rapports	-	1	1	1
Nombre maximal de canaux de télécopie simultanés	-	8	8	8
Nombre maximal d'utilisateurs de télécopie	-	150	150	1500
Nombre maximal de canaux pour les conférences UC	-	20	20	60
Communications unifiées (CRM, connectivité des bases de données)				
Lanceur d'applications	30 configurables / 30 actifs simultanément	500 configurables / 50 actifs simultanément	500 configurables / 50 actifs simultanément	500
Utilisateur TAPI 120/170 (via CSTA)	-	150	150	1500

	X1	X5R	X8	S
Utilisateur TAPI 120 (en mode UC Smart via la carte mère sans CSTA)	30	30	30	-
Connecteur de services d'annuaire	-	4	4	4

Pour une description détaillée des niveaux d'extension et des limites de capacité, voir également Limites de configuration et capacités .

Réseau de communications unifiées OpenScape Business

OpenScape Business offre de nombreuses options de connectivité réseau :

- Réseau étendu de voix et de communications unifiées entre les différentes plateformes OpenScape Business X et OpenScape Business S
- avec plusieurs bâtiments sur les locaux de l'entreprise
- avec des emplacements répartis
- Administration centrale, y compris les licences (HiPath 5000 RSM n'est plus requis)
- Préparation du réseau vocal avec OpenScape Enterprise

La mise en réseau vocale prend en charge les réseaux comportant jusqu'à 32 nœuds. La mise en réseau UC prend en charge les réseaux comportant jusqu'à 8 nœuds et jusqu'à 1000 stations (1500 stations avec OpenScape Business S). De plus, des versions spécifiques à chaque projet sont possibles.

Pour une description détaillée des scénarios de mise en réseau, consultez la section Limites et capacités de configuration. .

3.3.2 Modèles matériels UC

Les systèmes de communication OpenScape Business X offrent une grande flexibilité en termes de fonctionnalités et de conception. Selon le modèle OpenScape Business X, jusqu'à 500 stations sont prises en charge pour les connexions IP, numériques (ISDN), analogiques (a/b) et au réseau public utilisant ITSP (SIP), ISDN (BRI et PRI), CAS et analogiques et IP embarquées (fournies sur la carte mère).

- OpenScape Business X1R

  Système de communication livré dans un boîtier rack 19 pouces et pouvant être installé dans un rack 19 pouces, en tant qu'unité autonome (fonctionnement sur bureau) ou fixé au mur.
- OpenScape Business X5R

  Système de communication livré dans un boîtier rack 19 pouces et pouvant être installé dans un rack 19 pouces, en tant qu'unité autonome (fonctionnement sur bureau) ou fixé au mur.
- OpenScape Business X8

  Système de communication modulaire pouvant être utilisé comme système à un seul boîtier (boîtier de base) ou comme système à deux boîtiers (boîtier

[1] Nombre maximal d'utilisateurs IP et Deskshare : 20 (limité par la configuration) - Nombre maximal de postes IP, Deskshare, analogiques et numériques : 30 (limité par les licences)

de base + boîtier d'extension). Le système de communication peut être installé comme unité autonome ou monté dans une baie de 19 pouces.

Illustration 4 : Plateformes matérielles

3.3.3 Matériel d'amplification UC

Matériel UC Booster pour OpenScape Business X.

- Carte d'extension de canal vocal OpenScape Business

  Deux modules optionnels pour l'extension d'OpenScape Business X avec des canaux DSP supplémentaires (par exemple, pour des connexions vocales simultanées avec transitions IP/TDM).

  Huit canaux DSP sont disponibles sur la carte mère. La carte d'extension de canal vocal OCCB/1 fournit 48 canaux DSP supplémentaires, et la carte d'extension de canal vocal OCCB/3 fournit jusqu'à 128 canaux DSP.

3.3.4 Modèles UC Logiciel (commutateur logiciel)

Solution logicielle UC tout-en-un basée sur un serveur qui prend en charge jusqu'à 1000 stations IP avec des connexions au réseau public par ITSP (SIP).

Indépendamment de la plateforme utilisée, OpenScape Business S peut être installé sur un serveur Linux. Les systèmes d'exploitation utilisés sont SLES 12 SP5 64 bits ou SLES 15 SP6 64 bits. OpenScape Business S peut également être exécuté dans un environnement virtuel avec VMware vSphere. Si des interfaces TDM sont nécessaires pour la connexion à des téléphones TDM ou à des lignes réseaux TDM, les systèmes OpenScape Business X peuvent être utilisés comme passerelle.

3.3.5 Structure et conditions environnementales

	X1R	X5R	X8
Structure	Étagère	Étagère	Système standard (installation en rack également possible)

	X1R	X5R	X8
Dimensions (H x L x P en mm)	450x460x130	155x440x380 (3,5U)	490x440x430
Poids	environ 6 kg	environ 8 kg	environ 34 kg (pleine charge)
Couleur du boîtier	Noir	Vert / Gris foncé	Vert / Gris foncé
Alimentation électrique	Les modèles sont équipés pour le raccordement à l'alimentation électrique. • Tension d'entrée nominale (CA) : 100 à 240 V • Fréquence nominale : 50/60 Hz • Alimentation de la batterie (CC) : -48 V		
Consommation d'énergie	En fonction de la plateforme matérielle et de l'extension		
Conditions environnementales	• Conditions de fonctionnement : +5 à +40 °C (41 à 104 °F) • Humidité : 5 à 85 %		

3.3.6 Téléphones compatibles

OpenScape Business X permet la téléphonie sur IP/HFA (HiPath Feature Access), SIP, TDM, a/b, sans fil/DECT et WLAN. Les téléphones IP/HFA, SIP et sans fil peuvent être connectés à OpenScape Business S.

Téléphones OpenStage (IP, SIP et T)	• OpenStage 5/10/15/20/30/40/60/80
Téléphone de bureau OpenScape (IP, SIP et T)	• Téléphone de bureau OpenScape IP 35G/55G/35G Eco • Téléphone de bureau OpenScape CP 100/200/205/400/600/600E/700/700X HFA et SIP 200/400/205/405 TDM • Téléphone de bureau OpenScape CP 110/210/410/710 HFA et SIP

Modules clés	• Module clé OpenStage, uniquement pour OpenStage 15/40/60 • OpenStage BLF 40 (Busy Lamp Field), uniquement pour OpenStage 40 et OpenStage 30 T • Module de clé OpenScape 400/600, compatible uniquement avec les modèles CP 400/600/600E/700/700X • Module de clé OpenScape 410/710, uniquement pour CP 710
Clients PC (SIP)	• OpenScape Édition Personnelle (incluant la vidéo pour SIP)
Téléphones SIP (UC Suite) / Adaptateur AP	• Téléphones SIP compatibles avec la norme RFC 3725 • Mediatrix 4102S (pour connecter 2 téléphones analogiques ou appareils de télécopie)
Téléphones sans fil	• OpenStage WL3 professionnel • Téléphone WLAN OpenScape WL4/WL4 Plus
Téléphones analogiques et RNIS	• Téléphones analogiques (a/b) • Téléphones RNIS numériques ($_{S0}$)

Les appareils plus anciens (tels que optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 et optiPoint WL2 SIP) sont pris en charge. Les appareils Optiset E ne peuvent pas être utilisés.

Fonctions et configuration des téléphones SIP

OpenScape Business offre une gamme étendue de fonctionnalités de communication vocale pour les téléphones OpenStage HFA. De nombreuses fonctions sont également disponibles pour les téléphones SIP standard.

Vous trouverez une présentation des fonctionnalités prises en charge par les téléphones SIP OpenStage ainsi que des informations complémentaires sur le wiki Unify, à l'adresse suivante :

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

Le contrôle des appels vocaux pour les téléphones SIP via les clients UC Smart est pris en charge pour les modèles de rack OpenScape Business X5 avec la carte Booster.

Grâce aux fonctions DLI, les téléphones OpenScape Desk Phone (SIP) peuvent être administrés de manière centralisée et dotés de logiciels.

Concepts associés

CSTA à la page 1096

3.4 Autres informations

Vous trouverez d'autres informations sur Internet et sur Extranet. Pour les restrictions et les dernières modifications, consultez les notes de validation.

3.4.1 Langues prises en charge

Plusieurs variantes linguistiques sont disponibles pour les différents composants logiciels (clients et WBM) ainsi que pour la documentation et l'aide en ligne.

Les langues suivantes seront publiées dans le cadre du lancement spécifique à chaque pays.

	de en	es fr il nl pt	da Non sv	fi	ru	cs	pl	heure tr	hu	zh
Clients intelligents UC										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (Guide utilisateur)	X	X	X	X	X	X	X	-	-	-
TUI (Interface utilisateur téléphonique)	X	X	X	X	X	X	–	X	–	X
TUI (Guide de référence rapide)	X	X	–	–	–	–	–	–	–	–
Clients UC Suite										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (Guide utilisateur)	X	X	X	X	X	X	X	-	-	-
myPortal pour ordinateur (client)	X	X	X	X	X	X	X	X	X	X
myPortal pour ordinateur (Guide de l'utilisateur/Aide en ligne)	X	X	X	X	X	X	X	–	–	–
myPortal pour Outlook (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Outlook (Mode d’emploi/Aide en ligne)	X	X	X	X	X	X	X	–	–	–
myAttendant (Client)	X	X	X	X	X	X	X	X	X	X
myAttendant (Mode d’emploi/Aide en ligne)	X	X	X	X	X	X	X	–	–	–
myAgent (Client)	X	X	X	X	X	X	X	X	X	X
myAgent (Mode d’emploi/Aide en ligne)	X	X	X	X	X	X	X	–	–	–
myReports (Client)	X	X	–	X	X	X	X	–	–	–
myReports (Mode d’emploi/Aide en ligne)	X	X	–	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	X	X	X	X

	de en	es fr il nl pt	da Non sv	fi	ru	cs	pl	heure tr	hu	zh
TUI (Aide-mémoire)	X	X	–	–	–	–	–	–	–	–
Administration										
OpenScape Business Assistant (WBM)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Assistant (Documentation de l'administrateur/Aide en ligne)	X	X (pas de nl)	–	–	–	–	–	–	–	–
Manager E	X	X	X	X	X	X	X	–	–	–
Manager E (Documentation de l'administrateur/Aide en ligne)	X	X	–	–	X	–	–	–	–	–

De plus, la TUI UC Smart est également proposée en flamand (Belgique) et en slovène.

Conseil : Un système d'exploitation Windows russe ou chinois est la condition nécessaire pour pouvoir utiliser l'interface utilisateur russe ou chinois.

Les abréviations utilisées dans le tableau correspondent aux codes de langue suivant (ISO 639-1) :

- de = Allemand
- en = Anglais
- cs = Tchèque
- da = Danois
- es = Espagnol
- fi = Finlandais
- fr = Français
- hr = Croate
- hu = Hongrois
- it = Italien
- nl = Néerlandais
- no = Norvégien
- pl = Polonais
- pt = Portugais
- ru = Russe
- sv = Suédois
- tr = Turc
- zh = Chinois

3.4.2 Liens Internet

Vous trouverez des informations ou des renseignements plus actuels dans la page d'accueil Unify, dans notre Expert-Wiki et dans le portail Unify pour les partenaires.

Liens Internet

- Page d'accueil Unify :

  `http://www.unify.com`
- Wiki experts pour téléphones, systèmes de communication et UC :

  `http://wiki.unify.com`
- Portail partenaire (enregistrement nécessaire) :

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

  ou

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

4 Concept d'administration

L'administration du système de communication est réalisée avec OpenScape Business Assistant.

4.1 OpenScape Business Assistant (WBM)

L'assistant OpenScape Business est basé sur le Web et il donc également désigné sous le terme WBM (Web Based Management).

L'étendue des tâches d'administration proposées dépend du profil d'administrateur utilisé.

Pour chaque page de WBM, il existe une Aide en ligne.

4.1.1 Conditions nécessaires pour WBM

Pour l'utilisation du WBM, le PC d'administration a besoin des logiciels appropriés.

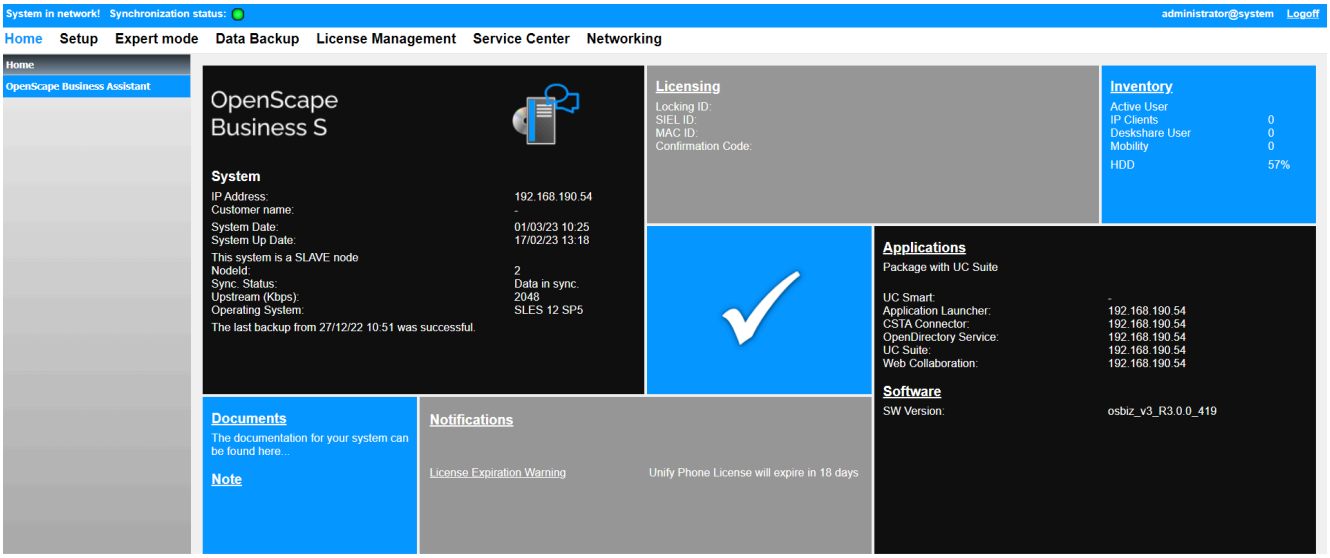
Navigateurs web supportés :

- Microsoft Internet Explorer 10 ou ultérieur
- Microsoft Edge
- Mozilla Firefox 18 ou ultérieure
- Google Chrome

4.1.2 Page d´accueil des WBM

La page d’accueil de la WBM présente des informations système importantes qui sont réparties dans différents secteurs (carreaux). Elle fournit en plus des indications et informe sur les erreurs système, événements et actions).

Les informations système offertes dépendent du profil d’administrateur utilisé. Les titres soulignés des différentes zones peuvent être cliquées et font référence au thème correspondant de WBM.



Les informations suivantes sont présentées :

- Zone : **État** (milieu)
  - Coche blanche sur fond bleu : le système de communication est entièrement fonctionnel ; les messages à fond rouge dans les autres champs font référence à des actions qui doivent être effectuées.
  - Point d'exclamation blanc sur fond rouge : le système de communication n'est pas entièrement fonctionnel et nécessite une intervention de la part de l'administrateur ; les messages à fond rouge dans les autres champs font référence à des erreurs système ou à des événements qui doivent être résolus.
- Zone : **Système**
  - Marque
  - Adresse IP du système de communication
  - Date et heure actuelles
  - Date et heure du dernier redémarrage du système
  - Remarques en cas d'utilisation dans une interconnexion de réseaux (le système est maître ou esclave, affichage de l'ID de noeud)
  - Etat de la synchronisation
  - Bande passante en amont en kbit/s
  - État d'intégrité de la carte SDHC
  - Instructions pour l'enregistrement et la restauration
  - Etat de la Booster Card
- Zone : **Documents**
  - Lien vers la documentation
- Zone : **Notifications**
  - Diverses notifications à propos du système
- Zone : **Remarque**
  - Indique les informations entrées en dernier par un administrateur. Un clic sur le titre souligné ouvre une fenêtre de texte où sont affichées

toutes les informations et où il est possible d’entrer des informations supplémentaires.

Les données du champ Remarque ne sont pas incluses dans le jeu de sauvegarde du système. Par conséquent, lors de la restauration d’un jeu de sauvegarde, ces données ne seront pas restaurées.

- Zone : **Gestion des licences**
  - ID de verrouillage pour la procédure de licence
  - ID SIEL pour la procédure de licence
  - Indication concernant l’état de la licence, précisant si le système est associé à une licence permanente ou de paiement à l’utilisation.
- Zone : **Inventaire**
  - Type et nombre des abonnés actifs
  - Nombre de ITSP activés et lien vers la boîte de dialogue d’état ITSP dans le Centre de service des postes actifs
- Zone : **Applications** et logiciels

  Applications :
  - Pack d’application utilisé (UC Smart ou UC Suite) et ses composantes y compris les adresses IP des serveurs utilisés.

  Logiciel :
  - Version du logiciel installé du système de communication
  - Date de fin de l’assistance logicielle de trois ans.

    Après la date d’expiration, le message "Licence de support logiciel expirée, veuillez mettre à jour la licence de support logiciel" s’affiche.
  - Indications sur la nouvelle version du logiciel

4.1.3 Introduction au WBM

Le WBM est l'application basée sur le Web dédiée à l'administration du système.

Langue de l'interface utilisateur

Vous pouvez sélectionner l'une des langues suivantes lors de la connexion :

- Allemand
- Anglais
- Français
- Italien
- Néerlandais (l'aide en ligne est uniquement disponible en anglais)
- Portugais
- Espagnol

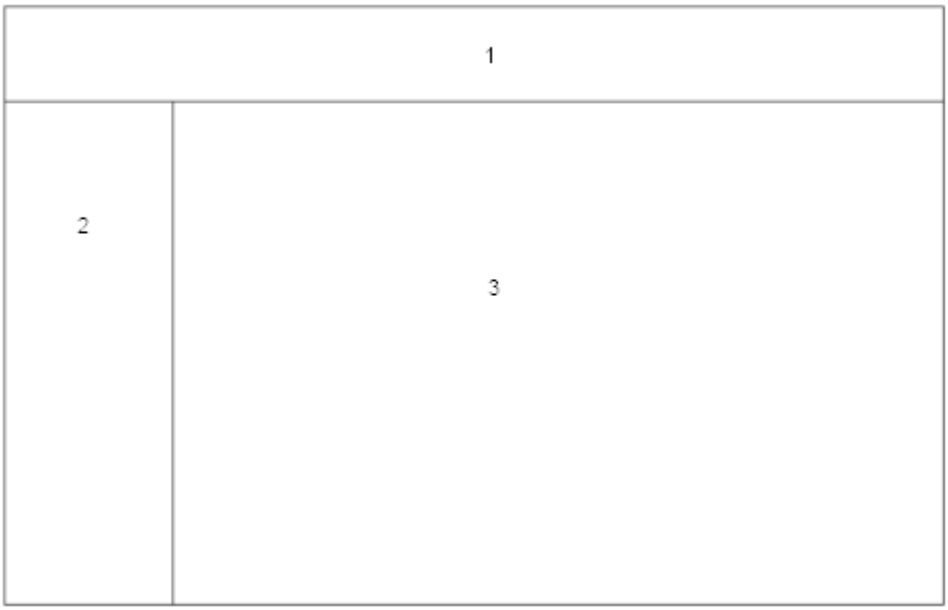
Ordre des interfaces utilisateur décrites

Toutes les tâches qui peuvent être effectuées dans un assistant sont décrites uniquement pour l'assistant correspondant.

D'autres tâches qui peuvent être effectuées en mode Expert ne sont décrites que pour le mode Expert.

Seules les tâches restantes sont décrites pour Manager E.

Éléments de l’interface utilisateur



- Barre de navigation (1)

  La navigation est la principale aide à la navigation et affiche toujours les mêmes liens vers les principaux centres de tâches, c'est-à-dire **Accueil**, **Administrateurs**, **Configuration**, **Mode expert**, **Sauvegarde des données**, **Gestion des licences**, **Centre de services**, ainsi que le nom de l'utilisateur actuel et le lien **Déconnexion**. Cliquez sur un centre de tâches pour ouvrir, dans la zone de navigation, l'arborescence de navigation correspondante et, dans l'espace de travail, la page d’accueil du centre de tâches.
- Zone de navigation (2)

  La zone de navigation est la navigation secondaire et comprend l'arborescence de navigation avec les options de menu du centre de tâches sélectionné. Dans l'arborescence de navigation, le nom du centre de tâches sélectionné est affiché en premier. En dessous figurent des groupes de menu qui peuvent être ouverts et refermés et des options de menu. Les groupes de menus offrent différentes options qui varient selon les situations. Cliquez sur une option de menu pour afficher la page correspondante dans l'espace de travail.
- Espace de travail (3)

  L'espace de travail permet d'exécuter les différentes tâches d'administration. L'espace de travail s'ouvre généralement dans sa propre fenêtre. Le nombre et le choix d'informations et d'actions affichées varient en fonction de l'option de menu sélectionnée dans l'arborescence. En mode Expert, l'arborescence de menu s'affiche à gauche dans l'espace de travail.

Navigation dans l'arborescence du menu

L'arborescence du menu sert à la navigation en mode Expert de WBM. L'arborescence du menu contient des dossiers (par ex. **Maintenance**) avec d'autres éléments (par ex. **Redémarrer / Recharger**).

Pour naviguer dans l'arborescence, vous devez cliquer sur les dossiers (ouverture et fermeture alternatives).

Déconnexion automatique après temporisation.

Vous êtes automatiquement déconnecté après 30 minutes d'inactivité. Pour continuer de travailler avec WBM, vous devez vous reconnecter. Après une pause, pour des raisons de sécurité, chargez de nouveau la page avant d'effectuer des modifications, afin que celles-ci ne soient pas perdues à la suite d'une déconnexion automatique.

4.1.3.1 Comment se connecter au WBM

Conditions préalables

Vous devez avoir accès à vos identifiants (nom d'utilisateur et mot de passe). Si ce n'est pas le cas, demandez-les à votre administrateur.

TLS 1.2 est activé dans les paramètres de votre navigateur web.

Étape par étape

1) Ouvrez la page de connexion dans votre navigateur web en saisissant l'adresse suivante : `https://<IP adresse du système de communication>`. L'adresse IP par défaut est 192.168.1.2.
2) Cliquez sur le code de langue en haut à droite et sélectionnez dans le menu la langue dans laquelle l'interface utilisateur du WBM doit être affichée. La page de connexion s'affiche dans la langue sélectionnée.
3) Saisissez le nom d'utilisateur sous **Connexion** dans le premier champ. La mention « @system » est ajoutée automatiquement en quittant le champ.
4) Saisissez votre mot de passe dans le deuxième champ sous **Connexion**. Tenez compte de la casse et de l'état de la touche **Num**. Le mot de passe est affiché avec des astérisques (*).
5) Cliquez sur **Connexion**.

Si vous saisissez des informations d'identification non valides, un message s'affiche après la troisième tentative de connexion infructueuse, vous informant que le compte est bloqué pendant 5 minutes. Vous pouvez essayer de vous connecter à nouveau après cette période.

Pour tout nouvel échec de connexion, ce délai est doublé et atteint 160 minutes à la huitième tentative. Pour chaque tentative échouée suivante, la durée de blocage du compte est de 160 minutes.

4.1.3.2 Comment se déconnecter de la WBM

Procédure

- Cliquez en haut à droite sur **Déconnexion**.

4.1.4 Gestion d’utilisateur du WBM

Vous pouvez configurer et gérer jusqu'à 16 administrateurs pour la gestion basée sur le web (WBM). Chaque administrateur se voit attribuer un profil qui spécifie l'étendue de son autorisation. Vous pouvez également modifier le mot de passe d'un administrateur Manager E.

Les utilisateurs de WBM sont également appelés administrateurs.

L'administrateur par défaut est `administrator@system` avec le mot de passe par défaut `administrator` et a le profil **Advanced**. Ce mot de passe doit être modifié lors de la première connexion. Le mot de passe d'un administrateur doit comporter au moins 8 caractères et au maximum 128 caractères, dont au moins un chiffre. En outre, pour que le mot de passe soit sûr, il doit comporter au moins une lettre majuscule, une lettre minuscule et un caractère spécial.

Remarque : L'accès administratif (y compris le rôle d'utilisateur admin) est enregistré dans le fichier journal des messages/ syslog. Il est accessible via le menu **Diagnostics** > **Trace**.

Profils

Le WBM prend en charge quatre profils avec différentes classes de service (autorisations) pour les administrateurs ayant différents niveaux d'expertise technique et de tâches.

Afin d'éviter qu'un utilisateur malveillant puisse se connecter via le RNIS et modifier le mot de passe par défaut lors de la première connexion, l'utilisateur doit obligatoirement modifier le mot de passe via le Manager E lors de l'étape d'installation.

Remarque : Un mot de passe composé de 5 caractères (*****) ne sera pas accepté par le système pour des raisons de sécurité.

Tableau 1 : Profil Classes de Service

Profil	Classe de discrimination
Base Connaissances de base pour la configuration du système	Informations sur le système sur la page d'accueil Assistant de **Programmation des touches** Assistant de **Répertoire téléphonique / Numérotation rapide** Assistant d' **Enregistrement des détails des appels** Assistant de **Musique d'attente / Annonces** Assistant de **Nom et libération du poste** Accès aux **Administrateurs** (uniquement pour modifier leurs propres mots de passe) Accès à la **Gestion des licences** > **Informations sur les licences** Accès au **Centre des services** > **Documents** Accès au **Centre des services** > **Logiciel**

Profil	Classe de discrimination
Amélioré Bonne connaissance de la configuration du système	Comme pour le profil de **Base**, plus : Accès à tous les assistants (à l'exception des assistants **Basic Installation**, **UC Suite** et **UC Smart**) **Remarque :** L'accès à tous les assistants n'est pas pris en charge dans les systèmes OpenScape Business S. Accès aux **Administrateurs** (uniquement pour modifier leurs propres mots de passe) Accès à la **sauvegarde et à la restauration** Accès à la **gestion des licences** (à l'exception de l'enregistrement, de l'activation des licences et des paramètres) Accès au **Centre de services** > **Inventaire** Accès au **Centre de services** > **Redémarrage / Rechargement** (sans rechargement) Accès au **Centre de services** > **Diagnostic** > **Statut** Accès au **Centre de services** > **Diagnostic** > **Visualisateur d'événements**
Avancé Utilisateurs formés	Comme pour le profil **amélioré**, plus : Accès à tous les assistants Accès aux **Administrateurs** (uniquement pour modifier leurs propres mots de passe) Accès au **gestion de licence** complète Accès au **Centre de services** complète Accès au **Réseau**
Expert Techniciens de service formés	Comme pour le profil **Avancé**, plus : Accès aux **Administrateurs** (complet) Accès au **mode Expert**

Tableau 2 : Gestion du Profil

Profil	Maintenance
Base Connaissances de base pour la configuration du système	Peut modifier son propre mot de passe. Ne voit pas d'autres administrateurs configurés à part lui-même.

Profil	Maintenance
Amélioré Bonne connaissance de la configuration du système	Peut modifier son propre mot de passe. Ne voit pas d'autres administrateurs configurés à part lui-même.
Avancé Utilisateurs formés	Peut modifier son propre mot de passe. Ne voit pas d'autres administrateurs configurés à part lui-même.
Expert Techniciens de service formés	Peut modifier son propre mot de passe ainsi que les noms d'utilisateur et les mots de passe des autres administrateurs. Il voit tous les administrateurs configurés. Peut ajouter, modifier et supprimer des administrateurs.

Remarque : Tant qu'il n'existe pas d'administrateur ayant le profil **Expert**, les administrateurs ayant le profil **Avancé** peuvent ajouter, modifier et supprimer d'autres administrateurs. Dès qu'un administrateur ayant le profil **Expert** existe, seuls les administrateurs ayant le profil **Expert** peuvent ajouter, modifier et supprimer d'autres administrateurs.

Gestion des administrateurs dans le réseau Internet

La gestion directe des administrateurs n'est possible que dans le WBM du nœud maître. Le menu **Administrateur** n'est pas affiché sur les nœuds esclaves. Toutes les configurations des administrateurs sont transmises aux nœuds esclaves. Il est toutefois possible d'appeler le WBM du nœud maître à partir du WBM du nœud esclave via la vue du nœud. Le menu **Administrateur** est affiché ici, et seuls les administrateurs peuvent être affichés.

Remarque : L'ajout/la modification/la suppression des utilisateurs n'est pas possible via l'accès au WBM en mode esclave (mais uniquement via l'accès au WBM en mode maître).

Administration du mot de passe Manager E

Un administrateur peut modifier (mais pas créer un nouveau rôle d'utilisateur) le mot de passe des utilisateurs existants qui peuvent accéder au système embarqué par l'intermédiaire du Manager E.

L'utilisateur sera invité à modifier les mots de passe uniquement pour les utilisateurs existants et ne pourra pas modifier le groupe de l'utilisateur et les options telles que Créé, Dernière utilisation ne sont pas visibles. Il s'agit d'une fonction de sécurité qui ne permet donc pas d'accéder à l'ensemble de l'écran d'administration du Manager E.

4.1.4.1 Comment ajouter un administrateur

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**. (Tant qu'il n'existe pas d'administrateur au profil **Expert**.)

Vous êtes inscrit dans la WBM avec le profil **Expert**. (S'il existe déjà un administrateur au profil **Expert**.)

Étape par étape

1) Cliquez dans la barre de navigation sur **Administrateurs**.
2) Cliquez sur **Ajouter...**.
3) Entrez les données suivants : **Nom d'utilisateur**, **Prénom**, **Nom de famille**, **Mot de passe**, **Répéter le mot de passe**.
4) Dans la liste déroulante **Fonction de l'utilisateur**, sélectionnez le profil utilisateur souhaité.
5) Cliquez sur **OK&Suivant**.

4.1.4.2 Comment modifier un administrateur

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Administrateurs**.
2) Dans la **Liste d'Administrateurs**, sélectionnez la case de l'administrateur souhaité.
3) Cliquez sur **Modifier**.
4) Adaptez les données (nom de connexion, prénom et nom de famille, mot de passe et fonction de l'utilisateur).
5) Cliquez sur **OK&Suite**.

4.1.4.3 Comment modifier le propre mot de passe d'administrateur

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Administrateurs**.
2) Dans le champ **Mot de passe** puis dans le champ **Répéter le mot de passe**, indiquez le nouveau mot de passe.

   Remarque : Pour des raisons de sécurité, un mot de passe composé de 5 étoiles (*****) n'est pas accepté par le système.

3) Cliquez sur **OK&Suite**.

Concepts associés

Sauvegarde immédiate à la page 1186

4.1.4.4 Comment effacer un administrateur

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Administrateurs**.
2) Dans la **Liste d'Administrateurs**, sélectionnez la case correspondante.
3) Cliquez sur **Effacer...**.

4.1.4.5 Comment modifier un mot de passe d'administrateur Manager E

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Administrateurs**.
2) Cliquer sur **Liste d'administrateurs** Manager E.
3) Modifiez les données (comptes d'utilisateur, nouveau mot de passe, confirmer le mot de passe) selon les besoins.
4) Cliquez sur **Sauvegarder**.

Remarque : Le mot de passe doit comporter au moins 5 chiffres. Il est interdit d'utiliser des lettres ou d'autres caractères. De plus, les anciens mots de passe ne peuvent pas être réutilisés.

4.1.5 Assistants

Les assistants permettent l'installation et la configuration simples du système. L'administrateur clients (profil **Basic**) dispose d'une partie sélectionnée de l'assistant ; un administrateur disposant de connaissances techniques et un technicien SAV formé (profil **Advanced**) bénéficient de tous les assistants.

Les assistants disponibles dépendent de la configuration sytème (UC Smart ou UC Suite) Les assistants peuvent se composer de plusieurs pages qui se succèdent. OK & Suivant enregistre les modifications effectuées et passe à la page suivante de l'assistant. Les modifications enregistrées avec OK & Suivant ne peuvent pas être supprimées. Si aucune modification n'a été enregistrée, **Annulation** permet de quitter l'assistant. Cliquer sur **X** en haut à droite de la fenêtre de l'assistant ferme celui-ci et conserve les modifications enregistrées précédemment avec OK & Suivant.

4.1.5.1 Assistants – Installation de base

Les assistants **Installation de base** facilitent l'installation de base.

Les assistants suivants sont disponibles sous **Installation de base** :

- **Première installation**

  Utilisation unique lors de la première configuration Initialisation du pays, adresse IP système et serveur DHCP.
- **Installation de base**

  Paramétrage de base du système avec données abonné, lignes réseau, paramètres de réseau, Internet.
- **Procédure de licence**

  Activer les licences en ligne à l'aide du serveur de licences.
- **Configuration du réseau**

  Paramétrage du système en tant que partie d'un réseau.
- **Gestion de l'alimentation**

  Configuration et activation de la gestion d'alimentation.

4.1.5.2 Assistants – Réseau / Internet

Les assistants **Réseau / Internet** facilitent la configuration du réseau et de l'accès Internet.

Les assistants suivants sont disponible sous **Réseau / Internet** :

- **Configuration du réseau**

  Paramétrage de DHCP, routage IP et serveur DNS.
- **Configuration Internet**

  Paramètres d'accès des données du fournisseur d'accès Internet, par ex. compte et mot de passe d'utilisateur.
- **Configuration VPN**

  Liaison des postes de travail via Internet.

4.1.5.3 Assistants - Téléphones / Abonnés

Les assistants sous **Téléphones / Abonnés** permettent de configurer simplement les téléphones et les abonnés.

Les assistants suivants sont disponibles sous **Téléphones / Abonnés** :

- **Périphériques IP**

  Configurer les téléphones IP et SIP spécifiques au système, les numéros d'appel FAX ainsi que les adaptateurs IP/analogiques.
- **Périphériques UP0**

  Configurer les téléphones UP0, les numéros d'appel FAX.
- **Téléphones DECT**

  Configurer les téléphones DECT, les numéros d'appel FAX.

- **Mitel SIP DECT**

  Configuration des périphériques RFP Mitel SIP DECT.
- **Périphériques ISDN**

  Ports ISDN non alimentés pour cartes ISDN / modems et stations S0.
- **Terminaux analogiques**

  Ports analogiques DTMF et CLIP pour fax et téléphone.
- **Programmation des touches**

  Programmation des touches de nom et de fonction pour les périphériques IP spécifiques au système et les téléphones UP0.

4.1.5.4 Assistants – Téléphonie centrale

Les assistants dans **Téléphonie centrale** facilitent la configuration des fonctionnalités de la téléphonie centrale.

Les assistants suivants sont disponibles dans **Téléphonie centrale** :

- **Ligne réseau RNIS / Analogique / ITSP**

  Raccordement multiple (MSN) et numéro d'installation pour raccordements RNIS, ainsi qu'affectation des lignes réseau et ITSP analogiques.
- **Téléphonie Internet**

  Paramètres d'accès du fournisseur de service de téléphonie Internet (ITSP), par ex. compte d'utilisateur, mot de passe, numéro d'abonné SIP.
- **Annuaire téléphonique / Numérotation rapide**

  Paramétrage de numéros abrégés centralisés pour l'annuaire téléphonique interne au système.
- **Enregistrement des données de taxation**

  Configuration des paramètres de connexion pour l'enregistrement des données de taxation pour les applications de taxation.
- **Musique d'attente/Annonces**

  Enregistrement de nouvelles mélodies et annonces pour la Musique d'attente et l'Annonce avant réponse.
- **Téléphone d'entrée (Portier)**

  Paramétrage de l'affectation de numéros et des autorisations d'accès pour le poste de portier sur le raccordement d'abonné analogique.
- **SmartVM**

  Configuration de la boîte vocale UC Smart (SmartVM).
- **Liste noire pour les appels entrants**

  Définissez une liste de numéros pour bloquer les appelants indésirables de façon permanente.
- **Intégration d'Active Directory Service**

  Configurer Active Directory.

4.1.5.5 Assistants – Téléphonie utilisateurs

Les assistants **Téléphonie utilisateurs** facilitent la configuration des fonctionnalités pour la Téléphonie utilisateurs.

Les assistants suivants sont disponibles dans **Téléphonie utilisateurs** :

- **Classe de discrimination**

  Configurer classes de discrimination avec les numéros externes qui peuvent être affectés aux abonnés, par ex. numéros d´urgence, numéros autorisés, numéros interdits, ainsi que l'affectation de la discrimination pour renvoi de nuit.
- **Nom et version d'abonné**

  Modification du nom d'abonne et de groupe et réinitialisation du code de verrouillage pour abonnés individuels.
- **Appel de groupe/Groupe d'appel collectif**

  Paramétrage d'appels entrants pour groupes d'abonnés (appels parallèles, linéaires ou cycliques).
- **Renvoi temporisé**

  Paramétrage d'affectations d'abonnés centralisée, sur l'ensemble du réseau, ainsi que renvoi temporisé et en cas d'occupation.
- **Interception d'appel**

  Affectation d'abonnés à un groupe avec possibilité de prise d''appel mutuelle.
- **Configuration Team**

  Paramétrage d'abonnés qui sont appelés parallèlement à l'abonné principal lors d'un appel entrant et qui peuvent utiliser son numéro pour une communication sortante.
- **Intégration de téléphones mobiles**

  Paramétrage d'une liaison entre un téléphone mobile et un abonné interne avec pour objectif d'assurer la disponibilité, dans le sens entrant et sortant, sous un seul numéro (One Number Service).
- **Chef / Secrétaire**

  Paramétrage d'une liaison entre un ou plusieurs téléphones Chef et un ou plusieurs téléphones Secrétaire avec pour objectif de simplifier les transferts de communication et les déviations d'appel.
- **UCD**

  Paramétrage d'une distribution d'appels automatique et intelligente dans un groupe avec des abonnés sélectionnés.
- **Poste opérateur**

  Paramétrage d'abonnés jouant le rôle de poste opérateur et paramétrage du comportement dans les cas Occupé, Erreur de numérotation et Sans réponse.
- **Profils d'abonnés**

  Affecter les postes à un profil et importer/exporter les données de profil.

4.1.5.6 Assistants – Sécurité

Les assistants sous **Sécurité** supporte la configuration simple du pare-feu.

Les assistants suivants sont disponibles sous **Sécurité** :

- **Pare-feu**

  Configurer l'ouverture du port afin de limiter le trafic Internet.

4.1.5.7 Assistants – UC Smart (uniquement avec UC Smart)

Les assistants sous **UC Smart** bénéficient de la configuration de la solution de communications unifiées UC Smart.

Les assistants suivants sont disponibles sous **UC Smart** :

- **UC Smart**

  Paramétrage de base et configuration des utilisateurs pour UC Smart.

4.1.5.8 Assistants – UC Suite (uniquement avec UC Suite)

Les assistants sous **UC Suite** aident à configurer la solution de communications unifiées UC Suite.

Les assistants suivants sont disponibles sous **UC Suite** :

- **Répertoire utilisateur**

  Configuration des utilisateurs.
- **Départements**

  Paramètres des départements.
- **Groupes**

  Configuration des groupes Boîte vocale et Fax.
- **Modèles**

  Configuration des modèles de SMS.
- **Annuaire externe**

  Ajout manuel de différents contacts à l’annuaire externe.
- **Config Fournisseurs externes**

  Entrée des données d'accès du serveur Exchange ou LDAP.
- **Centre de contacts**

  Configuration de base du centre d'appels.
- **Calendriers**

  Configuration des calendriers.
- **Chargement du fichier**

  Chargement des fichiers audio pour les annonces et la musique d'attente.
- **Conférences**

  Configuration des circuits de conférence.
- **Profils**

  Création de profils utilisateur.

- **Lignes d'en-tête de fax**

  Configuration des lignes d'en-tête de fax.

4.1.5.9 Assistants – Unified Directory

Les assistants sous **Unified Directory** prennent en charge l'importation et la modification des contacts de l'annuaire.

Les assistants suivants sont disponibles sous **Unified Directory** :

- **Importer des Contacts**

  L' assistant vous guidera à travers l' importation de données de contact dans l' Annuaire Global à partir de CSV.
- **Modifier les Contacts**

  Ajouter ou modifier manuellement des entrées de l'Annuaire Global.

4.1.5.10 Assistants - Services cloud

Les assistants de la rubrique **Services Cloud** prennent en charge les fonctionnalités supportées dans le cloud.

Les assistants suivants sont disponibles sous **Services Cloud** :

- **Module d'extension client Microsoft Teams**

  Configurez et téléchargez le plugin client myPortal pour Teams.
- **Connectivité téléphonique unifiée**

  Configuration des paramètres de base pour Unify Phone.
- **Instance utilisateur Unify Phone**

  Configurer l'instance des utilisateurs Unify Phone
- **Service Let's Encrypt**

  Configurer le service Let's Encrypt
- **Service CloudLink**

  Configurer le service CloudLink
- **Numéros pilotes de CloudLink**

  Configurer les numéros pilotes pour CloudLink
- **Connectivité Mitel WX**

  Configuration des paramètres de base pour Mitel WX
- **Instance utilisateur Mitel WX**

  Configurer l'instance des utilisateurs Mitel WX

4.1.6 Centre de service

Le **Centre de service** de WMB propose différentes fonctions de maintenance, démarre la mise à jour du logiciel et propose documentation et logiciel.

4.1.6.1 Centre de service – Documents

L'option **Documents** fournit des documentations, des modèles CSV et des liens avec des informations plus complètes. Les documentations peuvent être consultées au format PDF, dans toutes les langues supportées.

Suivant la configuration système, les contenus suivants sont disponibles.

Sommaire	UC Smart	UC Suite
Documentations de l'administrateur (PDF)	-	x
Documentations de l'utilisateur (PDF)	-	x
Liens (Wiki)	x	x
Modèles (format CSV) pour l'importation de donnés pour les • Abonnés • Numérotation abrégée centralisée • Annuaire externe	x	x
CLUF	x	x

Concepts associés

Outils de taxation à la page 1166

4.1.6.2 Centre de service – Logiciel

Logiciel fournit le logiciel pour les UC clients, les pilotes USB et les Outils.

Les contenus suivants sont disponibles :

Sommaire	UC Smart	UC Suite
Fichiers d'installation pour le logiciel de UC Clients	x	x
Pilote USB	x	x
Outils	x	x
Liens pour l'accès direct aux fichiers d'installation	-	x

4.1.6.3 Centre de service - Inventory > Système

Système fournit un aperçu des données de configuration de base du système.

4.1.6.4 Centre de service - Inventory > Numéros d'appel

Numéros d'appel affiche une liste de tous les numéros d'appel attribués.

4.1.6.5 Centre de service - Inventory > Vue d’ensemble du réseau

Vue d’ensemble du réseau affiche une liste contenant des informations sur les systèmes actuellement présents sur le réseau.

4.1.6.6 Centre de service – Mise à jour du logiciel

Software Update vérifie si une mise à jour logicielle est disponible sur le serveur Web et effectue l'actualisation.

4.1.6.7 Centre de service – Renvoi E-Mail

Renvoi E-Mail permet l'envoi d'e-mails avec messages système de la suite UC à l'administrateur, et l'envoi d'e-mail avec messages Voix ou Fax joint aux abonnés.

4.1.6.8 Centre de service – Accès distant

Accès Remote permet la configuration de l'accès pour l'administration du système, de manière indépendante à l'emplacement.

4.1.6.9 Centre de service – Redémarrer/Recharger

Restart/Reload permet le redémarrage du système, au choix avec retour aux paramètres usine.

4.1.6.10 Centre de service – Diagnostic > Etat

Etat fournit des informations d'état à propos du réseau, des abonnés, de l'établissement de la liaison, des ITSP et VPN.

Voir aussi Gestion Inventory .

4.1.6.11 Centre de service – Diagnostic > Observateur d’événements (Event Viewer)

L'**observateur d’événements** consigne les événements système.

Voir aussi Traces .

4.1.6.12 Centre de service – Diagnostic > Trace

Trace offre des possibilités de consignation des erreurs.

Voir aussi Traces .

4.1.6.13 Centre de service – Diagnostic > Journal Service

Le journal de service consigne plusieurs données système sous forme d'événement HiPath 3000.

Il est nécessaire d'être en mode d'affichage WBM pour actualiser ou télécharger le fichier.

4.1.7 Mode Expert

Le mode **Expert** fournit aux techniciens de maintenance formés (profil Expert) des menus avec des fonctions pour la configuration et la maintenance du système.

Vous trouverez des informations détaillées au chapitre Mode Expert.

4.1.8 Aide en ligne

L'Aide en ligne intégrée décrit les concepts importants et les instructions pour le comportement pratique. A chaque page WBM ouverte, il est associé de manière contextuelle la rubrique d'aide correspondante.

Navigation

Les boutons de l'Aide en ligne offrent les fonctions suivantes :

- **Contenu**

  fournit un aperçu sur la structure
- **Index**

  permet un accès direct à un sujet à l'aide de mots clés
- **Rechercher**

  vous permet de rechercher un texte complet pour accéder de façon ciblée aux rubriques correspondantes

4.1.8.1 Comment appeler l'aide en ligne contextuelle

Conditions préalables

Vous êtes connecté à WBM.

Procédure

- Cliquez dans la fenêtre WBM ouverte, soit sur le point d'interrogation à droite, soit sur le bouton Aide à gauche.

4.2 Gestionnaire E

Manager E est un outil de service avec une aide intégrée qui fonctionne sous Windows et peut être utilisé pour des tâches qui ne peuvent pas être effectuées via le WBM.

Manager E peut être utilisé pour OpenScape Business X1, OpenScape Business X5 et OpenScape Business X8. OpenScape Business S ne peut pas être administré à l'aide de Manager E.

Il est conseillé d'effectuer les modifications de configuration via Manager E uniquement lorsque vous ne pouvez pas les réaliser via WBM, par exemple, l'atténuation, l'impulsion de sonnerie, la fréquence de tonalité, etc. Les modifications effectuées via Manager E doivent être envoyées en mode delta.

Manager E est destiné au personnel de service formé et comprend les blocs fonctionnels suivants :

- Génération (y compris la génération hors ligne)
- Copie et sauvegarde des données client
- Les ordres de service, tels que le redémarrage des tableaux électriques
- Réinitialisation des fonctionnalités activées
- Création et impression de :
  - Étiquettes clés pour optiPoint 500
  - Impressions de données client
  - Agencement du cadre de distribution principal
- Gestion distincte des utilisateurs et des mots de passe pour le service après-vente.
- Routine de conversion de base de données pour la base de données clients (CDB).

L'accès au système via le Gestionnaire nécessite un nom d'utilisateur et un mot de passe. Le mode en ligne permet d'effectuer des modifications rapidement. Les fonctionnalités du mode en ligne correspondent à l'interface utilisateur de l'Assistant T.

Les fonctionnalités suivantes ne peuvent plus être administrées à l'aide de Manager E :

- Licence
- Réseau
  - Partenaire SNMP
  - Pair PSTN
  - Routage
  - Cartographie
  - Portier
  - Ext. H.323
  - Ports IP
- Entretien
  - Historique des erreurs
  - Journal des événements
  - Paramètres de traçage
  - Tableau des réactions d'erreur
  - État V.24
  - DMA
- Traces

Utilisation de la base de données clients (CDB)

Les étapes de base sont les suivantes :

- Charger la CDB du système dans Manager E
- Apportez les modifications nécessaires dans E Manager
- Utilisez le Gestionnaire E pour réenregistrer la CDB sur le système.

4.2.1 Comment charger KDS dans Manager E

Réaliser les opérations suivants afin de pouvoir ensuite effectuer des tâches de configuration dans Manager E.

Étape par étape

1) Sur le PC Admin, démarrer Manager E.
2) Entrez le **Nom utilisateur** pour Manager E.
3) Entrez le **Mot de passe** pour Manager E.
4) Cliquez sur **Fichier** > **Transférer**.
5) Cliquez sur l'onglet **Communications**.
6) Dans la zone **Accès**, activez l'option correspondante, en fonction du type de connexion du PC Admin au système.
7) Activez le champ d'option **Lecture/Ecriture KDS**.
8) Cliquez sur **Installation -> PC**.
9) Cliquez sur **OK**. Le KDS est transmis du système vers Manager E.
10) Une fois la transmission effectuée, cliquez sur **OK**.
11) Cliquez sur **Fermer**.

4.2.2 Comment sauvegarder le KDS dans le système

Réaliser les opérations suivantes afin d'enregistrer dans le système la configuration réalisée dans Manager E.

Étape par étape

1) Cliquez sur **Fichier** > **Transférer**.
2) Cliquez sur l'onglet **Communications**.
3) Dans la zone **Accès**, activez l'option correspondante, en fonction du type de connexion du PC Admin au système.
4) Activez le champ d'option **Lecture/Ecriture KDS**.
5) Cliquez sur **PC -> Système**.
6) Cliquez sur **OK**. Le KDS est transmis au système par Manager E.
7) Une fois la transmission effectuée, cliquez sur **OK**.
8) Cliquez sur **Fermer**.

5 Configuration initiale d'OpenScape Business X

Ce chapitre décrit la configuration initiale d'OpenScape Business X1/X5/X8. Le système de communication et ses composants sont intégrés à une infrastructure existante composée d'un réseau local client et d'un réseau téléphonique TDM. L'accès à Internet et la connexion réseau sont établis, et les postes connectés sont configurés.

La configuration initiale d'OpenScape Business X1/X5/X8 (c'est-à-dire le système de communication) est réalisée à l'aide du programme d'administration OpenScape Business Assistant (gestion basée sur le Web, également appelée WBM).

La configuration initiale standard des composants couramment utilisés est décrite ici. Les étapes d'installation spécifiques dépendent du système de communication et des composants impliqués. Lors de la configuration initiale, vous devrez peut-être choisir entre plusieurs options à certains endroits, voire ignorer complètement certaines configurations. Il est également possible que les étapes d'installation décrites ici n'apparaissent pas dans votre système de communication.

Les configurations détaillées des fonctionnalités non couvertes par la configuration initiale standard sont décrites dans les chapitres suivants.

La configuration initiale nécessite la création d'un schéma d'adressage IP et d'un plan de numérotation.

Les étapes d'installation les plus importantes sont les suivantes :

- Adresses IP et paramètres DHCP
- Paramètres du pays et de l'heure
- Numéros de téléphone et réseau du système
- Configuration ISDN
- accès Internet
- téléphonie par Internet
- Configuration de la station
- Licence
- Renforcement du système
- Sauvegarde des données

Avant de mettre en œuvre ces changements, tenez compte des points suivants :

Veillez à ce que les réseaux suivants ne se chevauchent pas avec d'autres réseaux du système. Spécifiquement:

- réseau DSP
- Réseau LAN1 (WAN)
- Réseau LAN2
- Réseau LAN3 (Administration)

De plus, assurez-vous qu'il n'y a pas de conflit avec l'adresse IP de la passerelle par défaut.

5.1 Prérequis pour l'installation initiale

Le respect des conditions préalables à l'installation initiale garantit le bon fonctionnement du système de communication.

Général

En fonction du matériel existant (cartes, téléphones, ...) et de l'infrastructure, les conditions générales suivantes s'appliquent :

- L'infrastructure (réseau local, réseau téléphonique TDM) est disponible et utilisable.
- Le matériel est installé et connecté correctement.
- Un port LAN est nécessaire pour intégrer la carte mère au réseau local du client.
- Le système de communication n'a pas encore été connecté au réseau local.
- L'accès à Internet est disponible via un fournisseur d'accès Internet.
- Une interface de débit primaire RNIS S_0 ou RNIS est nécessaire pour utiliser les lignes extérieures RNIS.
- Une connexion de tronc CAS est nécessaire pour utiliser une ligne extérieure CAS.
- Une connexion de réseau analogique est nécessaire pour utiliser une ligne extérieure analogique.
- Un schéma d'adresse IP existe et est connu (voir Schéma d'adresse IP).
- Un plan de numérotation (également appelé plan de numérotation) est présent et connu (voir Plan de numérotation).

PC d'administration

Les conditions préalables suivantes doivent être remplies pour le PC d'administration (PC Admin) utilisé pour la configuration initiale du système et pour l'administration ultérieure du système de communication :

- Interface réseau :

  Le PC d'administration nécessite un port LAN disponible.
- Système opérateur:

  La configuration du système de communication avec le Manager E n'est possible que sur un système d'exploitation Windows (Windows XP et versions ultérieures).

  La configuration WBM, cependant, est basée sur le navigateur et donc indépendante de la plateforme.
- Navigateur Web :

  Les navigateurs Web suivants sont pris en charge :

  – Microsoft Internet Explorer version 10 et ultérieures.
  – Microsoft Edge
  – Mozilla Firefox version 17 et ultérieures.
  – Google Chrome

  Si une ancienne version du navigateur Web est installée, vous devrez installer une version à jour avant de pouvoir commencer la configuration du système.

- Java:

  Oracle Java 8 ou supérieur, ou bien OpenJDK 8, doit être installé. Si une version antérieure est installée, vous devrez la mettre à jour vers la dernière version avant de pouvoir commencer la configuration du système.

5.2 Composantes

Les composantes de l'exemple d'installation sont décrites et illustrées ci-après.

L'exemple d'installation engloge les composantes suivantes.

- OpenScape Business X

  Le système de communication est intégré dans le LAN client existant via l'interface LAN
- PC Admin

  Le PC Admin est également intégré au système de communication via une interface LAN.
- Abonnés IP (IP-Clients)

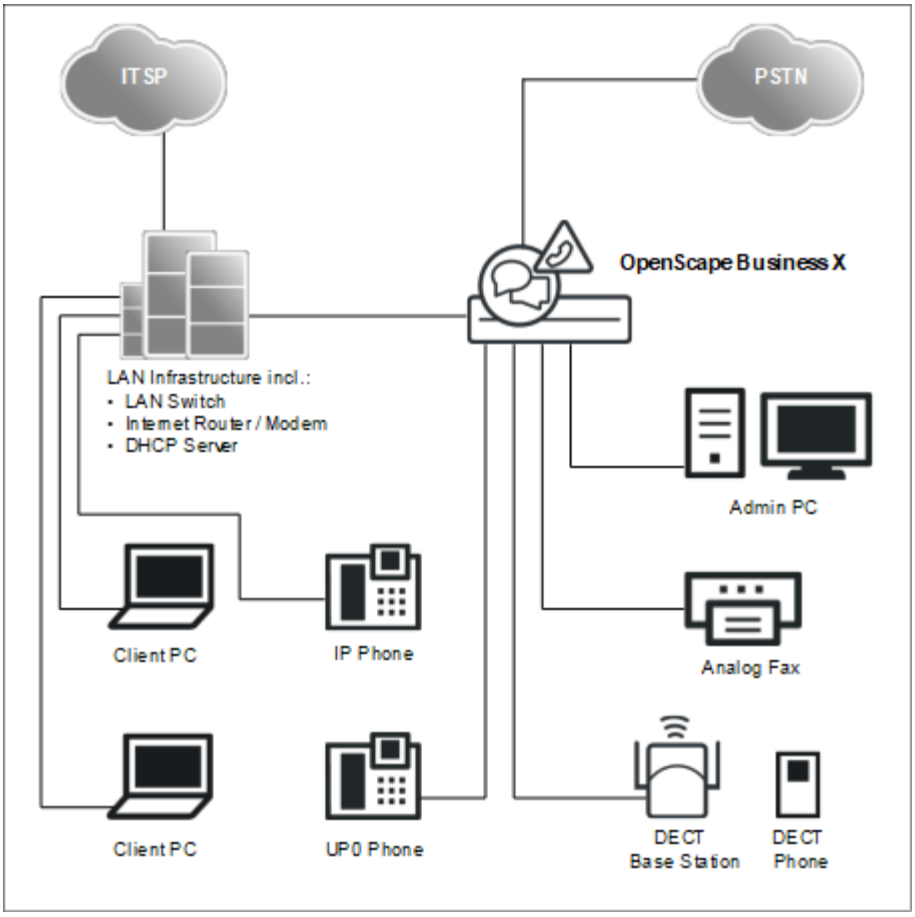
  Les abonnés IP (téléphones système IP, PC client, points d'accès WLAN, ...) sont intégrés au LAN via un ou plusieurs commutateurs.
- Abonné UP0

  Les abonnés UP0 (par ex. téléphones système TDM OpenStage 60T) sont raccordés directement au système de communication.
- Abonnés analogiques

  Les abonnés analogiques (par ex. fax analogique) sont raccordés directement au système de communication.
- Poste DECT

  Les abonnés DECT sont inscrits dans le système de communication via une station de base.

Les clients IP reçoivent leurs adresses IP de manière dynamique d'un serveur DHCP interne ou externe (par ex. routeur Internet).



5.3 Plan de numérotation

Un plan de numérotation est une liste de tous les numéros de téléphone disponibles dans le système de communication. Il comprend notamment les numéros d'appel internes, les numéros DID et les numéros d'appel de groupe.

Plan de numérotation par défaut

Les numéros d'appel internes sont des valeurs par défaut prédéfinies. Ces valeurs peuvent être adaptées aux besoins individuels (par exemple, pour créer des plans de numérotation personnalisés).

Extrait du plan de numérotation par défaut :

Type de numéros d'appel	**X1**	X5/X8
Numéros de station internes	11-30	100-742
Numéros d'appel direct entrants de l'utilisateur	11-30	100-742
numéro de station principale	700-703	à partir de 7801

Type de numéros d'appel	**X1**	X5/X8
Codes de saisie (codes externes) : Trk. Grp 1 (liaison principale : ISDN, analogique) Route 8 (Suite UC) Trk. Groupe 12-15 (tronc : ITSP) Route 16 (Réseautage)	0 = Monde / 9 = États-Unis - non préréglé non préréglé	0 = Monde / 9 = États-Unis 851 855-858 859
Numéro d'appel pour l'accès à distance	non préréglé	non préréglé
Numéro d'appel pour la messagerie vocale UC Smart Suite UC	351 -	351 non préréglé

Plan de numérotation individuel

Un plan de numérotation individuel peut être importé via un fichier XML lors de la configuration de base.

Le fichier XML contient plusieurs onglets. Outre les noms et numéros de téléphone des abonnés, l'onglet « Client » comprend également des données supplémentaires sur les abonnés, telles que leurs types et leurs adresses électroniques.

Vous trouverez un modèle XML avec les explications correspondantes dans WBM, sous **Centre de service** > **Documents** > **Modèles CSV**. Vous pouvez également utiliser le fichier XML qui y est stocké comme modèle pour vos données. Il peut être modifié avec Microsoft Excel, par exemple.

5.4 Schéma des adresses IP

Un schéma des adresses IP détermine comment les adresses IM sont attribuées dans le LAN client. Il comprend les adresses IP des PC, des serveurs, des routeurs Internet, des téléphones IP, du système de communication, etc.

Pour un meilleur aperçu lors de l'affectation des adresses IP, il est préférable de créer un schéma des adresses IP.

Exemple de schéma d'adresses IP avec la plage d'adresses IP `192.168.1."-x` :

Plage d'adresses IP	**Clients**
de **192.168.1.1** à **192.168.1.19**	Client avec adresse IP fixe :
192.168.1.1	Routeur Internet (passerelle)
192.168.1.2	Système de communication
192.168.1.3	Carte d'application (option)
192.168.1.10	Serveur e-mail

Plage d'adresses IP	Clients
de **192.168.1.50** à **192.168.1.254**	PC client & téléphones IP, en même temps carnet d'adresses IP du serveur DHCP, l'affectation des adresses IP aux clients est dynamique

Les plages d'adresses IP sont réservées en interne et ne doivent pas être occupées :

plages d'adresses IP exclues	Description
10.0.0.1; 10.0.0.2	réservé pour le serveur de licences
10.186.237.65 ; 10.186.237.66	réservé au RNIS distant (obsolète)
192.168.3.2	Adresse IP interne du système de communication
192.168.2.1	Adresse IP de l'interface LAN3 (Admin-Port)

Cette liste se trouve également dans la WBM sous **Centre de service** > **Diagnostics** > **État** > **Aperçu adresses IP**.

Extension du masque réseau grâce à l'utilisation du segment de réseau prédéfini.

L'adresse IP interne du système de communication et l'adresse IP de l'interface LAN3 (Admin-Port) ne doivent pas se trouver sur le même segment de réseau que l'adresse IP du système de communication.

Configuration prédéfinie de segment de réseau :

- 192.168.1.2 : Adresse IP du système de communication
- 255.255.255.0 : Masque de réseau
- 192.168.3.2 : Adresse IP interne du système de communication
- 192.168.2.1 : Adresse IP de l'interface LAN3 (Admin-Port)

Si le masque réseau bénéficie d'une extension de 255.255.255.0 à 255.255.0.0 par ex. grâce à l'utilisation du segment de réseau prédéfini, il faut modifier les adresses IP indiquées ci-dessus.

Exemple de configuration modifiée :

- 192.168.1.2 : Adresse IP du système de communication
- 255.255.**0**.0 : Masque de réseau
- 192.**169**.3.2 : Adresse IP interne du système de communication

  La modification se fait en sélectionnant **Mode Expert** > **Téléphonie** > **Charge utile** > **Modules matériels** > **Modifier les paramètres DSP**
- 192.**170**.2.1 : Adresse IP de l'interface LAN3 (Admin-Port)

  La modification se fait en sélectionnant **Mode Expert** > **Téléphonie** > **Interfaces réseau** > **Carte mère** > **LAN 3 (Admin)**

5.5 Démarrage initial

Le démarrage initial comprend le lancement du système de communication, la connexion et la configuration du PC d'administration et le lancement du programme d'administration OpenScape Business Assistant (WBM) pour la première fois.

La mise en service initiale du système de communication doit être effectuée avant son intégration au réseau local interne. Des problèmes peuvent survenir si l'adresse IP préconfigurée du système de communication existe déjà sur le réseau local interne et/ou si un serveur DHCP est déjà utilisé. Dans de tels cas, l'adresse IP du système de communication doit d'abord être reconfigurée et/ou le serveur DHCP du système de communication doit être désactivé. Ce n'est qu'alors que le système de communication pourra être intégré au réseau local interne.

Remarque : Avant la première mise en service, veuillez suivre les instructions relatives à la protection et à la sécurité des données.

DANGER : OpenScape Business X8 ne peut être mis sous tension que si tous les boîtiers du système sont scellés à l'arrière avec les panneaux de connexion et de remplissage fournis.

DANGER : L'OpenScape Business X5 ne doit pas être mis sous tension si le panneau avant du boîtier n'est pas fermé. Utilisez toujours des panneaux factices (C39165-A7027-B115) pour couvrir les emplacements qui ne sont pas équipés de cartes.

Connexion du PC administrateur

Pour configurer le système de communication, le PC administrateur est directement connecté à l'interface « LAN » du système de communication. Le système de communication est ensuite configuré pour obtenir son adresse IP auprès du serveur DHCP interne du système de communication. Après une installation réussie, le PC d'administration peut être intégré au réseau local interne sans aucune autre modification de configuration.

5.5.1 Comment démarrer le système de communication

Conditions préalables

Le montage du matériel a été effectué de manière correcte (voir *OpenScape Business, Guide d'installation*).

La carte mémoire (avec le logiciel système) est insérée.

Le système de communication n'est pas encore intégré dans le LAN client.

Étape par étape

Branchez le système de communication sur le réseau électrique.

Avertissement :

Choc électrique en cas de contact avec les lignes sous tension

Veillez à ce que le système de communication (et avec OpenScape Business X8, chaque boîtier système) soit mis à la terre à l'aide d'un conducteur de protection séparé (voir *OpenScape Business, Guide d'installation*).

Le système de communication monte maintenant en puissance. Les LED du système s'allument avec différentes couleurs et séquences (Détails voir *OpenScape Business, Guide d'installation*). Durant la mise en route, il ne faut pas débranche le système de communication du réseau électrique.

Une fois la montée en puissance effectuée, la LED "Run" de la carte mère clignote en vert à un rythme de 1 Hz (0,5 s allumée / 0,5 s éteinte).

5.5.2 Comment raccorder le PC Admin au système de communication

Conditions préalables

Le système de communication ist opérationnel.

Étape par étape

1) Démarrez l'Admin-PC.

2) Vérifier si une adresse IP dynamique a bien été attribuée au PC. Si ce n'est pas le cas, vous devez reconfigurer l'Admin-PC. Pour cela, vous devez disposer des droit de l'administrateur.

Remarque : Les paramètres IP décrits ici sont valables pour Windows 7. Reportez-vous au manuel du système d'exploitation pour obtenir des informations plus complètes sur le paramétrage sous d'autres systèmes d'exploitation Windows.

a) Sélectionnez **Démarrer** > **Panneau de configuration** et double-cliquez sur **Réseau et Internet** puis sur **Centre réseau et partage**.

b) Dans le réseau actif correspondant, cliquez sur **Connexion LAN** et ensuite sur **Propriétés**.

c) Dans l'onglet **Mise en réseau**, sélectionnez avec le bouton gauche de la souris l'entrée **Protocole Internet Version 4 (TCP/IPv4)** et cliquez sur **Propriétés**.

d) Cliquez sur l'onglet **Généralités** et vérifiez si l'option **Obtenir automatiquement l'adresse IP** est bien paramétré. Si ce n'est pas le cas, activez-le.

e) Fermez toutes les fenêtres ouvertes avec **OK**.

3) A l'aide d'un câble LAN reliez l'interface LAN nouvellement créée du PC Admin avec l'interface "LAN" du système de communication. Via cette interface, il est attribué au PC Admin une adresse IP dynamique.

Remarque : Vous pouvez aussi raccorder le PC Admin à l'interface "Admin" ; pour cela, il faut toutefois attribuer au PC

Admin une adresse IP fixe dans la plage 192.168.2.xxx (par ex. : 192.168.2.40) et le masque de réseau 255.255.255.0. Le système de communication dispose via l'interface LAN "Admin" de l'adresse IP 192.168.2.1 - important pour l'accès WBM !

5.5.3 Comment démarrer WBM

Conditions préalables

Le système de communication ist opérationnel. La LED "Run" de la carte mère clignote en vert à un rythme de 1 Hz (0,5 s allumée / 0,5 s éteinte).

L'Admin-PC et le système de communication peuvent communiquer via un réseau LAN.

Étape par étape

1) Sur le PC Admin, démarrez le navigateur Web et sélectionnez la page d'accueil d'OpenScape Business Assistant (WBM), à l'adresse ci-après :

`https://192.168.1.2`

Remarque : S'il est impossible de démarrer la WBM, contrôlez la liaison LAN et répétez l'appel. S'il est toujours impossible de démarrer, vérifiez si l'adresse IP n'est pas bloquée par votre pare-feu. Vous trouverez des informations plus précises dans la documentation de votre pare-feu.

2) Lorsque le navigateur web signale un problème avec un certificat de sécurité, installez le certificat (à l'exemple d'Internet Explorer V10).

a) Fermez le navigateur web.

b) Ouvrez le navigateur web avec droits d'administrateur : pour cela, cliquez avec le bouton droit de la souris sur l'icône du Navigateur web

et sélectionnez dans le menu contextuel l'entrée **Exécuter en tant qu'administrateur**.

c) Autorisez la gestion des comptes utilisateur.

d) Sélectionnez dans le navigateur Web du Admin-PC la page d'accueil d'OpenScape Business Assistant (WBM), à l'adresse suivante :

`https://192.168.1.2`

e) Cliquez sur **Poursuivre le chargement de ce site Web**.

f) Cliquez sur le message **Erreur de certificat** dans la barre de navigation du navigateur Web.

g) Cliquez sur **Afficher les certificats**.

h) Cliquez sur **Installer le certificat** (visible uniquement avec des droits d'administrateur).

i) Sélectionnez l'option **Ordinateur local** et confirmez avec **Suivant**.

j) Sélectionnez l'option **Enregistrer tous les certificats dans la mémoire suivante**, cliquez sur **Parcourir** et indiquez des **entités de certification d'origine (Root CA) dignes de confiance**.

k) Confirmez avec **OK** et ensuite avec **Suivant** et **Terminer**.

l) Confirmez l'importation de certificat avec **OK** et fermez la fenêtre de certificat avec **OK**.

m) Fermez le navigateur web.

n) Démarrez de nouveau le navigateur Web (sans droits d'administrateur) et sélectionnez la page d'accueil d'OpenScape Business Assistant (WBM), à l'adresse ci-après :

`https://192.168.1.2`

3) Cliquez en haut à droite sur l'abréviation de la langue et sélectionnez dans le menu la langue dans laquelle sera affichée l'interface de WBM. La page d'accueil est affichée dans la langue sélectionnée.

4) Dans le premier champ dans **Connexion** indiquez le nom d'utilisateur par défaut `administrator@system` pour l'accès en tant qu'administrateur.

> **Remarque :** Si, après l'entrée de `Administrateur` vous allez dans le champ **Mot de passe**, la mention `@système` est automatiquement ajoutée.

5) Dans le deuxième champ dans **Connexion** entrez le mot de passe par défaut `administrator` pour accéder en tant qu'administrateur.

6) Cliquez sur **Connexion**.

7) Les étapes suivantes ne sont réalisées qu'une seule fois, lors de la première connexion au WBM.

a) Dans **Mot de passe** entrez une nouvelle fois le mot de passe par défaut `administrator`.

b) Dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**, entrez un nouveau mot de passe afin de protéger le système contre les utilisations malveillantes. Tenir compte des majuscules/minuscules et de l'état des touches `Num` et `CapsLock` (touche de blocage). Le mot de passe est masqué, le système affiche uniquement des étoiles (*).

> **Remarque :** Le mot de passe doit comprendre au moins 8 caractères et un chiffre. Mémorisez votre nouveau mot de passe.

c) Cliquez sur **Connexion**.
d) Sélectionnez la date actuelle et inscrivez l'heure correctement.
e) Cliquez sur **OK&Suivant**. Vous serez automatiquement déconnecté de la WBM.
f) Dans le premier champ dans **Connexion** indiquez le nom d'utilisateur par défaut `administrator@system` pour l'accès en tant qu'administrateur.

> **Remarque :** Si, après l'entrée de `Administrateur` vous allez dans le champ **Mot de passe**, la mention `@système` est automatiquement ajoutée.

g) Dans le deuxième champ dan **Connexion** entrez votre nouveau mot de passe pour accéder en tant qu'administrateur.
h) Cliquez sur **Connexion**. La page de démarrage de la gestion WBM s'affiche.

Étapes suivantes

Lancer la première installation.

5.6 Intégration dans LAN client

L'intégration dans le LAN client est réalisée avec l'assistant **Première installation** du WBM. Dans ce cadre, les paramètres fondamentaux pour l'intégration du système de communication dans le LAN existant sont définis.

5.6.1 Comment démarrer l'assistant Lancer la première installation

Conditions préalables

WBM est démarré.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** pour lancer l'Assistant **Première installation**.

> **Remarque :** Sur les écrans à faible résolution, lorsque l'espace de travail n'est pas entièrement affiché en raison de la taille de la fenêtre du navigateur, il s'affiche des barres de défilement horizontales et verticales de manière à pouvoir dérouler la partie affichée.

Étapes suivantes

Effectuez la première installation comme indiqué ci-après, étape après étape. Les champs qui ne sont pas décrits ici sont paramétrés de manière adaptée à un cas normal ; ils ne doivent être modifiés que s'ils ne correspondent pas à vos données réseau. Les informations complètes figurent dans la description de chacun des Assistants.

5.6.2 Paramètres système

La fenêtre **Paramètres système** permet de configurer les paramètres système du système de communication.

Procédez comme suit :

1) Définissez le logo d'affichage et le nom du produit

   Spécifiez le texte à afficher sur l'écran des téléphones du système. De plus, vous pouvez également sélectionner le nom du produit.
2) Modifier les adresses IP (si nécessaire)

   Par défaut, le système de communication se voit attribuer une adresse IP et un masque de sous-réseau. Vous devrez peut-être ajuster l'adresse IP et/ou le masque de sous-réseau à votre propre plage d'adresses IP.

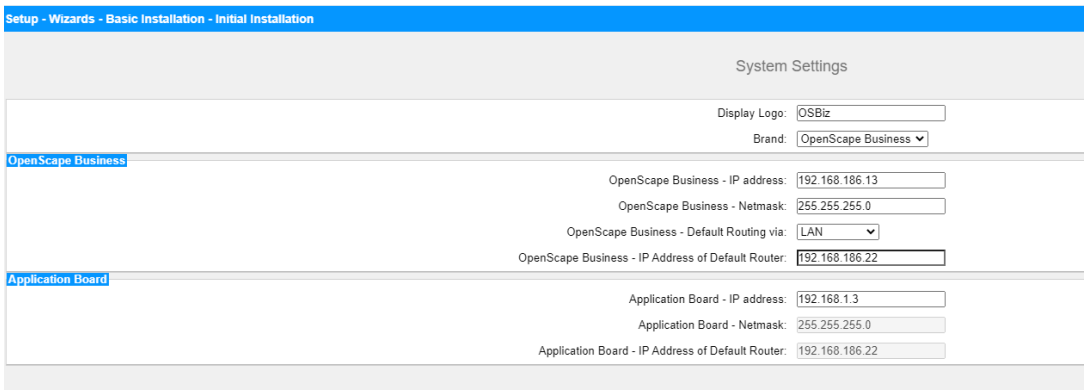
   De plus, vous pouvez spécifier l'adresse IP de votre routeur par défaut, par exemple l'adresse IP du routeur Internet.

Si le masque de sous-réseau doit être étendu, par exemple de **255.255.255.0** à **255.255.0.0** , l'adresse IP interne du système de communication et l'adresse IP du port LAN3 (port d'administration) doivent être modifiées car elles ne peuvent pas se trouver dans le même segment de réseau que l'adresse IP du système de communication (voir également le schéma d'adressage IP).

5.6.2.1 Comment déterminer le logo d'écran et la désignation du produit

Conditions préalables

Vous êtes dans la fenêtre **Paramètres système**.



Étape par étape

1) Dans le champ **Logo d'écran** entrez un texte de votre choix (par ex. OpenScape Biz). Le texte peut avoir jusqu'à 16 caractères. Evitez les inflexions et les caractères spéciaux.
2) Dans la liste déroulante **Produit**, sélectionnez la désignation du produit.

Étapes suivantes

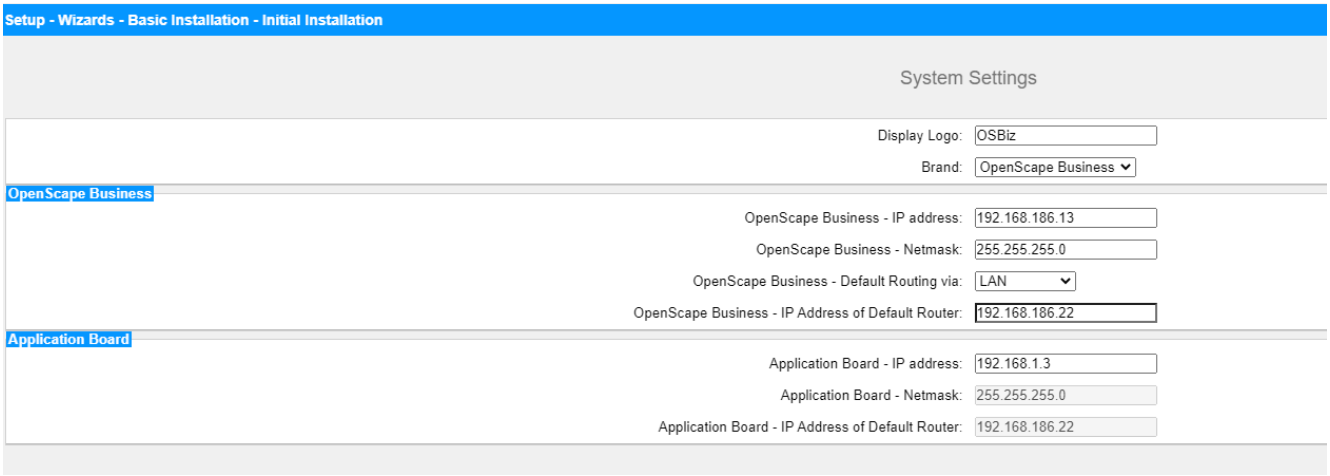
Modifier les adresses IP (si nécessaire) ou configurer DHCP.

5.6.2.2 Comment spécifier les adresses IP (facultatif)

Conditions préalables

Vous connaissez la plage d'adresses IP de votre réseau interne.

Vous vous trouvez dans la fenêtre **Paramètres système** .



Étape par étape

1) Spécifiez l'adresse IP du système de communication :

a) Dans le champ **OpenScape Business - Adresse IP**, saisissez une adresse IP qui figure dans la plage d'adresses IP de votre réseau interne (par ex. réseau interne : `192.168.1.x`, OpenScape Business : `192.168.1.2`).

> **Remarque :** L'adresse IP d'OpenScape Business ne doit pas être attribuée à un autre client du réseau existant, car cela entraînerait un conflit d'adresses IP.

b) Saisissez le masque de sous-réseau de votre réseau interne (par exemple, `255.255.255.0`) dans le champ **OpenScape Business - Masque de sous-réseau** .

2) Spécifiez l'adresse IP du routeur par défaut :

a) Dans le champ **OpenScape Business - Routage par défaut via** , sélectionnez l'entrée **LAN** .

b) Dans le champ **Unify OpenScape Business - Adresse IP du routeur par défaut**, saisissez l'adresse IP de votre routeur par défaut (par ex. réseau interne : `192.168.1.x`, routeur Internet comme routeur par défaut : `192.168.1.1`).

3) Cliquez sur **OK et Suivant** .

Étapes suivantes

Configurer le DHCP.

5.6.2.3 Comment spécifier le nom de l’équipement

Conditions préalables

Vous êtes dans la fenêtre **Paramètres système**.

Le système est en mode DTAG.

Étape par étape

1) Cochez la case **Enregistrement automatique RSP.servicelink** :

   Le champ **Nom de l’équipement** peut être modifié.
2) Spécifiez le **nom de l’équipement**.

   Si vous sélectionnez l'enregistrement automatique RSP.servicelink, le système va essayer automatiquement toutes les 10 minutes de s'enregistrer et de se connecter aux serveurs RSP en utilisant le nom d'équipement fourni.
3) Cliquez sur **OK & Suivant.**

Étapes suivantes

Configurer DHCP.

5.6.3 Paramètres DHCP

Dans la fenêtre **Paramètres généraux DHCP** activez et configurez ou désactivez le serveur DHCP interne du système de communication.

Un serveur DHCP attribue automatiquement aux abonnés IP (téléphones système IP, PC, etc.) une adresse IP et leur fournit des données spécifiques du réseau, par exemple l'adresse IP de la passerelle par défaut (routeur Internet).

On peut utiliser comme serveur DHCP un serveur DHCP externe (par ex. le serveur DHCP du routeur Internet) ou le serveur DHCP interne qui est intégré dans le système de communication.

Pour l'actualisation automatique du logiciel des téléphones système IP, on utilise le DLI intégré dans le système de communication ou un serveur DLS (Deployment Service (DLI et DLS)). Le serveur DHCP doit connaître l'adresse IP de DLI intégré ou du serveur DLS intégré.

Vous disposez des possibilités suivantes :

- Activer et configuer le serveur DHCP

  Si l'on utilise serveur DHCP interne du système de communication, il faut désactiver un serveur DHCP externe (par ex. le serveur DHCP du routeur Internet). Eventuellement, il est nécessaire d'adapter les paramètres du serveur DHCP interne au LAN client. Si l'on utilise le serveur DHCP interne et le DLI interne, les téléphones système sont automatiquement actualisés. Si 'on utilise un serveur DLS externe, il faut inscrire son adresse IP dans le serveur DHCP interne en se servant du mode Expert (Deployment Service (DLS and DLI)).
- Désactiver le serveur DHCP interne

  Si l'on utilise un serveur DHCP externe, le serveur DHCP interne du système de communication doit être désactivé. Afin que les téléphones système IP reçoivent automatiquement le logiciel de téléphonie le plus récent, il faut

entrer dans le serveur DHCP externe les données spécifique réseau comme l'adresse IP du DLI interne ou du serveur DLS externe.

Remarque : Tous les serveurs DHCP externes ne supportent pas la saisie de données spécifiques réseau ! Dans ce cas, les données doivent être fournies manuellement à tous les téléphones système IP.

5.6.3.1 Comment désactiver le serveur DHCP interne

Conditions préalables

Un serveur DHCP externe (par exemple, le serveur DHCP du routeur Internet) est activé dans le réseau interne.

Vous êtes dans la fenêtre **DHCP Global Settings** (Paramètres globaux DHCP).

Étape par étape

1) Laissez la case **Activer le serveur DHCP**.
2) Cliquez sur **OK & Suivant**.

Étapes suivantes

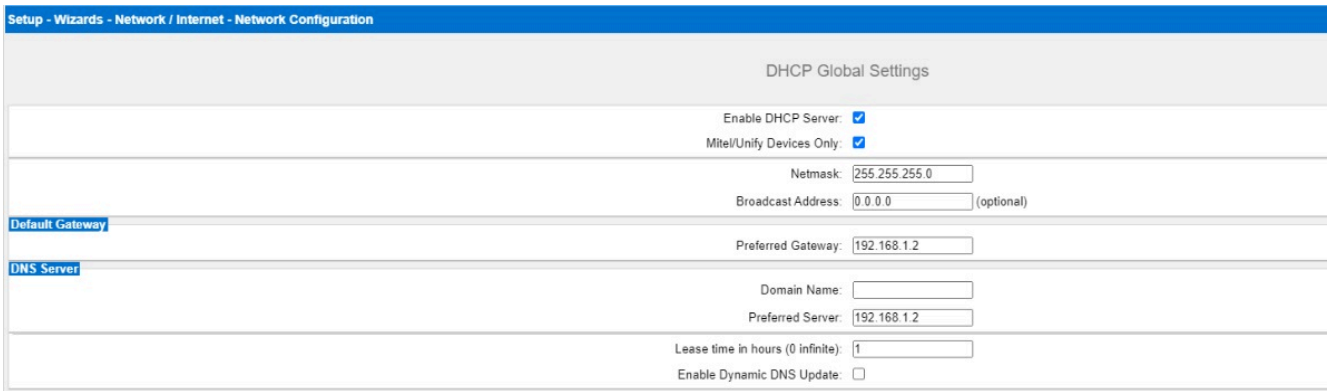
Configurez les paramètres de pays et d'heure.

5.6.3.2 Comment activer et configurer le serveur DHCP interne

Conditions préalables

Le serveur DHCP externe (par exemple, le serveur DHCP du routeur Internet) a été désactivé sur le réseau interne.

Vous êtes dans la fenêtre **Paramètres système**.



Étape par étape

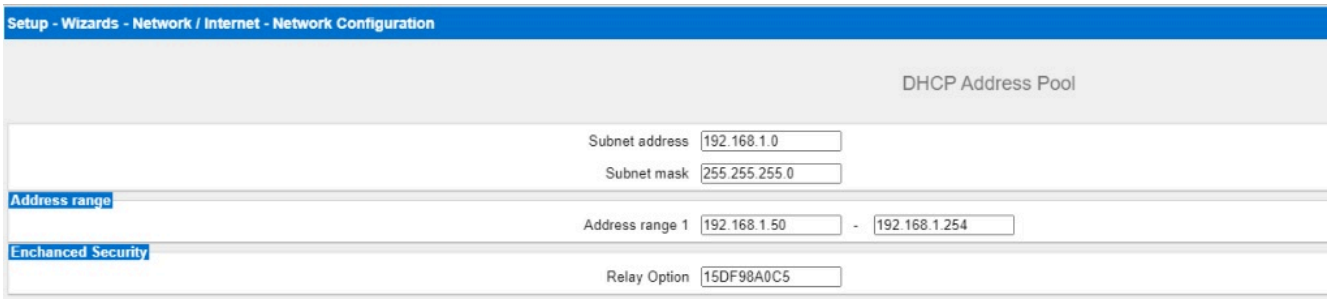
1) Laissez la case à cocher **Activer le serveur DHCP** activée.

2) Si nécessaire, activez la case à cocher **Mitel/Unify Devices Only**.

Remarque : Cette option est uniquement disponible pour les cartes mères V3.

---

3) Accédez au champ **Netmask** et ajustez le masque de sous-réseau à votre plage d'adresses IP (par exemple, `255.255.255.0`).
4) Entrez dans le champ **Passerelle par défaut** l'adresse IP du routeur Internet (par ex. `192.168.1.1`).
5) Dans le champ **Serveur par défaut**, entrez l'adresse IP d'un serveur DNS disponible, par ex. l'adresse IP du routeur Internet, `192.168.1.1`.
6) Cliquez sur **OK et Suivant** . La fenêtre **Pool d'adresses DHCP** apparaît.



7) Spécifiez les valeurs pour **l'adresse de sous-réseau**, **le masque de réseau** et **la plage d'adresses 1** afin de définir la plage d'adresses IP à gérer par le serveur DHCP interne.

   Si le réseau interne utilise des adresses IP statiques (par exemple, pour un serveur d'impression), la plage d'adresses IP (pool d'adresses DHCP) doit être sélectionnée de manière à ce que les adresses IP fixes ne soient pas incluses dans cette plage.

   Exemple:

   Routeur Internet : `192.168.1.1`

   OpenScape Business : `192.168.1.2`

   Adresse du sous-réseau : `192.168.1.0`

   Masque de sous-réseau : `255.255.255.0`

   Serveur d'imprimante : `192.168.1.10`

   Pool d'adresses DHCP : `192.168.1.50` à `192.168.1.254`
8) Si nécessaire, spécifiez la valeur du champ **Option de relais**.

Remarque : Cette option est uniquement disponible pour les cartes mères V3.

---

9) Cliquez sur **OK et Suivant** .

Étapes suivantes

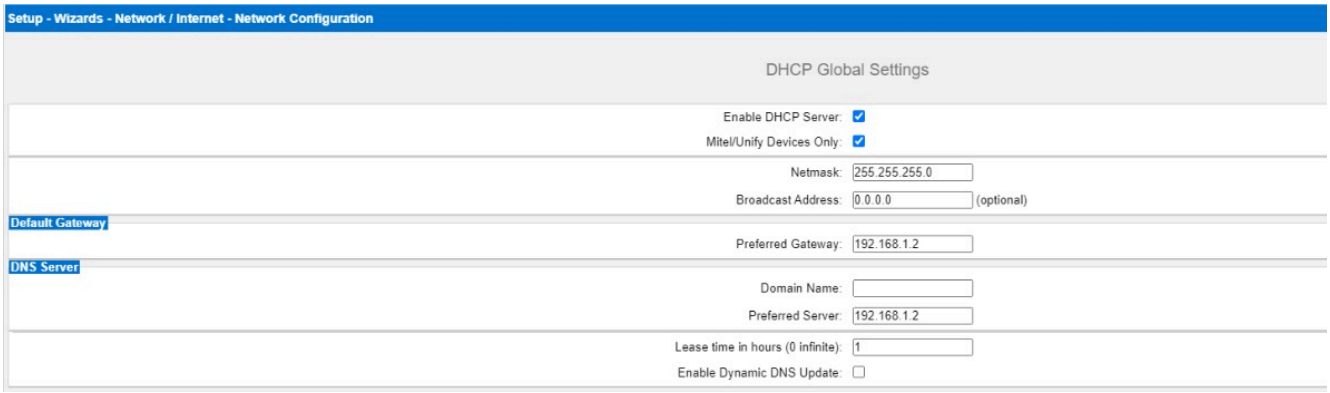
Configurer les paramètres de pays et d'heure.

5.6.3.3 Comment activer DHCP pour les appareils Mitel/Unify uniquement

Cette option permet à l'administrateur système d'activer le service DHCP Unify OpenScape Business exclusivement pour les appareils Mitel et Unify.

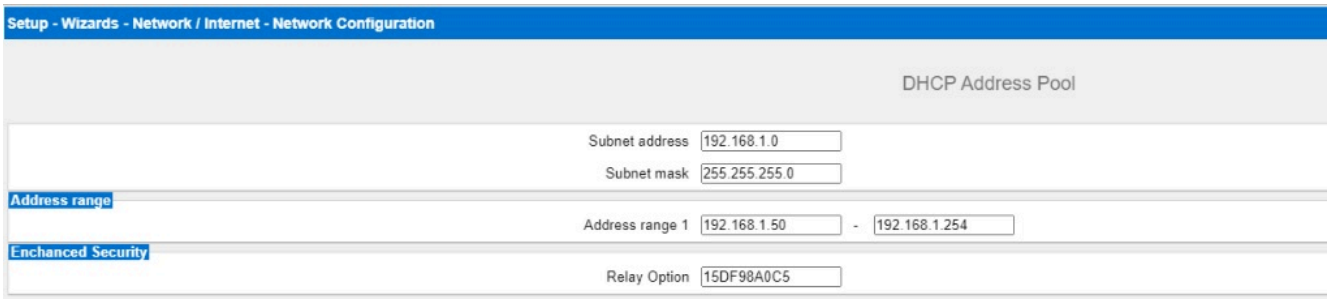
Conditions préalables

Vous êtes dans la fenêtre **Paramètres globaux DHCP**.



Étape par étape

1) Laissez la case à cocher **Activer le serveur DHCP** activée.
2) Cliquez pour activer la case à cocher **Mitel/Unify Devices Only**. Voir Serveur DHCP > Paramètres globaux pour plus d'informations sur cette option.
3) Accédez au champ **Netmask** et ajustez le masque de sous-réseau à votre plage d'adresses IP (par exemple, `255.255.255.0`).
4) Entrez dans le champ **Passerelle par défaut** l'adresse IP du routeur Internet (par ex., `192.168.1.1`).
5) Dans le champ **Serveur par défaut**, entrez l'adresse IP du serveur DNS (par ex., l'adresse IP du routeur Internet, `192.168.1.1`).
6) Cliquez sur **OK & Suivant**. La fenêtre **Pool d'adresses DHCP** apparaît.



7) Spécifiez les valeurs pour **l'adresse de sous-réseau**, **le masque de sous-réseau** et **la plage d'adresses 1** pour définir la plage d'adresses IP à gérer par le serveur DHCP interne.

   Si le réseau interne utilise des adresses IP statiques (par exemple, pour un serveur d'imprimante), la plage d'adresses IP (pool d'adresses DHCP) doit

être sélectionnée de sorte que les adresses IP fixes ne soient pas incluses dans cette plage.

Exemple:

Routeur Internet : `192.168.1.1`

Unify OpenScape Business : `192.168.1.2`

Adresse du sous-réseau : `192.168.1.0`

Masque de sous-réseau : `255.255.255.0`

Serveur d'imprimante : `192.168.1.10`

Pool d'adresses DHCP : `192.168.1.50` à `192.168.1.254`

8) Spécifiez la valeur du champ **Option de relais**.

9) Cliquez sur **OK & Suivant**.

Étapes suivantes

Paramètres de pays et d'heure

5.6.4 Paramètres de pays et de temps

Dans la fenêtre **Configuration de base** sélectionnez votre pays et la langue pour les journaux d'événements et réglez la date et l'heure. Si vous utilisez la solution cordless intégrée, indiquez ici l'identifiant système DECT pour l'ensemble du système.

Procédez de la manière suivante :

1) Sélectionnez l'identification du pays et la langue pour les journaux d'événements

Pour une initialisation correcte du pays, vous devez choisir le pays dans lequel le système de communication est utilisé. En plus, vous pouvez choisir la langue dans laquelle les journaux d'événements (journaux des événements système, des erreurs, etc.) seront enregistrés.

2) Entrez l'identifiant système DECT (uniquement pour solution Cordless intégrée)

Si vous utilisez la solution cordless intégrée, indiquez ici l'identifiant système DECT pour l'ensemble du système.

3) Comment paramétrer la date et l'heure

- Comment paramétrer manuellement la date et l'heure

  Le système de communication et les abonnés (téléphones IP, téléphones TM, PC client) devraient disposer d'une base de temps unifiée (date et heure). Si aucun serveur SNTP n'est connu pour la synchronisation du temps, vous pouvez aussi entrer la date et l'heure manuellement.

  Remarque : La date et l'heure sont également actualisées lorsque une liaison est établie via une ligne réseau RNIS.

- Comment reprendre la date et l'heure d'un serveur SNTP

  Le système de communication et les abonnés IP (téléphones IP, PC client) devraient disposer d'une base de temps unifiée (date et heure).

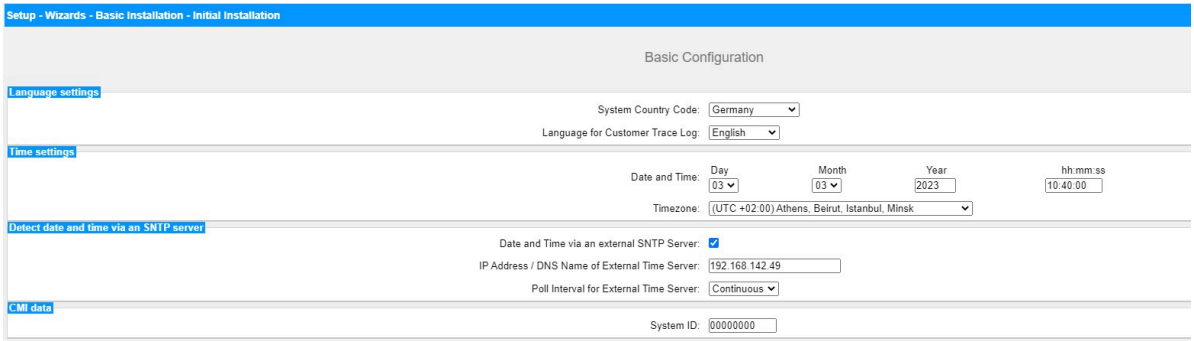
Cette base de temps peut être fournie par un serveur SNTP. Le serveur SNTP peut se trouver dans le réseau interne ou sur Internet.

Les téléphones IP reçoivent la date et l'heure automatiquement du système de communication. Les PC client sur lesquels fonctionnent les UC-Clients doivent être paramétrés de manière à être en parfait synchronisme de temps avec le système de communication (voir Instructions du système d'exploitation des PC client).

5.6.4.1 Comment sélectionner l'indicatif de pays et la langue du journal des événements

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration de base**.



Étape par étape

1) Dans la liste déroulante **Codes système de pays**, sélectionnez le pays où le système de communication sera utilisé.
2) Dans le champ **Langue du Journal d'événements client** sélectionnez la langue dans laquelle les journaux d'événements (journaux des événements système, des erreurs, etc.) seront publiés.

Étapes suivantes

Entrez l'identifiant système DECT (uniquement pour solution Cordless intégrée)

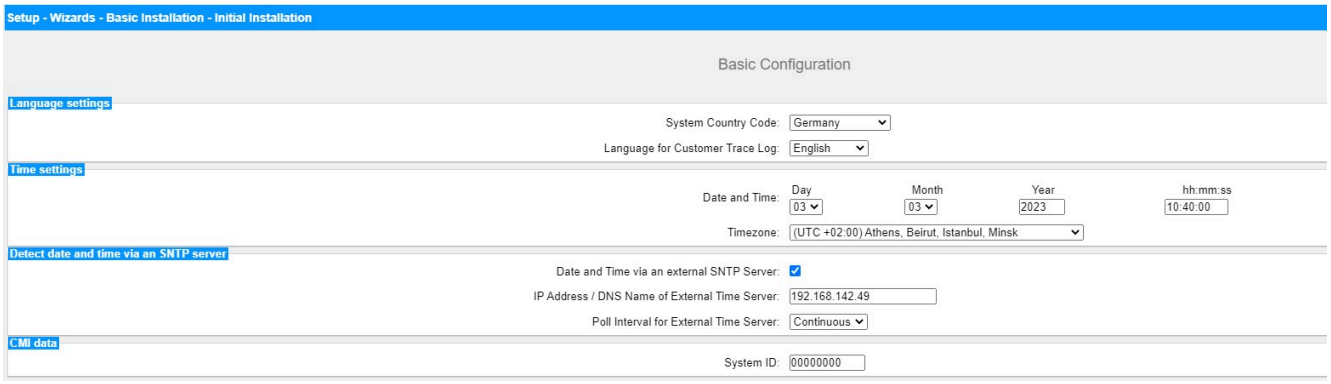
ou

Paramétrer manuellement la date et l'heure ou reprendre la date et l'heure d'un serveur SNTP.

5.6.4.2 Comment entrer l'identifiant système DECT

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration de base**.



Étape par étape

Dans la zone **Données CMI**, **Code système**, indiquez l'identifiant système DECT hexadécimal à 8 caractères, que vous avez reçu lors de l'achat de la solution Cordless intégrée.

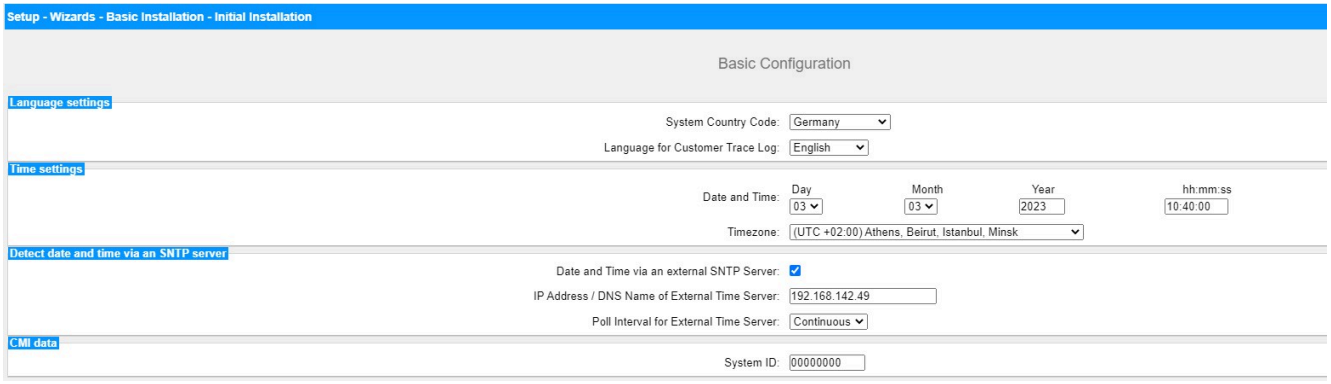
Étapes suivantes

Paramétrer manuellement la date et l'heure ou reprendre la date et l'heure d'un serveur SNTP.

5.6.4.3 Comment régler manuellement la date et l'heure

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration de base**.



Étape par étape

1) Dans **Date et heure**, saisissez les valeurs actuelles.
2) Dans **Fuseau horaire**, sélectionnez le fuseau horaire souhaité.

3) Cliquez sur **OK & Suivant**.

Remarque : Si le réglage du fuseau horaire est modifié, **le système sera redémarré** à la dernière étape de l'assistant Première installation.

Si le réglage du fuseau horaire n'est pas modifié, le système ne redémarrera pas.

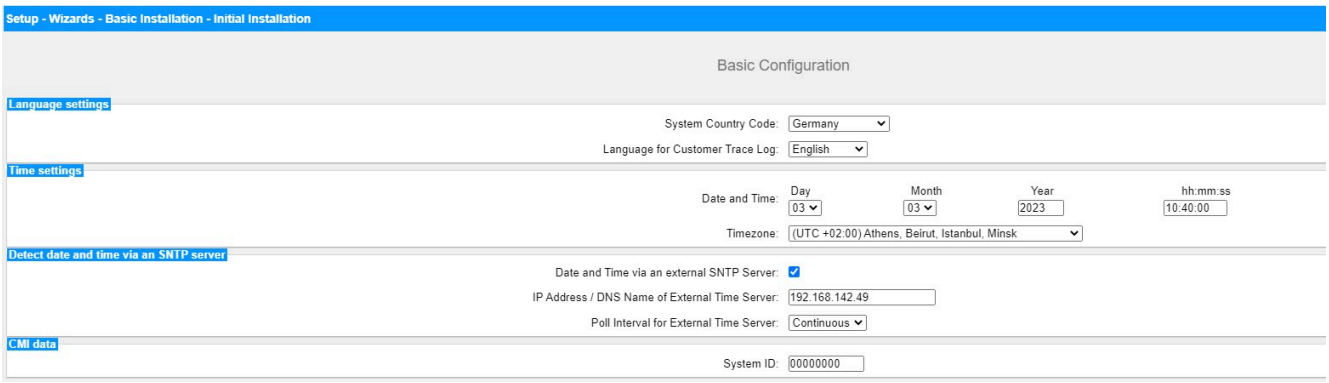
Étapes suivantes

Définir la solution UC.

5.6.4.4 Comment obtenir la date et l'heure d'un serveur SNTP

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration de base**.



Étape par étape

1) Cochez la case **Date et heure via un serveur SNTP externe**.
2) Dans le champ **Adresse IP/nom DNS du serveur de temps externe**, saisissez l'adresse IP ou le nom DNS du serveur SNTP (par ex. `0.de.pool.ntp.org`).
3) Dans la liste déroulante **Intervalle d'interrogation pour le serveur de temps externe**, indiquez au bout de combien d'heures le serveur SNTP doit synchroniser la date et l'heure (valeur recommandée : `4 heures`).
4) Cliquez sur **OK & Suivant**.

Étapes suivantes

Définir la solution UC.

5.6.5 Solution UC intégrée

Dans la fenêtre **Modifier la sélection de l'application**, vous définissez la solution UC que vous utilisez.

Vous disposez des possibilités suivantes :

- **Téléphonie avec UC Smart**

  La solution UC Smart est intégrée sur la carte mère Unify OpenScape Business X.
- **Téléphonie avec UC Suite**

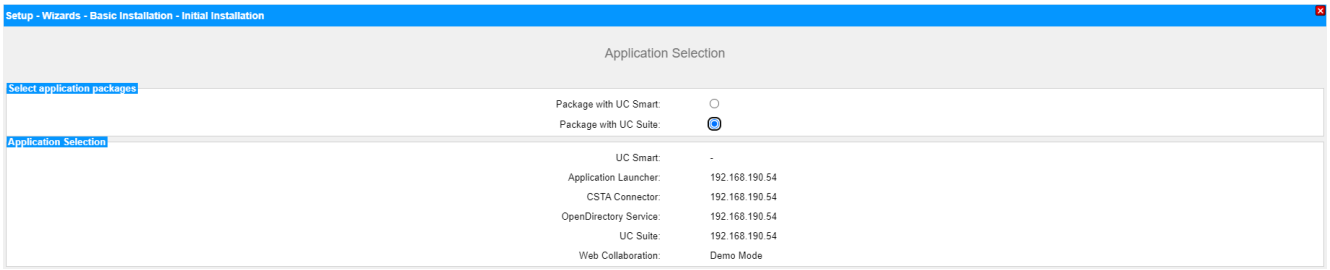
  La solution UC UC Suite est intégrée sur la carte mère Unify OpenScape Business X.

5.6.5.1 Comment définir la solution UC

Conditions préalables

Vous avez fait l'acquisition de licences soit pour la solution UC Smart soit pour la solution UC Suite.

Vous êtes dans la fenêtre **Sélection de l'application**.



Étape par étape

1) Si vous utilisez la solution UC Smart, cliquez sur **Pack avec UC Smart**.
2) Si vous utilisez la solution UC Suite, cliquez sur **Pack avec UC Suite**.
3) Cliquez sur **OK & Suivant**.
4) L'assistant **Première installation** se ferme. Cliquez sur **Terminer**.
5) Pour quitter la WBM, cliquez en haut à droite sur le lien **Déconnexion**, puis fermez la fenêtre.

> **Remarque :** Si les adresses IP ou les paramètres du serveur DHCP ont été modifiés, le système de communication effectue un redémarrage. Cela peut durer plusieurs minutes.

Étapes suivantes

Raccprder le système de communication au LAN client.

5.6.6 raccordement du système de communication au LAN client

Une fois que la première installation a été effectuée avec succès, le système de communication est raccordé au LAN client en place.

5.6.6.1 Comment connecter le système de communication au réseau local du client

Conditions préalables

Le système de communication est prêt à l'emploi.

Étape par étape

1) Retirez le câble LAN du PC d'administration du port LAN central « LAN » et intégrez le PC d'administration au réseau local du client en le connectant à un commutateur, par exemple.
2) Connectez un câble LAN au port « LAN » central du système de communication.
3) Intégrez le système de communication via ce câble LAN dans le réseau local du client en le connectant par exemple à un commutateur.

Étapes suivantes

Commencez la configuration de base.

5.7 Configuration de base

La configuration de base est effectuée avec l'assistant **Installation de base** de la WBM. Les principaux paramètres d'exploitation du système de communication sont définis.

L'assistant d'installation de base comprend un indicateur de progression qui montre l'étape actuelle ainsi que les étapes suivantes.

5.7.1 Comment démarrer l'assistant Installation de base

Conditions préalables

L'Assistant **Première installation** est achevé.

Le système de communication est intégré dans le LAN clients.

Le système de communication ist opérationnel. La LED "Run" de la carte mère clignote en vert à un rythme de 1 Hz (0,5 s allumée / 0,5 s éteinte).

Étape par étape

1) Sélectionnez dans votre navigateur Web du Admin-PC la page d'accueil de la WBM, à l'adresse suivante :

   `https://<Adresse IP de OpenScape Business>`

   L'adresse IP par défaut d'OpenScape Business est `192.168.1.2`, donc par ex. `https://192.168.1.2`
2) Dans **Nom utilisateur** indiquez le nom d'utilisateur par défaut `administrator@system` pour l'accès en tant qu'administrateur.
3) Dans **Mot de passe**, entrez le mot de passe que vous avez défini lors de la première mise en service.
4) Cliquez sur **Connexion**.
5) Cliquez dans la barre de navigation sur **Configuration**.
6) Cliquez sur **Modifier** pour lancer l'Assistant **Installation de base**.

Étapes suivantes

Effectuez l'installation de base comme indiqué ci-après, étape après étape. Les champs qui ne sont pas décrits ici sont paramétrés de manière adaptée à un cas normal ; ils ne doivent être modifiés que s'ils ne correspondent pas à vos données réseau. Les informations complètes figurent dans la description de chacun des Assistants.

5.7.2 Numéros système et mise en réseau

Dans la fenêtre **Présentation** entrez les numéros système (Numéro de l'installation, indicatif et indicatif local, préfixe international) et précisez si OpenScape Business doit être mis en réseau avec d'autres systèmes OpenScape Business.

Procédez de la manière suivante :

1) Entrer les numéros système

- Entrez les numéros système pour connexion d'installation

  Entrez ici le numéro de l'installation pour votre connexion à l'installation ainsi que l'indicatif national et local.

  L'entrée de l'indicatif national est obligatoire pour la téléphonie Internet et pour les fonctions de serveur de conférence.

  Le préfix international dépend de l'indicatif de pays prédéfini auparavant.
- Entrez le numéro système pour raccordement multiposte

  Entrez ici l'indicatif national et local pour votre raccordement multiposte.

  L'entrée de l'indicatif national est obligatoire pour la téléphonie Internet et pour les conférences MeetMe.

  Le préfix international dépend de l'indicatif de pays prédéfini auparavant.

2) Comment activer ou désactiver la mise en réseau

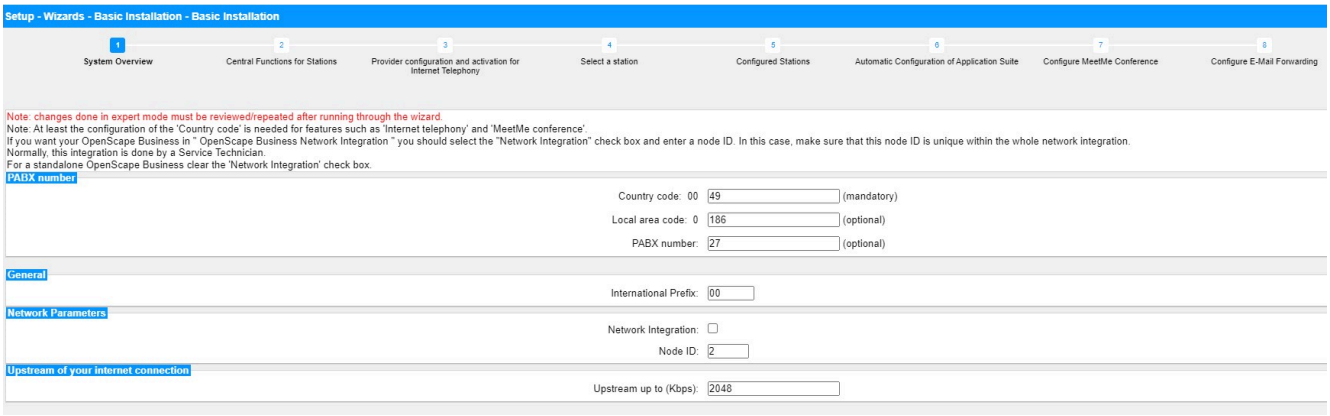
Si OpenScape Business doit être mis en réseau avec d'autres systèmes OpenScape Business, il faut activer la mise en réseau et attribuer à OpenScape Business un ID de noeud. Chaque OpenScape Business en interconnexion de réseaux doit disposer d'un ID de noeud univoque.

5.7.2.1 Comment entrer les numéros de téléphone système pour un raccordement installation

Conditions préalables

Vous disposez d’un raccordement installation.

Vous êtes dans la fenêtre **Vue d’ensemble du système** de l’assistant **Installation de base**.



Étape par étape

1) Dans le champ **Indicatif national**, saisissez l'indicatif national correspondant, par ex. `49` pour l'Allemagne ou `1` pour les États-Unis.
2) Dans le champ **Préfixe du réseau local**, saisissez le préfixe du réseau local, par ex. `89` pour Munich.
3) Dans le champ **N° installation**, saisissez le numéro de l'installation de votre raccordement réseau, par ex. `7007` (votre numéro de raccordement).
4) Modifiez le champ **Préfixe international** uniquement si nécessaire. Les valeurs applicables respectives pour l'Allemagne et les États-Unis sont `00` et `011`.

   Lors des appels téléphoniques à l'étranger, le numéro de téléphone est précédé du préfixe international et de l'indicatif national, par ex. d'Allemagne vers les Etats-Unis par 00-1 et des Etats-Unis vers l'Allemagne par 011-49.

Étapes suivantes

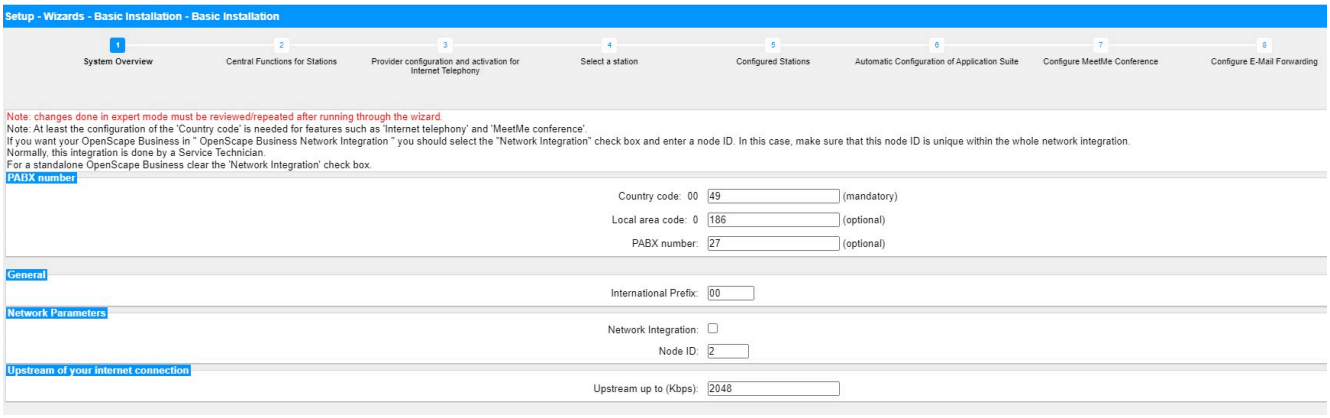
Comment activer ou désactiver la mise en réseau

5.7.2.2 Comment entrer les numéros de téléphone système pour une connexion point à multipoint

Conditions préalables

Vous disposez d'un raccordement multiposte.

Vous êtes dans la fenêtre **Vue d'ensemble du système** de l'assistant **Installation de base**.



Étape par étape

1) Dans le champ **Indicatif national**, saisissez l'indicatif national correspondant, par ex. `49` pour l'Allemagne ou `1` pour les États-Unis.
2) Dans le champ **Préfixe du réseau local**, saisissez le préfixe du réseau local, par ex. `89` pour Munich.
3) Laissez vide le champ **Numéro de l'installation**.
4) Modifiez le champ **Préfixe international** uniquement si nécessaire. Les valeurs applicables respectives pour l'Allemagne et les États-Unis sont `00` et `011`.

   Lors des appels téléphoniques à l'étranger, le numéro de téléphone est précédé du préfixe international et de l'indicatif national, par ex. d'Allemagne vers les Etats-Unis par 00-1 et des Etats-Unis vers l'Allemagne par 011-49.

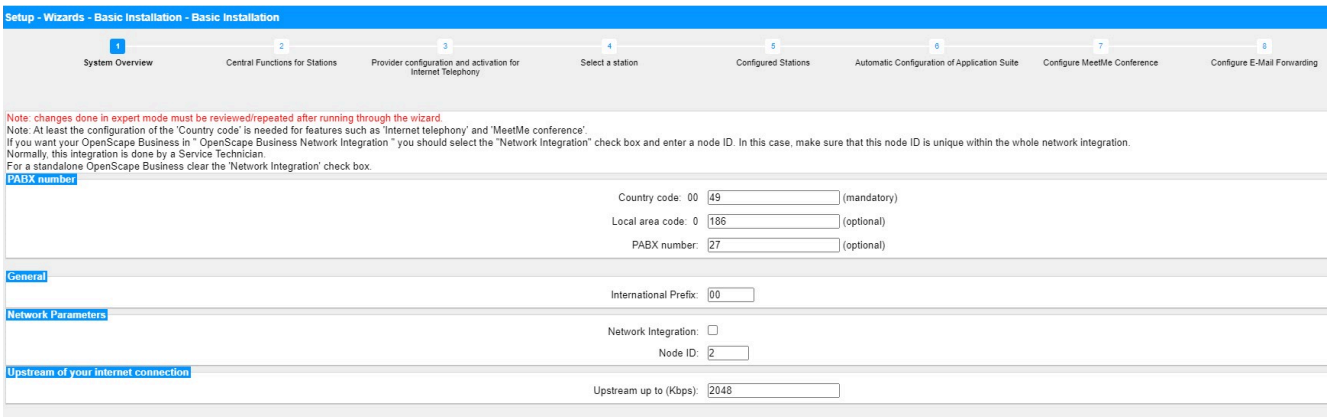
Étapes suivantes

Comment activer ou désactiver la mise en réseau

5.7.2.3 Comment activer ou désactiver la mise en réseau

Conditions préalables

Vous êtes dans la fenêtre **Vue d'ensemble du système** de l'assistant **Installation de base**.



Étape par étape

1) Si le système de communication doit être mis en réseau avec d'autres systèmes de communication :
   a) Cochez la case **Intégration réseau**.
   b) Dans le champ **ID de nœud** attribuez au système de communication un ID de nœud univoque dans l'interconnexion de réseaux (chiffres de `1` à `100` possibles).
2) Si le système de communication ne doit pas être mis en réseau avec d'autres systèmes de communication, ne cochez pas la case **Intégration réseau**.

Étapes suivantes

Configurez le débit remontant de votre connexion Internet.

5.7.3 Données abonnés

Dans la fenêtre **Fonctions centrales pour les abonnés** vous pouvez, si nécessaire, à la place du plan de numérotation standard prédéfini, configurer votre propre plan de numérotation et importer d'autres données d'abonné. Dans une interconnexion de réseaux, le plan de numérotation par défaut doit être harmonisé au plan de numérotation de l'interconnexion de réseaux.

Le plan de numérotation standard contient des numéros prédéfinis pour différents types d'abonné (téléphones IP, téléphones analogiques...) et pour les fonctions spéciales (téléphonie Internet, messagerie vocale, standard automatique...).

Les données d'abonné comprennent notamment les numéros internes, les numéros de sélection directe à l'arrivée et les noms des abonnés. A l'aide d'un fichier XML au format UTF-8, il est possible d'importer ces données et d'autres données d'abonné dans le système de communication durant la configuration de base.

Remarque :

Vous trouverez un modèle XML avec les explications correspondantes dans WBM, sous **Centre de service** > **Documents** > **Modèles CSV**. Dans ce modèle, vous pouvez par ex. inscrire vos données avec Microsoft Excel.

Vous disposez des possibilités suivantes :

- **Configurer les données abonnés sans interconnexion de réseaux**

  Procédez de la manière suivante :

  1) Afficher les données abonné

  Vous pouvez afficher tous les numéros d'appel et toutes les données d'abonné préconfigurées.

  2) Supprimer tous les numéros d'abonnés (option)

  Si vous utilisez un plan de numérotation individuel, vous devez effacer tous les numéros préconfigurés.

  3) Adapter les numéros d'appel préconfigurés au plan de numérotation individuel (option)

  Si vous utilisez un plan de numérotation individuel, vous pouvez adapter les numéros d'appel préconfigurés à votre propre plan de numérotation.

  Remarque :

  Si l'utilisateur passe au travers de **Modifier les numéros d'appel préconfigurés,** toute configuration personnalisée existante au sein d'UC Suite doit être revue ou répétée (par exemple des files d'attente pilotes)

  ---

  4) Importer les données d'abonné via fichier XML (option)

  Vous pouvez aisément importer vos numéros d'appels individuels ainsi que les données d'abonné supplémentaires à l'aide d'un fichier XML durant la configuration de base.

- **Configurer les données d'abonné avec interconnexion de réseaux**

  Procédez de la manière suivante :

  1) Supprimer tous les numéros d'abonnés

  Si UC Suite est utilisé dans l'interconnexion de réseaux, il faut recourir à un plan de numérotation fermé, c.-à-d. que tous les numéros de l'interconnexion de réseaux doivent être univoques. Il faut donc effacer les numéros d'appel préconfigurés et utiliser des numéros d'appels adaptés à l'interconnexion de réseaux.

  2) Importer les données d'abonné via fichier XML ()

  Les numéros d'appel adaptés à l'interconnexion de réseaux ainsi que les données d'abonné supplémentaires peuvent être aisément importés à l'aide d'un fichier XML durant la configuration de base. Ce fichier peut contenir tous les abonnées de l'interconnexion de réseaux. Lors de l'importation, seuls sont repris les numéros d'appel et les données d'abonné correspondant à l'ID de noeud du système de communication indiqué précédemment.

Tâches associées

Comment afficher les données de masse à la page 134
Comment réinitialiser les entrées LCR à la page 1354

Référence associée

LCR > Flags LCR à la page 1540

5.7.3.1 Comment afficher les données d’abonné

Conditions préalables

Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l’assistant **Installation de base**.

Étape par étape

1) Cochez le champ d’option **Afficher la configuration des abonnés**.
2) Cliquez sur **Exécuter la fonction**. Une liste des abonnés avec les numéros préconfiguré (plan de numérotation par défaut) s'affiche pour vous.
3) Cliquez sur **OK**. Vous revenez à la fenêtre **Fonctions centrales pour les abonnés**.
4) Si vous ne souhaitez pas modifier les données d’abonné, cliquez sur **OK & Suivant**.

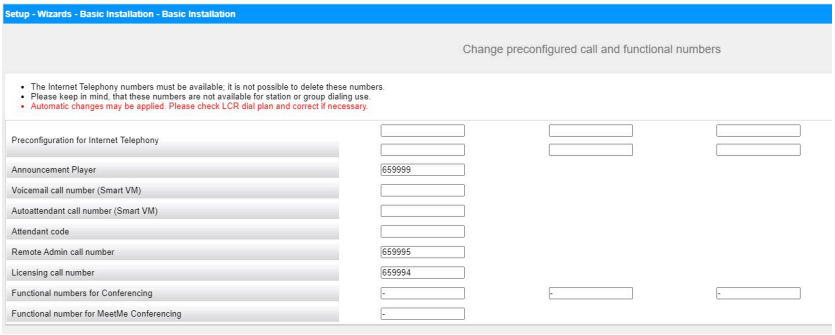
5.7.3.2 Comment supprimer tous les numéros d’appel

Conditions préalables

Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l’assistant **Installation de base**.

Étape par étape

1) Activez le champ d’option **Supprimer tous les numéros d’abonné**.
2) Cochez **Effacer tous les numéros**.
3) Cliquez sur **Exécuter la fonction**. Tous les numéros d’appel prédéfinis sont effacés à l’exception de **Lecteur annonce, Numéro d’appel Admin distant** et **Numéro d’appel Licences**. Apparaît ensuite la fenêtre **Modifier les numéros d’appel préconfigurés**.



4) Adaptez les indicatifs et les numéros d’appel spéciaux à vos souhaits et cliquez ensuite sur **OK**. Vous revenez à la fenêtre **Fonctions centrales pour les abonnés**.
5) Si vous ne souhaitez plus configurer d’autres données d’abonné, cliquez sur **OK & Suivant**.

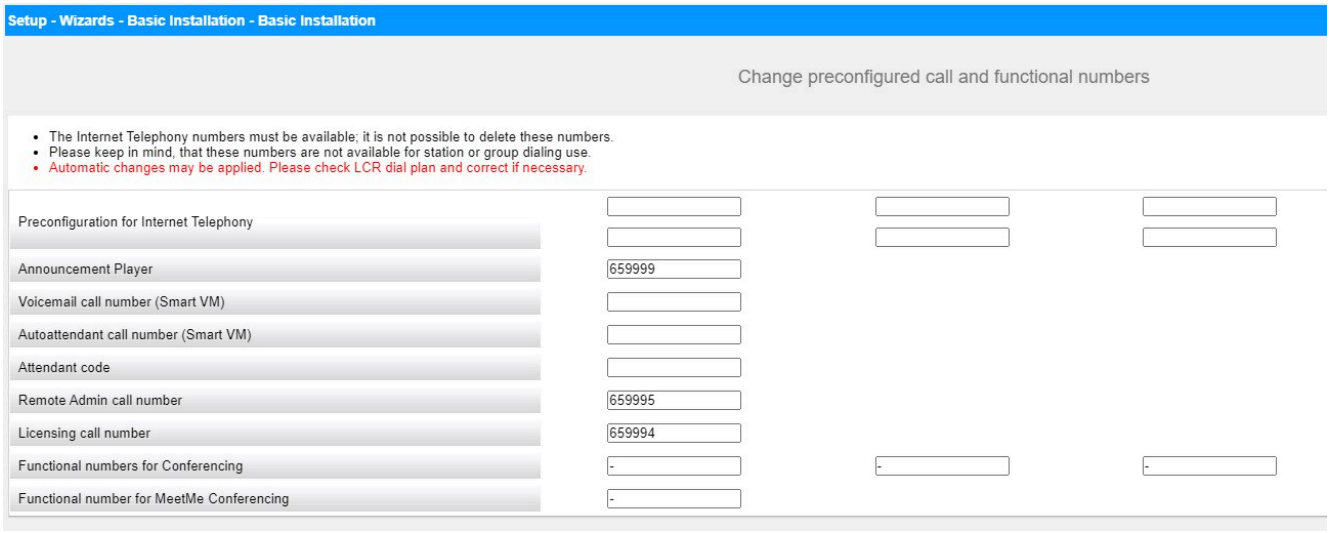
5.7.3.3 Adapter les numéros d’appel préconfigurés au plan de numérotation individuel

Conditions préalables

Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l’assistant **Installation de base**.

Étape par étape

1) Activez le bouton radio **Modifier les numéros d’appel et les numéros fonctionnels préconfigurés**.
2) Cliquez sur **Exécuter la fonction**. La fenêtre **Modifier les numéros d’appel préconfigurés** s’affiche.



3) Adaptez les numéros d’appel préconfigurés à vos souhaits et cliquez ensuite sur **OK**. Vous revenez à la fenêtre **Fonctions centrales pour les abonnés**.
4) Si vous ne souhaitez plus configurer d’autres données d’abonné, cliquez sur **OK & Suivant**.

5.7.3.4 Comment importer les données d’abonné via un fichier XML

Conditions préalables

Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l’assistant **Installation de base**.

Un fichier XML au format UTF-8 avec les données inscrites est disponible. Vous trouverez un modèle XML dans **Centre de service** > **Documents** > **Modèles CSV**.

Étape par étape

1) Cochez le champ d’option **Importer le fichier CSV/XML avec les données d’abonné**.
2) Cliquez sur **Exécuter la fonction**.
3) Avec **Parcourir**, sélectionnez le fichier XML souhaité et cliquez sur **Ouvrir**.
4) Pour finir, cliquez sur **OK**. Les données d’abonnés sont importées.
5) Cliquez sur **OK & Suivant**.

5.7.3.5 Comment afficher les données de masse

Conditions préalables

- Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l'assistant **Installation de base**.
- Vous pouvez également avoir accès à l'assistant de **données de masse** depuis **Configuration** > **Assistants**.

Étape par étape

1) Activez le bouton **Assistant de données de masse**.

2) Cliquez sur **Exécuter la fonction**.

3) Dans la fenêtre **Assistant de données de masse**, vous pouvez valider les entrées du système en cliquant sur **Valider**. Il existe deux types de validation, le contrôle de cohérence front end et le contrôle de cohérence back end.
La couleur verte dans le champ de validation indique uniquement les actions qui ont été validées récemment. La validation des données n'est pas enregistrée, donc si les valeurs sont modifiées, l'utilisateur doit valider à nouveau les données.

4) Pendant le contrôle de cohérence back end et après la validation des données, aucune modification n'est possible dans la fenêtre **Assistant de données de masse**. Une fois la validation réussie, **OK&Suivant** devient disponible avec le mode Edition restreint. Si l'utilisateur clique sur **Retour**, le mode Edition devient disponible mais **OK&Suivant** disparaît. Lorsque la validation échoue, le mode Edition reste intact et **OK&Suivant** reste masqué.

> **Remarque :** L'utilisateur peut cliquer sur **Retour** pour ré-éditer les données et la fenêtre retourne au mode Edition. Le mode Restriction édition garantit que l'utilisateur ne peut pas cliquer sur OK & Suivant et soumettre des modifications non validées.

5) Une fois que l'**Assistant de données de masse** a été configuré avec succès, cliquez sur **Terminer**. Dans la page de fin, il est indiqué une synthèse de tous les changements.

Les champs non modifiables sont déjà remplis avec les valeurs pertinentes obtenues par la base de données. Par conséquent, la fonction copier/coller n'impactera pas ces données.

Le champ Type est un menu déroulant sélectionnable avec des fonctionnalités d'édition. Toutefois, les seules options acceptées sont Aucun port, Client système, Client SIP, Utilisateur Deskshare et potentiellement une valeur prédéfinie, basée sur le module correspondant. Si l'utilisateur essaie d'entrer autre chose, cela n'est pas accepté et le menu déroulant ne disparaît pas mais attend une entrée appropriée.

Une autre restriction est que certains ports ne sont pas modifiables (par exemple pour les ports appartenant à une carte analogique, le type n'est pas modifiable et doit rester Station analogique). Toutes les restrictions s'appliquent lorsque l'utilisateur essaie d'effectuer un copier-coller en haut de la colonne Type. Si l'utilisateur essaie de coller des données non

pertinentes ne compromettant pas les règles ci-dessus, la fonction coller n'est pas exécutée du tout.

Le copier-coller peut s'appliquer à l'ensemble du tableau ou à des parties spécifiques.

Remarque : Lorsque vous sélectionnez deux cellules successives avec une valeur numérique, et que vous déroulez les champs, les colonnes suivantes ne sont pas remplies avec des nombres croissants, mais avec une copie des cellules sélectionnées.

Concepts associés

Données abonnés à la page 130

5.7.4 Configuration RNIS

Dans la fenêtre **Configuration RNIS**, vous déterminez si les abonnés RNIS doivent être raccordés ou non et si le raccordement réseau doit être effectué via RNIS ou non. Le raccordement réseau RNIS peut être configuré comme raccordement système RNIS et/ou raccordement multiposte RNIS. Selon le système de communication et évent. le module utilisé, on dispose pour cela d'un nombre d'interfaces S_0 différent.

Vous disposez des possibilités suivantes :

- Activer la configuration RNIS :
  1) Comment configurer le raccordement système RNIS

     Vous pouvez configurer un raccordement réseau RNIS en tant que raccordement système avec numéros SDA.
  2) Comment configurer un raccordement multiposte RNIS

     Vous pouvez configurer un raccordement réseau RNIS comme raccordement multiposte avec MSN.
  3) Comment configurer le raccordemment des abonnés RNIS (option)

     Il est possible de configurer une ou plusieurs interfaces S_0 comme raccordements S_0 internes afin d'y raccorde les abonnés RNIS (téléphone ou fax RNIS). Pour chaque abonné RNIS vous avez besoin d'une licence d'abonné.
- Comment désactiver la configuration RNIS

  Si vous n'avez pas de raccordement réseau RNIS, vous devez désactiver la configuration RNIS. Toutes les interfaces S_0 sont automatiquement configurées en tant que raccordements S_0 internes.

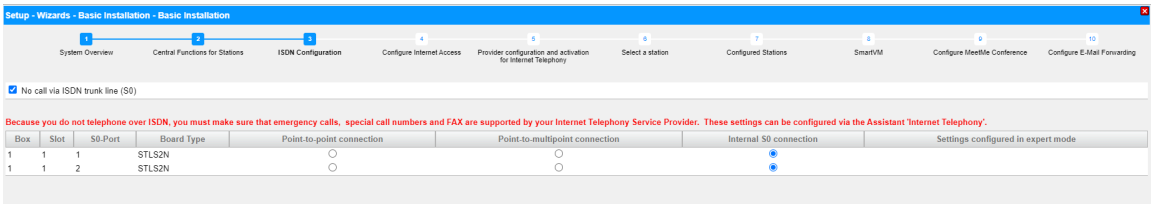
Autres possibilités pour un raccordement réseau

A la place du raccordement réseau RNIS, vous pouvez configurer un raccordement réseau analogique ou un raccordement réseau via un fournisseur de service de téléphonie sur Internet (ITSP, SIP-Provider). La configuration du raccordement réseau analogique n'est possible qu'une fois l'installation de base terminée.

5.7.4.1 Comment configurer la connexion des abonnés RNIS

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration ISDN** de l'assistant **Installation de base**.



Étape par étape

1) Laissez la case **Pas de téléphonie par la ligne réseau RNIS (S0)** décochée.
2) Dans l'interface S_0 souhaitée, activez le champ d'option **Connexion S0 interne**.

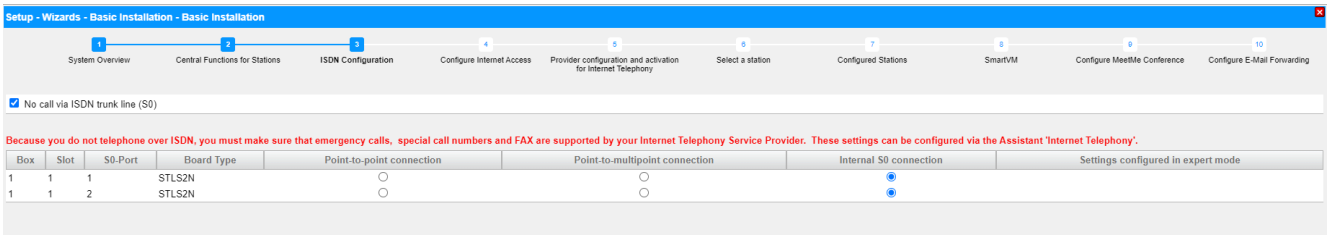
Étapes suivantes

Configurer un raccordement d'installation RNIS et/ou configurer un raccordement multiposte RNIS

5.7.4.2 Comment configurer l'accès réseau RNIS

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration ISDN** de l'assistant **Installation de base**.



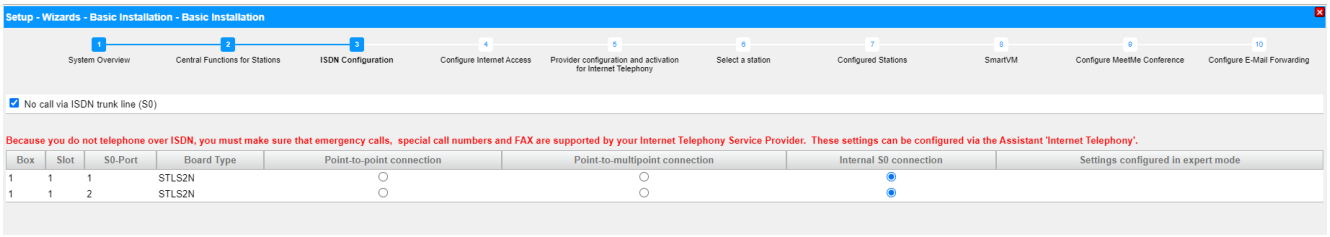
Étape par étape

1) Pour paramétrer la connexion réseau RNIS, vous devez laisser décochée la case **Pas de téléphonie par la ligne réseau RNIS (S0)**.
2) Dans le champ d'option S_0 souhaité, activez le champ d'option **Raccordement système**.
3) Cliquez sur **OK & Suivant**.

5.7.4.3 Comment configurer un raccordement multiposte RNIS

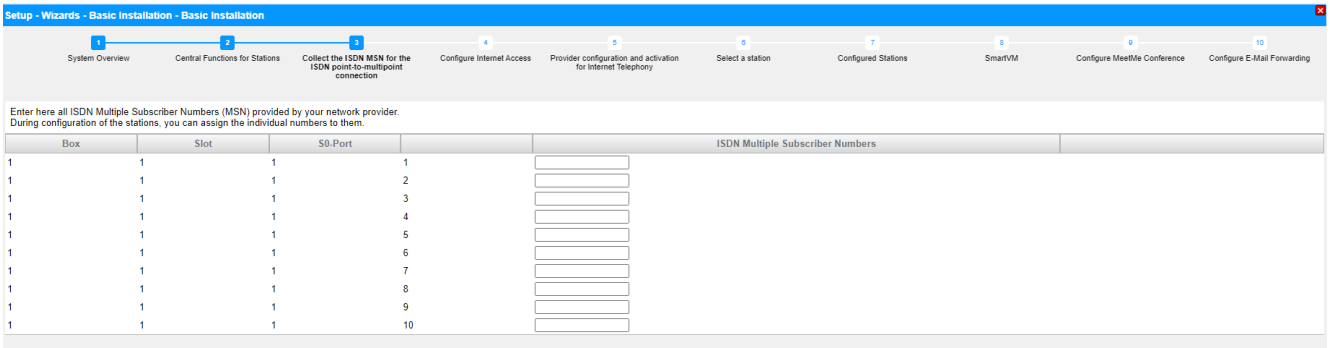
Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration ISDN** de l'assistant **Installation de base**.



Étape par étape

1) Pour paramétrer la connexion réseau RNIS, vous devez laisser décochée la case **Pas de téléphonie par la ligne réseau RNIS (S0)**.
2) Dans le champ d'option S**0** souhaité, activez le champ d'option **Raccordement multiposte**.
3) Cliquez sur **OK & Suivant**.



4) Entrez dans la colonne **Numéros d'appel multiples RNIS** tous les numéros (MSN) que votre opérateur réseau vous a communiqué. Vous pouvez entrer jusqu'à 10 MSN par raccordement S_0. Le nombre des raccordements S_0 est fonction du système de communication et du module éventuellement utilisé.
5) Cliquez sur **OK & Suivant**.

5.7.4.4 Comment désactiver la configuration RNIS

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration ISDN** de l'assistant **Installation de base**.

Étape par étape

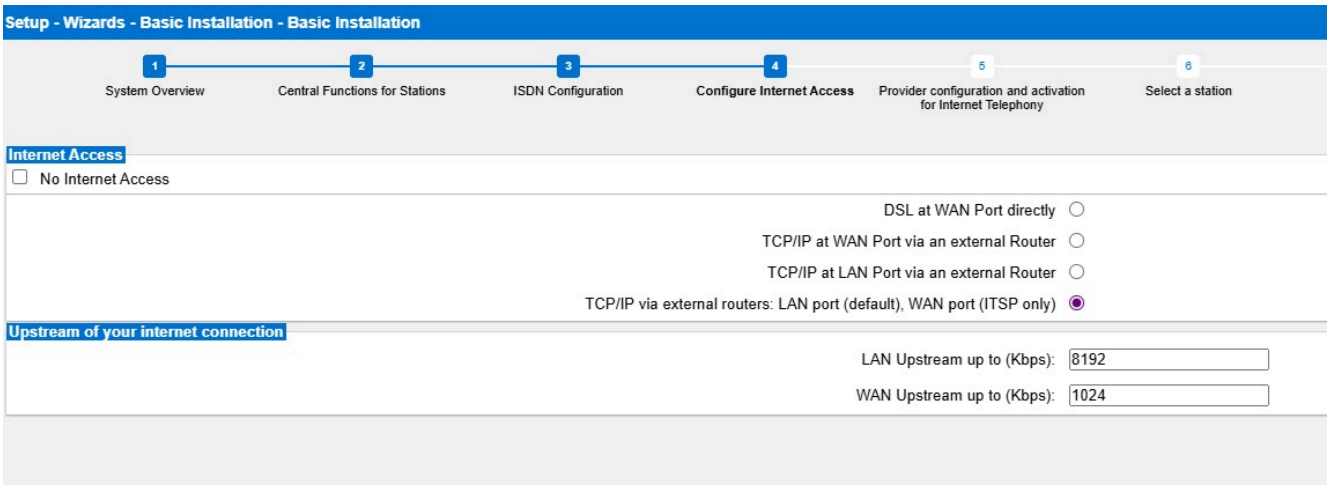
1) Cochez la case **Pas de téléphonie par la ligne réseau RNIS (S0)**.

> **Remarque :** Les communications peuvent aussi être menées via un fournisseur de service de téléphonie Internet (ITSP) (voir Téléphonie Internet.

2) Cliquez sur **OK & Suivant**.

5.7.5 Accès Internet

La fenêtre **Configurer l'accès à Internet** permet de configurer l'accès à Internet.



La configuration de l'accès à Internet dans le WBM dépend du fait que la connexion Internet a déjà été configurée dans un routeur externe ou qu'elle s'effectue via un modem Internet et doit donc être configurée dans le WBM.

Une seule des options énumérées ici peut être sélectionnée.

- Accès à l'internet via un modem internet (**DSL sur le port WAN directement**)

  Vous souhaitez utiliser le système de communication directement sur un modem Internet (DSL, câble, UMTS ...). OpenScape Business dispose d'un routeur Internet intégré. Introduisez les données d'accès du fournisseur

d'accès Internet (FAI) directement dans le système de communication et utilisez le port WAN du système de communication.

Vous disposez des possibilités suivantes :

– **Accès à l'Internet via un FAI préconfiguré**
– **Accès à l'internet via le FAI standard PPPoE**
– **Accès à l'internet via le FAI standard PPTP**

Si votre FAI ne figure pas dans la liste des FAI préconfigurés, utilisez le FAI par défaut PPPoE ou PPTP.

- Accès à l'internet via un routeur internet externe

  Vous souhaitez faire fonctionner le système de communication à partir d'un routeur Internet externe. Le fournisseur d'accès Internet est déjà configuré dans le routeur Internet.

  Vous disposez des possibilités suivantes :

  – **Accès à Internet via un routeur Internet externe au niveau du port WAN**

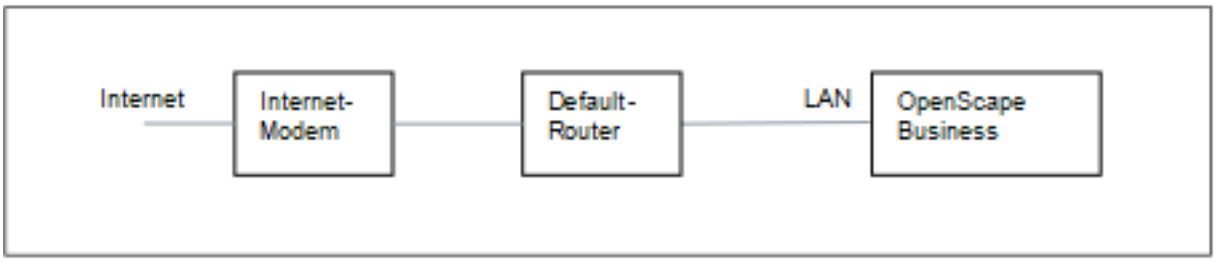
    (**TCP/IP sur le port WAN via un routeur externe**)

Pour ce faire, vous utilisez le port WAN du système de communication. OpenScape Business connaît le routeur Internet ou fonctionne comme client DHCP. Cette option peut être utilisée si le routeur Internet se trouve

dans un autre segment de réseau et dispose de son propre serveur DHCP.

– **Accès à Internet via un routeur Internet externe au niveau du port LAN**

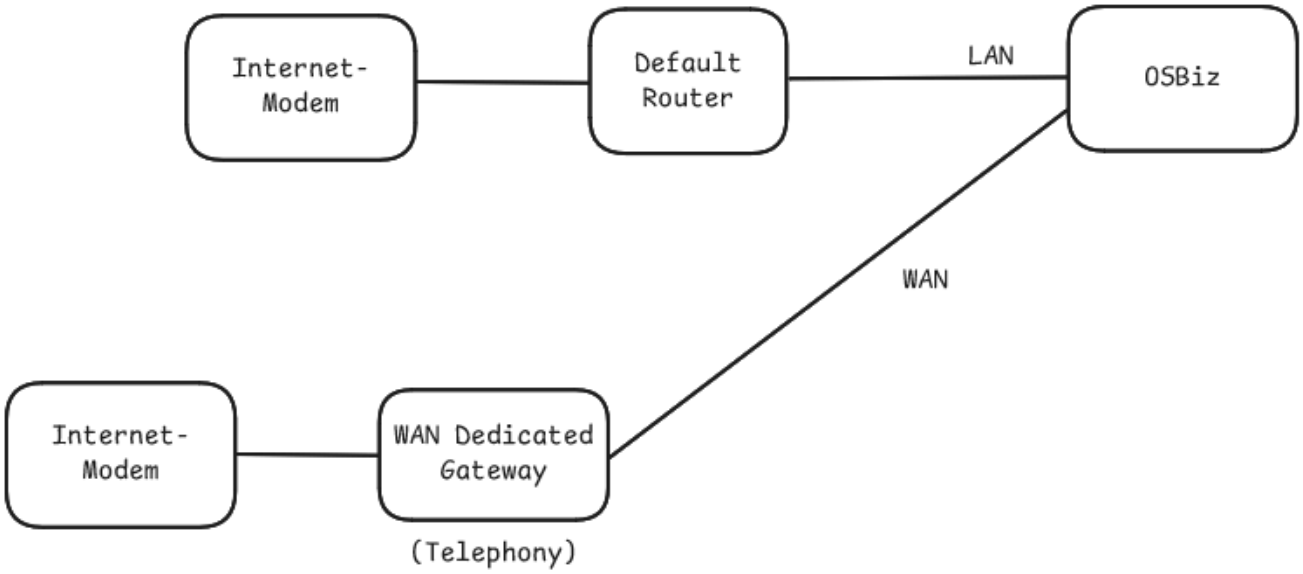
(**TCP/IP sur le port LAN via un routeur externe**)



Pour ce faire, vous utilisez le port LAN du système de communication. OpenScape Business ne connaît que le routeur par défaut et non l'infrastructure sous-jacente. Pour activer la connexion au routeur Internet, l'adresse IP du routeur par défaut et celle du serveur DNS doivent être communiquées au système de communication.

– **Accès à Internet via un routeur Internet externe au niveau du port LAN**

(**TCP/IP au port LAN/WAN via un routeur externe avec port WAN dédié à ITSP**)



Pour ce faire, vous utilisez le port LAN du système de communication, tandis que le port WAN est dédié à l'ITSP. OpenScape Business ne connaît que le routeur par défaut et non l'infrastructure sous-jacente. Pour activer la connexion au routeur Internet, l'adresse IP du routeur par défaut et celle du serveur DNS doivent être communiquées au système de communication.

- Désactiver l'accès à Internet (paramètre par défaut)

  Vous ne souhaitez pas utiliser l'Internet.

5.7.5.1 Comment configurer l’accès Internet par un routeur Internet externe avec raccordement LAN

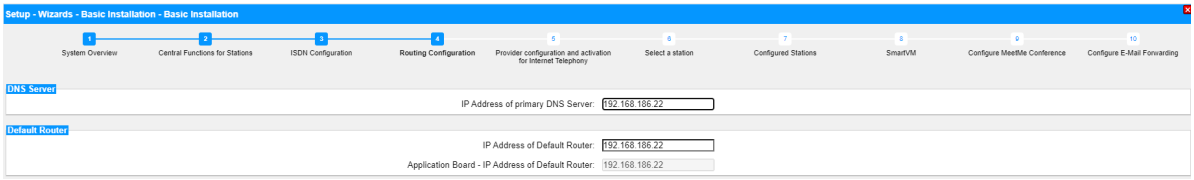
Conditions préalables

Le système de communication doit être relié au LAN client via l’interface LAN "LAN". La liaison ne doit pas se faire par le raccordement WAN, car ce dernier est désactivé.

Vous vous trouvez dans la fenêtre **Configuration de l’accès à Internet** de l’assistant **Installation de base**.

Étape par étape

1) Décochez la case **Pas d’accès Internet**.
2) Activez le bouton radio **TCP/IP au port LAN via un routeur externe**, entrez la vitesse de débit remontant de votre connexion Internet dans le champ **Transfert jusqu’à (kbit/s)** et cliquez sur **OK&Suivant**.



3) Dans le champ **Adresse IP du serveur DNS** saisissez l’adresse IP du serveur DNS local (par ex. Routeur Internet) ou du serveur DNS Internet (par ex. pour la téléphonie Internet).
4) Dans **Adresse IP du routeur par défaut**, saisissez l’adresse IP du routeur Internet externe.
5) Cliquez sur **OK & Suivant**.

5.7.5.2 Comment configurer l’accès Internet par un routeur Internet externe par le raccordement WAN

Conditions préalables

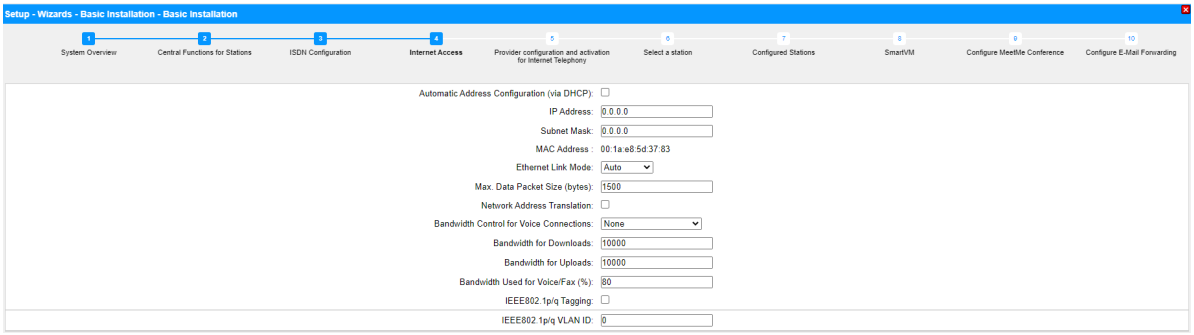
Le système de communication doit être connecté au segment LAN du réseau client où se trouve le routeur Internet, au moyen de l’interface "WAN".

Vous vous trouvez dans la fenêtre **Configuration de l’accès à Internet** de l’assistant **Installation de base**.

Étape par étape

1) Décochez la case **Pas d’accès Internet**.

2) Cochez le bouton d'option **TCP/IP sur port WAN via un routeur externe** et cliquez sur **OK & Suivant**.



3) S'il est nécessaire de récupérer pour l'interface WAN les données spécifiques réseau à partir d'un serveur DHCP déjà activé, procédez comme indiqué ci-après.
   a) Cochez la case **Configuration automatique de l'adresse (via DHCP)**.
   b) Cochez la case **Accepter l'adresse IP du routeur par défaut** si vous souhaitez utiliser cette adresse IP.
   c) Si nécessaire, cochez la case **Accepter Adresse IP du serveur DNS**.
   d) Si nécessaire, cochez la case **Accepter Adresse IP du serveur SNTP**.
4) S'il faut affecter une adresse IP fixe à l'interface WAN :
   a) Décochez la case **Configuration automatique de l'adresse (via DHCP)**.
   b) Indiquez l'**Adresse IP** et le **Masque de réseau IP** souhaités de l'interface WAN.
5) Cochez la case **Conversion d'adresse réseau (NAT)**.
6) Si vous voulez utiliser en plus la téléphonie Internet, sélectionnez dans la liste déroulante **Gestion de la bande passante pour les connexions vocales** l'entrée **Liaison montante seulement** ou **Liaison montante et descendante** selon les besoins. Si la bande passante de la liaison descendante est élevée et la bande passante de la liaison montante est parallèlement basse, la gestion de la bande passante ne doit être activée que pour la liaison montante afin que ne soit pas réservée inutilement une bande passante descendante pour la transmission de la voix.
7) Dans **Bande passante pour les liaisons descendantes** et **Bande passante pour les liaisons montantes** indiquez la bande passante en kbit/s pour le téléchargement ou le chargement que votre fournisseur d'accès à Internet vous a fourni.
8) Cliquez sur **OK & Suivant**.

5.7.5.3 Comment configurer l'accès Internet via un FAI préconfiguré

Conditions préalables

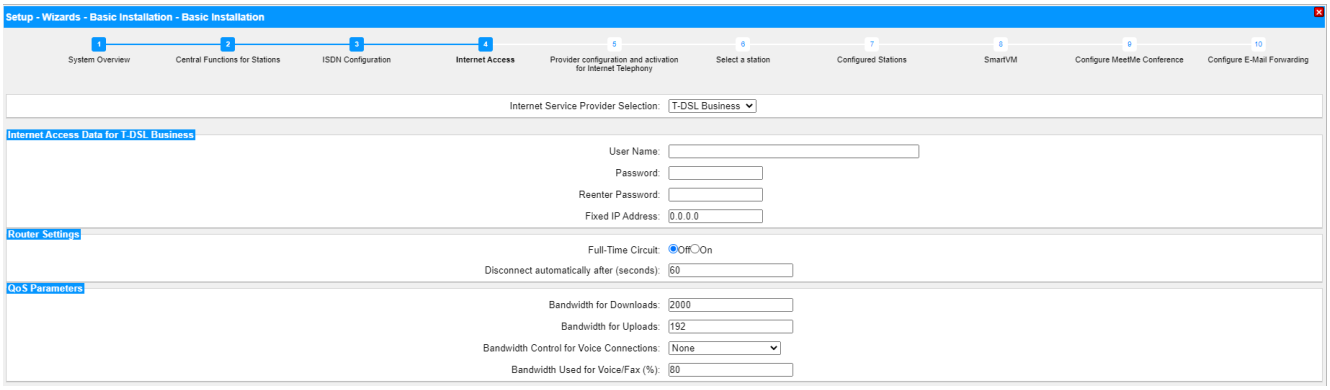
Vous vous trouvez dans la fenêtre **Configuration de l'accès à Internet** de l'assistant **Installation de base**.

Vous disposez des données d'accès Internet de votre FAI (par ex. ID utilisateur, mot de passe, bande passante pour liaison montante et la liaison descendante).

Optionnel : Les données pour un compte DynDNS sont disponibles (nom, mot de passe, nom d'hôte, nom de domaine du provider DynDNS)

Étape par étape

1) Décochez la case **Pas d'accès Internet**.
2) Cochez le champ d'option **DSL sur port WAN de la carte mère directement** et cliquez sur **OK & Suivant**.



3) Dans la liste déroulante **Sélection de fournisseur de service** sélectionnez votre FAI.
4) Entrez dans la zone **Données d'accès Internet pour...** les données d'accès que vous avez reçues de votre FAI. Les champs de cette zone sont fonction du fournisseur. Lors de l'entrée des données, veillez à entrer correctement les majuscules et les minuscules.
5) Sélectionnez une des deux options suivantes dans la zone **Paramètres de routeur** sous **Liaison permanente**, en fonction de votre modèle tarifaire :
   - Si votre modèle de tarif correspond à un forfait, activez le champ d'option **Activé**. Dans **Coupure forcée à (h:min)**, définissez l'heure à laquelle la connexion Internet doit être coupée (par ex. 01:30). A ce moment, il ne devrait pas y avoir d'échange de données avec Internet (par ex. téléchargements de logiciel ou téléphonie Internet).
   - Si votre modèle de tarif correspond à un tarif en fonction du temps, activez le champ d'option **Désactivé**. Dans le champ **Couper automatiquement au bout de (secondes)**, entrez la durée d'inactivité au bout de laquelle la liaison doit être coupée (par ex. 60 secondes).
6) Paramétrez dans la zone **Paramètres QoS** les valeurs suivantes :
   a) Dans **Bande passante pour les liaisons descendantes** et **Bande passante pour les liaisons montantes** indiquez la bande passante en kbit/s pour le téléchargement ou le chargement que votre FAI vous a fournie.
   b) Si vous voulez utiliser en plus la téléphonie Internet, sélectionnez dans la liste déroulante **Gestion de la bande passante pour les connexions vocales** l'entrée **Liaison montante seulement** ou **Liaison montante et descendante** selon les besoins. Dans **Bande passante pour les connexions voix/fax (%)**, entrez en pourcentage quelle bande passante doit être réservée pour les liaisons voix et fax (valeur par défaut : 80%).
7) Cliquez sur **OK & Suivant**. Le système ouvre la fenêtre **Configurer le compte DynDNS**.

8) Si vous voulez utiliser VPN ou l'accès distant et que vous ne disposez pas d'une adresse IP publique statique, vous devez avoir demandé un compte DynDNS (par ex. auprès de dyndns.org) et le configurer.
   a) Si le fournisseur DynDNS de votre choix figure dans la liste déroulante **Nom de domaine**, sélectionnez-le à partir de la liste (par ex. dyndns.org).
   b) Si le fournisseur DynDNS de votre choix ne figure pas dans la liste déroulante **Nom de domaine**, cochez la case **Domaine défini par l'utilisateur**. Dans le champ **Nom de domaine**, indiquez le fournisseur DynDNS souhaité et dans le champ **Mise à jour-URL** l'URL de mise à jour du fournisseur DynDNS. La configuration de cette URL dépend du fournisseur DynDNS. En plus, les paramètres spécifiques client (en *caractères italiques* dans l'exemple) doivent être complétés.

      `http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
   c) Entrez le **Nom utilisateur** et le **Mot de passe** de votre compte DynDNS.
   d) Dans le champ **Nom d'hôte**, entrez le nom d'hôte que vous a attribué votre fournisseur DynDNS sans le nom de domaine, par ex. myhost. Votre nom de domaine complet est alors par ex. myhost.dyndns.org.
   e) Testez le compte DynDNS avec **Test connexion**.
   f) Une fois le test effectué avec succès, cliquez sur **OK**.
   g) Cliquez sur **OK & Suivant**.
9) Si vous disposez d'une adresse IP publique statique ou si vous ne voulez pas utiliser VPN ou l'accès distant, cliquez sur **Pas de DynDNS**.
10) Cliquez sur **OK & Suivant**.

5.7.5.4 Comment configurer l'accès Internet via le FAI PPPoE par défaut

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration de l'accès à Internet** de l'assistant **Installation de base**.

Vous disposez des données d'accès Internet suivantes de votre FAI :

Champ	Description	Valeur du FAI
Paramètres IP (uniquement pour adresse IP fixe)		
Adresse IP partenaire de la connexion PPP	Adresse IP du serveur de votre FAI	
Adresse IP locale de la connexion PPP	Adresse IP qui vous a été communiquée par le FAI pour l'accès Internet	
Authentification (par PAP ou CHAP). PAP n'est presque plus utilisé car l'authentification n'est pas cryptée.		
Nom d'utilisateur PPP	Nom de l'utilisation de la liaison PPP qui vous a été attribuée par le FAI.	
Mode d'authentification PAP	Mode d'authentification pour la connexion PPP via PAP : **PAP Client**, **PAP Host** ou **Non utilisé**.	

Champ	Description	Valeur du FAI
Mot de passe PAP	Mot de passe pour l'authentification par PAP qui vous a été attribué par le FAI	
Mode d'authentification CHAP	Mode d'authentification pour la connexion PPP via CHAP : **CHAP Client**, **CHAP Host**, **CHAP Client et Host** ou **Non utilisé**.	
Mot de passe CHAP	Mot de passe pour l'authentification par CHAP qui vous a été attribué par le FAI	
Paramètres QoS de l'interface		
Bande passante pour les liaisons descendantes	Valeur de bande passante totale en kbit/s pour le téléchargement à partir du FAI.	
Bande passante pour les liaisons montantes	Valeur de bande passante totale en kbit/s pour le transfert au FAI.	

Optionnel : Les données pour un compte DynDNS sont disponibles (nom, mot de passe, nom d'hôte, nom de domaine du provider DynDNS)

Étape par étape

1) Décochez la case **Pas d'accès Internet**.
2) Activez le bouton radio **DSL sur port WAN directement** et cliquez sur **OK & Suivant**.
3) Sélectionnez dans la liste déroulante **Utiliser le WAN comme** le type de FAI par défaut **Fournisseur-PPPoE**.
4) Dans la zone **Paramètres IP**, cochez la case **Paramètres IP** uniquement si une adaptation est demandée par le FAI. Dans les champs **Adresse IP partenaire de la connexion PPP**, **Adresse IP locale de la connexion PPP** et **Longueur de paquet de données maxi. (octets)**, entrez les valeurs que vous avez reçues de votre FAI. Sélectionnez dans la liste déroulante **Négociation de l'adresse IP** l'entrée **Utiliser l'adresse IP configurée**.
5) Sélectionnez une des deux options suivantes dans la zone **Paramètres de routeur** sous **Liaison permanente**, en fonction de votre modèle tarifaire :
   - Si votre modèle de tarif correspond à un forfait, activez le champ d'option **Activé**. Dans **Coupure forcée à (h:min)**, définissez l'heure à laquelle la connexion Internet doit être coupée (par ex. 01:30). A ce moment, il ne devrait pas y avoir d'échange de données avec Internet (par ex. téléchargements de logiciel ou téléphonie Internet).
   - Si votre modèle de tarif correspond à un tarif en fonction du temps, activez le champ d'option **Désactivé**. Dans le champ **Couper automatiquement au bout de (secondes)**, entrez la durée d'inactivité au bout de laquelle la liaison doit être coupée (par ex. 60 secondes).
6) Le paramétrage dans **Authentification** dépend de la nécessité d'authentifier ou non le FAI via PPP.
   - Authentification requise par le FAI : Assurez-vous que la case à cocher **Authentification PPP** est activée. Entrez comme nom d'utilisateur

PPP le nom de l'accès Internet du FAI. La norme habituelle est le mode d'authentification **Client CHAP**.

- Authentification non requise par le FAI : Assurez-vous que la case à cocher Authentification PPP est désactivée.

7) Si vous voulez utiliser NAT, vous devez, dans la zone **Traduction d'adresses** cocher la case **NAT** (cochée par défaut).

8) Dans la zone **Paramètres QoS de l'interface**, paramétrez les valeurs suivantes :

a) Dans **Bande passante pour les liaisons descendantes** et **Bande passante pour les liaisons montantes** indiquez la bande passante en kbit/s pour le téléchargement ou le chargement que votre FAI vous a fournie.

b) Si vous voulez utiliser en plus la téléphonie Internet, sélectionnez dans la liste déroulante **Gestion de la bande passante pour les connexions vocales** l'entrée **Liaison montante seulement** ou **Liaison montante et descendante** selon les besoins. Dans **Bande passante pour les connexions voix/fax (%)**, entrez en pourcentage quelle bande passante doit être réservée pour les liaisons voix et fax (valeur par défaut : 80%).

9) Cliquez sur **OK & Suivant**. Le système ouvre la fenêtre **Configurer le compte DynDNS**.

10) Si vous voulez utiliser VPN ou l'accès distant et que vous ne disposez pas d'une adresse IP publique statique, vous devez avoir demandé un compte DynDNS (par ex. auprès de dyndns.org) et le configurer.

a) Si le fournisseur DynDNS de votre choix figure dans la liste déroulante **Nom de domaine**, sélectionnez-le à partir de la liste (par ex. dyndns.org).

b) Si le fournisseur DynDNS de votre choix ne figure pas dans la liste déroulante **Nom de domaine**, cochez la case **Domaine défini par l'utilisateur**. Dans le champ **Nom de domaine**, indiquez le fournisseur DynDNS souhaité et dans le champ **Mise à jour-URL** l'URL de mise à jour du fournisseur DynDNS. La configuration de cette URL dépend du fournisseur DynDNS. En plus, les paramètres spécifiques client (en *caractères italiques* dans l'exemple) doivent être complétés.

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Entrez le **Nom utilisateur** et le **Mot de passe** de votre compte DynDNS.

d) Dans le champ **Nom d'hôte**, entrez le nom d'hôte que vous a attribué votre fournisseur DynDNS sans le nom de domaine, par ex. myhost. Votre nom de domaine complet est alors par ex. myhost.dyndns.org.

e) Testez le compte DynDNS avec **Test connexion**.

f) Une fois le test effectué avec succès, cliquez sur **OK**.

g) Cliquez sur **OK & Suivant**.

11) Si vous disposez d'une adresse IP publique statique ou si vous ne voulez pas utiliser VPN ou l'accès distant, cliquez sur **Pas de DynDNS**.

12) Cliquez sur **OK & Suivant**.

5.7.5.5 Comment configurer l’accès Internet via un FAI PPTP par défaut

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration de l’accès à Internet** de l’assistant **Installation de base**.

Vous disposez des données d’accès Internet suivantes de votre FAI :

Champ	Description	Valeur du FAI
Paramètres IP (uniquement pour adresse IP fixe)		
Adresse IP partenaire de la liaison PPP	Adresse IP du serveur de votre FAI	
Adresse IP locale de la connexion PPP	Adresse IP qui vous a été communiquée par le FAI pour l’accès Internet	
Paramètres PPTP		
Adresse IP locale de la connexion de contrôle	Adresse IP qui vous a été attribuée par le FAI pour la liaison PPTP. La valeur par défaut est : 10.0.0.140.	
Adresse IP partenaire de la connexion de contrôle	Adresse IP du serveur de votre FAI pour la connexion PPTP. La valeur par défaut est : 10.0.0.138.	
Masque de réseau partenaire pour la connexion de contrôle	Masque de réseau qui vous a été attribué par le FAI pour la liaison PPTP. La valeur par défaut est : 255.255.255.248.	
Authentification (par PAP ou CHAP). PAP n’est presque plus utilisé car l’authentification n’est pas cryptée.		
Nom d’utilisateur PPP	Nom de l’utilisation de la liaison PPP qui vous a été attribuée par le FAI.	
Mode d’authentification PAP	Mode d’authentification pour la liaison PPP par PAP : **Client PAP**, **Hôte PAP** ou **Non utilisé**.	
Mot de passe PAP	Mot de passe pour l’authentification par PAP qui vous a été attribué par le FAI	
Mode d’authentification CHAP	Mode d’authentification pour la liaison PPP par CHAP : **Client CHAP**, **Hôte CHAP**, **Client et hôte CHAP** ou **Non utilisé**.	
Mot de passe CHAP	Mot de passe pour l’authentification par CHAP qui vous a été attribué par le FAI	
Paramètres QoS de l’interface		
Bande passante pour les liaisons descendantes	Valeur de bande passante totale en kbit/s pour le téléchargement à partir du FAI.	

Champ	Description	Valeur du FAI
Bande passante pour les liaisons montantes	Valeur de bande passante totale en kbit/s pour le transfert au FAI.	

Option : les données pour un compte DynDNS sont disponibles (nom, mot de passe, nom d'hôte, nom de domaine du provider DynDNS)

Étape par étape

1) Décochez la case **Pas d'accès Internet**.
2) Cochez **DSL sur port WAN directement** et cliquez sur **OK & Suivant**.
3) Sélectionnez dans la liste déroulante **Utiliser le WAN comme** le type de FAI par défaut **Fournisseur-PPTP**.
4) Dans la zone **Paramètres IP**, cochez la case **Paramètres IP** uniquement si une adaptation est demandée par le FAI. Dans les champs **Adresse IP partenaire de la connexion PPP**, **Adresse IP locale de la connexion PPP** et **Longueur de paquet de données maxi. (octets)**, entrez les valeurs que vous avez reçues de votre FAI. Sélectionnez dans la liste déroulante **Négociation de l'adresse IP** l'entrée **Utiliser l'adresse IP configurée**.
5) Entrez dans la zone **Paramètres PPTP** les valeurs que vous avez reçues de votre FAI.
6) Si vous avez un forfait horaire comme modèle tarifaire, cochez la case **Mode Short-Hold**. Entrez dans **Durée Short-Hold (s)** le délai d'inactivité au bout duquel la liaison doit être coupée (par ex. 60 secondes).
7) Le paramétrage dans **Authentification** dépend de la nécessité d'authentifier ou non le FAI via PPP.
   - L'authentification est demandée par le FAI : vérifiez que la case **Authentification PPP** est bien cochée. Entrez comme nom d'utilisateur PPP le nom de l'accès Internet du FAI. Effectuez les paramétrages PAP et CHAP tels que vous les avez reçus de votre FAI.
   - L'authentification n'est pas demandée par le FAI : vérifiez que la case Authentification PPP est bien décochée.
8) Si vous voulez utiliser NAT, vous devez, dans la zone **Traduction d'adresses** cocher la case **NAT** (cochée par défaut).
9) Dans la zone **Paramètres QoS de l'interface**, paramétrez les valeurs suivantes :
   a) Dans **Bande passante pour les liaisons descendantes** et **Bande passante pour les liaisons montantes** indiquez la bande passante en kbit/s pour le téléchargement ou le chargement que votre FAI vous a fournie.
   b) Si vous voulez utiliser en plus la téléphonie Internet, sélectionnez dans la liste déroulante **Gestion de la bande passante pour les connexions vocales** l'entrée **Liaison montante seulement** ou **Liaison montante et descendante** selon les besoins. Dans **Bande passante pour les connexions voix/fax (%)**, entrez en pourcentage quelle bande passante doit être réservée pour les liaisons voix et fax (valeur par défaut : 80%).
10) Cliquez sur **OK & Suivant**. Le système ouvre la fenêtre **Configurer le compte DynDNS**.

11) Si vous voulez utiliser VPN ou l’accès distant et que vous ne disposez pas d’une adresse IP publique statique, vous devez avoir demandé un compte DynDNS (par ex. auprès de dyndns.org) et le configurer.

a) Si le fournisseur DynDNS de votre choix figure dans la liste déroulante **Nom de domaine**, sélectionnez-le à partir de la liste (par ex. dyndns.org).

b) Si le fournisseur DynDNS de votre choix ne figure pas dans la liste déroulante **Nom de domaine**, cochez la case **Domaine défini par l’utilisateur**. Dans le champ **Nom de domaine**, indiquez le fournisseur DynDNS souhaité et dans le champ **Mise à jour-URL** l’URL de mise à jour du fournisseur DynDNS. La configuration de cette URL dépend du fournisseur DynDNS. En plus, les paramètres spécifiques client (en *caractères italiques* dans l’exemple) doivent être complétés.

`http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`

c) Entrez le **Nom utilisateur** et le **Mot de passe** de votre compte DynDNS.

d) Dans le champ **Nom d’hôte**, entrez le nom d’hôte que vous a attribué votre fournisseur DynDNS sans le nom de domaine, par ex. myhost. Votre nom de domaine complet est alors par ex. myhost.dyndns.org.

e) Testez le compte DynDNS avec **Test connexion**.

f) Une fois le test effectué avec succès, cliquez sur **OK**.

g) Cliquez sur **OK & Suivant**.

12) Si vous disposez d’une adresse IP publique statique ou si vous ne voulez pas utiliser VPN ou l’accès distant, cliquez sur **Pas de DynDNS**.

13) Cliquez sur **OK & Suivant**.

5.7.5.6 Comment configurer l'accès à Internet via un routeur Internet externe sur le LAN avec un port WAN dédié à l'ITSP

Conditions préalables

Vous êtes dans la fenêtre **Configurer un accès à Internet** de l'assistant d’ **installation de base**.

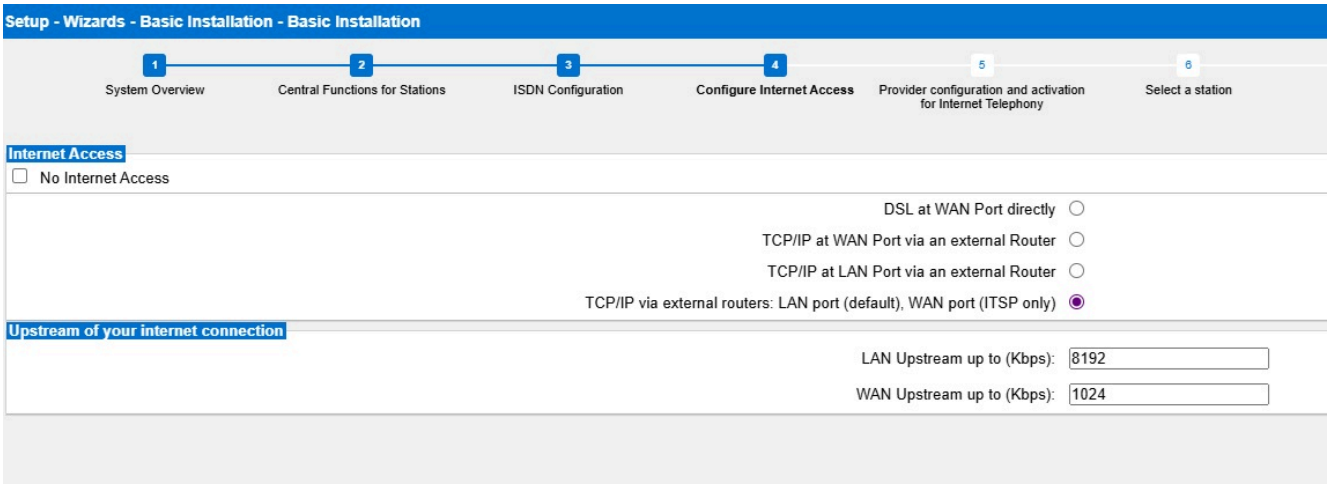
Cette fonctionnalité ne s'applique qu'aux ITSP qui n'exigent pas l'utilisation de STUN dans les paramètres du fournisseur.

Il n'est pas possible de connecter simultanément deux ITSP identiques (avec le même registraire/proxy) via LAN et WAN.

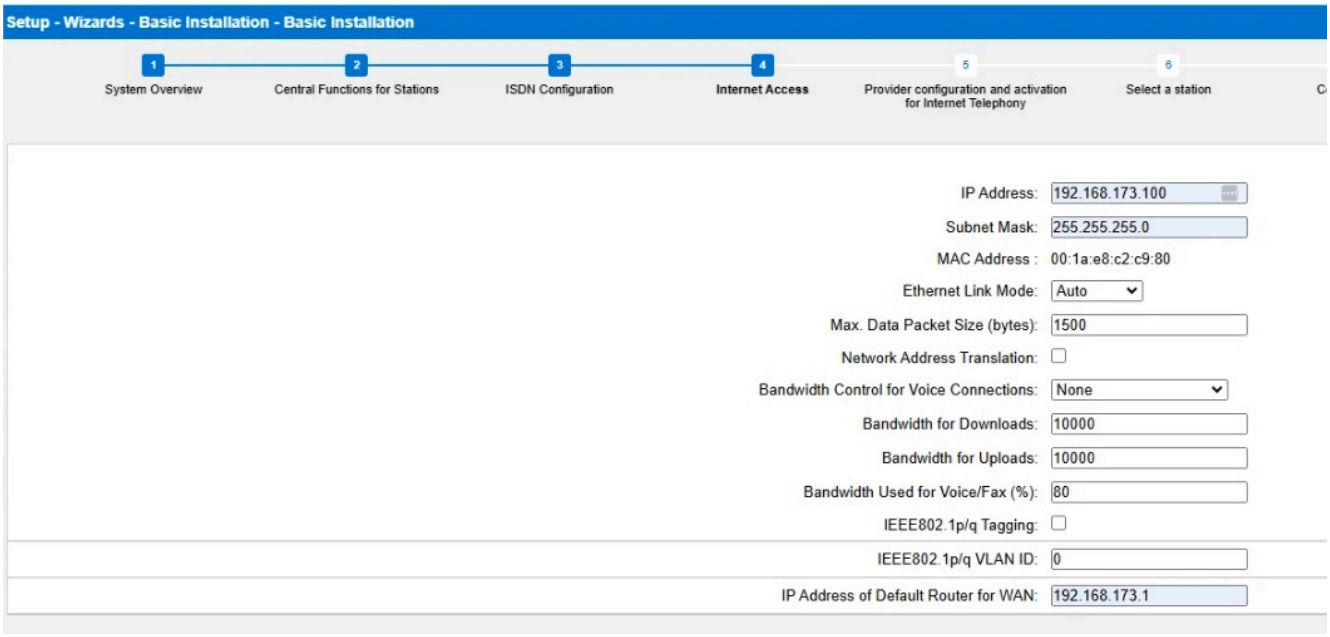
Étape par étape

1) Décochez la case **Pas d’accès Internet**.

2) Activez le bouton radio **TCP/IP via des routeurs externes : Port LAN (par défaut), port WAN ITSP uniquement**.



3) Configurez la valeur maximale en Kbps en amont pour chaque interface dans **LAN Upstream jusqu'à (Kbps)** et **WAN Upstream jusqu'à (Kbps)**.
4) Cliquez sur **OK & Suivant**.
5) Entrer la configuration IP du port WAN et en plus l'adresse IP du routeur par défaut pour le port WAN.



6) Cliquez sur **OK & Suivant**.

5.7.5.7 Comment désactiver l’accès Internet

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration de l’accès à Internet** de l’assistant **Installation de base**.

Étape par étape

1) Laissez cochée la case **Pas d'accès Internet**.
2) Cliquez sur **OK & Suivant**.

5.7.6 Téléphonie Internet

Dans la fenêtre **Configuration et activation du fournisseur pour la téléphonie Internet**, vous configurez la téléphonie Internet. Vous pouvez configurer des fournisseurs de service de téléphonie sur Internet (ITSP - Internet Telephony Service Provider) préconfigurés ou nouveaux. Pour chaque fournisseur ITSP, vous pouvez configurer un ou plusieurs comptes. Au maximum 8 fournisseurs ITSP peuvent être actifs simultanément.

Vous disposez des possibilités suivantes :

- **Configurer un ITSP prédéfini**

  Vous pouvez utiliser des modèles ITSP prédéfinis. Pour cela, on entre dans ce modèle les propres données d'accès et numéros d'appel et on les active ensuite.
- **Configurer un nouvel ITSP**

  Vous pouvez aussi ajouter et activer de nouveaux ITSP.

  Configurer un nouvel ITSP n'est nécessaire que dans des cas rares et demande beaucoup de temps. C'est pourquoi cette possibilité n'est pas décrite dans la première installation. Vous trouverez des informations plus précises au chapitre Configuration d'un ITSP.
- **Désactiver la téléphonie Internet**

  Vous pouvez désactiver la téléphonie Internet.

Remarque :

Vous trouverez des exemples de configuration sur Internet dans **Unify Experts Wiki** sous *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Affectation des numéros de téléphone ITSP

- Dans un **raccordement d'installation téléphonie Internet**, l'ITSP fournit des numéros de téléphone individuels, par ex. 70005555, 70005556, ... Ces numéros de téléphone individuels sont ensuite attribués manuellement aux numéros internes des abonnés.
- Dans un **raccordement d'installation téléphonie Internet**, l'ITSP fournit un groupe de numéros de téléphone (plage de numéros de téléphone), par ex.(+49) 89 7007-100 à (+49) 89 7007-147. Les numéros de téléphone de ce groupe de numéros sont ensuite attribués manuellement aux numéros internes des abonnés.

Les deux types de raccordement peuvent être combinés.

Autre variante : pour les deux types de raccordement, les numéros ITSP peuvent être inscrits comme numéros SDA des abonnés lors de la configuration des stations.

Numéro interne	Nom	SDA
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Les numéros de téléphone ITSP résultent donc des numéros d'installation créés (par ex. indicatif national 49) et des numéros de sélection directe à l'arrivée au format long qui ont été inscrits. Cela a des avantages pour l'évaluation de la numérotation et la gestion des appels dans une interconnexion de réseaux. Ainsi, le raccordement ITSP permet par ex. la sélection en direction d'un autre noeud.

Un autre raccordement réseau via RNIS n'est dans ce cas possible qu'avec certaines restrictions (utile toutefois pour appels d'urgence).

5.7.6.1 Comment configurer un ITSP prédéfini

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration et activation du fournisseur pour la téléphonie Internet** de l’assistant **Installation de base**.

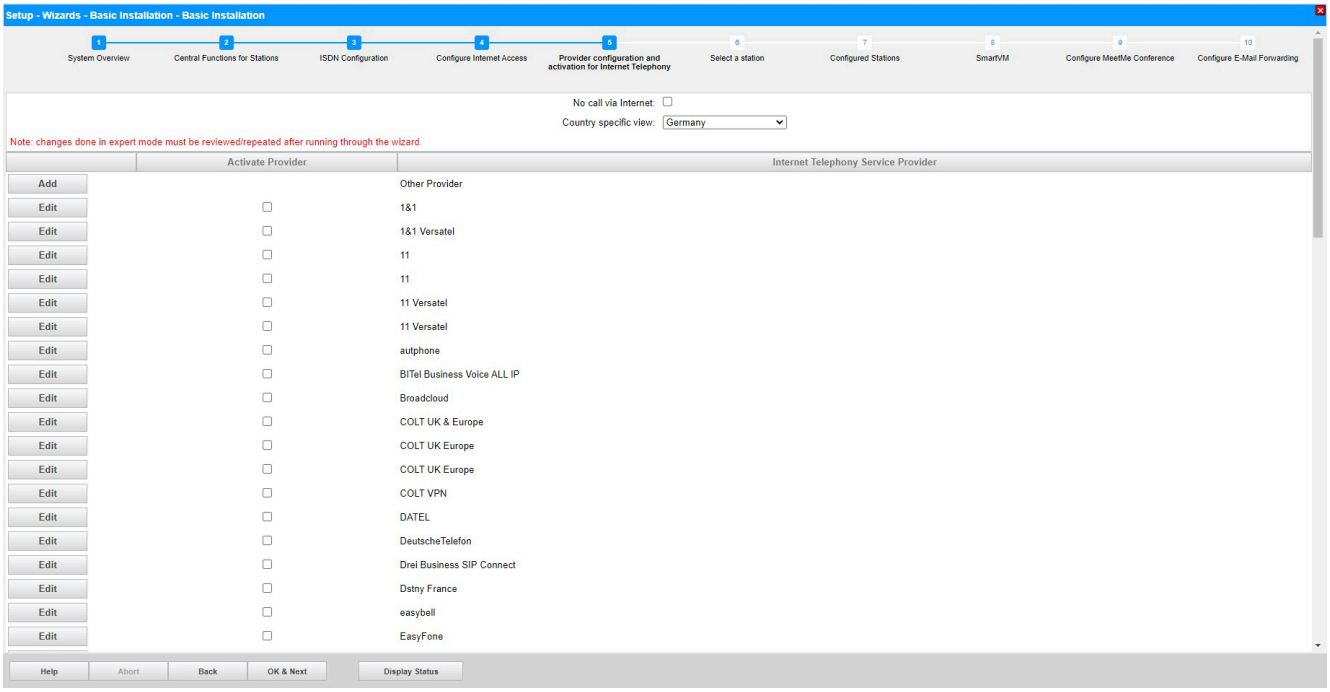
La connexion à Internet est opérationnelle.

Vous disposez des données d’accès de téléphonie Internet de votre ITSP (par ex. ID utilisateur, mot de passe, numéros d’abonné de la téléphonie Internet).

Étape par étape

1) Décochez **Pas de téléphonie par Internet**. Le système affiche une liste des ITSP disponibles, en fonction du pays. La liste contient les

ITSP prédéfinis pour le pays sélectionné et éventuellement les ITSP nouvellement ajoutés.



2) Si vous souhaitez modifier le pays présélectionné, sélectionnez le pays souhaité dans la liste **Affichage spécifique du pays**. Les ITSP possibles pour le pays sélectionné s'affichent.

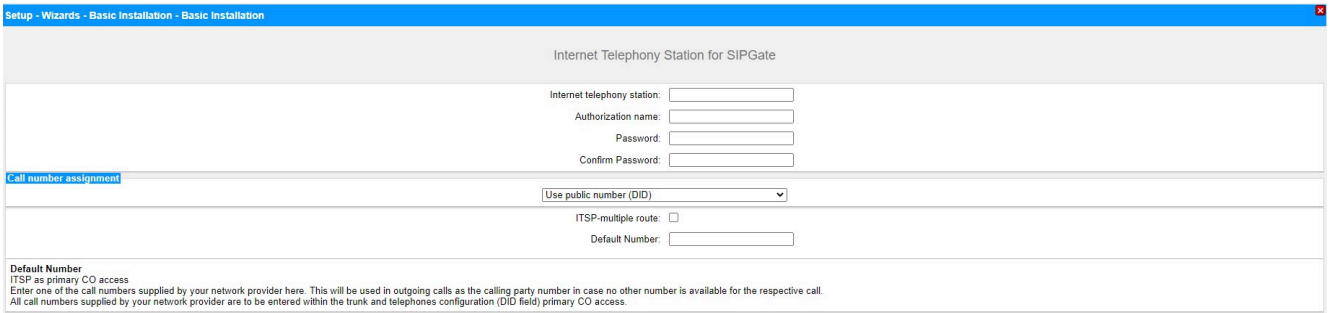
3) Si nécessaire, cliquez sur **Afficher le statut** pour savoir quels ITSP sont déjà activés et quels abonnés téléphonie Internet sont déjà inscrits sur les ITSP. Vous pouvez activer 8 ITSP au maximum. Pour finir, cliquez sur **OK**.

4) Dans la ligne du ITSP correspondant, cliquez sur **Modifier** afin d'activer un ITSP prédéfini.

5) Cochez **Activer le fournisseur**.

6) Cliquez sur **OK & Suivant**.

7) Cliquez sur **Ajouter** pour configurer vos comptes ITSP avec les numéros correspondants de téléphonie sur Internet. Les champs affichés ensuite sont fonction du fournisseur d'accès.



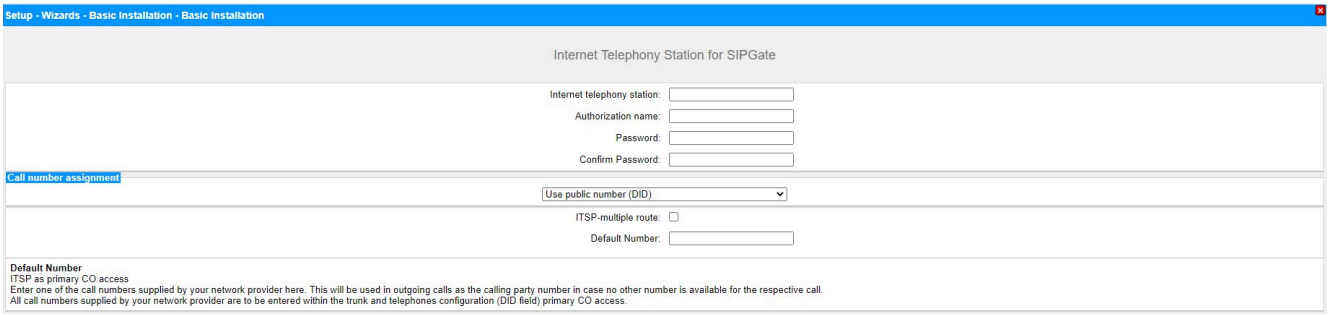
8) Dans le champ **Abonné de téléphonie Internet** entrez les données d'accès de votre compte. Les données ont été fournies par votre ITSP. Suivant l'ITSP, des désignations différentes sont utilisées, par ex. : Utilisateur SIP, ID SIP, etc.

9) Entrez dans **Nom d'autorisation** le nom d'autorisation. Les données ont été fournies par votre ITSP. Si vous n'avez pas reçu de nom d'autorisation, entrez les mêmes données que dans **Abonné de téléphonie Internet**.

10) Dans les champs **Nouveau mot de passe** et **Répéter le mot de passe**, entrez le mot de passe que vous avez reçu du ITSP. Suivant l'ITSP, des désignations différentes sont utilisées, par ex. : Mot de passe, mot de passe SIP, etc.

11) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 1 :

Numéro de téléphone public (SDA) : les numéros de téléphone Internet de votre raccordement d'abonné ou de votre raccordement d'installation Internet ne sont pas inscrits ici dans la configuration ITSP, mais dans la configuration de l'abonné, dans les champs **SDA**.



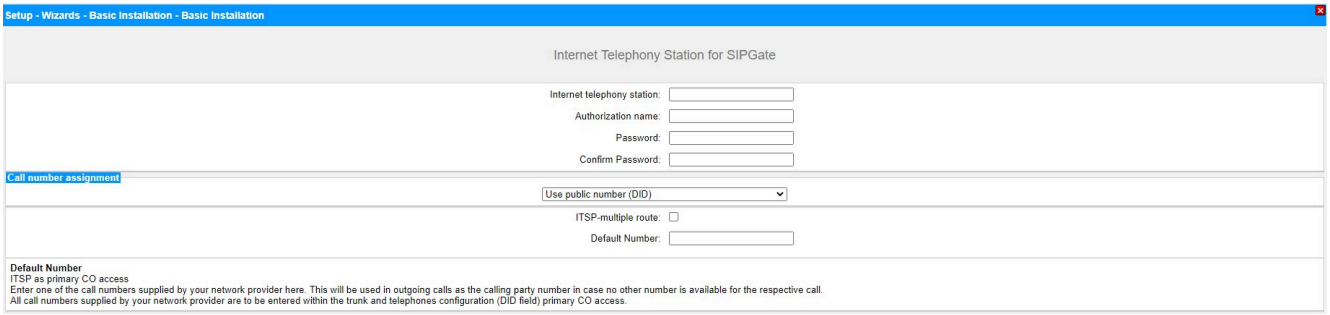
a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **N° de téléphone public (SDA)**.

b) Sous **Numéro par défaut**, entrez le numéro de téléphone à utiliser pour les appels sortants lorsqu'aucun numéro SDA n'est disponible.

c) Si votre ITSP supporte la fonctionnalité "Mobile Extension (MEX)", entrez dans **Numéro MEX** le numéro MEX fourni par l'ITSP (8 positions, chiffres uniquement).

12) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 2 :

Utiliser numéro interne (n° appel) / entrées individuelles : Vous disposez d'un raccordement d'abonné de téléphonie Internet et vous avez reçu des numéros individuels comme numéros de téléphonie Internet (par ex. 70005555, 70005556,...). Vous affectez ensuite ces numéros individuels aux numéros internes des abonnés.



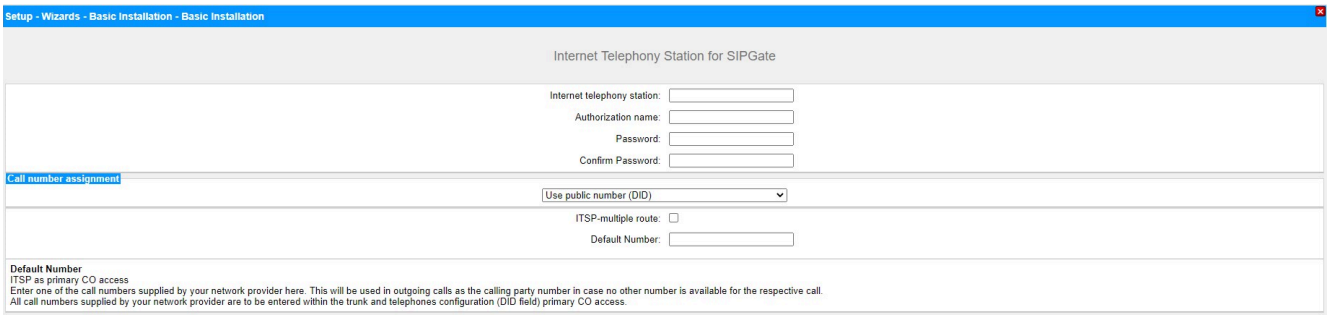
a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **Utiliser le numéro interne (N° tél)/entrées individuelles**.

b) Dans la zone **Téléphonie Internet-Numéros des abonnés**, dans le champ situé à côté du bouton **Ajouter**, saisissez un numéro d'abonné de téléphonie Internet communiqué par le ITSP et cliquez sur **Ajouter**.

c) Si vous souhaitez attribuer d'autres numéros de téléphonie Internet au compte, répétez l'étape b).

13) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 3 :

Utiliser numéro interne (N° appel) / plage d'entrées : Vous disposez d'une connexion Téléphonie Internet et, comme numéros de téléphonie Internet, d'une plage de numéros, par ex. (+49) 89 7007-100 à (+49) 89 7007-147. Vous affectez ensuite les numéros de la plage aux numéros internes des abonnés.



a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **Utiliser le numéro interne (N° tél)/Entrée individuelle**.

b) Dans **Numéro de l'installation (préfixe)**, entrez le numéro de l'installation.

c) Entrez la série de numéros SDA souhaitée pour la station de téléphonie Internet dans les champs 'de' **et** 'à **' après** Bande de numérotation directe à l'arrivée. Par défaut, la valeur 100 - 147 est entrée.

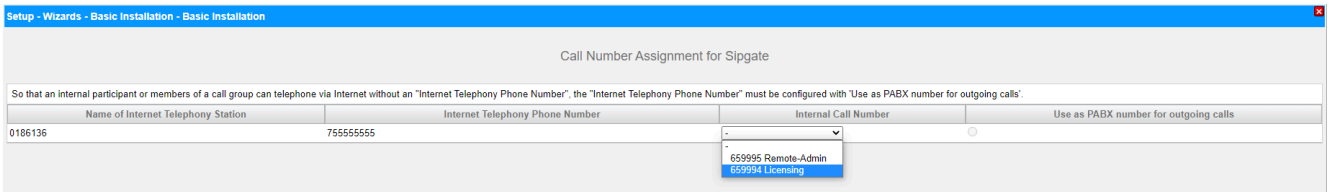
14) Cliquez sur **OK & Suivant**.

15) Si vous souhaitez configurer d'autres comptes avec les numéros d'abonnés de téléphonie Internet correspondants, répétez les étapes 7 à 14.

16) Cliquez sur **OK & Suivant**. Vous visualisez une vue d'ensemble indiquant la correspondance entre les numéros de téléphonie Internet et les comptes.

17) Affectez respectivement le numéro interne d'un abonné à tous les numéros de téléphonie Internet.

Cette étape est supprimée si vous avez choisi la possibilité 1 pour l'affectation des numéros de téléphonie Internet. Dans ce cas, l'affectation est effectuée lors de la configuration des stations (c'est-à-dire des téléphones et des abonnés) dans le champ **SDA**.



a) Dans la ligne correspondante de la liste déroulante **Numéro interne**, sélectionnez un numéro de téléphone interne.

b) Si les abonnés sans numéro de téléphone Internet ou les membres d'un groupe d'appel doivent être autorisés à effectuer des appels externes via Internet, le bouton radio **Utiliser comme numéro PABX pour les appels sortants** doit être activé. La case doit être cochée uniquement pour un seul numéro de téléphonie Internet.

18) Cliquez sur **OK & Suivant**. Vous voyez de nouveau la liste des ITSP prédéfinis et nouveaux. Les ITSP activés sont cochés dans la colonne

Activer le fournisseur. **Redémarrage ITSP** vous permet, en cas de problèmes de liaison, de vous enregistrer de nouveau lorsque les ITSP sont déjà activés.

19) Cliquez sur **OK & Suivant**.

20) Dans le champ **Flux ascendant jusqu'à (kbit/s)** entrez la valeur de la vitesse du flux ascendant de votre connexion Internet. A ne pas confondre avec la vitesse de téléchargement !

Remarque : Dans le champ **Nombre de communications téléphoniques Internet simultanées**, le système indique le nombre maximal de communications téléphoniques Internet simultanées possibles. Si la qualité de la communication se détériore en raison de la charge du réseau, vous devez réduire ce nombre.

Pour plus d'informations sur le nombre d'appels Internet simultanés, veuillez vous référer à Limitation du nombre de communications simultanées via ITSP à la page 775.

---

21) Cliquez sur **OK & Suivant**.

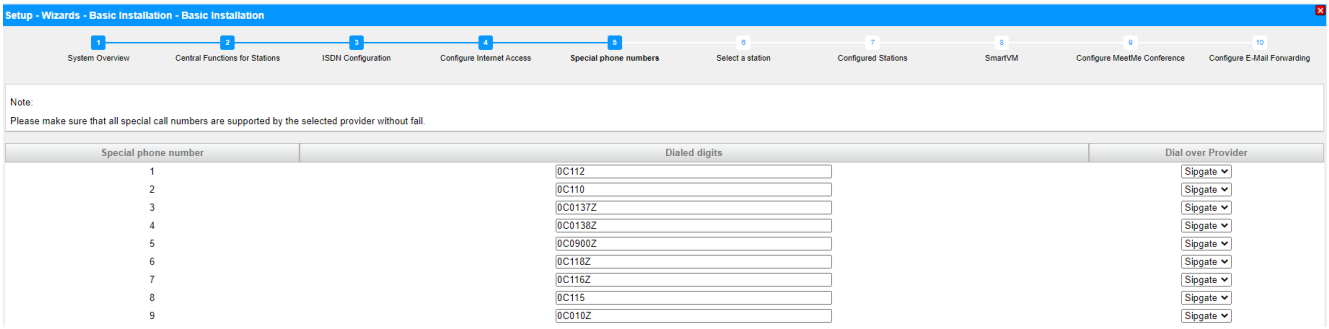
22) Si, lors du paramétrage de votre accès Internet, vous n'avez pas encore activé la liaison permanente, vous pouvez le faire ici. Sans liaison permanente, vous ne pouvez pas recevoir d'appels via Internet. Si la liaison permanente est déjà paramétrée, les champs décrits dans a) à c) ne sont pas visibles.

a) Dans **Liaison permanente**, activez le champ d'option **A l'attention de**.

b) Dans le champ **Coupure forcée à (heure:min)**, définissez l'heure à laquelle la connexion Internet doit être coupée (par ex. 04:59).

c) Cliquez sur **OK & Suivant**.

23) Entrez dans la colonne **Chiffres composés** les numéros spéciaux souhaités.



Les entrées de numéro de station suivantes sont valides :

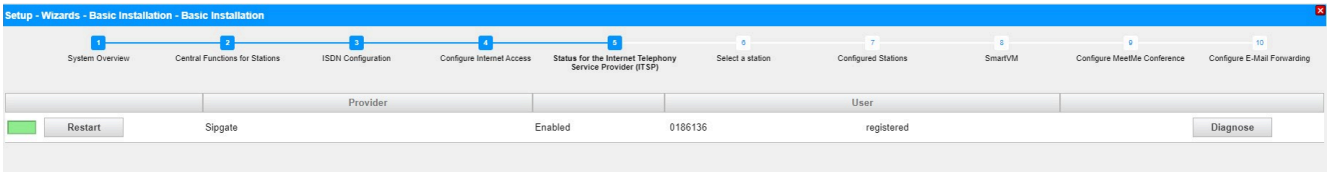
- 0 à 9: chiffres autorisés
- -: Séparateur de champ
- X : Chiffre au choix entre 0 et 9
- N : Chiffre au choix entre 2 et 9
- Z : Un ou plusieurs chiffres suivent jusqu'à la fin de la numérotation
- C : Tonalité d'invitation à numéroter simulée (peut être entrée max. trois fois)

24) Choisissez dans la colonne **Appeler par le fournisseur** si le numéro spécial doit être composé par RNIS ou par un ITSP. Seuls les ITSP activés sont affichés.

Remarque : Assurez-vous que les numéros d'urgence puissent toujours être composés. S'il est nécessaire de sélectionner des numéros d'urgence via un fournisseur de téléphonie sur Internet (ITSP), le fournisseur doit supporter ce service.

---

25) Cliquez sur **OK & Suivant**. Le système vous indique l'état du ITSP.



En vert figurent les ITSP qui sont configurés et sur lesquels vous êtes déjà enregistré.

En orange figurent les ITSP qui sont configurés et sur lesquels vous n'êtes pas encore enregistré.

26) Cliquez sur **Suivant** puis sur **Terminer**.

5.7.6.2 Comment désactiver la téléphonie Internet

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration et activation du fournisseur pour la téléphonie Internet** de l'assistant **Installation de base**.

Étape par étape

1) Cochez **Pas de téléphonie par Internet**.
2) Ensuite, cliquez deux fois sur **OK & Suivant**.

5.7.7 Abonnés

Dans les fenêtres **Sélectionner un abonné/groupe - ...** configurez les abonnés raccordé au système de communication.

Pour cela, procédez comme indiqué ci-après.

1) Configurer les abonnés RNIS

   Les abonné RNIS sont par ex. des téléphones RNIS ou des fax RNIS. Vous ne pouvez configurer les abonnés RNIS que si vous avez configuré une interface S_0 comme connexion S_0.
2) Configurer les abonnés analogiques

   Les abonnés analogiques sind par ex. des téléphones analogiques ou des fax analogiques.
3) Configurer l'abonné UP0

   Les abonné UP0 sont des téléphones systèmes comme OpenStage 60 T.

4) Configurer les abonnés DECT

   Les abonnés DECT sont des réléphones Cordless/DECT. Vous pouvez uniquement configurer les abonnés DECT lorsque une ou plusieurs stations de base Cordless sont raccordées et que les téléphone DECT y sont connectés. La configuration de la station de base est effectuée avec Manager E. Pour des informations plus précises sur la configuration cordless, voir Configuration de la solution cordless intégrée

5) Configurer les abonnés IP et SIP

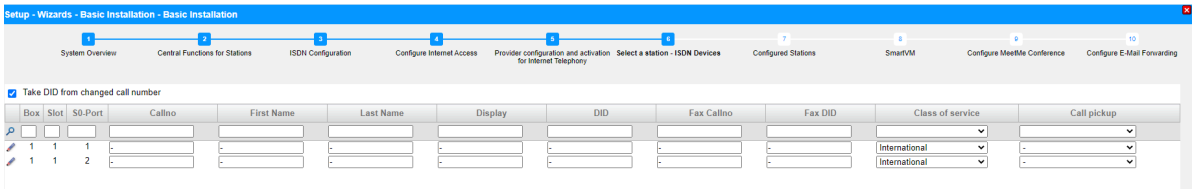
   Les abonnés IP et les abonnés SIP sont par ex. des téléphones LAN ou WLAN.

5.7.7.1 Comment configurer les abonnés RNIS

Conditions préalables

Vous vous trouvez dans la fenêtre **Sélectionner l'abonné - Terminaux ISDN** de l'assistant **Installation de base**.

Les raccordements S_0 auxquels sont connectés les téléphones RNIS doivent être paramétrés en tant que raccordement S_0 internes.



Étape par étape

1) Si le numéro SDA de l'abonné doit être différent de son numéro, entrez dans la ligne de l'abonné souhaité dans **SDA** le numéro SDA de l'abonné :

   - Uniquement pour le raccordement système :

     Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
   - uniquement pour un raccordement multiposte :

     A partir de la liste déroulante, sélectionnez un numéro MSN. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
   - pour le raccordement système et un raccordement multiposte :

     Sélectionnez dans le champ souhaité par la liste déroulante l'entrée **xxx - modifiable** (xxx correspond au numéro interne) et entrez le numéro SDA à l'aide du clavier ou sélectionnez un MSN dans la liste déroulante.

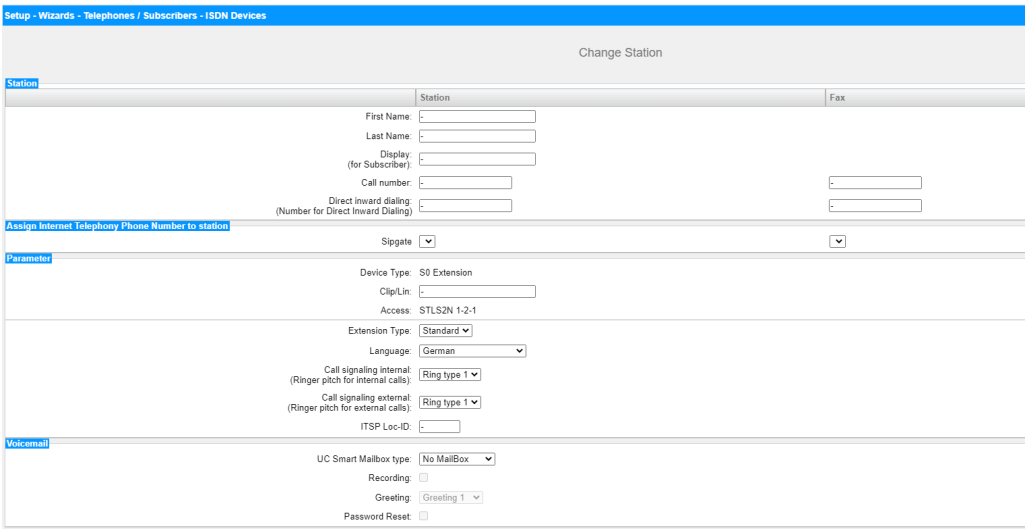
2) A la ligne de l'abonné souhaité, entrez dans **Numéro de téléphone** le numéro de téléphone interne de l'abonné. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

3) Entrez dans la ligne de l'abonné souhaité sous **Nom** un nom, sous la forme `Nom de famille, Prénom` ou `Prénom Nom de famille`.

Remarque : Le nom peut comporter jusqu'à 16 caractères, mais ne doit contenir ni inflexions ni caractères spéciaux.

---

4) Si une boîte Fax doit être paramétrée pour l'abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme indiqué ci-après :
   a) Dans la ligne de l'abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l'utilisateur pourra recevoir des messages Fax internes.
   b) Si un numéro SDA doit être configuré pour la boîte Fax, saisissez dans la ligne de l'abonné souhaité, champ **SDA Fax**, le numéro de fax externe sous lequel l'abonné pourra recevoir des messages Fax externes.
5) A la ligne de l'abonné souhaité, sélectionnez dans la liste déroulante **Classe de discrimination** le groupe de classe de discrimination souhaité.
6) Pour intégrer l'abonné dans un groupe d'interception, sélectionnez un groupe d'interception dans la ligne de l'abonné souhaité de la liste déroulante **Interception**.
7) N'effectuez les paramétrages décrits dans ce point que si cela est nécessaire :
   a) Dans la ligne de l'abonné RNIS souhaité, cliquez sur l'icône **Modifier**.



   b) Dans **Clip/Lin**, entrez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant et le numéro

interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

c) Dans la liste déroulante **Type d'abonné**, sélectionnez le type de terminal RNIS.

d) Sélectionnez un numéro SDA dans une liste déroulante de la zone **SDA pour la téléphonie Internet**. Pour chaque ITSP actif, une liste déroulante s'affiche.

Remarque : Le champ **SDA pour la téléphonie Internet** n'est pas visible lorsque la téléphonie Internet n'est pas paramétrée ou lorsque aucun fournisseur de services de téléphonie sur Internet n'est activé.

e) Depuis la liste déroulante **Signalisation des appels internes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres abonnés internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

f) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (Par défaut Type de sonnerie 1).

g) Cliquez sur **OK & Suivant**.

h) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonnés, voir Abonnés > Abonnés > Paramètres d'abonné.

i) Cliquez sur **OK & Suivant**.

8) Si vous souhaitez paramétrer d'autres abonnés RNIS, cliquez sur **Enregistrer les données** et répétez les points 1 à 7.

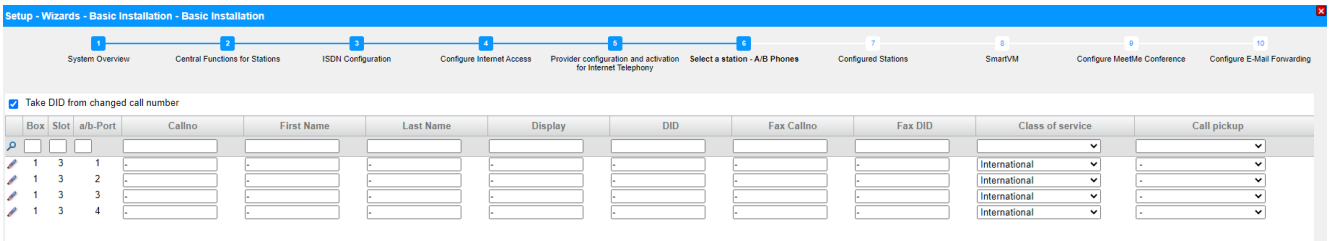
9) Cliquez sur **OK & Suivant**.

5.7.7.2 Comment configurer les abonnés analogiques

Conditions préalables

Vous vous trouvez dans la fenêtre **Sélectionner l'abonné - Terminaux A/B** de l'assistant **Installation de base**.

Il existe une carte mère ou un module avec interfaces analogiques.



Étape par étape

1) Si le numéro SDA de l'abonné doit être différent de son numéro d'appel, saisissez un numéro SDA dans le champ **SDA** de la ligne de l'abonné concerné :

- Uniquement pour le raccordement système :

  Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
- uniquement pour un raccordement multiposte :

  À partir de la liste déroulante, sélectionnez un numéro MSN. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
- pour le raccordement système et un raccordement multiposte :

  Dans la liste déroulante du champ souhaité, sélectionnez l'entrée **xxx - modifiable** (xxx correspondant au numéro interne) et saisissez le numéro SDA à l'aide du clavier ou sélectionnez un MSN (Multiple Subscriber Number, numéro de téléphone multiple).

2) Sur la ligne de l'abonné souhaité, saisissez le numéro de téléphone interne de l'abonné dans **Numéro de téléphone**. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

3) Dans le champ **Nom** de la ligne de l'abonné souhaité, saisissez un nom au format `Nom de famille, Prénom` ou `Prénom Nom de famille`.

Remarque : Le nom peut comporter jusqu'à 16 caractères, mais ne doit contenir ni inflexions ni caractères spéciaux.

---

4) Si vous souhaitez configurer une boîte Fax pour l'abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme suit :

a) Dans la ligne de l'abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l'utilisateur pourra recevoir des messages Fax internes.

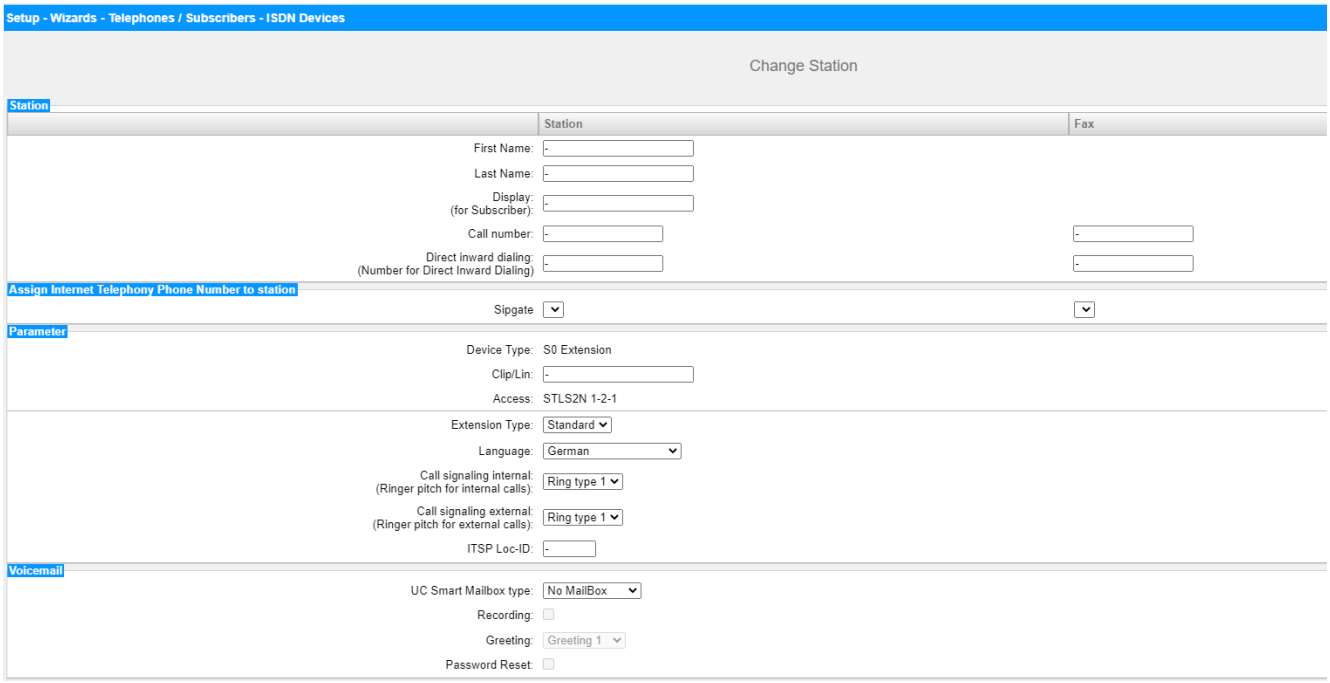
b) Si un numéro SDA doit être configuré pour la boîte Fax, entrez dans la ligne de l'abonné souhaité, champ **SDA Fax**, le numéro de fax externe souhaité sous lequel l'abonné pourra recevoir des messages Fax externes.

5) Dans la liste déroulante **Classe de service** de la ligne de l'abonné concerné, sélectionnez le groupe de classe de service souhaité.

6) Pour intégrer l'abonné à un groupe d'interception, sélectionnez un groupe dans la liste déroulante **Interception** de la ligne de l'abonné souhaité.

7) N'effectuez les paramétrages décrits dans ce point que si cela est nécessaire :

a) Sur la ligne de l'abonné analogique souhaité, cliquez sur l'icône **Modifier**.



b) Dans le champ **Clip/Lin**, saisissez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant, et le numéro interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

---

c) Sélectionnez dans la liste déroulante **Type d'abonné** le type de terminal analogique (par ex. fax).

d) Sélectionnez un numéro SDA dans une liste déroulante de la zone **SDA pour la téléphonie Internet**. Pour chaque ITSP actif, une liste déroulante s'affiche.

Remarque : Le champ **SDA pour la téléphonie Internet** n'est pas visible lorsque la téléphonie Internet n'est pas configurée ou lorsqu'aucun fournisseur de services de téléphonie sur Internet n'est activé.

---

e) Dans la liste déroulante **Signalisation des appels internes**, affectez à l'abonné l'une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres abonnés

internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

f) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

g) Cliquez sur **OK & Suivant**.

h) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonné, voir Abonnés > Abonnés > Paramètres d'abonné.

i) Cliquez sur **OK & Suivant**.

8) Si vous souhaitez paramétrer un autre abonné analogique, cliquez sur **Enregistrer les données** et répétez les points 1 à 7.

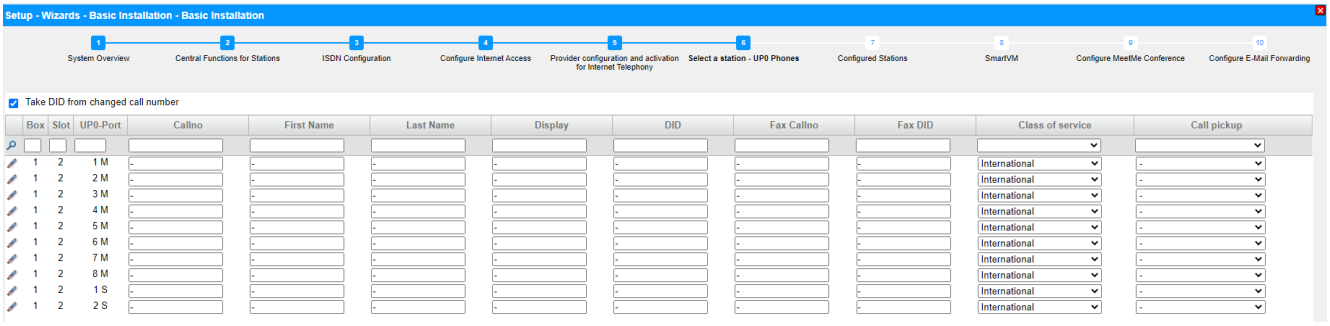
9) Cliquez sur **OK & Suivant**.

5.7.7.3 Comment configurer les abonnés UP0

Conditions préalables

Vous vous trouvez dans la fenêtre **Sélectionner l'abonné - Abonnés UP0** de l'assistant **Installation de base**.

Il existe une carte mère ou un module avec interfaces UP0.



Étape par étape

1) Si le numéro SDA de l'abonné doit être différent de son numéro d'appel, saisissez un numéro SDA dans le champ **SDA** de la ligne de l'abonné concerné :

- Uniquement pour le raccordement système :

  Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
- uniquement pour un raccordement multiposte :

  À partir de la liste déroulante, sélectionnez un numéro MSN. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
- pour le raccordement système et un raccordement multiposte :

  Dans la liste déroulante du champ souhaité, sélectionnez l'entrée **xxx - modifiable** (xxx correspondant au numéro interne) et saisissez le numéro SDA à l'aide du clavier ou sélectionnez un MSN (Multiple Subscriber Number, numéro de téléphone multiple).

2) Sur la ligne de l'abonné souhaité, saisissez le numéro de téléphone interne de l'abonné dans **Numéro de téléphone**. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.
3) Dans le champ **Nom** de la ligne de l'abonné souhaité, saisissez un nom au format `Nom de famille, Prénom` ou `Prénom Nom de famille`.

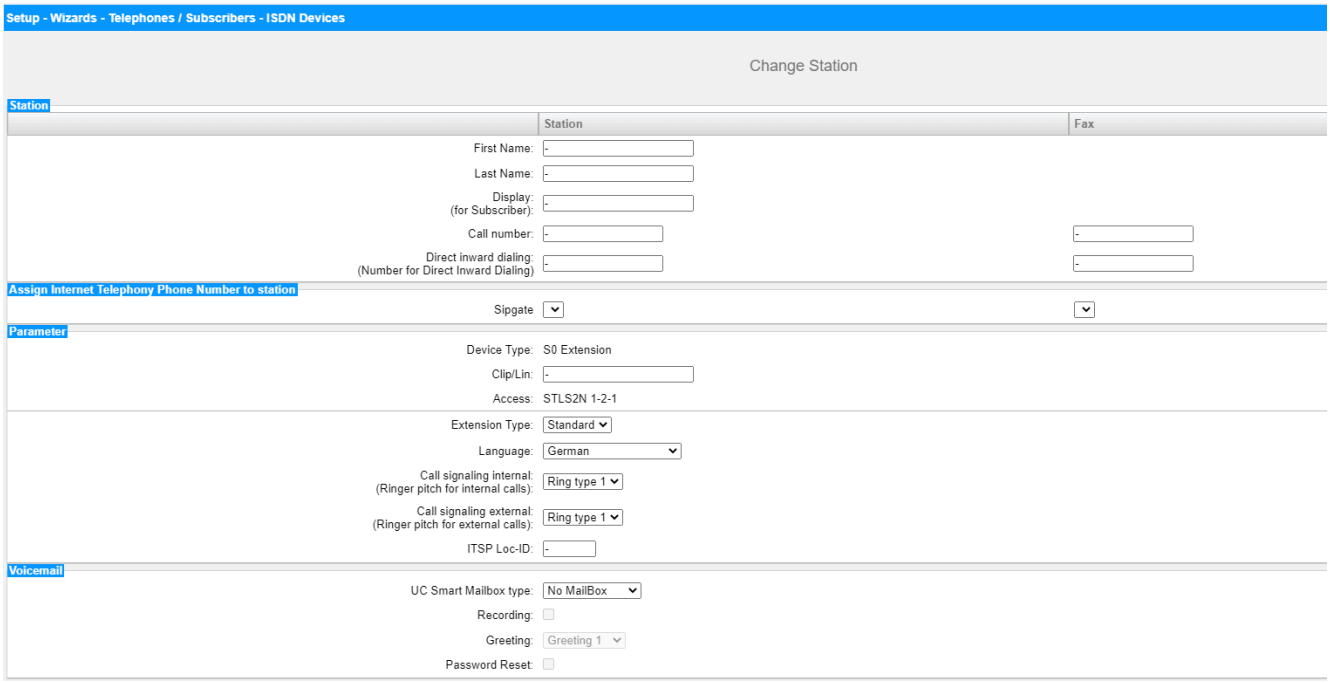
Remarque : Le nom peut comporter jusqu'à 16 caractères, mais ne doit contenir ni inflexions ni caractères spéciaux.

---

4) Si vous souhaitez configurer une boîte Fax pour l'abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme suit :
   a) Dans la ligne de l'abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l'utilisateur pourra recevoir des messages Fax internes.
   b) Si un numéro SDA doit être configuré pour la boîte Fax, saisissez dans la ligne de l'abonné souhaité, champ **SDA Fax**, le numéro de fax externe sous lequel l'abonné pourra recevoir des messages Fax externes.
5) Dans la liste déroulante **Classe de service** de la ligne de l'abonné concerné, sélectionnez le groupe de classe de service souhaité.
6) Pour intégrer l'abonné à un groupe d'interception, sélectionnez un groupe dans la liste déroulante **Interception** de la ligne de l'abonné souhaité.

7) N'effectuez les paramétrages décrits dans ce point que si cela est nécessaire :

a) Sur la ligne de l'abonné souhaité, cliquez sur l'icône **Modifier**.



b) Dans le champ **Clip/Lin**, saisissez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant, et le numéro interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

---

c) Dans la liste déroulante **Type d'abonné**, sélectionnez le type de terminal TDM.

d) Ne modifiez pas la sélection par défaut de la liste déroulante **Langue**. Pour les terminaux TDM, ce paramétrage est sans importance.

e) Sélectionnez un numéro SDA dans une liste déroulante de la zone **SDA pour la téléphonie Internet**. Pour chaque ITSP actif, une liste déroulante s'affiche.

Remarque : Le champ **SDA pour la téléphonie Internet** n'est pas visible lorsque la téléphonie Internet n'est pas configurée ou lorsqu'aucun fournisseur de services de téléphonie sur Internet n'est activé.

---

f) Dans la liste déroulante **Signalisation des appels internes**, affectez à l'abonné l'une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres abonnés

internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

g) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

h) Cliquez sur **OK & Suivant**.

i) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonné, voir Abonnés > Abonnés > Paramètres d'abonné.

j) Cliquez sur **OK & Suivant**.

8) Si vous souhaitez configurer un autre abonné UP0, cliquez sur **Stocker les données** et répétez les étapes 1 à 7.

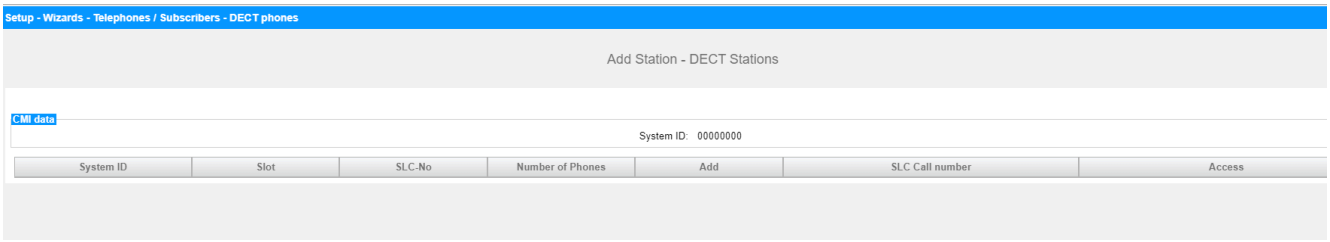
9) Cliquez sur **OK & Suivant**.

5.7.7.4 Comment configurer les abonnés DECT

Conditions préalables

Vous vous trouvez dans la fenêtre **Sélectionner l'abonné - Terminaux DECT** de l'assistant **Installation de base**.

Pour la configuration des abonnés DECT, il faut raccorder une station de base et y connecter les téléphones DECT. Si ce n'est pas le cas, ignorez cette fenêtre. Vous pouvez configurer les abonnés DECT plus tard (voir Configuration des abonnés).



Étape par étape

1) Si le numéro SDA de l'abonné doit être différent de son numéro d'appel, saisissez un numéro SDA dans le champ **SDA** de la ligne de l'abonné concerné :

- Uniquement pour le raccordement système :

  Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
- uniquement pour un raccordement multiposte :

  À partir de la liste déroulante, sélectionnez un numéro MSN. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
- pour le raccordement système et un raccordement multiposte :

  Dans la liste déroulante du champ souhaité, sélectionnez l'entrée **xxx - modifiable** (xxx correspondant au numéro interne) et saisissez le numéro SDA à l'aide du clavier ou sélectionnez un MSN (Multiple Subscriber Number, numéro de téléphone multiple).

2) Sur la ligne de l’abonné souhaité, saisissez le numéro de téléphone interne de l’abonné dans **Numéro de téléphone**. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

3) Si vous souhaitez configurer une boîte Fax pour l’abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme suit :

a) Dans la ligne de l’abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l’utilisateur pourra recevoir des messages Fax internes.

b) Si un numéro SDA doit être configuré pour la boîte Fax, saisissez dans la ligne de l’abonné souhaité, champ **SDA Fax**, le numéro de fax externe sous lequel l’abonné pourra recevoir des messages Fax externes.

4) Dans le champ **Nom** de la ligne de l’abonné souhaité, saisissez un nom au format `Nom de famille, Prénom` ou `Prénom Nom de famille`.

Remarque : Le nom peut comporter jusqu’à 16 caractères, mais ne doit contenir ni inflexions ni caractères spéciaux.

---

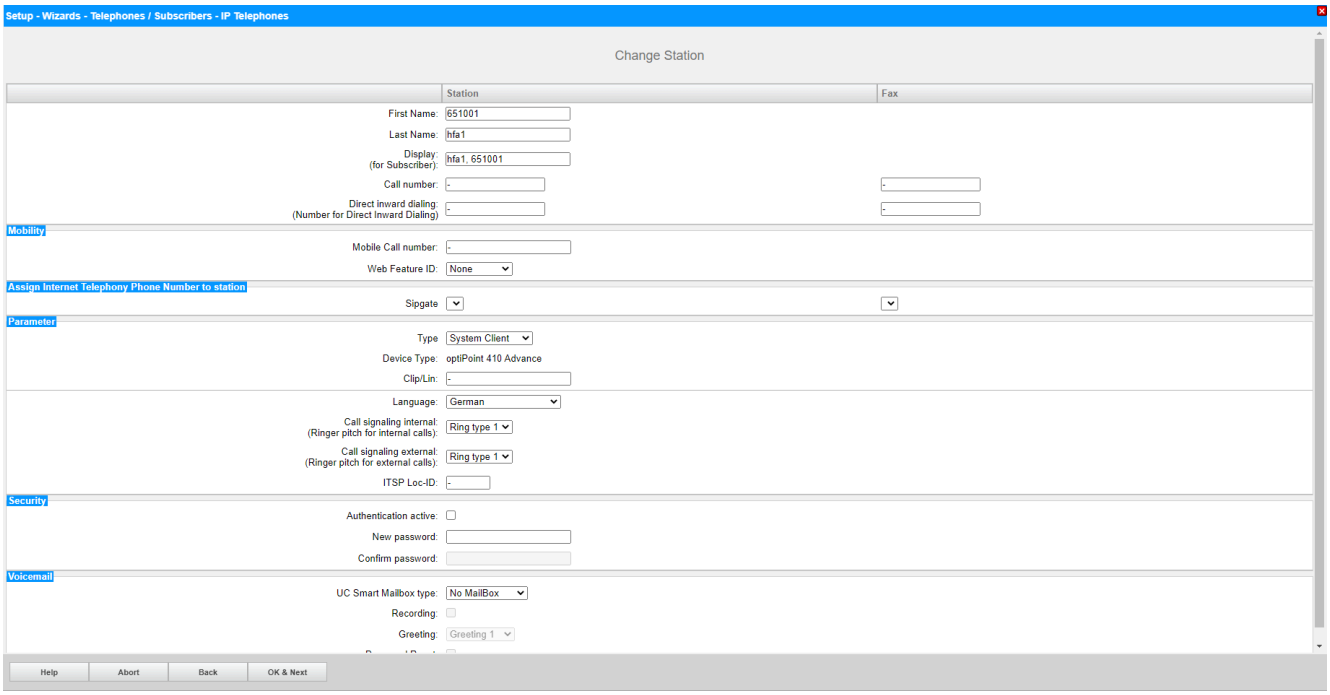
5) Dans la liste déroulante **Classe de service** de la ligne de l’abonné concerné, sélectionnez le groupe de classe de service souhaité.

6) Pour intégrer l’abonné à un groupe d’interception, sélectionnez un groupe dans la liste déroulante **Interception** de la ligne de l’abonné souhaité.

7) Si vous voulez modifier le code téléphone DECT (PIN), entrez le nouveau code dans la ligne de l’abonné souhaité, dans **Code mobile**. Les abonnés DECT doivent se reconnecter à la station de base en utilisant ce code.

8) N’effectuez les paramétrages décrits dans ce point que si cela est nécessaire :

a) Sur la ligne de l’abonné souhaité, cliquez sur l’icône **Modifier**.



b) Dans le champ **Clip/Lin**, saisissez un numéro de téléphone (numéro SDA ou MSN) qui, lors d’un appel externe, sera affiché sur l’écran de l’appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l’opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l’appelant, et le numéro interne est formaté et envoyé comme numéro de l’appelant pour l’appel externe.

---

c) Dans la liste déroulante **Type de poste**, sélectionnez le type de terminal sans fil.

d) Ne modifiez pas la sélection par défaut de la liste déroulante **Langue**. Pour les terminaux sans fil, ce paramétrage est sans importance.

e) Sélectionnez un numéro SDA dans une liste déroulante de la zone **SDA pour la téléphonie Internet**. Pour chaque ITSP actif, une liste déroulante s’affiche.

Remarque : Le champ **SDA pour la téléphonie Internet** n’est pas visible lorsque la téléphonie Internet n’est pas configurée ou lorsqu’aucun fournisseur de services de téléphonie sur Internet n’est activé.

---

f) Dans la liste déroulante **Signalisation des appels internes**, affectez à l’abonné l’une des huit signalisations d’appel acoustiques possibles

pour les appels internes (au total). Ainsi, l'abonné adresse aux autres abonnés internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

g) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

h) Cliquez sur **OK & Suivant**.

i) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonné, voir Abonnés > Abonnés > Paramètres d'abonné.

j) Cliquez sur **OK & Suivant**.

9) Si vous souhaitez paramétrer un autre abonné, cliquez sur **Enregistrer les données** et répétez les points 1 à 8.

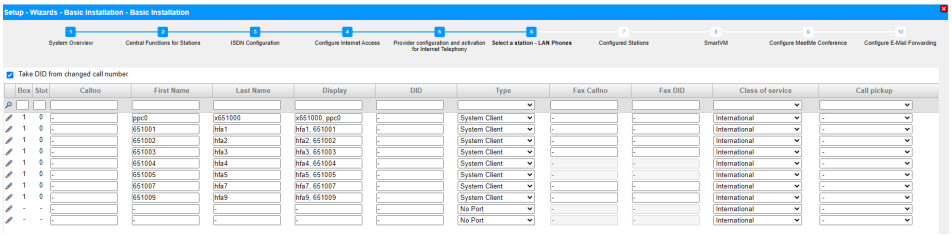
10) Cliquez sur **OK & Suivant**.

5.7.7.5 Comment configurer les abonnés IP et SIP

Conditions préalables

Vous vous trouvez dans la fenêtre **Sélectionner l'abonné - Téléphones LAN** de l'assistant **Installation de base**.

Pour que les téléphones WLAN fonctionnent, vous avez besoin d'un réseau LAN sans fil fonctionnel.



Étape par étape

1) Si le numéro SDA de l'abonné doit être différent de son numéro d'appel, saisissez un numéro SDA dans le champ **SDA** de la ligne de l'abonné souhaité :

- Uniquement pour le raccordement système :

  Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
- uniquement pour un raccordement multiposte :

  À partir de la liste déroulante, sélectionnez un numéro MSN. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
- pour le raccordement système et un raccordement multiposte :

  Dans la liste déroulante du champ souhaité, sélectionnez l'entrée **xxx - modifiable** (xxx correspondant au numéro interne) et saisissez le numéro SDA à l'aide du clavier ou sélectionnez un MSN (Multiple Subscriber Number, numéro de téléphone multiple).

2) Sur la ligne de l'abonné souhaité, saisissez le numéro de téléphone interne de l'abonné dans **Numéro de téléphone**. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

3) Entrez dans la ligne de l'abonné souhaité sous **Nom** un nom, sous la forme `Nom de famille, Prénom`.

Remarque : Le nom peut comporter jusqu'à 16 caractères, mais ne doit contenir ni inflexions ni caractères spéciaux. Le nom est inscrit comme nom de famille, comme indiqué ici pour les clients UC, mais il peut être modifié ultérieurement.

---

4) Sur la ligne de l'abonné souhaité, sélectionnez le type d'abonné IP (par ex. "Client système" ou "Client SIP") dans la liste déroulante **Type**.

5) Si vous souhaitez configurer une boîte Fax pour l'abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme suit :

a) Dans la ligne de l'abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l'utilisateur pourra recevoir des messages Fax internes.

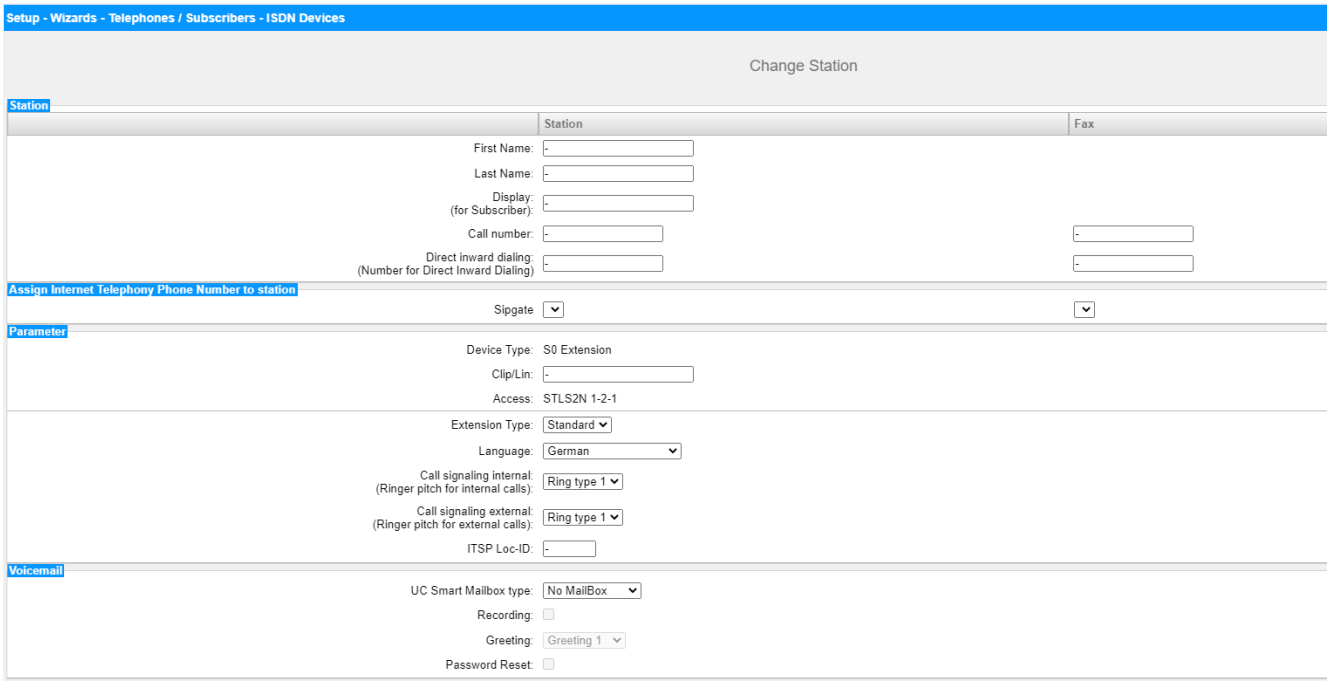
b) Si un numéro SDA doit être configuré pour la boîte Fax, saisissez dans la ligne de l'abonné souhaité, champ **SDA Fax**, le numéro de fax externe sous lequel l'abonné pourra recevoir des messages Fax externes.

6) Dans la liste déroulante **Classe de service** de la ligne de l'abonné concerné, sélectionnez le groupe de classe de service souhaité.

7) Pour intégrer l'abonné à un groupe d'interception, sélectionnez un groupe dans la liste déroulante **Interception** de la ligne de l'abonné souhaité.

8) N'effectuez les paramétrages décrits dans ce point qu'en cas de besoin ou pour un téléphone SIP :

a) Sur la ligne de l'abonné souhaité, cliquez sur l'icône **Modifier**.



b) Uniquement pour les téléphones SIP : Si ce téléphone SIP doit être utilisé en même temps qu'un téléphone mobile dual mode, saisissez dans la zone **Mobilité**, `Numéro de mobile` l'indicatif réseau suivi du numéro du téléphone mobile (par ex. **0016012345678**). Sélectionnez en plus dans la liste déroulante **Web Feature ID** ce client SIP. (Voir Téléphonie dual mode).

c) Dans le champ **Clip/Lin**, saisissez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant, et le numéro interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

---

d) Sélectionnez dans la liste déroulante **Langue** la langue des menus du téléphone.

e) Dans la liste déroulante **Signalisation des appels internes**, affectez à l'abonné l'une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres abonnés internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

f) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

g) Pour les téléphones SIP uniquement : Entrez le mot de passe d'authentification dans les champs **Mot de passe** et **Valider mot de passe**.
h) Pour les téléphones SIP uniquement : indiquez dans le champ **Identifiant utilisateur SIP/Nom d'utilisateur** l'identifiant utilisateur pour l'authentification.
i) Pour les téléphones SIP uniquement : indiquez dans **Realm** la zone correspondante pour l'authentification.
j) Cliquez sur **OK & Suivant**.
k) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonné, voir Abonnés > Abonnés > Paramètres d'abonné.
l) Cliquez sur **OK & Suivant**.

9) Si vous souhaitez paramétrer un autre abonné IP, cliquez sur **Enregistrer les données** et répétez les points 1 à 8.

10) Cliquez sur **OK & Suivant**. Le système affiche une liste de tous les abonnés paramétrés. Cette liste correspond à un plan de numérotation.

11) Si besoin est, cliquez sur **Imprimer** pour imprimer les données de l'abonné paramétré.

12) Pour terminer, cliquez sur **OK & Suivant**

Concepts associés

Texte en plusieurs langues à la page 1173

5.7.8 Configuration de UC Suite

Dans la fenêtre **Configuration automatique de la suite d'application**, vous pouvez effectuer la configuration automatique de la solution UC Suite.

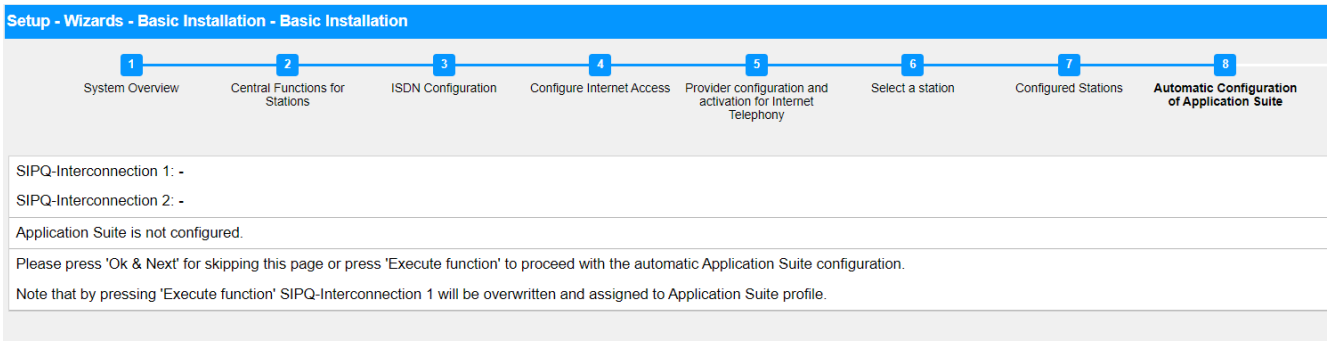
Remarque : Cette fenêtre ne s'affiche que si, dans l'assistant **Première installation**, il a été choisi **Pack avec UC Suite** lors de la sélection de l'application.

La configuration automatique de la solution UC Suite nécessite un certain nombre de lignes analogiques libres qui seront occupées de manière statique pour l'application. Ce nombre dépend des capacités de spécification du système et est indiqué dans la section Valeurs maximales des lignes à la page 1373 (voir *Canaux de ligne MEB Trunk pour UC Suite* dans les tableaux). Si la limite globale de 250 lignes est dépassée, la configuration d'UC Suite n'est pas possible.

5.7.8.1 Comment configurer la UC Suite

Conditions préalables

Vous êtes dans la fenêtre **Configuration automatique de la suite d'applications** de l'assistant d'**installation de base**.



Étape par étape

1) Si la suite UC n'est pas requise ou doit être configurée ultérieurement, cliquez sur **OK & Suite**. La configuration sera ignorée.
2) Si la suite UC doit être configurée automatiquement, cliquez sur **Exécuter la fonction**. La suite UC est configurée automatiquement à l'aide des packages système intégrés. Dès que la barre de progression indique 100%, cliquez sur **OK & Suivant**.

Remarque :

Pour OpenScape Business X, l'assistant génère automatiquement 76 canaux multimédias.

5.7.9 Configuration des boîtes de messagerie vocale de UC Smart

Dans la fenêtre **Configuration automatique de Smart VM**, vous pouvez effectuer la configuration automatique des boîtes de messagerie vocale UC Smart(Smart VM, Smart VoiceMail) si vous utilisez la solution UC Smart.

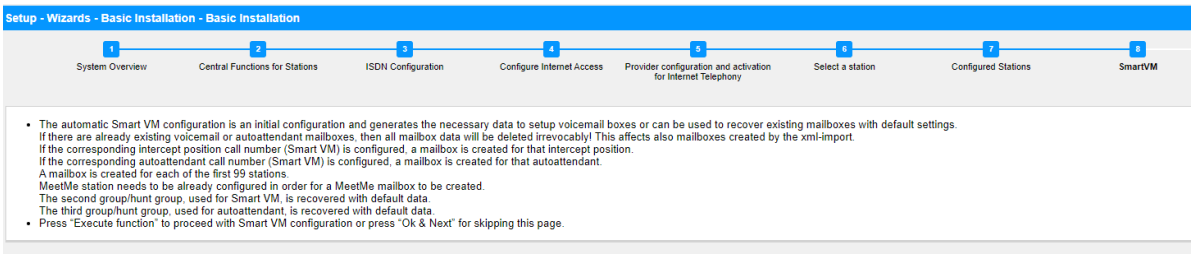
Remarque :

Cette fenêtre ne s'affiche que si, dans l'assistant **Première installation**, il a été choisi **Pack avec UC Smart** lors de la sélection de l'application.

5.7.9.1 Comment configurer les boîtes vocales UC Smart

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration automatique de Smart VM** de l'assistant **Installation de base**.



Étape par étape

1) Si les boîtes vocales UC Smart ne doivent pas être utilisées, cliquez sur **OK & Suivant**. La configuration des boîtes de messagerie vocale est sautée.
2) Si les boîtes vocales UC Smart doivent être utilisées, cliquez sur **Exécuter la fonction**. Les boîtes de messagerie vocale sont automatiquement configurées pour les 100 premiers abonnés. Dès que la barre de progression indique 100%, cliquez sur **OK & Suivant**.

Remarque : Les boîtes vocales UC Smart ou les boîtes vocales UC Smart AutoAttendant existantes sont supprimées définitivement dans ce cas.

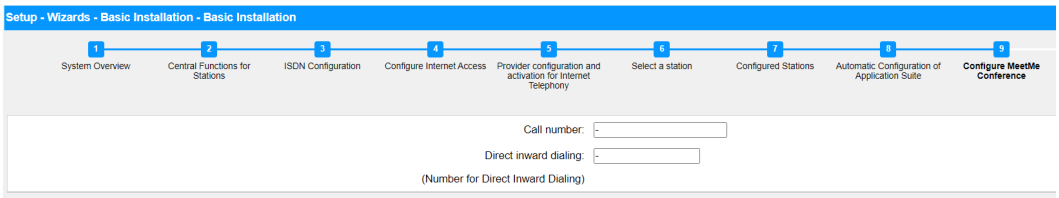
5.7.10 Paramètres du serveur de conférence

Dans la fenêtre **Conférence "Rendez-vous" - Modifier les paramètres** vous pouvez définir le numéro d'appel et le numéro de sélection d'une conférence.

5.7.10.1 Comment modifier la configuration du serveur de conférence

Conditions préalables

Vous vous trouvez dans la fenêtre **Configurer la conférence MeetMe** de l'assistant **Installation de base**.



Étape par étape

1) Dans **Numéro de téléphone**, indiquez un numéro pour la conférence.
2) Dans le champ **N° SDA**, définissez le numéro de sélection de la conférence (SDA conférence), afin de permettre aux abonnés d'entrer dans une conférence en place.
3) Cliquez sur **OK & Suivant**.

5.7.11 Envoi d'e-mails (option)

Dans la fenêtre **Modifier les renvois E-Mail**, vous pouvez configurer l'envoi d'e-mails. Les abonnés sont ainsi informés des nouveaux messages vocaux et fax et l'administrateur reçoit les messages système.

Vous disposez des possibilités suivantes :

- Configurer l'envoi d'e-mails

  Vous pouvez définir un serveur e-mail externe à l'aide duquel OpenScape Business va envoyer les e-mails. Les messages Voix et Fax ou messages système internes sont renvoyés via ce serveur d'e-mails à une ou différentes adresses e-mail configurables.

Remarque : Le paramétrage d'un serveur e-mail est important lorsqu'il doit être envoyé automatiquement aux utilisateurs de la suite UC, par e-mail, un lien vers le(s) fichier(s) d'installation.

5.7.11.1 Comment configurer l'envoi d'e-mails

Conditions préalables

Si le serveur de messagerie externe a été configuré pour utiliser l'authentification de base, assurez-vous qu'un compte e-mail avec mot de passe existe auprès d'un fournisseur d'e-mail et que vous connaissez les données d'accès à ce compte.

Si le serveur de messagerie externe a été configuré pour utiliser une authentification moderne (basée sur un jeton Microsoft OAuth 2.0), comme dans le cas d'Exchange Online, vérifiez les éléments suivants :

- Le compte de messagerie de l'expéditeur doit être autorisé à utiliser le protocole SMTP authentifié (par défaut, cette option est désactivée dans le client Microsoft 365). Une fois que le protocole SMTP authentifié est activé, le renvoi d'e-mail OAUTH 2.0 fonctionne normalement avec toutes les cartes mères OpenScape Business.
- Une application dotée des autorisations requises a été enregistrée dans Microsoft Azure Active Directory (Azure AD) pour permettre à votre système OpenScape Business d'envoyer des e-mails.
- Vous connaissez l'ID d'application (ou client) et l'ID de répertoire (ou locataire) de l'application enregistrée.

  Demandez à votre administrateur Azure AD de vous fournir ces valeurs, si nécessaire.
- L'adresse e-mail qui apparaîtra comme adresse d'expédition des e-mails appartient au même répertoire Azure AD (ou locataire) que l'application enregistrée.

Vous vous trouvez dans la fenêtre **Configurer le renvoi E-Mail** de l'assistant **Installation de base**.

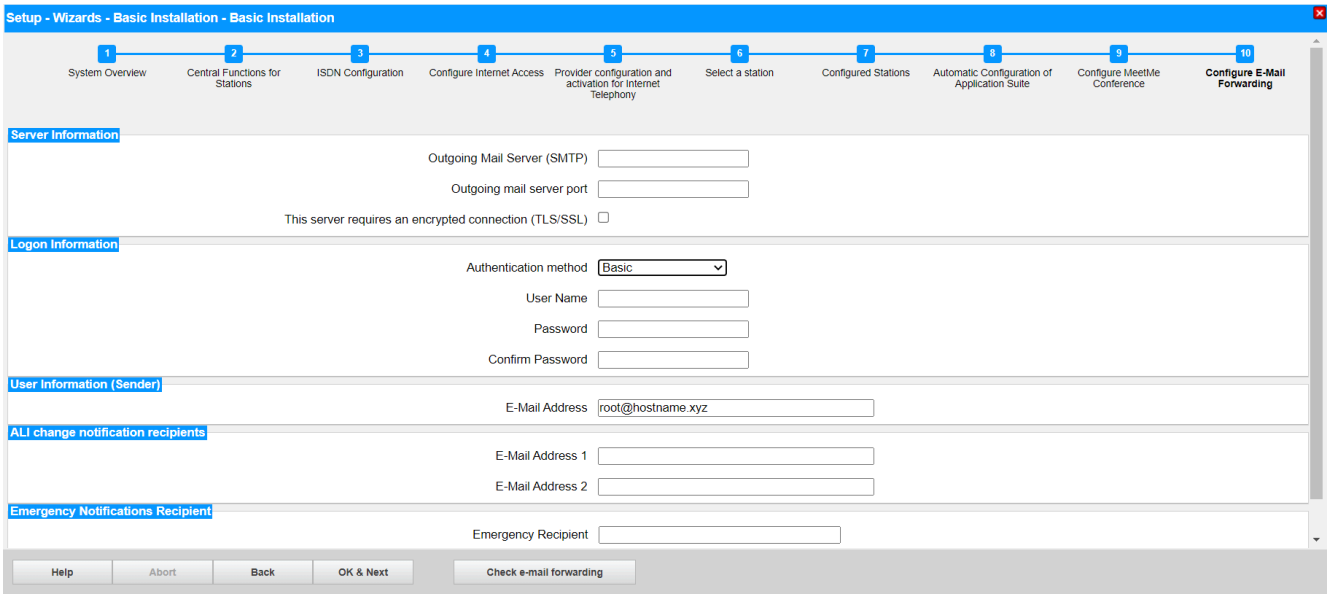


Illustration 5 : Options de renvoi d’e-mail lorsque la méthode d’authentification de base est sélectionnée

Étape par étape

1) Saisissez le **serveur de messagerie sortant (SMTP)** pour le serveur de messagerie qui doit être utilisé pour l’envoi d’e-mails, par ex. `smtp.web.fr`. Si nécessaire, interrogez le serveur de la boîte d’envoi ou bien votre fournisseur e-mail.

Remarque : Veillez à ce que le nom du serveur de messagerie sortant puisse être résolu. Si ce n'est pas le cas, vous devez démarrer la fonction d'envoi d'e-mails via **Centre de service** > **Renvoi e-Mail** et saisir l'adresse IP du serveur de courrier sortant (au lieu de son nom).

---

2) Pour le port de serveur qui doit être utilisé pour envoyer les e-mails, saisissez le **port du serveur de courrier sortant**. Si nécessaire, interrogez le serveur de la boîte d’envoi ou bien votre fournisseur e-mail.

3) Si une connexion sécurisée est requise, cochez la case **Ce serveur nécessite une connexion cryptée (TLS/SSL)**. Demandez le cas échéant à votre fournisseur d’e-mail, si cette option doit être activée.

4) Si le serveur de messagerie externe a été configuré pour utiliser l’authentification de base, procédez comme suit :

a) Dans la liste déroulante **Méthode d’authentification**, sélectionnez **Basique**.

b) Saisissez le **nom d’utilisateur** du compte e-mail, par ex. `jean.exemple`.

c) Dans **Mot de passe** et **Valider mot de passe**, saisissez le mot de passe du compte e-mail.

5) Si le serveur de messagerie externe a été configuré pour utiliser l'authentification moderne, procédez comme suit :

a) Dans la liste déroulante **Méthode d'authentification**, sélectionnez **Microsoft OAuth 2.0**.

b) Dans le champ **ID d'application**, saisissez l'ID d'application (client) obtenu à partir du portail Microsoft Azure.

c) Dans le champ **Locataire**, saisissez l'ID de répertoire (locataire) obtenu à partir du portail Microsoft Azure.

6) Saisissez l'**adresse e-mail** qui apparaîtra comme adresse d'expédition des e-mails, par exemple `john.doe@web.de`.

7) Saisissez l'**adresse e-mail 1** pour obtenir un e-mail de notification lorsque la tolérance ALI a été utilisée. Vous pouvez également saisir une deuxième adresse e-mail dans le champ **Adresse e-mail 2**.

8) Dans le champ **Destinataire d'urgence**, saisissez l'adresse e-mail d'un agent de sécurité sur site à laquelle un e-mail est envoyé lorsqu'un numéro d'urgence est composé.

L'objet de l'e-mail sera « Nouvel appel d'urgence ». Le numéro d'appel et le nom de l'appelant (s'ils sont configurés) sont inclus dans l'e-mail et récupérés auprès de la base de données du système.

9) Si vous avez sélectionné **Microsoft OAuth 2.0** comme méthode d'authentification, procédez comme suit :

a) Cliquez sur **OK & Suivant**.

b) Attendez qu'un lien d'autorisation et un code d'utilisateur apparaissent.

Le code d'autorisation expire après quelques minutes.

c) Ouvrez le lien d'autorisation et saisissez le code d'utilisateur dans la fenêtre contextuelle.

d) Connectez-vous avec l'adresse e-mail que vous avez saisie à l'étape 6 à la page 177 (**Adresse e-mail**).

L'adresse e-mail doit se trouver dans le même répertoire Azure AD (ou locataire) que l'application enregistrée.

e) Une fois l'authentification réussie, la fenêtre contextuelle affiche le message suivant :

```
Vous vous êtes connecté à <nom de l'application> sur
votre appareil. Vous pouvez maintenant fermer cette
fenêtre.
```

f) Fermez la fenêtre contextuelle et retournez dans la WBM.
Si l'authentification a réussi, le message suivant s'affiche :
`L'authentification est réussie !.`

10) Si vous souhaitez vérifier les paramètres d'e-mail saisis, procédez comme suit :
    a) Cliquez sur **Contrôler le renvoi d'e-mail**.
    b) Dans **Envoyer à l'adresse e-mail**, saisissez l'adresse e-mail de la messagerie e-mail à laquelle vous avez accès. L'e-mail de test est envoyé à cette adresse e-mail.
    c) Dans **Objet de l'e-mail**, saisissez un texte descriptif permettant d'identifier l'e-mail dans votre messagerie e-mail.
    d) Cliquez sur **Envoyer un e-mail de test**. Les paramètres e-mail sont contrôlés et l'e-mail est envoyé à la messagerie e-mail indiquée.
    e) Vérifiez si l'e-mail est bien arrivée dans votre messagerie e-mail.
    f) Si l'envoi de l'e-mail s'est bien déroulé, cliquez sur **Retour** et passez à l'étape suivante.
    g) Si l'envoi d'e-mails n'a pas abouti, cliquez sur **Retour** et corrigez vos paramètres e-mail.
11) Cliquez sur **OK & Suivant**, puis sur **Quitter**. L'installation de base est terminée. Avant d'effectuer la sauvegarde de données mentionnées dans l'Assistant, vous devez activer les licences.

5.8 Activités finales

Une fois terminées la première installation et l'installation de base avec WBM, il faut encore procéder à certains paramétrages essentiels pour l'utilisation d'OpenScape Business.

Pour cela, suivez les étapes suivantes :

1) Activer et affecter les licences

   Les licences acquises avec OpenScape Business doivent être activées dans un délai de 30 jours. La période de temps débute avec la première connexion au WBM. Une fois ce délai écoulé, le système de communication ne peut être utilisé que dans une version restreinte. Après l'activation, les licences doivent être affectées aux abonnés et aux lignes. Les fonctionnalités sur l'ensemble du réseau sont validés lors de l'activation dans un système indépendant.
2) Comment préparer le client UC Smart pour l'installation (Uniquement pour UC Smart)

   Le client UC Smart myPortal Smart fait partie de UC Smart. Le fichier d'installation de myPortal est accessible par la WBM et peuvent être mis à disposition des abonnés IP, automatiquement ou manuellement. Pour des informations supplémentaires, voir UC Smart Clients.
3) Préparer les clients UC Suite pour l'installation (seulement pour UC Suite)

   Les clients UC font partie intégrante de UC Suite. Les fichiers d'installation des clients UC sont accessible par le WBM et peuvent être mis à disposition des clients IP, automatiquement ou manuellement.

   En plus, l'administrateur dispose de la possibilité Silent Installation. C'est une méthode basée sur des lignes de commande permettant l'installation, la désinstallation et la modification automatiques des clients UC Suite, sans avoir à effectuer d'autres entrées. Pour des informations supplémentaires, voir Installation/Désinstallation silencieuse pour PC client UC Suite.

4) Réaliser la sauvegarde des données

Les modifications apportées à OpenScape Business doivent être enregistrées. La sauvegarde peut être enregistrée comme jeu de sauvegarde par ex. sur un support USB ou dans le réseau interne.

5.8.1 Comment activer et affecter les licences

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Vous connaissez le code LAC (code d'autorisation de licence) pour la validation de la licence et vous disposez d'un identifiant et d'un mot de passe pour accéder au serveur de licence.

Pour accéder au serveur de licence il faut disposer d'un accès Internet.

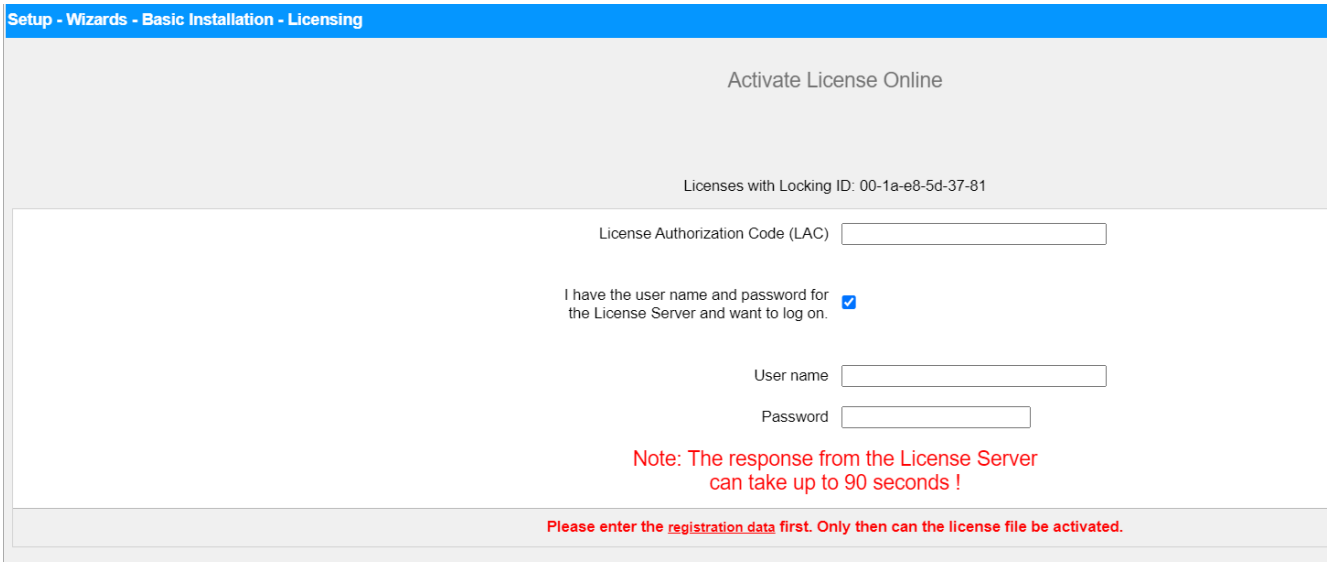
Étape par étape

1) Activer la licence en ligne :

a) Cliquez dans la barre de navigation sur **Configuration**.

b) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.

c) Cliquez sur **Modifier** pour lancer l'Assistant **Procédure de licence**.



d) Dans **Code d'autorisation de licence (LAC)**, entrez le code LAC.

e) Cochez la case **J'ai un nom d'utilisateur et un mot de passe pour le serveur de licence et souhaite ouvrir une connexion**.

f) Entrez le **Nom utilisateur** et le **Mot de passe** pour la connexion au serveur de licences.

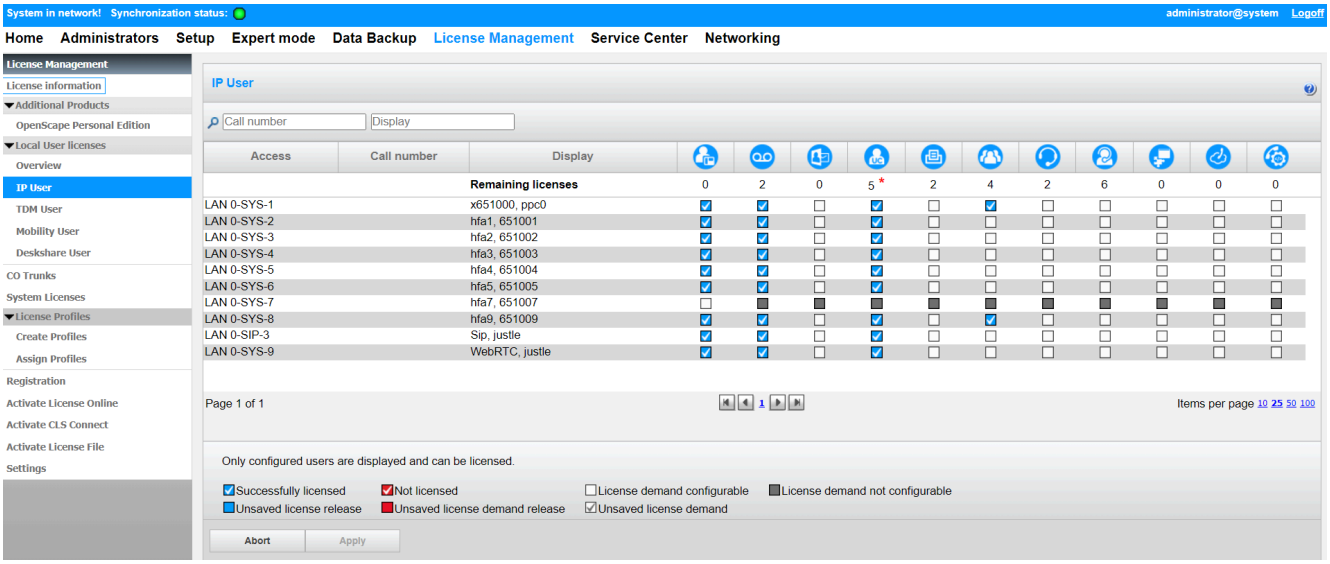
g) Cliquez sur **OK & Suivant**. La connexion avec le serveur de licences est établie et les licences sont validées.

2) Affecter les licences aux abonnés :

a) Cliquez sur **Gestion des licences** dans la barre de navigation.

b) Dans l'arborescence de navigation, accédez au type d'abonné souhaité sous **Licences d'utilisateur local** > **...**. Une liste de tous les abonnés du type d'abonné sélectionné s'affichera.

c) Dans la ligne de l'abonné souhaité, cochez la case figurant dans la colonne **Licences utilisateur** (première colonne avec case à cocher).



d) Dans la ligne de l'abonné souhaité, activez les licences orientées utilisateur en cochant les cases correspondantes.

Remarque : Il ne peut être attribué à un abonné une licence orientée utilisateur que si l'abonné précédent s'est vu attribuer une licence d'abonné (licences utilisateur) (Etape c).

---

e) Cliquez sur **OK & Suivant**. Une vérification est effectuée pour déterminer s'il y a suffisamment de licences pour votre affectation.

S'il y a suffisamment de licences, la procédure de licence des abonnés est terminée.

f) S'il manque des licences, les erreurs sont indiquées dans une case à fond rouge. Corrigez ces erreurs et répétez l'étape e.

3) Affecter les licences aux lignes

a) Dans l'arborescence de navigation, cliquez sur **Lignes réseau**. Dans la plage **Lignes réseau** il vous est présenté le nombre des licences de ligne acquises.

b) Pour les lignes SIP : dans la plage Demande de licence pour le nombre d'appels Internet simultanés dans ce nœud entrez le nombre des

communications Internet qui peuvent se dérouler simultanément via un ITSP.

c) Pour les lignes S_{2M} : dans la plage **S2M**, dans la ligne de l'emplacement souhaité, dans la liste déroulante de la colonne **Demandes**; sélectionnez le nombre des canaux B souhaités.
d) Pour les lignes T1 (uniquement pour les États-Unis) : dans la plage **T1**, dans la ligne de l'emplacement souhaité, dans la liste déroulante de la colonne **Demandes**; sélectionnez le nombre des canaux B souhaités.
e) Cliquez sur **OK & Suivant**.

Remarque : Le nombre des lignes SIP sous licence et le nombre des lignes S_{2M}/T1 sous licence ne doit pas dépasser le nombre des licences de ligne acquises.

5.8.2 Comment préparer le clients UC Smart pour l'installation

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Le matériel et le logiciel nécessaires à l'utilisation de UC Smart sont disponibles.

Remarque : Pour l'utilisation du client UC Smart myPortal Smart, des licences sont nécessaires.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Logicielle**.
3) Cliquez sur l'icône de téléchargement de **myPortal Smart** et enregistrez le fichier d'installation dans un lecteur réseau validé.
4) Cliquez sur l'icône de lien d'**Adobe AIR** et chargez le fichier d'installation sur un lecteur réseau validé.
5) Envoyez aux utilisateurs de myPortal Smart les deux fichiers d'installation.
6) Vous pouvez également envoyer aux utilisateurs de myPortal Smart deux liens qui leur permettent d'accéder directement aux fichiers d'installation.

```
https://<Adresse IP du système de communication>/
management/downloads/SmartClient.air
```

```
http://www.adobe.com/air
```

5.8.3 Comment préparer les clients UC Suite pour l'installation

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Le matériel et le logiciel nécessaires à l'utilisation de UC Suite sont disponibles.

Remarque : Pour l'utilisation des clients UC Suite, des licences sont nécessaires.

Étape par étape

1) Afin que les fichiers d'installation soient mis automatiquement à disposition de l'abonné, assurez-vous que les opérations suivantes ont bien été respectées.

a) Les adresses e-mail des abonnés doivent avoir été importées en même temps que les données d'abonné à l'aide d'un fichier XML ou bien être inscrits dans **Configuration** > **UC Suite** > **Répertoire utilisateur**.

b) Un serveur Mail doit être inscrit.

Remarque : Vous pouvez aussi inscrire a posteriori un serveur e-mail dans **Centre de service** > **Renvoi E-Mail**.

Tous les clients dont les adresses e-mail sont connues reçoivent un e-mail avec le lien pour l'installation des clients UC et des instructions concernant les premières étapes. Dans le répertoire Installation figure en outre un fichier Readme avec des informations sur l'installation du logiciel sur les PC client.

2) Si les étapes nécessaires pour une information automatique ne sont pas réalisées, vous pouvez aussi mettre à disposition manuellement les fichiers d'installation. Pour cela, procédez comme indiqué ci-après.

a) Cliquez dans la barre de navigation sur **Centre de service**.

b) Dans l'arborescence de navigation, cliquez sur **Logicielle**.

c) Cliquez sur le client UC souhaité et enregistrez le fichier d'installation zippé sur un lecteur réseau partagé.

d) Dans l'arborescence de navigation, cliquez sur **Documents** et sélectionnez la liste déroulante **Mode d'emploi**.

e) Cliquez sur la documentation du client UC souhaité et enregistrez le fichier de documentation sur un lecteur réseau validé.

f) Envoyez par e-mail aux utilisateurs de la suite UC le fichier d'installation zippé et le fichier de documentation zippé ou indiquez aux utilisateurs où les fichiers sont enregistrés.

g) Le fichier ZIP qui contient les fichiers d'installation comprend aussi un fichier Readme. Précisez aux utilisateurs que l'installation des clients UC doit être effectuée conformément aux conseils d'installation figurant dans le fichier Readme.

3) Vous pouvez également envoyer aux utilisateurs UC des liens qui leur permettent d'accéder directement aux fichiers d'installation des UC Clients.

a) Cliquez dans la barre de navigation sur **Centre de service**.

b) Dans l'arborescence de navigation, cliquez sur **Logicielle**.

c) Cliquez sur le bouton **Afficher les liens d'application**. Il vous est présenté plusieurs liens en fonction du système d'exploitation utilisé et du client UC souhaité. Par exemple :

```
https://<Adresse IP du système de communication>/
management/downloads/install-common.zip
```

5.8.4 Comment réaliser la sauvegarde des données

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Pour une sauvegarde des données sur un support USB (clé USB ou disque dur USB), le support USB doit être raccordé à l'interface du serveur USB.

Remarque : Informations supplémentaires sur la sauvegarde des données voir Sauvegarde immédiate .

Étape par étape

1) Cliquez dans la barre de navigation sur **Sauvegarde et restauration**.
2) Dans l'arborescence de navigation, cliquez sur **Sauvegarde - immédiate**.
3) Dans la plage **Nom** dans le champ **Commentaire**, entrez un commentaire pour le jeu de sauvegarde afin de pouvoir plus facilement identifier le jeu de sauvegarde lors d'une éventuelle restauration. Lors de la saisie, évitez les inflexions et les caractères spéciaux.
4) Dans la zone **Système** activez le lecteur de destination où le jeu de sauvegarde doit être enregistré.
5) Cliquez sur **OK&Suivant**. Dans une autre fenêtre, le système affiche la progression de la sauvegarde.
6) La sauvegarde a été effectuée lorsque le message **Sauvegarde effectuée !** s'affiche. Cliquez sur **Terminer**.
7) Si vous utilisez une clé USB comme moyen de sauvegarde, attendez que la LED de la clé USB ait fini de clignoter. C'est seulement alors que la sauvegarde est terminée sur la clé USB. Retirez ensuite la clé USB.
8) La première mise en service avec la WBM est maintenant terminée. Pour quitter WBM, cliquez en haut à droite sur le lien **Déconnexion** puis refermez la fenêtre.

Remarque : Si une nouvelle version logicielle pour le système de communication est disponible, cela est indiqué à la page de démarrage de la WBM - à condition que le raccordement Internet soit correctement paramétré. Si une nouvelle version logicielle est disponible, effectuez une mise à jour (voir Mise à jour du système de communication).

5.9 Mise en service des téléphones IP

Une mise en service confortable des téléphones IP nécessite un serveur DHCP qui fournit au téléphone IP les données importantes pour l'inscription dans le système de communication (données spécifiques du réseau).

Données spécifiques du réseau

Pour l'inscription sur le système de communication, un téléphone IP a besoin de données spécifiques du réseau. Ces données peuvent soit être enregistrées dans le serveur DHCP, soit avoir été entrées directement dans le téléphone IP.

L'avantage d'un serveur DHCP est que tous les téléphones IP raccordés sont automatiquement alimentés avec ces données.

Les données suivantes sont nécessaire pour le téléphone IP :

- Adresse IP du système de communication
- Adresse IP du serveur DLS

En plus, le téléphone IP a besoin de son propre numéro. Celui-ci doit être inscrit manuellement sur le téléphone durant l'inscription.

Enregistrement des téléphones SIP

Pour des raisons de sécurité, il est recommandé d'enregistrer les téléphones SIP sur le système de communication. Pour cela, les données d'enregistrement du téléphone IP et du système de communication doivent correspondre.

Les données suivantes sont nécessires pour la connexion :

- ID utilisateur SIP
- Mot de passe SIP
- Realm SIP (option)

Utilisez un mot de passe SIP hors du commun, qui répond aux règles suivantes :

- Au moins 8 positions
- Au moins une majuscule (A - Z)
- Au moins une minuscule (a - z)
- Au moins un chiffre (0-9)
- Au moins un caractère spécial

Utilisez un ID utilisateur SIP qui ne contient pas le n° de téléphone.

Remarque : Vous trouverez des informations supplémentaires sur la configuration des téléphones SIP dans `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Utilisation du serveur DHCP interne

Si l'on utilise le serveur DHCP interne du système de communication, celui-ci contient déjà les données spécifiques réseau. Afin qu'un téléphone IP puisse s'enregistrer sur le système de communication, il ne enregistrer sur le téléphone IP que le numéro de téléphone défini. Pour un téléphone SIP, il faut en plus que les données d'enregistrement SIP sur le téléphone SIP et sur le système de communication correspondent.

Utilisation d'un serveur DHCP externe avec données spécifiques du réseau

Si l'on utilise un serveur DHCP externe, il faut y entrer les données spécifiques réseau. Afin qu'un téléphone IP puisse s'enregistrer sur le système de communication, il ne enregistrer sur le téléphone IP que le numéro de téléphone défini. Pour un téléphone SIP, il faut en plus que les données d'enregistrement SIP sur le téléphone SIP et sur le système de communication correspondent.

Utilisation d'un serveur DHCP externe sans données spécifiques du réseau

Si l'on utilise un serveur DHCP externe sur lequel il est impossible d'entrer les données spécifique réseau, celles-ci doivent alors être entrées sur le téléphone IP. Pour qu'un téléphone IP puisse s'enregistrer sur le système de communication, il faut inscrire sur le téléphone IP le numéro et l'adresse IP du système de communication et éventuellement modifier les paramètres du service de déploiement. Pour un téléphone SIP, il faut en plus que les données d'enregistrement SIP sur le téléphone SIP et sur le système de communication correspondent.

5.9.1 Comment configurer le téléphone IP

Conditions préalables

Le téléphone IP est raccordé au réseau interne et il est opérationnel.

Remarque : Il est décrit ici la configuration à l'exemple d'un téléphone système IP OpenStage 40/60/80. Ce paramétrage doit être effectué par analogie pour un autre téléphone IP. Consultez à ce sujet de mode d'emploi de votre téléphone IP.

Étape par étape

1) Pour accéder au mode Administration du téléphone système IP, appuyez sur la touche du téléphone correspondant au menu Paramètres / Applications.
2) Dans l'onglet `Paramètres` à `Admin` et confirmez avec la touche OK.
3) Entrez le mot de passe Administrateur (par défaut : `123456` et confirmez avec la touche OK.
4) Si vous utilisez dans le réseau interne le serveur DHCP du système de communication, sautez le point suivant.
5) Si vous n'utilisez pas dans le réseau interne le serveur DHCP du système de communication, vous devez entrer l'adresse IP du Deployment Server (DLS) et du système de communication de manière à ce que le logiciel du téléphone système IP puisse être actualisé automatiquement. Cela s'applique uniquement aux téléphones système IP. Pour cela, suivez les étapes suivantes :
   a) Recherchez `Network` (réseau) et confirmez avec la touche OK.
   b) Recherchez `Update service (DLS)` (service de mise à jour DLS) et confirmez avec la touche OK.
   c) Recherchez `DLS address` (adresse DLS) et confirmez avec la touche OK.
   d) Entrez comme Deployment Server l'adresse IP du système de communication `(par défaut :` 192.168.1.2) et confirmez avec la touche OK.
   e) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.
   f) Recherchez `IPv4 configuration` (configuration IPv4) et confirmez avec la touche OK.
   g) Recherchez `Route (default)` (route par défaut) et confirmez avec la touche OK.

h) Entrez l'adresse IP du système de communication (par défaut `192.168.1.2`) et confirmez avec la touche OK.
i) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.
j) Utilisez la touche Retour pour revenir au niveau de menu précédent.

6) Fixez le numéro de téléphone du téléphone :
a) Recherchez `System` (système) et confirmez avec la touche OK.
b) Recherchez `Identity` (identité) et confirmez avec la touche OK.
c) Recherchez `Terminal number` (numéro du terminal) et confirmez avec la touche OK.
d) Entrez le numéro de téléphone défini (par ex. `120` et confirmez avec la touche OK.
e) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

7) Utilisez la touche Retour pour revenir au niveau de menu précédent.

8) Si, en raison des modifications, le téléphone système doit effectuer un redémarrage, il apparaît dans le menu `Admin` l'option de menu `Redémarrage`. Confirmez `Redémarrage` avec le touche OK puis `Oui` ainsi que la touche OK. Le téléphone système effectue un redémarrage et se connecte au système de communication.

5.9.2 Comment configurer un téléphone SIP

Conditions préalables

Le téléphone IP est raccordé au LAN client et il est opérationnel.

Remarque : Il est décrit ici la configuration à l'exemple d'un téléphone système OpenStage 40/60/80 SIP. Ce paramétrage doit être effectué par analogie pour un autre téléphone SIP. Consultez à ce sujet de mode d'emploi du téléphone SIP.

Étape par étape

1) Pour accéder au mode Administration du téléphone système SIP, appuyez sur la touche du téléphone correspondant au menu Paramètres / Applications.

2) Dans l'onglet `Paramètres` à `Administrateur (Admin)` et confirmez avec la touche OK.

3) Entrez le mot de passe Administrateur (par défaut : `123456` et confirmez avec la touche OK.

4) Si vous utilisez dans le réseau interne le serveur DHCP du système de communication, sautez le point suivant.

5) Si vous n'utilisez pas dans le réseau interne le serveur DHCP du système de communication, vous devez entrer l'adresse IP du Deployment Server (DLS) et du système de communication de manière à ce que le logiciel du téléphone système SIP puisse être actualisé automatiquement. Cela s'applique uniquement aux téléphones système SIP. Pour cela, suivez les étapes suivantes :
a) Recherchez `Network` (réseau) et confirmez avec la touche OK.

b) Recherchez `Update service (DLS)` (service de mise à jour DLS) et confirmez avec la touche OK.
c) Recherchez `DLS address` (adresse DLS) et confirmez avec la touche OK.
d) Entrez comme Deployment Server l'adresse IP du système de communication `(par défaut :` 192.168.1.2) et confirmez avec la touche OK.
e) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.
f) Recherchez `IPv4 configuration` (configuration IPv4) et confirmez avec la touche OK.
g) Recherchez `Route (default)` (route par défaut) et confirmez avec la touche OK.
h) Entrez l'adresse IP du système de communication (par défaut `192.168.1.2`) et confirmez avec la touche OK.
i) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.
j) Utilisez la touche Retour pour revenir au niveau de menu précédent.

6) Définissez les paramètres de temps SNTP :

a) Recherchez `Date and Time` (date et heure) et confirmez avec la touche OK.
b) Recherchez `Time source` (source de temps) et confirmez avec la touche OK.
c) Recherchez `SNTP IP address` (adresse IP SNTP) et confirmez avec la touche OK.
d) Entrez l'adresse IP du système de communication (par défaut `192.168.1.2`) et confirmez avec la touche OK.
e) Recherchez `Timezone offset` (décalage horaire) et confirmez avec la touche OK.
f) Indiquez l'écart entre l'heure locale et l'heure universelle (Universal Time Coordinated) en heures (Allemagne : `1`) et confirmez avec OK.
g) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.
h) Utilisez la touche Retour pour revenir au niveau de menu précédent.

7) Fixez le numéro de téléphone du téléphone :

a) Recherchez `System` (système) et confirmez avec la touche OK.
b) Recherchez `Identity` (identité) et confirmez avec la touche OK.
c) Recherchez `Terminal number` (numéro du terminal) et confirmez avec la touche OK.
d) Entrez le numéro de téléphone défini (par ex. `120` et confirmez avec la touche OK.
e) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

8) Définissez les données d'authentification SIP :

a) Recherchez `Registration` et confirmez avec la touche OK.

b) Recherchez `SIP session` (session SIP) et confirmez avec la touche OK.

c) Notez le `Realm` ou entrez si nécessaire un nouveau Realm (par ex. `OSBIZ-SIP`).

d) Notez le `User ID` ou indiquez si nécessaire un nouvel User ID (par ex. `SIP-120`) un.

e) Attribuez un `Mot de passe` pour l'enregistrement sur le serveur SIP.

f) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

9) A l'aide de la touche Précédent, revenir au menu `Admin`.

10) Si, en raison des modifications, le téléphone système doit effectuer un redémarrage, il apparaît dans le menu `Admin` l'option de menu `Redémarrage`. Confirmez `Redémarrage` avec le touche OK puis `Oui` ainsi que la touche OK. Le téléphone système effectue un redémarrage et se connecte au système de communication.

5.10 Comment collecter les traces de diagnostic pour les incidents de type erreur

Vous pouvez automatiquement collecter les données de traces de diagnostic nécessaires pour un incident de type erreur. L'assistant **Gestion des erreurs** vous guidera tout au long du processus.

Vous devez exécuter deux fois l'assistant **Gestion des erreurs** : avant et après l'exécution du scénario problématique. Durant la première exécution (phase 1), vous activez l'ensemble des traces de diagnostics. Après l'exécution du scénario problématique, exécutez de nouveau l'assistant pour collecter les données de trace de diagnostic (phase 2). Une fois la phase 2 terminée, vous pouvez télécharger le fichier de trace pour l'inclure dans le système de tickets.

Procédez comme suit pour collecter les données de traces de diagnostic pour l'incident de type erreur :

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Cliquez sur **Modifier** à côté de **Gestion des erreurs**.

3) Cliquez sur **OK & Suivant**.

4) Si vous souhaitez collecter les traces par défaut, cochez la case **Traces par défaut**.

5) Si vous souhaitez définir les types de traces à collecter, sélectionnez les traces souhaitées dans la liste. Plusieurs sélections sont possibles.

Pour plus d'informations sur les traces, consultez le guide de résolution des problèmes.

6) Cliquez sur **OK & Suivant**.

7) Une liste d'informations supplémentaires, de documents pertinents et d'astuces s'affiche. Cliquez sur **OK & Suivant**.

8) Les scénarios et les types de trace que vous allez collecter s'affichent. Cliquez sur **Terminer**.

9) Continuez en exécutant le scénario problématique.

10) Une fois le scénario terminé, accédez de nouveau à **Configuration > Gestion des erreurs** et cliquez sur **Modifier**.

Vous êtes redirigé vers l'étape 2 de la collecte des traces de diagnostic. Si vous souhaitez interrompre le processus et le recommander, cliquez sur le bouton **Annuler**.

11) Cliquez sur **OK & Suivant**.

12) Saisissez les informations requises et cliquez sur **OK & Suivant**.

13) Une liste répertoriant les informations requises et certaines actions supplémentaires s'affiche.

14) Cliquez sur **OK & Suivant**.

15) Cliquez sur **Terminer** pour commencer à télécharger les données de traces de diagnostic.

5.11 Refaire le flashage

En suivant les étapes ci-dessous, vous pouvez facilement changer le type de logiciel d'un périphérique.

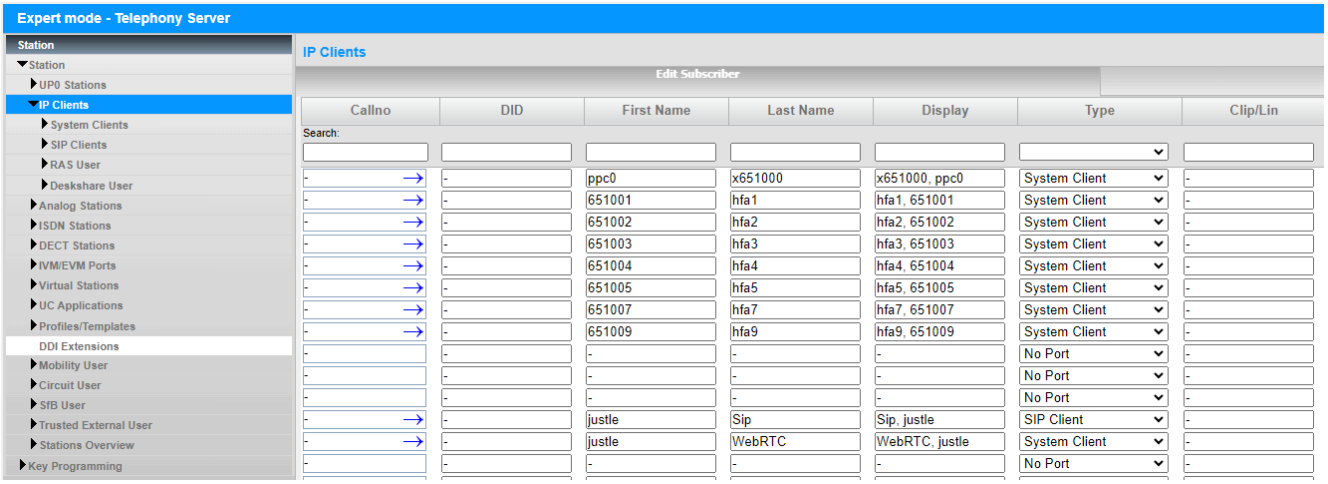
Le concept derrière cette fonction est de simplifier la façon d'obtenir un périphérique SIP (prêt à l'emploi) et de l'enregistrer dans le système OSBiz en tant que périphérique HFA. Les seules exigences sont les suivantes :

- le téléphone doit obtenir l'adresse DLI (soit à partir d'un serveur DHCP, soit manuellement)
- l'administrateur doit entrer le numéro du téléphone (qui doit être préconfiguré en tant que client du système)

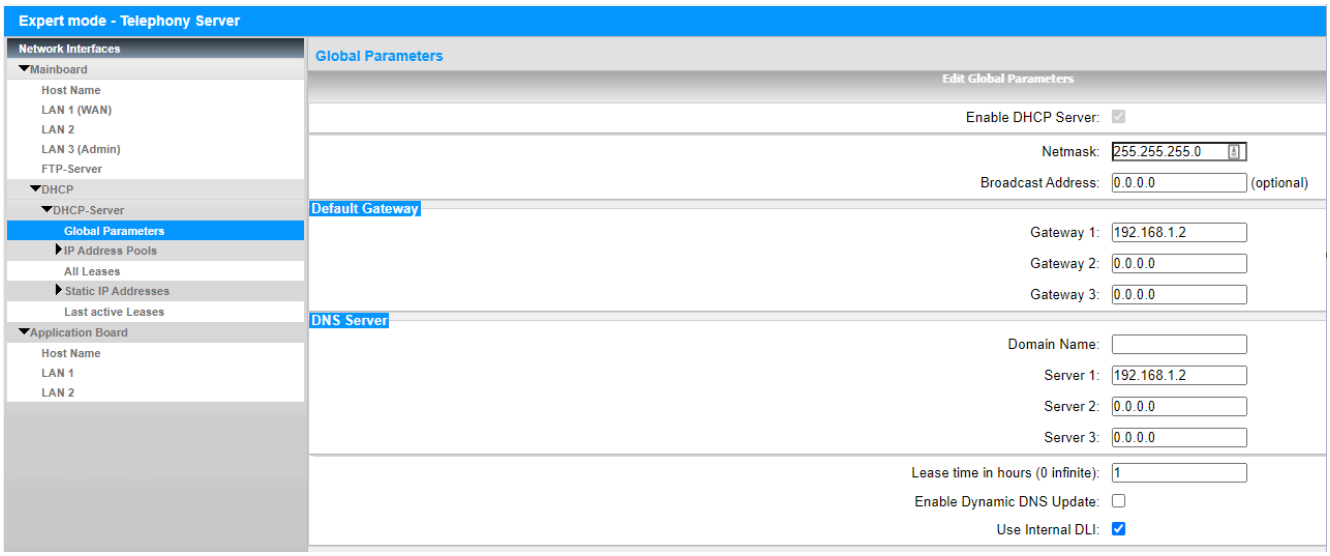
Lorsque le client reçoit un nouveau périphérique, il est préconfiguré en tant que périphérique SIP (paramètres d'usine). Les étapes pour reconfigurer ce périphérique en périphérique HFA sont les suivantes :

Étape par étape

1) Configurer dans la base de données OSBIZ le numéro de téléphone souhaité en tant que client système (HFA).



2) Configurer le serveur DHCP pour qu'il envoie l'adresse IP de DLI. Cette opération peut être effectuée soit sur le serveur DHCP externe, soit sur le serveur DHCP interne.



3) Si aucun serveur DHCP n'est utilisé, vous devez configurer manuellement l'adresse IP de DLI sur le téléphone.

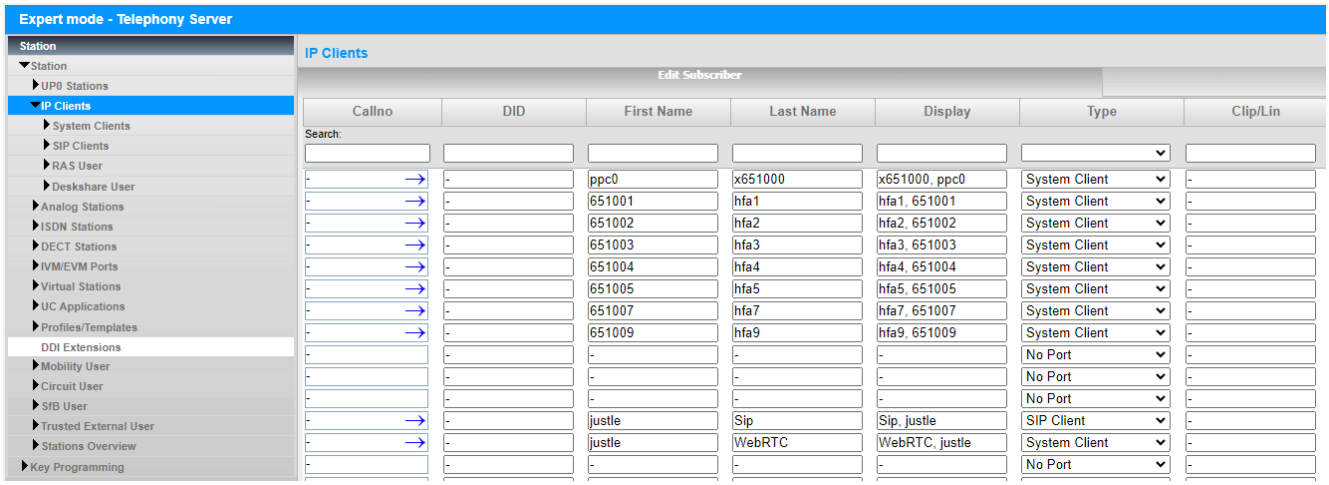
4) Une fois que le téléphone SIP obtient une IP et l'IP DLI, l'appareil téléphonique sera enregistré dans la base de données DLI et une invite s'affichera pour entrer le numéro de poste.

5) Saisissez le numéro de terminal sur le téléphone (le numéro doit être le même que celui configuré lors de la première étape, par exemple 4111).

6) Le reflash démarre et la nouvelle image HFA est téléchargée sur le téléphone. Lorsque le téléphone redémarre, il est enregistré en tant que téléphone HFA et les données « plug and play » sont envoyées par le système au téléphone.

7) **Pour reflasher un téléphone SIP déjà enregistré :**

8) Changez le périphérique SIP de travail en « Client système ».



9) Redémarrez le téléphone

10) Le reflash démarre et la nouvelle image HFA est téléchargée sur le téléphone. Lorsque le téléphone redémarre, il est enregistré en tant que

téléphone HFA et les données « plug and play » sont envoyées par le système au téléphone.

6 Première configuration de OpenScape Business S

Il est décrit la première mise en service d'OpenScape Business S (appelé aussi commutateur logiciel - softswitch). Le commutateur logiciel et les composantes correspondantes sont intégrés dans le LAN client existant. Il est paramétré l'accès Internet pour la téléphonie Internet et les abonnés raccordés sont configurés.

Pour OpenScape Business S, le logiciel de communication OpenScape Business est installé sur le système d'exploitation Linux SLES 12 SP5 64 bits ou SLES 15 SP6 64 bits. Le logiciel de communication peut être utilisé directement sur un serveur Linux ou dans un environnement virtuel avec VMware vSphere ou Microsoft Hyper-V. L'installation du système d'exploitation Linux est décrite dans le Guide d'installation *OpenScape Business, Installation du serveur Linux*.

La première installation de OpenScape Business S est réalisée à l'aide du programme d'administration OpenScape Business Assistant (Gestion basée sur le Web, en abrégé WBM).

Il est décrit la configuration des composantes utilisées le plus fréquemment. Toutes ces composantes ne seront pas utilisées chez vous. Lors de la première configuration, vous aurez donc le choix entre plusieurs possibilités à certains endroits, ou vous pourrez même sauter des configurations selon les composantes utilisées dans votre installation.

L'administration détaillée des fonctionnalités, au-delà de la première configuration, est traitée dans les chapitres ci-après.

Condition pour la première configuration : création d'un schéma d'adresses IP et d'un plan de numérotation.

Aperçu des principales opérations d'installation

- Paramètres système
- Numéros système et mise en réseau
- Téléphonie Internet
- Configuration des abonnés
- Octroi de licence
- Durcissement du système
- Sauvegarde des données

6.1 Conditions de la première configuration

Le respect des conditions préalables à l'installation initiale garantit le bon fonctionnement d'OpenScape Business S.

Général

Les conditions générales suivantes s'appliquent en fonction du matériel utilisé (téléphones, ...) et de l'infrastructure existante :

- L'infrastructure LAN (routeurs Internet, commutateurs, etc.) est présente et utilisable.
- Les téléphones IP sont connectés au réseau LAN du client.

- Le serveur Linux nécessaire à OpenScape Business S a été installé conformément aux *Instructions d'installation OpenScape Business Linux Server*, il est opérationnel et intégré au LAN client.
- Toutes les licences requises pour OpenScape Business S sont présentes (par exemple, clients UC, services de répertoire, etc.).
- Un plan d'adresses IP existe et est connu.
- Un plan de numérotation (également appelé plan de numérotation) est présent et connu.

Logiciel

Les logiciels suivants sont nécessaires à l'installation d'OpenScape Business S :

- DVD ou image .ISO avec logiciel de communication OpenScape Business

  Contient le logiciel de communication OpenScape Business. Ce DVD ou cette image .ISO fait partie de la livraison.
- DVD ou clé USB avec le système d'exploitation Linux SLES 12 SP5 ou SLES 15 SP6.

  Le DVD ou fichier .ISO Linux est éventuellement nécessaire lors de l'installation du logiciel de communication OpenScape Business s'il faut installer ensuite des packs logiciels (RPM) qui sont nécessaires au logiciel de communication.

Administration

Pour la configuration initiale d'OpenScape Business S avec OpenScape Business Assistant (WBM), le serveur Linux ou le PC d'administration peuvent être utilisés. Le WBM est basé sur un navigateur et est donc indépendant du système d'exploitation.

- Navigateurs web :

  Les navigateurs web suivants, compatibles avec HTML 5, sont pris en charge :

  – Microsoft Internet Explorer version 11 et ultérieure (PC d'administration).
  – Microsoft Edge
  – Mozilla Firefox Version 37.x et 38.x
  – Mozilla Firefox ESR Version 24.x et 31.x
  – Google Chrome

  Si une ancienne version du navigateur web est installée, vous devrez installer une version plus récente avant de pouvoir commencer la configuration initiale du système.
- Java :

  Oracle Java 8 ou une version plus récente, ou encore OpenJDK 8, doit être installé. Si une version plus ancienne est installée, vous devrez la mettre à jour avant de pouvoir configurer le système pour la première fois.

- Résolution d'écran : 1024x768 ou supérieure

Pare-feu

Lorsqu'il est connecté à Internet, le serveur Linux doit être équipé d'un pare-feu afin d'empêcher tout accès non autorisé depuis l'extérieur. Après l'installation de Linux, le pare-feu Linux est activé. L'installateur du logiciel de communication

ajuste les paramètres du pare-feu afin que le logiciel de communication puisse fonctionner correctement. Les ports du logiciel de communication sont ouverts et tous les autres ports sont fermés.

Si un pare-feu externe est utilisé dans le réseau, le pare-feu Linux doit être désactivé et les adresses et ports nécessaires pour le logiciel de communication doivent être validés (voir Ports utilisés).

Accès Internet

Le PC serveur doit disposer d'un accès à l'internet à large bande pour :

- Les correctifs de sécurité et les mises à jour générales du logiciel Linux

OpenScape Business nécessite une connexion Internet pour :

- Les mises à jour du logiciel OpenScape Business
- Les fonctions d'OpenScape Business telles que la téléphonie par Internet, par exemple
- Clients d'OpenScape Business
- Service à distance

Serveur e-mail (facultatif)

Pour pouvoir envoyer des e-mails, OpenScape Business doit avoir accès à un serveur e-mail. Pour ce faire, les données d'accès au serveur de messagerie doivent être saisies dans OpenScape Business et les comptes correspondants (adresse IP, URL, données de connexion du serveur de messagerie) doivent être configurés dans le serveur de messagerie.

Si la fonctionnalité e-mail n'est pas utilisée dans OpenScape Business, il n'est pas nécessaire de saisir ces données.

Téléphonie Internet, VoIP (optionnel)

Si la téléphonie par Internet est utilisée dans OpenScape Business, OpenScape Business a besoin d'un accès à large bande à Internet et à un fournisseur de services de téléphonie par Internet (ITSP, SIP Provider) pour la téléphonie SIP sur Internet. Pour ce faire, les comptes appropriés doivent être obtenus auprès de l'ITSP et les données d'accès à l'ITSP (adresse IP, URL, données de connexion du fournisseur SIP) doivent être configurées dans OpenScape Business.

Deuxième port LAN

Si OpenScape Business S (ou le serveur Linux) dispose d'un deuxième raccordement LAN, vous pouvez le paramétrer en tant qu'interface WAN pour l'accès Internet et pour la téléphonie Internet via ITSP. Le premier raccordement LAN sert comme d'habitude en tant qu'interface LAN pour les téléphones et PC internes. La configuration de l'accès à Internet s'effectue dans le routeur Internet externe du réseau LAN du client. La configuration du deuxième port LAN se fait directement lors de l'installation initiale de Linux ou peut être effectuée ultérieurement à l'aide de YaST. Dans le WBM, il suffit d'activer le deuxième port LAN en tant qu'interface WAN.

Fax en PDF

Si les télécopies doivent être enregistrées au format PDF, le PC serveur nécessite au moins 4 Go de RAM. Si Unify OpenScape Business S est exploité

dans un environnement virtuel, la machine virtuelle doit également recevoir 4 Go de RAM.

6.2 Composantes

Les composantes de l'exemple d'installation sont décrites et illustrées ci-après.

L'exemple d'installation engloge les composantes suivantes.

- OpenScape Business S

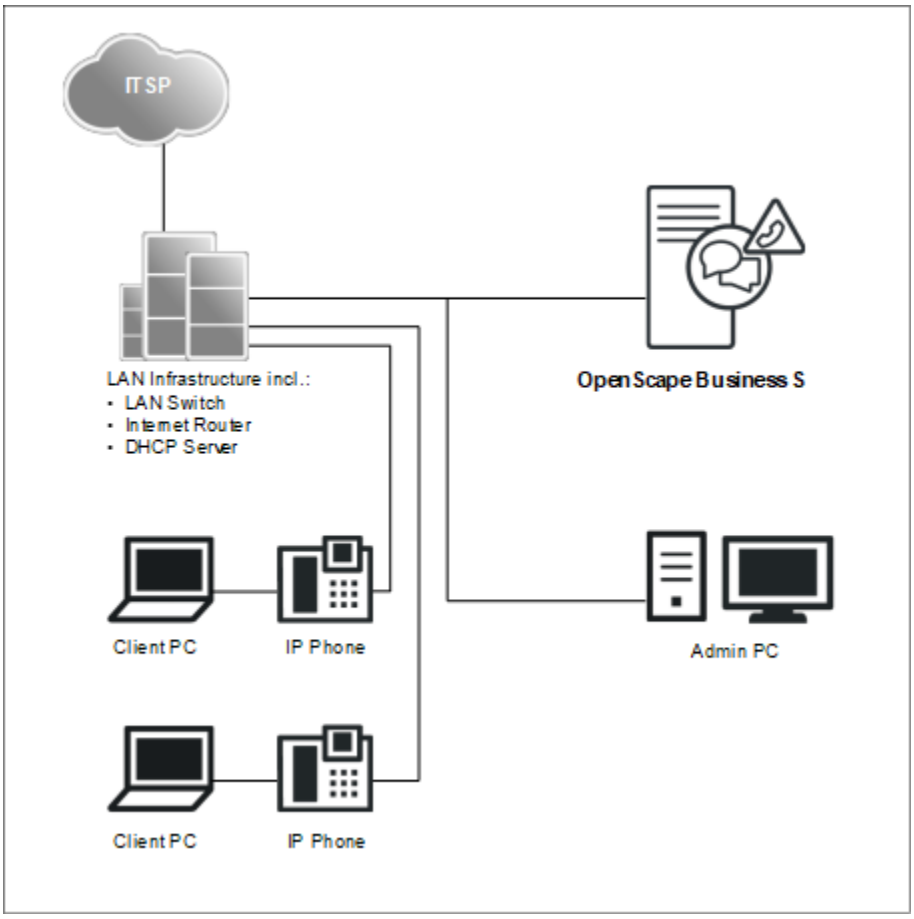
  Le serveur Linux avec logiciel de communication OpenScape Business S est intégré au LAN client en place via son interface LAN.
- PC Admin

  Le PC Admin est également intégré au LAN client en place via son interface LAN.
- Abonnés IP (IP-Clients)

  Les abonnés IP (téléphones système IP, PC client, points d'accès WLAN, ...) sont intégrés au LAN via un ou plusieurs commutateurs.

Les clients IP reçoivent leurs adresses IP de manière dynamique d'un serveur DHCP interne (serveur DHCP du serveur Linux) ou d'un serveur DHCP externe (par ex. serveur DHCP du routeur Internet).

L'accès à Internet est configuré dans le routeur Internet.



6.3 Schéma des adresses IP

Un schéma des adresses IP détermine comment les adresses IM sont attribuées dans le LAN client. Il comprend les adresses IP des PC, des serveurs, des routeurs Internet, des téléphones IP, etc.

Pour un meilleur aperçu lors de l'affectation des adresses IP, il est préférable de créer un schéma des adresses IP.

Exemple de schéma d'adresses IP avec la plage d'adresses IP `192.168.5.x` :

Plage d'adresses IP	Clients
192.168.5.1 à **192.168.5.49**	Client avec adresse IP fixe
192.168.5.1	Routeur Internet (passerelle)
192.168.5.10	PC serveur (OpenScape Business S)
192.168.5.20	Serveur e-mail
192.168.5.100 à **192.168.5.254**	PC client & téléphones IP, en même temps carnet d'adresses IP du serveur DHCP, l'affectation des adresses IP aux clients est dynamique

6.4 Plan de numérotation

Le plan de numérotation est une liste de tous les numéros de téléphone disponibles dans le système de communication. Il comprend des numéros internes, des numéros SDA et des numéros de groupe.

Plan de numérotation par défaut

La plupart des numéros sont prédéfinis avec des valeurs par défaut. Si nécessaire, ces valeurs peuvent être adaptées en fonction des exigences propres (plan de numérotation individuel).

Extrait du plan de numérotation par défaut :

Type de numéros de téléphone	Numéros par défaut
Numéros d'abonnés internes	100-349, 500-709
Numéros SDA d'abonnés	100-349, 500-709
Numéros de groupes	350-439
Numéro de messagerie vocale	71
Numéro de téléphone du lecteur d'annonces (Announcement Player)	72
Préfixes faisceaux (indicatifs externes) : Réseau ITSP	855-858
Numéro de téléphone pour conférences	7400-7404

Type de numéros de téléphone	Numéros par défaut
Numéro pour le parcage	7405
Numéro de téléphone pour standard automatique	7410-7429
Numéro de téléphone pour conférence MeetMe (rendez-vous)	7430

Plan de numérotation individuel

Durant la configuration de base, il est possible d'importer un plan de numérotation individuel dans WBM à l'aide d'un fichier XML.

Le fichier XML comprend plusieurs onglets. En plus du nom et du numéro de téléphone des abonnés, l'onglet "Client" contient d'autres renseignements sur les abonnés, par ex. les types d'abonnés et les adresses e-mail des abonnés.

Vous trouverez un exemple de fichier XML avec les explications correspondantes dans WBM, **Centre de service** > **Documents** > **Modèles** > **Modèles CSV**. Vous pouvez utiliser comme modèle pour vos données le fichier XML enregistré là. Il peut être traité à l'aide de Microsoft Excel par exemple.

6.5 Installation du logiciel de communication

Le logiciel de communication OpenScape Business S est installé sur le serveur Linux.

Assurez-vous que les adresses IP et les masques de réseau à configurer sont adaptés au LAN du client.

Serveur DHCP

Un serveur DHCP attribue automatiquement une adresse IP unique à chaque station IP (téléphones IP, PC, etc.) et fournit aux stations IP des données spécifiques au réseau telles que l'adresse IP de la passerelle par défaut, par exemple.

Un serveur DHCP externe (par exemple, le serveur DHCP du routeur Internet ou du système de communication) ou le serveur DHCP du serveur Linux peut être utilisé comme serveur DHCP. Si le serveur DHCP du serveur Linux est utilisé, le serveur DHCP externe doit être désactivé. La configuration du serveur DHCP Linux peut être effectuée lors de l'installation du logiciel de communication OpenScape Business.

Remarque : Vous devez activer le DHCP soit à partir de yast, soit à partir de WBM, mais pas à partir des deux. Si vous activez le DHCP pendant l'installation initiale d'OpenScape Business S, cela équivaut à activer le DHCP via yast. Si vous souhaitez activer le DHCP sur OpenScape Business S à partir de WBM, le DHCP ne doit pas être activé lors de l'installation initiale du logiciel de communication.

Environnement virtuel

Le logiciel de communication peut être exécuté dans un environnement virtuel. Il y a deux façons d'effectuer l'installation :

- Installation séparée de Linux et du logiciel de communication

  Pour ce faire, le logiciel de virtualisation (système d'exploitation hôte) doit d'abord être installé et configuré sur le PC serveur. Linux est installé dans l'environnement virtuel en tant que système d'exploitation invité. Dans le système d'exploitation Linux, le logiciel de communication est installé en dernier à l'aide du DVD OpenScape Business ou du fichier .ISO (voir *OpenScape Business Linux Server, Guide d'installation* pour plus de détails).
- Installation combinée de Linux et du logiciel de communication (VMWare uniquement)

  Pour ce faire, le logiciel de virtualisation (système d'exploitation hôte) doit d'abord être installé et configuré sur le PC serveur. Une image OVA (Open Virtualization Appliance), qui comprend Linux et le logiciel de communication, est installée dans l'environnement virtuel. L'image OVA est fournie par le serveur de fourniture de logiciels (SWS).

  Pour plus de 50 utilisateurs, la partition d'origine doit être redimensionnée après l'installation à 100 GO (pour 50 à 100 utilisateurs) ou 200 GO (pour jusqu'à 500 utilisateurs ou pour OpenScape Business Contact Center) ou 500 GO (pour plus de 500 utilisateurs).

  Pour les mises à jour Linux, vous avez également besoin de la clé de mise à niveau OpenScape Business SLES pour pouvoir vous enregistrer auprès de Linux.

Utilisation de snapshots sur les machines virtuelles (VM) :

Les instantanés peuvent constituer un mécanisme de maintenance précieux, par exemple pour effectuer un retour rapide à un état de fonctionnement prédéfini de la VM après l'échec d'un script de distribution de masse.

- Les instantanés ne peuvent pas être créés en fonctionnement normal. L'état de fonctionnement actuel de la machine virtuelle est gelé lors de la prise d'un instantané. Par conséquent, les terminaux et applications connectés, tels que les téléphones IP ou les clients UC, peuvent perdre la connexion avec le serveur.
- Les instantanés peuvent entraîner une perte de synchronisation des processus internes du serveur, ce qui signifie que le fonctionnement stable du système de communication ne peut plus être garanti. Un redémarrage du serveur après l'instantané doit donc également être prévu dans le calendrier de maintenance.
- Les instantanés précédents ne doivent pas rester dans l'environnement de production pendant le fonctionnement normal.
- Les instantanés peuvent être pris pendant une fenêtre de maintenance planifiée ou dans le cadre de l'installation.
- Les instantanés sont utilisés en interne par les outils de sauvegarde tels que VDP ou VDR. Il faut veiller à ce que ces opérations de sauvegarde soient programmées en dehors des heures de bureau et que les instantanés générés par ces outils soient supprimés à la fin de l'opération.

De plus amples informations sur les instantanés sont disponibles dans la base de connaissances (KB) de VMware. Le point de départ est l'article KB 1025279 - Bonnes pratiques pour les instantanés de machines virtuelles dans l'environnement VMware (`http://kb.vmware.com/kb/1025279`).

Toutes les informations sur les instantanés dans Microsoft Hyper-V se trouvent dans la bibliothèque technet à l'adresse technet.microsoft.com, dans le chapitre Hyper-V.

6.5.1 Comment installer le logiciel de communication

Conditions préalables

- Le système d'exploitation SLES 12 SP5 ou SLES 15 SP6 a été correctement installé et démarré sur le serveur Linux.
- DVD ou fichier .ISO avec le logiciel de communication OpenScape Business.
- DVD ou fichier .ISO ou clé USB avec le système d'exploitation Linux SLES 12 SP5 64 bits ou SLES 15 SP6 64 bits, pour toute installation ultérieure de progiciels (RPM) éventuellement nécessaire.
- Les données d'accès à la racine (nom d'utilisateur et mot de passe) pour se connecter au serveur Linux sont disponibles.

Important : Le logiciel de communication OpenScape Business écrase tous les fichiers de configuration existants (par exemple, pour DHCP, FTP, Postfix, etc.) pendant l'installation.

Étape par étape

1) Connectez-vous au serveur Linux avec les privilèges root.

2) Insérez le DVD OpenScape Business ou le fichier .ISO dans le lecteur de DVD.

3) Confirmez le message en cliquant sur **Exécuter**. La fenêtre "Bienvenu" s'affiche.

4) Sélectionnez la langue d'installation souhaitée (par exemple, l' **anglais**) et cliquez sur **Démarrer**. La suite de l'installation est décrite ici pour la langue anglaise.

5) Sélectionnez le produit souhaité dans la liste et cliquez sur **Sélectionner**. Une vérification est effectuée pour déterminer si le matériel répond à toutes les exigences de l'installation. Un avertissement s'affiche en cas de manquement mineur. Après confirmation, l'installation peut se poursuivre. En cas de manquement grave, l'installation est automatiquement annulée.

6) Une vérification est effectuée pour déterminer si des paquets RPM supplémentaires doivent être installés. Si c'est le cas, vous devez le confirmer en cliquant sur **Confirmer**. Si cela se produit, vous devrez revenir à SLES 12 ou SLES 15, DVD ou fichier .ISO plus tard.

7) Une fenêtre contenant les termes de la licence (c'est-à-dire le Contrat de licence de l'utilisateur final ou EULA) s'affiche. Lisez les termes de la licence et acceptez le contrat de licence en cliquant sur **Oui**.

8) Si un serveur DHCP est déjà présent dans le LAN du client (par exemple, le serveur DHCP du routeur Internet), arrêtez la configuration du serveur DHCP Linux en cliquant sur **Non** et passez à l'étape 12 pour continuer.

Remarque : Pour que le logiciel des téléphones système puisse être mis à jour automatiquement même en cas

d'utilisation d'un serveur DHCP externe, deux possibilités s'offrent à vous :

a) L'adresse IP du serveur Linux doit être saisie comme adresse DLS sur chaque téléphone système.

b) Les données spécifiques au réseau doivent être saisies sur le serveur DHCP externe. Les paramètres correspondants se trouvent sous `/var/log/OPTI.txt`.

---

9) Si vous souhaitez utiliser le serveur DHCP Linux, cliquez sur **Oui** pour activer et configurer le serveur DHCP Linux.

10) Entrez les valeurs suivantes (prédéfinies avec les valeurs par défaut) :

- **Route par défaut** : Adresse IP de la passerelle par défaut ; en règle générale, l'adresse IP du routeur Internet, par exemple `192.168.5.1`.
- **Domaine** (facultatif) : le domaine spécifié lors de l'installation de Linux, par exemple, `<customer>.com`
- **DNS - Server** (facultatif) : Adresse IP du serveur DNS spécifié lors de l'installation de Linux. Si aucun serveur DNS n'est disponible dans le réseau interne, vous pouvez entrer l'adresse IP du routeur Internet (par exemple, `192.168.5.1`) ici.
- **Serveur SNTP** : Adresse IP du serveur NTP interne ou externe.
- **Serveur DLS/DLI** : Adresse IP du serveur DLS, c'est-à-dire l'adresse IP du serveur Linux (par ex : `192.168.5.10`).
- **Sous-réseau**: sous-réseau approprié pour la plage d'adresses IP, par ex : `192.168.5.0`.
- **Masque de réseau** : Masque de sous-réseau du serveur Linux qui a été spécifié lors de l'installation de Linux, par ex : `255.255.255.0`.
- **Début de la plage d'adresses IP** et **Fin de la plage d'adresses IP** : Plage d'adresses IP à partir de laquelle le serveur DHCP peut attribuer des adresses IP, par ex : `192.168.5.100` à `192.168.5.254`.

11) Cliquez sur **Continuer**.

12) Après l'installation, le système d'exploitation Linux doit être redémarré. Cochez la case **Redémarrage du PC** et confirmez en cliquant sur **Continuer**.

13) Si des paquets RPM supplémentaires doivent être installés, vous serez invité à insérer le DVD SLES 12 ou la clé USB SLES 15. Insérez le DVD ou la clé USB et confirmez en cliquant sur **Continuer**. Une fois l'installation des paquets RPM réalisée avec succès, réinsérez le DVD ou le fichier .ISO d'OpenScape Business et confirmez en cliquant sur **Continuer**, puis sur **Exécuter**.

14) Le logiciel de communication OpenScape Business est installé. Le système d'exploitation effectue ensuite un redémarrage automatique.

15) Après le redémarrage, connectez-vous avec le compte d'utilisateur configuré précédemment lors de l'installation de Linux.

16) Cliquez avec le bouton droit de la souris sur l'icône du lecteur de DVD sur le bureau et sélectionnez l'élément de menu **Éjecter**. Retirez le DVD OpenScape Business du lecteur de DVD.

Remarque : Il faut quelques minutes pour que tous les composants du logiciel de communication OpenScape Business soient actifs.

6.6 Mise en service

La configuration de base est effectuée avec l'assistant **Première installation** du WBM.

6.6.1 Comment démarrer l'assistant Lancer la première installation

Conditions préalables

WBM est démarré.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** pour lancer l'Assistant **Première installation**.

Remarque : Sur les écrans à faible résolution, lorsque l'espace de travail n'est pas entièrement affiché en raison de la taille de la fenêtre du navigateur, il s'affiche des barres de défilement horizontales et verticales de manière à pouvoir dérouler la partie affichée.

Étapes suivantes

Effectuez la première installation comme indiqué ci-après, étape après étape. Les champs qui ne sont pas décrits ici sont paramétrés de manière adaptée à un cas normal ; ils ne doivent être modifiés que s'ils ne correspondent pas à vos données réseau. Les informations complètes figurent dans la description de chacun des Assistants.

6.6.2 Paramètres système

Dans la fenêtre **Paramètres système** configurez les paramètres du système de communication.

Pour cela, suivez les étapes suivantes :

1) Définir le logo écran et la désignation du produit

   Vous pouvez définir un texte qui va s'afficher à l'écran des téléphones système. En plus, vous pouvez sélectionner la désignation du produit.
2) Sélectionnez l'identification du pays et la langue pour les journaux d'événements

   Pour une initialisation correcte du pays, vous devez choisir le pays dans lequel le système de communication est utilisé. En plus, vous pouvez choisir la langue dans laquelle les journaux d'événements (journaux des événements système, des erreurs, etc.) seront enregistrés.
3) Uniquement en cas de besoin : activer un raccordement LAN supplémentaire en tant qu'interface WAN

   Si OpenScape Business S (ou le serveur Linux) dispose d'un deuxième raccordement LAN, vous pouvez le paramétrer en tant qu'interface WAN pour l'accès Internet et pour la téléphonie Internet via ITSP. Le premier

raccordement LAN sert comme d'habitude en tant qu'interface LAN pour les téléphones et PC internes.

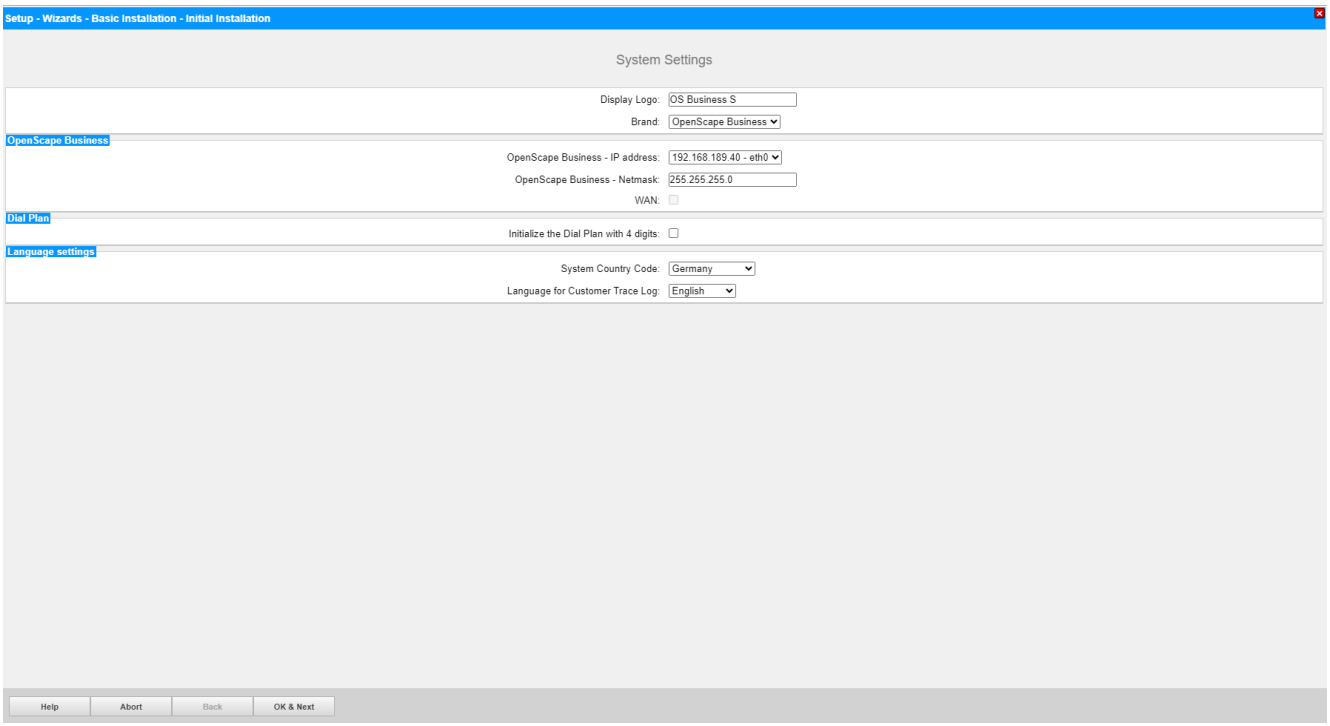
4) Modifier le plan de numérotation par défaut pour des numéros à 4 chiffres (disponible uniquement pour OSBiz S)

Lors d'une nouvelle installation du système, vous pouvez initialiser le plan de numérotation avec 4 chiffres au lieu de 3. Ce faisant, les numéros par défaut du système passent de 100, 101, 102, ..., à 1000, 1001, 1002, et ainsi de suite. Cela permet l'attribution automatique de numéros d'appel pour un grand nombre de postes utilisateurs. Notez qu'après avoir activé cet indicateur, le système redémarre.

6.6.2.1 Comment déterminer le logo d'écran et la désignation du produit

Conditions préalables

Vous êtes dans la fenêtre **Paramètres système**.



Étape par étape

1) Dans le champ **Logo d'écran** entrez un texte de votre choix (par ex. OS Business S). Le texte peut avoir jusqu'à 16 caractères. Evitez les inflexions et les caractères spéciaux.

2) Sélectionnez le nom du produit souhaité dans la liste déroulante **Marque**.

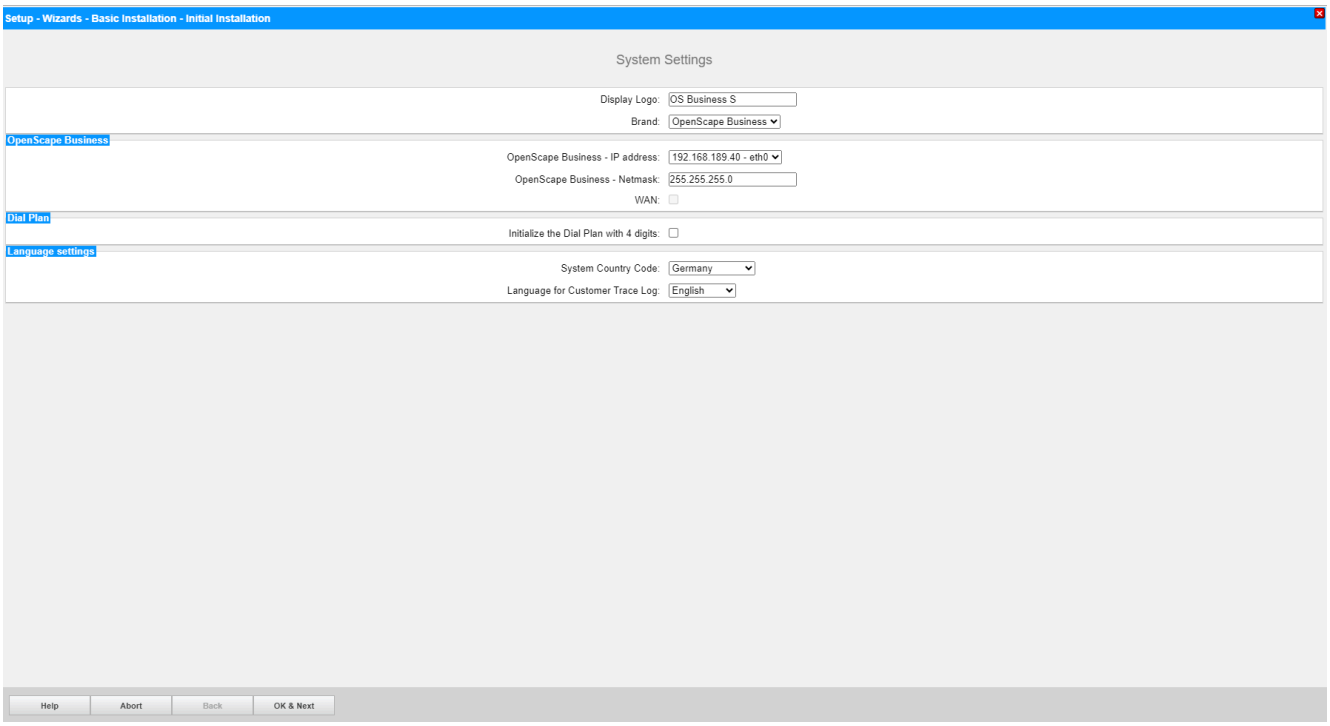
Étapes suivantes

Sélectionnez l'indicatif de pays et la langue pour les journaux de trace.

6.6.2.2 Comment sélectionner l'indicatif de pays et la langue du journal de trace

Conditions préalables

Vous êtes dans la fenêtre **Paramètres système**.



Étape par étape

1) Dans la liste déroulante **Indicatif de pays du système**, sélectionnez le pays où le système de communication sera utilisé.
2) Dans le champ **Langue du Journal de trace client** sélectionnez la langue dans laquelle les journaux d'événements (journaux des événements système, des erreurs, etc.) seront publiés.

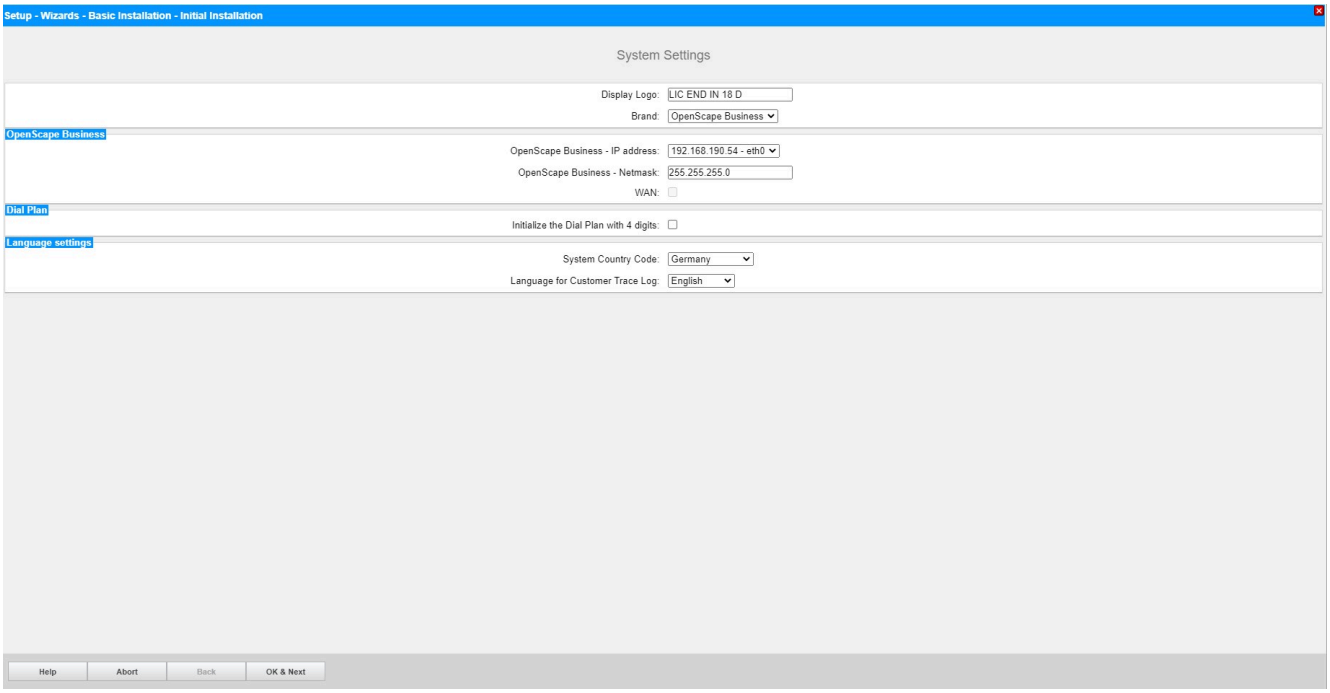
Étapes suivantes

Démarrer la configuration de base

6.6.2.3 Comment activer un port LAN supplémentaire en tant qu'interface WAN

Conditions préalables

Vous êtes dans la fenêtre **Paramètres système**.



Étape par étape

1) Cochez la case **WAN**.
2) Sélectionnez le port LAN souhaité (par exemple, `eth1` ou `eth2`) dans la liste déroulante **OpenScape Business - Adresse IP (WAN)**. Si seuls deux ports LAN sont disponibles, le deuxième port LAN `eth1` est activé automatiquement.

Important : Veillez à sélectionner l'interface réseau réelle et non l'hôte local.

Remarque : L'attribution des adresses IP et des masques de sous-réseau aux ports LAN s'effectue lors de l'installation initiale de Linux ou ultérieurement via YaST.

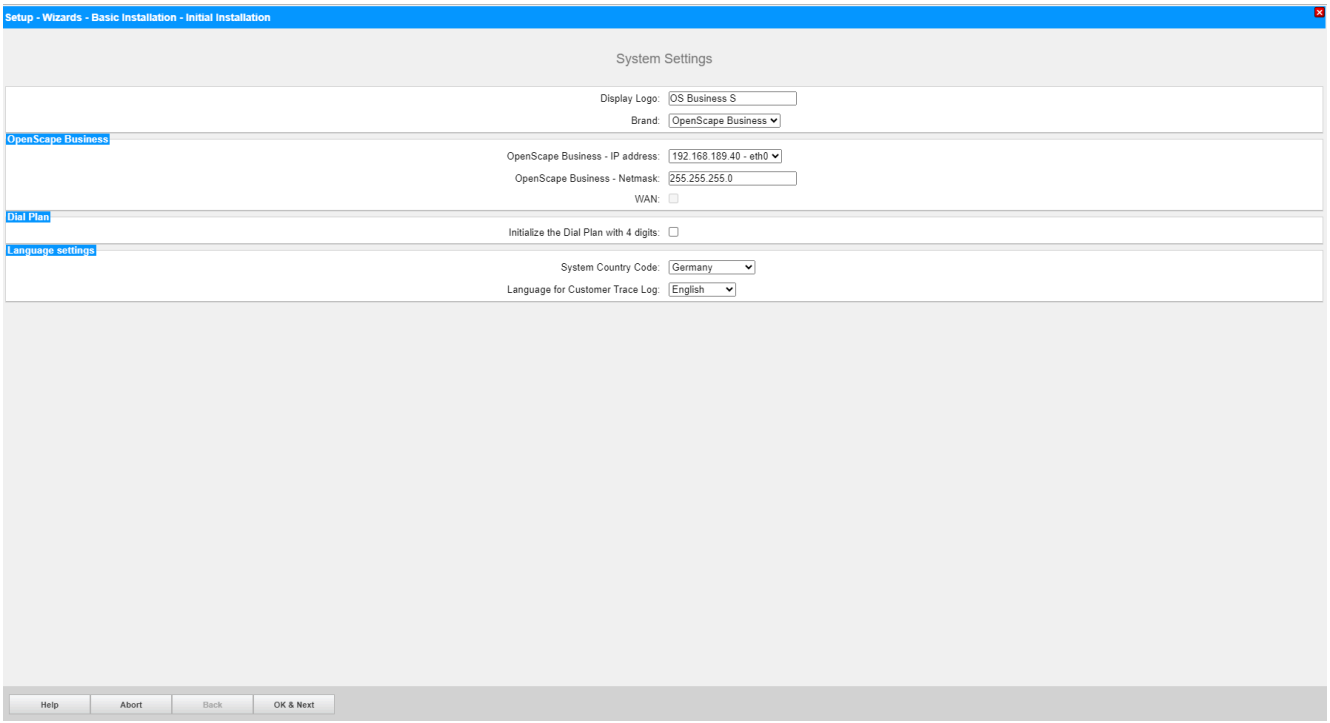
Étapes suivantes

Précisez la solution UC.

6.6.2.4 Comment modifier le plan de numérotation à 4 chiffres

Conditions préalables

Vous êtes dans la fenêtre **Paramètres système**.



Étape par étape

Cliquez sur la case à cocher du champ **Initialiser le plan de numérotation à 4 chiffres**.

Étapes suivantes

Le système redémarre

6.6.3 Solution UC

Dans la fenêtre **Modifier la sélection de l'application**, vous définissez la solution UC que vous utilisez.

Vous disposez des possibilités suivantes :

- **Pack avec UC Smart**

  La solution UC Smart est intégrée dans OpenScape Business S.
- **Pack avec UC Suite**

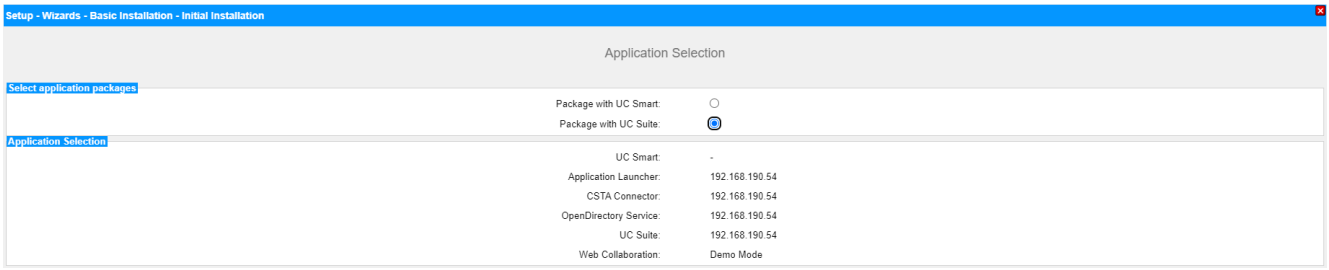
  La solution UC Suite est intégrée dans OpenScape Business S.

6.6.3.1 Comment définir la solution UC

Conditions préalables

Vous avez fait l'acquisition de licences soit pour la solution UC Smart soit pour la solution UC Suite.

Vous êtes dans la fenêtre **Sélection de l'application**.



Étape par étape

1) Si vous utilisez la solution UC Smart, cliquez sur **Pack avec UC Smart**.
2) Si vous utilisez la solution UC Suite, cliquez sur **Pack avec UC Suite**.
3) Cliquez sur **OK & Suivant**.
4) L'assistant **Première installation** se ferme. Cliquez sur **Terminer**.

Étapes suivantes

Démarrer la configuration de base

6.7 Configuration de base

La configuration de base est effectuée avec l'assistant **Installation de base** de la WBM. Les principaux paramètres d'exploitation du système de communication sont définis.

L'assistant d'installation de base comprend un indicateur de progression qui montre l'étape actuelle ainsi que les étapes suivantes.

6.7.1 Comment démarrer l'assistant Installation de base

Conditions préalables

L'Assistant **Première installation** est achevé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** pour lancer l'Assistant **Installation de base**.

Étapes suivantes

Effectuez l'installation de base comme indiqué ci-après, étape après étape. Les champs qui ne sont pas décrits ici sont paramétrés de manière adaptée à un cas normal ; ils ne doivent être modifiés que s'ils ne correspondent pas à vos données réseau. Les informations complètes figurent dans la description de chacun des Assistants.

6.7.2 Numéros système et mise en réseau

Dans la fenêtre **Présentation** entrez les numéros système (Numéro de l'installation, indicatif et indicatif local, préfixe international) et précisez

si OpenScape Business doit être mis en réseau avec d'autres systèmes OpenScape Business.

Procédez de la manière suivante :

1) Entrer les numéros système

- Entrez les numéros système pour connexion d'installation

  Entrez ici le numéro de l'installation pour votre connexion à l'installation ainsi que l'indicatif national et local.

  L'entrée de l'indicatif national est obligatoire pour la téléphonie Internet et pour les fonctions de serveur de conférence.

  Le préfix international dépend de l'indicatif de pays prédéfini auparavant.
- Entrez le numéro système pour raccordement multiposte

  Entrez ici l'indicatif national et local pour votre raccordement multiposte.

  L'entrée de l'indicatif national est obligatoire pour la téléphonie Internet et pour les conférences MeetMe.

  Le préfix international dépend de l'indicatif de pays prédéfini auparavant.

2) Comment activer ou désactiver la mise en réseau

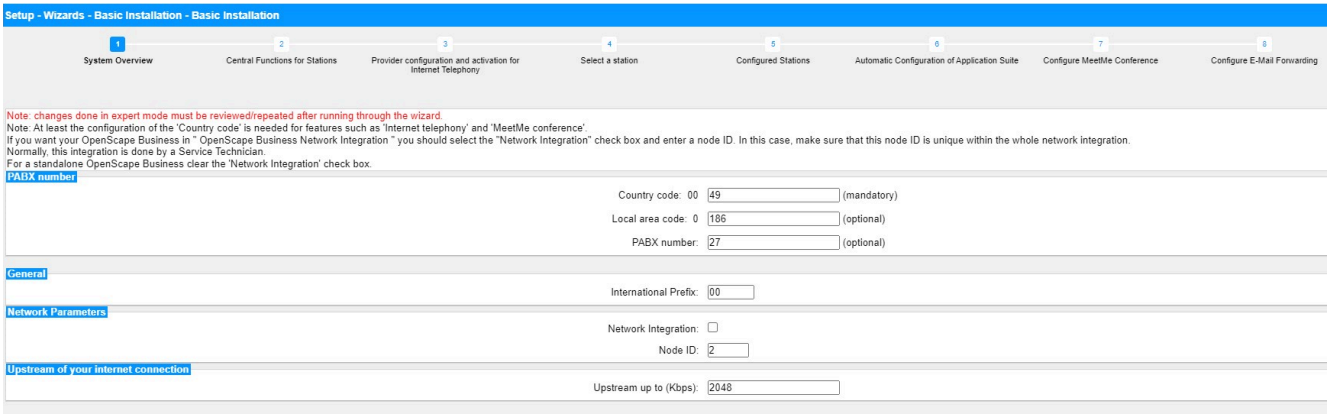
Si OpenScape Business doit être mis en réseau avec d'autres systèmes OpenScape Business, il faut activer la mise en réseau et attribuer à OpenScape Business un ID de noeud. Chaque OpenScape Business en interconnexion de réseaux doit disposer d'un ID de noeud univoque.

6.7.2.1 Comment entrer les numéros de téléphone système pour un raccordement installation

Conditions préalables

Vous disposez d'un raccordement installation.

Vous êtes dans la fenêtre **Vue d'ensemble du système** de l'assistant **Installation de base**.



Étape par étape

1) Dans le champ **Indicatif national**, saisissez l'indicatif national correspondant, par ex. `49` pour l'Allemagne ou `1` pour les États-Unis.

2) Dans le champ **Préfixe du réseau local**, saisissez le préfixe du réseau local, par ex. `89` pour Munich.
3) Dans le champ **N° installation**, saisissez le numéro de l'installation de votre raccordement réseau, par ex. `7007` (votre numéro de raccordement).
4) Modifiez le champ **Préfixe international** uniquement si nécessaire. Les valeurs applicables respectives pour l'Allemagne et les États-Unis sont `00` et `011`.

   Lors des appels téléphoniques à l'étranger, le numéro de téléphone est précédé du préfixe international et de l'indicatif national, par ex. d'Allemagne vers les Etats-Unis par 00-1 et des Etats-Unis vers l'Allemagne par 011-49.

Étapes suivantes

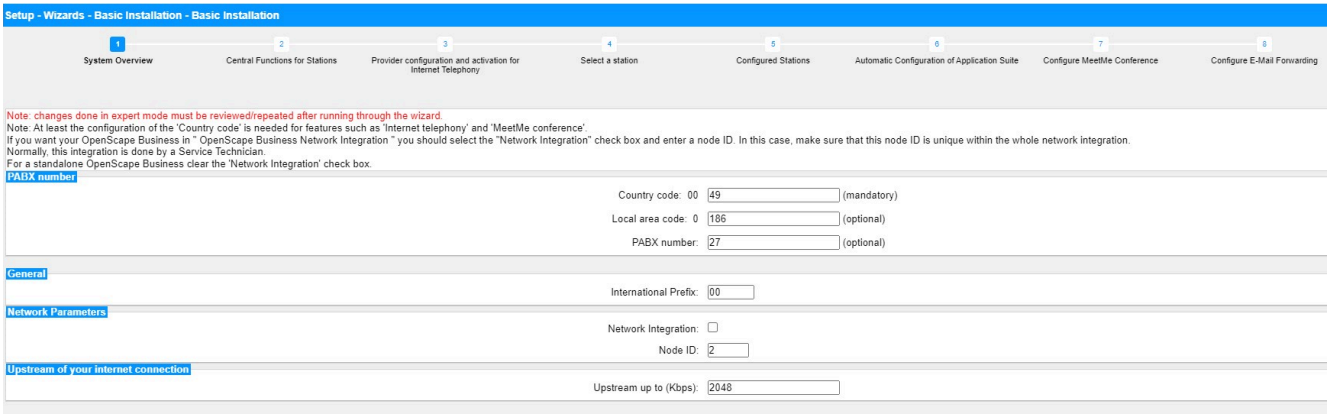
Comment activer ou désactiver la mise en réseau

6.7.2.2 Comment entrer les numéros de téléphone système pour une connexion point à multipoint

Conditions préalables

Vous disposez d'un raccordement multiposte.

Vous êtes dans la fenêtre **Vue d'ensemble du système** de l'assistant **Installation de base**.



Étape par étape

1) Dans le champ **Indicatif national**, saisissez l'indicatif national correspondant, par ex. `49` pour l'Allemagne ou `1` pour les États-Unis.
2) Dans le champ **Préfixe du réseau local**, saisissez le préfixe du réseau local, par ex. `89` pour Munich.
3) Laissez vide le champ **Numéro de l'installation**.
4) Modifiez le champ **Préfixe international** uniquement si nécessaire. Les valeurs applicables respectives pour l'Allemagne et les États-Unis sont `00` et `011`.

   Lors des appels téléphoniques à l'étranger, le numéro de téléphone est précédé du préfixe international et de l'indicatif national, par ex. d'Allemagne vers les Etats-Unis par 00-1 et des Etats-Unis vers l'Allemagne par 011-49.

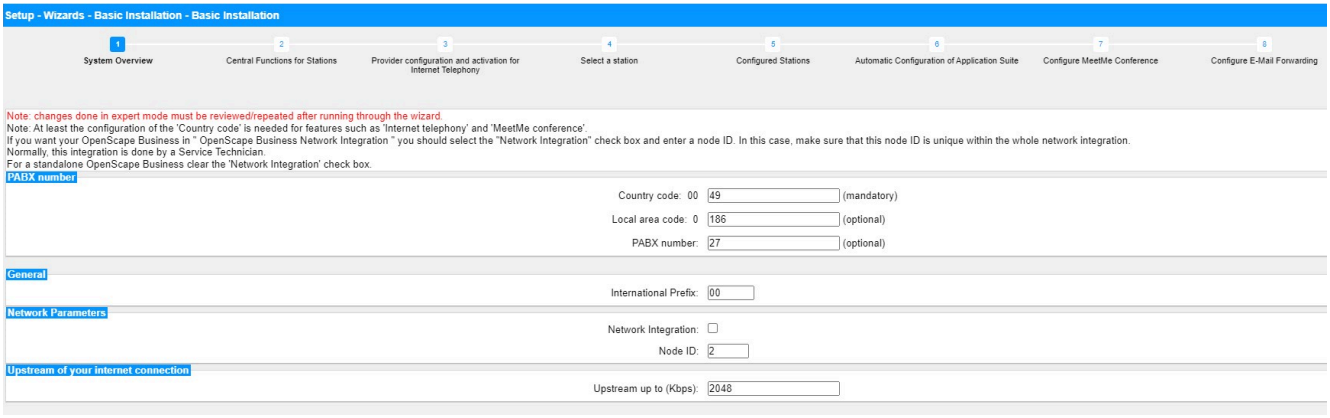
Étapes suivantes

Comment activer ou désactiver la mise en réseau

6.7.2.3 Comment activer ou désactiver la mise en réseau

Conditions préalables

Vous êtes dans la fenêtre **Vue d'ensemble du système** de l'assistant **Installation de base**.



Étape par étape

1) Si le système de communication doit être mis en réseau avec d'autres systèmes de communication :
   a) Cochez la case **Intégration réseau**.
   b) Dans le champ **ID de nœud** attribuez au système de communication un ID de nœud univoque dans l'interconnexion de réseaux (chiffres de `1` à `100` possibles).
2) Si le système de communication ne doit pas être mis en réseau avec d'autres systèmes de communication, ne cochez pas la case **Intégration réseau**.

Étapes suivantes

Configurez le débit remontant de votre connexion Internet.

6.7.2.4 Comment configurer le débit remontant de votre connexion Internet

Conditions préalables

Vous vous trouvez dans la fenêtre **Aperçu**.

Étape par étape

1) Dans le champ **Transfert jusqu'à (kbit/s)**, entrez la vitesse de votre connexion Internet.
2) Cliquez sur **OK&Suivant**.

Étapes suivantes

Comment configurer les données d'abonné.

6.7.3 Données abonnés

Dans la fenêtre **Fonctions centrales pour les abonnés** vous pouvez, si nécessaire, à la place du plan de numérotation standard prédéfini, configurer votre propre plan de numérotation et importer d'autres données d'abonné. Dans une interconnexion de réseaux, le plan de numérotation par défaut doit être harmonisé au plan de numérotation de l'interconnexion de réseaux.

Le plan de numérotation standard contient des numéros prédéfinis pour différents types d'abonné (téléphones IP, téléphones analogiques...) et pour les fonctions spéciales (téléphonie Internet, messagerie vocale, standard automatique...).

Les données d'abonné comprennent notamment les numéros internes, les numéros de sélection directe à l'arrivée et les noms des abonnés. A l'aide d'un fichier XML au format UTF-8, il est possible d'importer ces données et d'autres données d'abonné dans le système de communication durant la configuration de base.

Remarque :

Vous trouverez un modèle XML avec les explications correspondantes dans WBM, sous **Centre de service** > **Documents** > **Modèles CSV**. Dans ce modèle, vous pouvez par ex. inscrire vos données avec Microsoft Excel.

Vous disposez des possibilités suivantes :

- **Configurer les données abonnés sans interconnexion de réseaux**

  Procédez de la manière suivante :

  1) Afficher les données abonné

  Vous pouvez afficher tous les numéros d'appel et toutes les données d'abonné préconfigurées.

  2) Supprimer tous les numéros d'abonnés (option)

  Si vous utilisez un plan de numérotation individuel, vous devez effacer tous les numéros préconfigurés.

  3) Adapter les numéros d'appel préconfigurés au plan de numérotation individuel (option)

  Si vous utilisez un plan de numérotation individuel, vous pouvez adapter les numéros d'appel préconfigurés à votre propre plan de numérotation.

  Remarque :

  Si l'utilisateur passe au travers de **Modifier les numéros d'appel préconfigurés,** toute configuration personnalisée

existante au sein d'UC Suite doit être revue ou répétée (par exemple des files d'attente pilotes)

4) Importer les données d'abonné via fichier XML (option)

   Vous pouvez aisément importer vos numéros d'appels individuels ainsi que les données d'abonné supplémentaires à l'aide d'un fichier XML durant la configuration de base.

- **Configurer les données d'abonné avec interconnexion de réseaux**

  Procédez de la manière suivante :

  1) Supprimer tous les numéros d'abonnés

     Si UC Suite est utilisé dans l'interconnexion de réseaux, il faut recourir à un plan de numérotation fermé, c.-à-d. que tous les numéros de l'interconnexion de réseaux doivent être univoques. Il faut donc effacer les numéros d'appel préconfigurés et utiliser des numéros d'appels adaptés à l'interconnexion de réseaux.
  2) Importer les données d'abonné via fichier XML ()

     Les numéros d'appel adaptés à l'interconnexion de réseaux ainsi que les données d'abonné supplémentaires peuvent être aisément importés à l'aide d'un fichier XML durant la configuration de base. Ce fichier peut contenir tous les abonnées de l'interconnexion de réseaux. Lors de l'importation, seuls sont repris les numéros d'appel et les données d'abonné correspondant à l'ID de noeud du système de communication indiqué précédemment.

Tâches associées

Comment afficher les données de masse à la page 134
Comment réinitialiser les entrées LCR à la page 1354

Référence associée

LCR > Flags LCR à la page 1540

6.7.3.1 Comment afficher les données d'abonné

Conditions préalables

Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l'assistant **Installation de base**.

Étape par étape

1) Cochez le champ d'option **Afficher la configuration des abonnés**.
2) Cliquez sur **Exécuter la fonction**. Une liste des abonnés avec les numéros préconfiguré (plan de numérotation par défaut) s'affiche pour vous.
3) Cliquez sur **OK**. Vous revenez à la fenêtre **Fonctions centrales pour les abonnés**.
4) Si vous ne souhaitez pas modifier les données d'abonné, cliquez sur **OK & Suivant**.

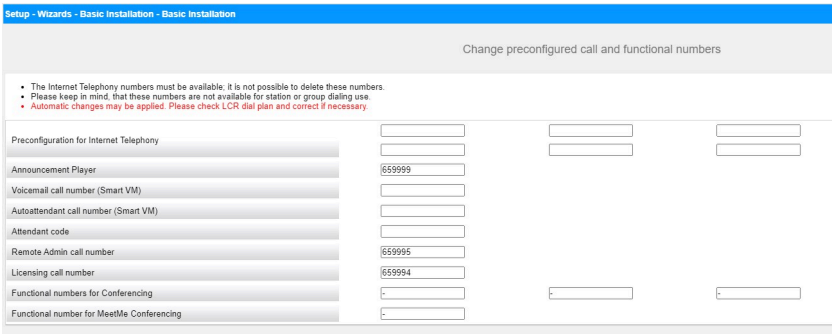
6.7.3.2 Comment supprimer tous les numéros d’appel

Conditions préalables

Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l’assistant **Installation de base**.

Étape par étape

1) Activez le champ d’option **Supprimer tous les numéros d’abonné**.
2) Cochez **Effacer tous les numéros**.
3) Cliquez sur **Exécuter la fonction**. Tous les numéros d’appel prédéfinis sont effacés à l’exception de **Lecteur annonce, Numéro d’appel Admin distant** et **Numéro d’appel Licences**. Apparaît ensuite la fenêtre **Modifier les numéros d’appel préconfigurés**.



4) Adaptez les indicatifs et les numéros d’appel spéciaux à vos souhaits et cliquez ensuite sur **OK**. Vous revenez à la fenêtre **Fonctions centrales pour les abonnés**.
5) Si vous ne souhaitez plus configurer d’autres données d’abonné, cliquez sur **OK & Suivant**.

6.7.3.3 Adapter les numéros d’appel préconfigurés au plan de numérotation individuel

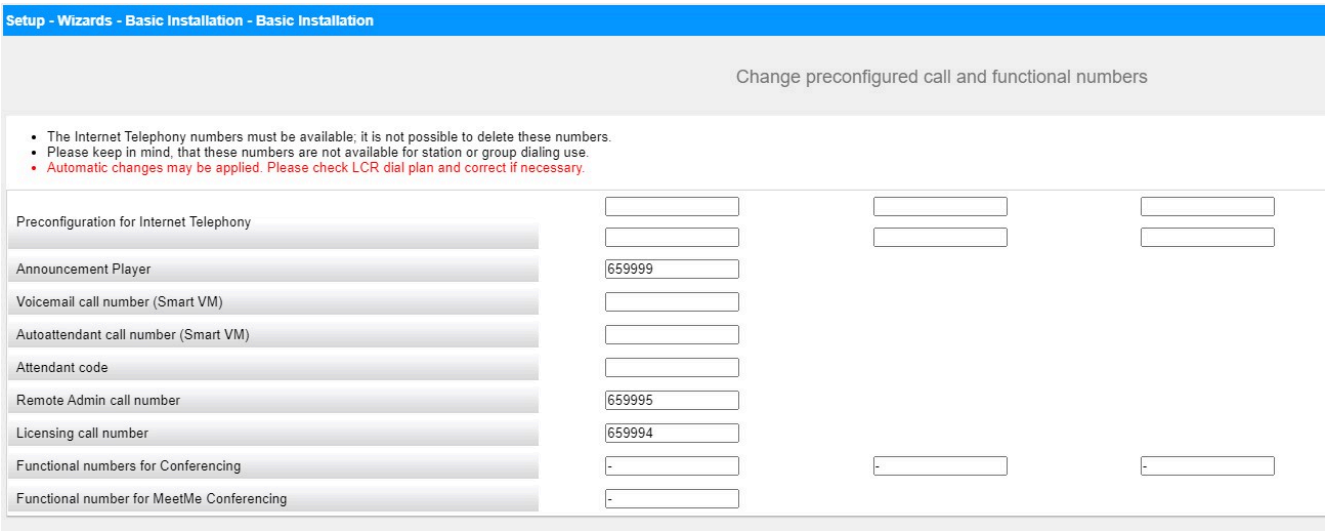
Conditions préalables

Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l’assistant **Installation de base**.

Étape par étape

1) Activez le bouton radio **Modifier les numéros d’appel et les numéros fonctionnels préconfigurés**.

2) Cliquez sur **Exécuter la fonction**. La fenêtre **Modifier les numéros d'appel préconfigurés** s'affiche.



3) Adaptez les numéros d'appel préconfigurés à vos souhaits et cliquez ensuite sur **OK**. Vous revenez à la fenêtre **Fonctions centrales pour les abonnés**.
4) Si vous ne souhaitez plus configurer d'autres données d'abonné, cliquez sur **OK & Suivant**.

6.7.3.4 Comment importer les données d'abonné via un fichier XML

Conditions préalables

Vous êtes dans la fenêtre **Fonctions centrales pour les abonnés** de l'assistant **Installation de base**.

Un fichier XML au format UTF-8 avec les données inscrites est disponible. Vous trouverez un modèle XML dans **Centre de service** > **Documents** > **Modèles CSV**.

Étape par étape

1) Cochez le champ d'option **Importer le fichier CSV/XML avec les données d'abonné**.
2) Cliquez sur **Exécuter la fonction**.
3) Avec **Parcourir**, sélectionnez le fichier XML souhaité et cliquez sur **Ouvrir**.
4) Pour finir, cliquez sur **OK**. Les données d'abonnés sont importées.
5) Cliquez sur **OK & Suivant**.

6.7.4 Accès Internet

6.7.4.1 Comment configurer l'accès à Internet via un routeur Internet externe sur le LAN avec un port WAN dédié à l'ITSP

Conditions préalables

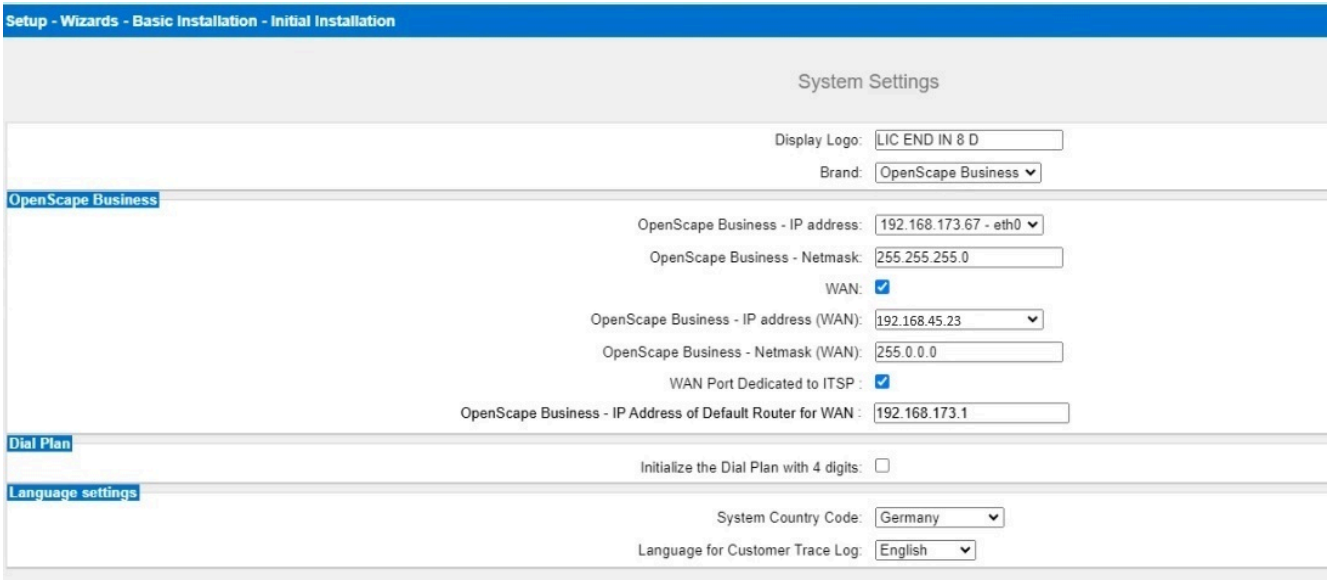
Vous avez créé une nouvelle interface réseau dans le SLES.

Vous êtes dans la fenêtre **Paramètres du système** de l'assistant d'**installation initiale**.

Veuillez noter que cette fonctionnalité ne s'applique qu'aux ITSP qui n'exigent pas l'utilisation de STUN dans les paramètres du fournisseur.

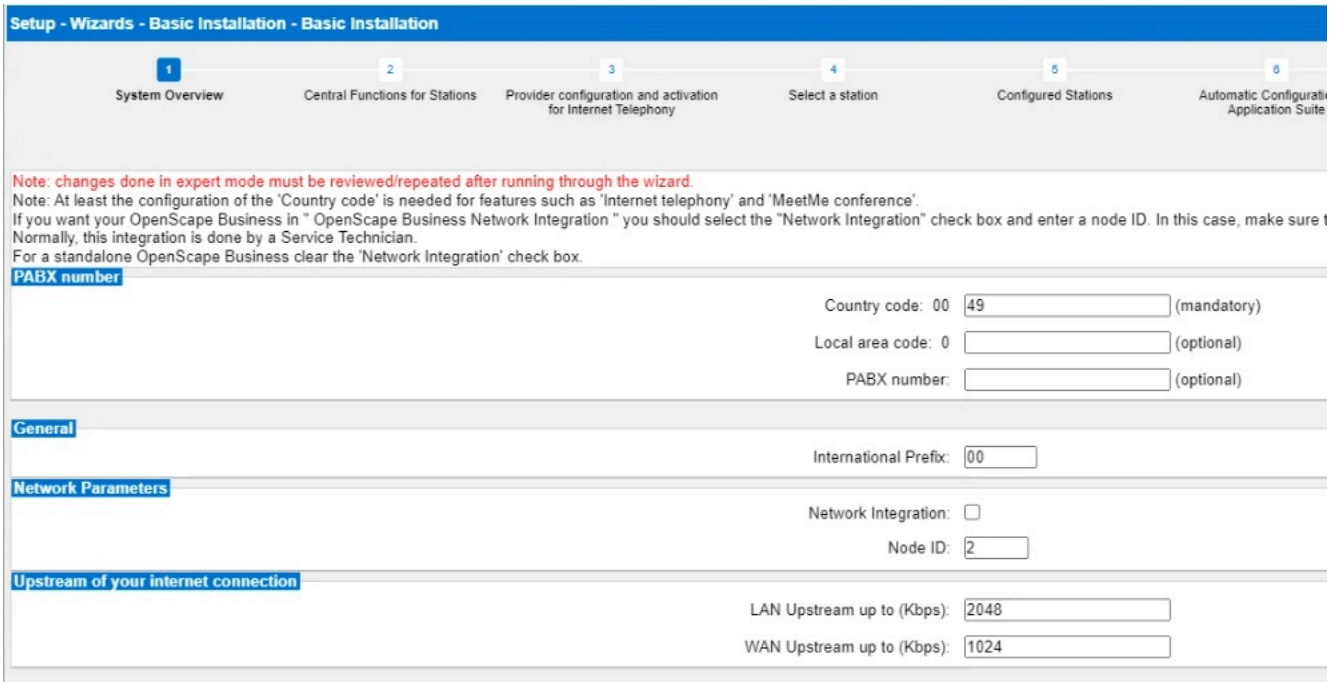
Étape par étape

1) Activez la case à cocher **WAN** et sélectionnez l'interface réseau appropriée. L'option **Interface WAN dédiée à l'ITSP** devient disponible.
2) Cliquez sur pour activer la case à cocher **Interface WAN dédiée à l'ITSP**.



3) Cliquez sur **OK & Suivant**.
4) Naviguez vers **Configuration > Installation de base** et exécutez l'assistant d'**installation de base**.

5) Configurez les valeurs maximales en amont dans les champs correspondants **LAN Upstream jusqu'à (Kbps)** et **WAN Upstream jusqu'à (Kbps)**.



6) Cliquez sur **OK & Suivant**.

7) Après avoir appliqué la configuration, un redémarrage du système est nécessaire.

6.7.5 Téléphonie Internet

Dans la fenêtre **Configuration et activation du fournisseur pour la téléphonie Internet**, vous configurez la téléphonie Internet. Vous pouvez configurer des fournisseurs de service de téléphonie sur Internet (ITSP - Internet Telephony Service Provider) préconfigurés ou nouveaux. Pour chaque fournisseur ITSP, vous pouvez configurer un ou plusieurs comptes. Au maximum 8 fournisseurs ITSP peuvent être actifs simultanément.

Vous disposez des possibilités suivantes :

- **Configurer un ITSP prédéfini**

  Vous pouvez utiliser des modèles ITSP prédéfinis. Pour cela, on entre dans ce modèle les propres données d'accès et numéros d'appel et on les active ensuite.
- **Configurer un nouvel ITSP**

  Vous pouvez aussi ajouter et activer de nouveaux ITSP.

  Configurer un nouvel ITSP n'est nécessaire que dans des cas rares et demande beaucoup de temps. C'est pourquoi cette possibilité n'est pas décrite dans la première installation. Vous trouverez des informations plus précises au chapitre Configuration d'un ITSP.
- **Désactiver la téléphonie Internet**

  Vous pouvez désactiver la téléphonie Internet.

Remarque :

Vous trouverez des exemples de configuration sur Internet dans **Unify Experts Wiki** sous *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Affectation des numéros de téléphone ITSP

- Dans un **raccordement d'installation téléphonie Internet**, l'ITSP fournit des numéros de téléphone individuels, par ex. 70005555, 70005556, ... Ces numéros de téléphone individuels sont ensuite attribués manuellement aux numéros internes des abonnés.
- Dans un **raccordement d'installation téléphonie Internet**, l'ITSP fournit un groupe de numéros de téléphone (plage de numéros de téléphone), par ex.(+49) 89 7007-100 à (+49) 89 7007-147. Les numéros de téléphone de ce groupe de numéros sont ensuite attribués manuellement aux numéros internes des abonnés.

Les deux types de raccordement peuvent être combinés.

Autre variante : pour les deux types de raccordement, les numéros ITSP peuvent être inscrits comme numéros SDA des abonnés lors de la configuration des stations.

Numéro interne	Nom	SDA
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Les numéros de téléphone ITSP résultent donc des numéros d'installation créés (par ex. indicatif national 49) et des numéros de sélection directe à l'arrivée au format long qui ont été inscrits. Cela a des avantages pour l'évaluation de la numérotation et la gestion des appels dans une interconnexion de réseaux. Ainsi, le raccordement ITSP permet par ex. la sélection en direction d'un autre noeud.

Un autre raccordement réseau via RNIS n'est dans ce cas possible qu'avec certaines restrictions (utile toutefois pour appels d'urgence).

6.7.5.1 Comment configurer un ITSP prédéfini

Conditions préalables

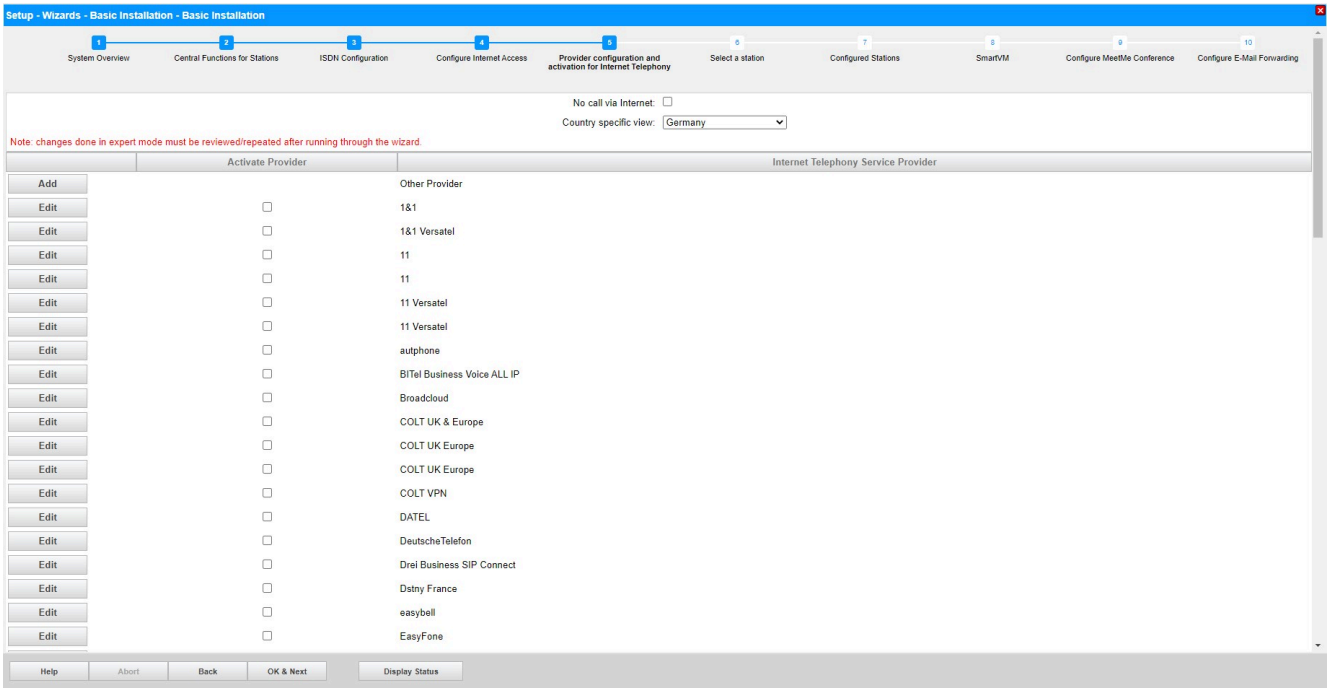
Vous vous trouvez dans la fenêtre **Configuration et activation du fournisseur pour la téléphonie Internet** de l'assistant **Installation de base**.

La connexion à Internet est opérationnelle.

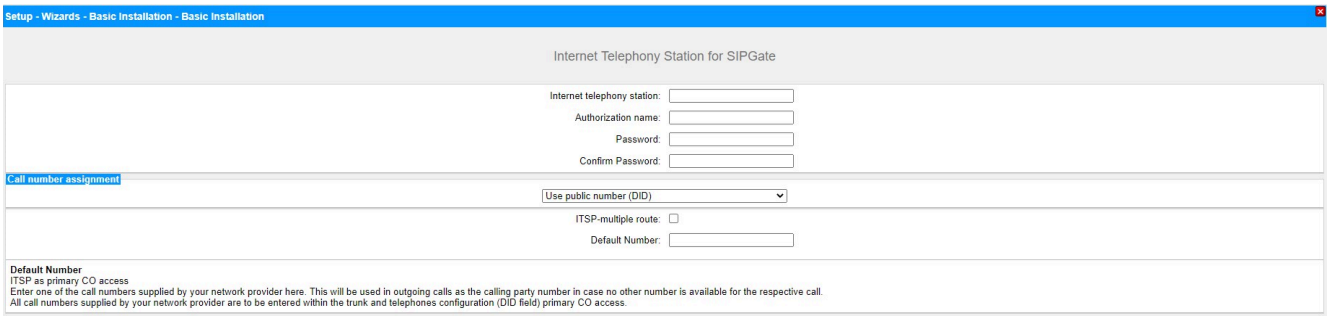
Vous disposez des données d'accès de téléphonie Internet de votre ITSP (par ex. ID utilisateur, mot de passe, numéros d'abonné de la téléphonie Internet).

Étape par étape

1) Décochez **Pas de téléphonie par Internet**. Le système affiche une liste des ITSP disponibles, en fonction du pays. La liste contient les ITSP prédéfinis pour le pays sélectionné et éventuellement les ITSP nouvellement ajoutés.



2) Si vous souhaitez modifier le pays présélectionné, sélectionnez le pays souhaité dans la liste **Affichage spécifique du pays**. Les ITSP possibles pour le pays sélectionné s'affichent.
3) Si nécessaire, cliquez sur **Afficher le statut** pour savoir quels ITSP sont déjà activés et quels abonnés téléphonie Internet sont déjà inscrits sur les ITSP. Vous pouvez activer 8 ITSP au maximum. Pour finir, cliquez sur **OK**.
4) Dans la ligne du ITSP correspondant, cliquez sur **Modifier** afin d'activer un ITSP prédéfini.
5) Cochez **Activer le fournisseur**.
6) Cliquez sur **OK & Suivant**.
7) Cliquez sur **Ajouter** pour configurer vos comptes ITSP avec les numéros correspondants de téléphonie sur Internet. Les champs affichés ensuite sont fonction du fournisseur d'accès.



8) Dans le champ **Abonné de téléphonie Internet** entrez les données d'accès de votre compte. Les données ont été fournies par votre ITSP.

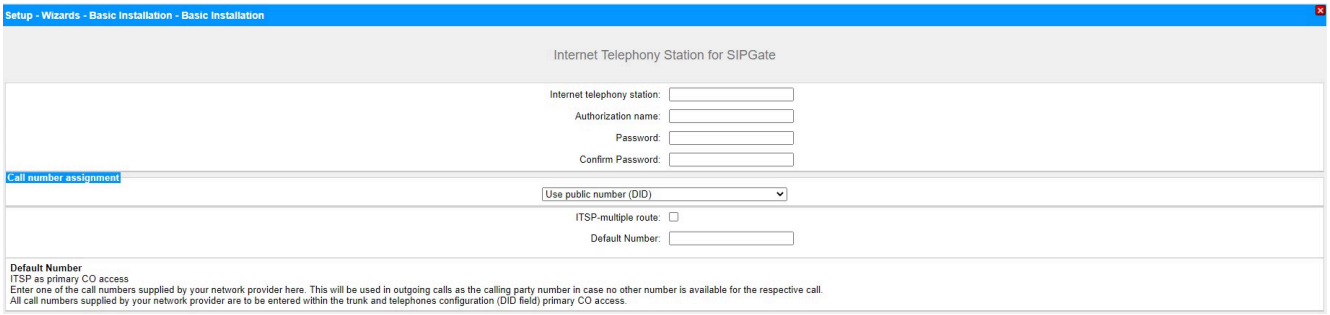
Suivant l'ITSP, des désignations différentes sont utilisées, par ex. : Utilisateur SIP, ID SIP, etc.

9) Entrez dans **Nom d'autorisation** le nom d'autorisation. Les données ont été fournies par votre ITSP. Si vous n'avez pas reçu de nom d'autorisation, entrez les mêmes données que dans **Abonné de téléphonie Internet**.

10) Dans les champs **Nouveau mot de passe** et **Répéter le mot de passe**, entrez le mot de passe que vous avez reçu du ITSP. Suivant l'ITSP, des désignations différentes sont utilisées, par ex. : Mot de passe, mot de passe SIP, etc.

11) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 1 :

Numéro de téléphone public (SDA) : les numéros de téléphone Internet de votre raccordement d'abonné ou de votre raccordement d'installation Internet ne sont pas inscrits ici dans la configuration ITSP, mais dans la configuration de l'abonné, dans les champs **SDA**.



a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **N° de téléphone public (SDA)**.

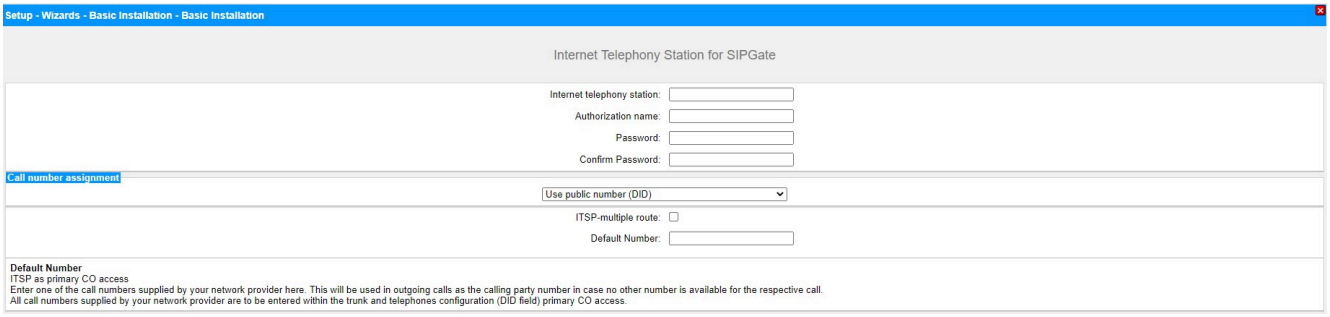
b) Sous **Numéro par défaut**, entrez le numéro de téléphone à utiliser pour les appels sortants lorsqu'aucun numéro SDA n'est disponible.

c) Si votre ITSP supporte la fonctionnalité "Mobile Extension (MEX)", entrez dans **Numéro MEX** le numéro MEX fourni par l'ITSP (8 positions, chiffres uniquement).

12) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 2 :

Utiliser numéro interne (n° appel) / entrées individuelles : Vous disposez d'un raccordement d'abonné de téléphonie Internet et vous avez reçu des numéros individuels comme numéros de téléphonie Internet

(par ex. 70005555, 70005556,...). Vous affectez ensuite ces numéros individuels aux numéros internes des abonnés.



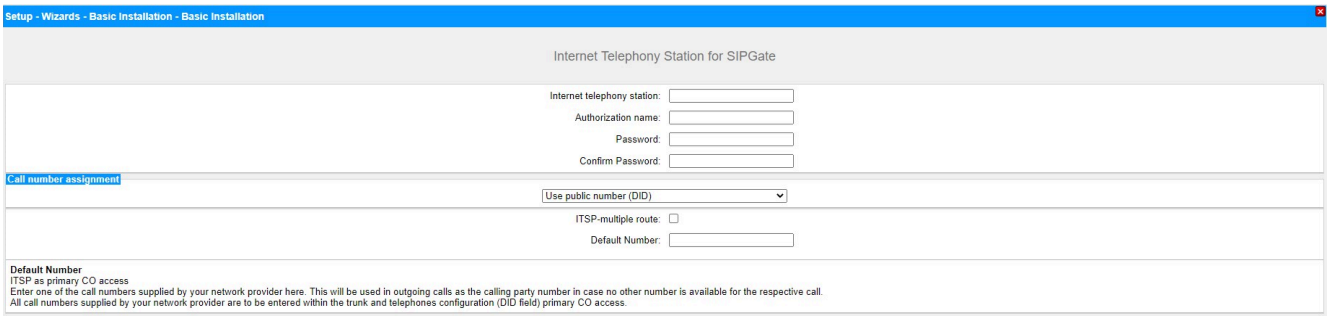
a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **Utiliser le numéro interne (N° tél)/entrées individuelles**.

b) Dans la zone **Téléphonie Internet-Numéros des abonnés**, dans le champ situé à côté du bouton **Ajouter**, saisissez un numéro d'abonné de téléphonie Internet communiqué par le ITSP et cliquez sur **Ajouter**.

c) Si vous souhaitez attribuer d'autres numéros de téléphonie Internet au compte, répétez l'étape b).

13) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 3 :

Utiliser numéro interne (N° appel) / plage d'entrées : Vous disposez d'une connexion Téléphonie Internet et, comme numéros de téléphonie Internet, d'une plage de numéros, par ex. (+49) 89 7007-100 à (+49) 89 7007-147. Vous affectez ensuite les numéros de la plage aux numéros internes des abonnés.



a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **Utiliser le numéro interne (N° tél)/Entrée individuelle**.

b) Dans **Numéro de l'installation (préfixe)**, entrez le numéro de l'installation.

c) Entrez la série de numéros SDA souhaitée pour la station de téléphonie Internet dans les champs 'de' **et** 'à **' après** Bande de numérotation directe à l'arrivée. Par défaut, la valeur 100 - 147 est entrée.

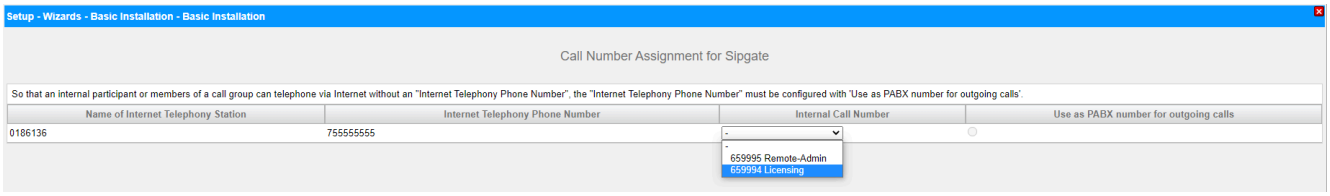
14) Cliquez sur **OK & Suivant**.

15) Si vous souhaitez configurer d'autres comptes avec les numéros d'abonnés de téléphonie Internet correspondants, répétez les étapes 7 à 14.

16) Cliquez sur **OK & Suivant**. Vous visualisez une vue d'ensemble indiquant la correspondance entre les numéros de téléphonie Internet et les comptes.

17) Affectez respectivement le numéro interne d'un abonné à tous les numéros de téléphonie Internet.

Cette étape est supprimée si vous avez choisi la possibilité 1 pour l'affectation des numéros de téléphonie Internet. Dans ce cas, l'affectation est effectuée lors de la configuration des stations (c'est-à-dire des téléphones et des abonnés) dans le champ **SDA**.



a) Dans la ligne correspondante de la liste déroulante **Numéro interne**, sélectionnez un numéro de téléphone interne.

b) Si les abonnés sans numéro de téléphone Internet ou les membres d'un groupe d'appel doivent être autorisés à effectuer des appels externes via Internet, le bouton radio **Utiliser comme numéro PABX pour les appels sortants** doit être activé. La case doit être cochée uniquement pour un seul numéro de téléphonie Internet.

18) Cliquez sur **OK & Suivant**. Vous voyez de nouveau la liste des ITSP prédéfinis et nouveaux. Les ITSP activés sont cochés dans la colonne **Activer le fournisseur**. **Redémarrage ITSP** vous permet, en cas de problèmes de liaison, de vous enregistrer de nouveau lorsque les ITSP sont déjà activés.

19) Cliquez sur **OK & Suivant**.

20) Dans le champ **Flux ascendant jusqu'à (kbit/s)** entrez la valeur de la vitesse du flux ascendant de votre connexion Internet. A ne pas confondre avec la vitesse de téléchargement !

Remarque : Dans le champ **Nombre de communications téléphoniques Internet simultanées**, le système indique le nombre maximal de communications téléphoniques Internet simultanées possibles. Si la qualité de la communication se détériore en raison de la charge du réseau, vous devez réduire ce nombre.

Pour plus d'informations sur le nombre d'appels Internet simultanés, veuillez vous référer à Limitation du nombre de communications simultanées via ITSP à la page 775.

---

21) Cliquez sur **OK & Suivant**.

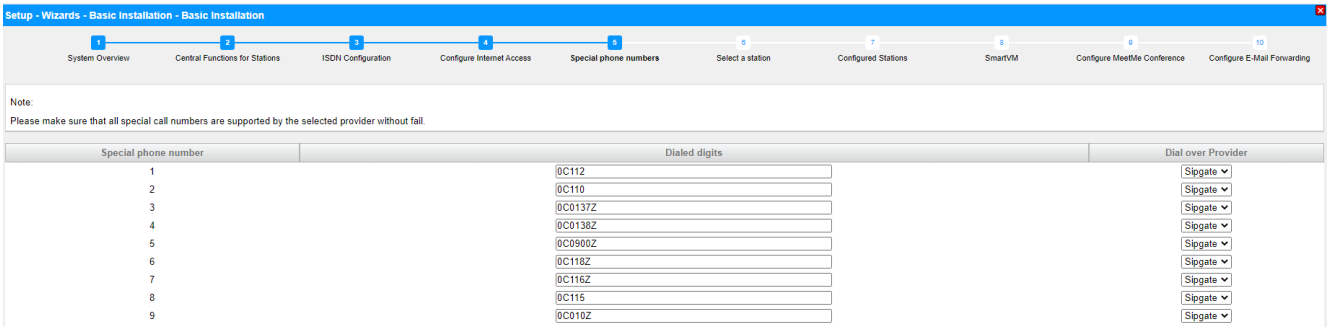
22) Si, lors du paramétrage de votre accès Internet, vous n'avez pas encore activé la liaison permanente, vous pouvez le faire ici. Sans liaison permanente, vous ne pouvez pas recevoir d'appels via Internet. Si la liaison permanente est déjà paramétrée, les champs décrits dans a) à c) ne sont pas visibles.

a) Dans **Liaison permanente**, activez le champ d'option **A l'attention de**.

b) Dans le champ **Coupure forcée à (heure:min)**, définissez l'heure à laquelle la connexion Internet doit être coupée (par ex. 04:59).

c) Cliquez sur **OK & Suivant**.

23) Entrez dans la colonne **Chiffres composés** les numéros spéciaux souhaités.



Les entrées de numéro de station suivantes sont valides :

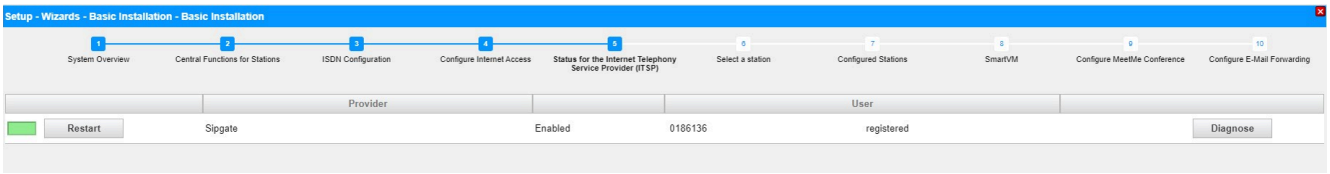
- 0 à 9: chiffres autorisés
- -: Séparateur de champ
- X : Chiffre au choix entre 0 et 9
- N : Chiffre au choix entre 2 et 9
- Z : Un ou plusieurs chiffres suivent jusqu'à la fin de la numérotation
- C : Tonalité d'invitation à numéroter simulée (peut être entrée max. trois fois)

24) Choisissez dans la colonne **Appeler par le fournisseur** si le numéro spécial doit être composé par RNIS ou par un ITSP. Seuls les ITSP activés sont affichés.

Remarque : Assurez-vous que les numéros d'urgence puissent toujours être composés. S'il est nécessaire de sélectionner des numéros d'urgence via un fournisseur de téléphonie sur Internet (ITSP), le fournisseur doit supporter ce service.

---

25) Cliquez sur **OK & Suivant**. Le système vous indique l'état du ITSP.



En vert figurent les ITSP qui sont configurés et sur lesquels vous êtes déjà enregistré.

En orange figurent les ITSP qui sont configurés et sur lesquels vous n'êtes pas encore enregistré.

26) Cliquez sur **Suivant** puis sur **Terminer**.

6.7.5.2 Comment désactiver la téléphonie Internet

Conditions préalables

Vous vous trouvez dans la fenêtre **Configuration et activation du fournisseur pour la téléphonie Internet** de l'assistant **Installation de base**.

Étape par étape

1) Cochez **Pas de téléphonie par Internet**.
2) Ensuite, cliquez deux fois sur **OK & Suivant**.

6.7.6 Abonnés

Dans les fenêtres **Sélectionner un abonné/groupe - ...** configurez les abonnés raccordé au système de communication.

Pour cela, procédez comme indiqué ci-après.

1) Configurer les abonnés IP et SIP

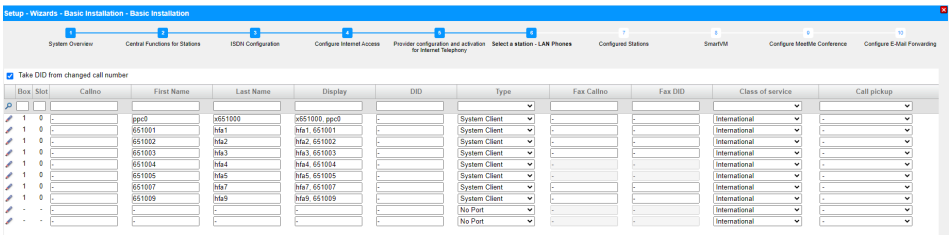
   Les abonnés IP et les abonnés SIP sont par ex. des téléphones LAN ou WLAN.

6.7.6.1 Comment configurer les abonnés IP et SIP

Conditions préalables

Vous vous trouvez dans la fenêtre **Sélectionner l'abonné - Téléphones LAN** de l'assistant **Installation de base**.

Pour que les téléphones WLAN fonctionnent, vous avez besoin d'un réseau LAN sans fil fonctionnel.



Étape par étape

1) Si le numéro SDA de l'abonné doit être différent de son numéro d'appel, saisissez un numéro SDA dans le champ **SDA** de la ligne de l'abonné souhaité :

   - Uniquement pour le raccordement système :

     Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
   - uniquement pour un raccordement multiposte :

     À partir de la liste déroulante, sélectionnez un numéro MSN. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
   - pour le raccordement système et un raccordement multiposte :

     Dans la liste déroulante du champ souhaité, sélectionnez l'entrée **xxx - modifiable** (xxx correspondant au numéro interne) et saisissez le numéro SDA à l'aide du clavier ou sélectionnez un MSN (Multiple Subscriber Number, numéro de téléphone multiple).

2) Sur la ligne de l'abonné souhaité, saisissez le numéro de téléphone interne de l'abonné dans **Numéro de téléphone**. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

3) Entrez dans la ligne de l'abonné souhaité sous **Nom** un nom, sous la forme `Nom de famille, Prénom`.

Remarque : Le nom peut comporter jusqu'à 16 caractères, mais ne doit contenir ni inflexions ni caractères spéciaux. Le nom est inscrit comme nom de famille, comme indiqué ici pour les clients UC, mais il peut être modifié ultérieurement.

---

4) Sur la ligne de l'abonné souhaité, sélectionnez le type d'abonné IP (par ex. "Client système" ou "Client SIP") dans la liste déroulante **Type**.

5) Si vous souhaitez configurer une boîte Fax pour l'abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme suit :

a) Dans la ligne de l'abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l'utilisateur pourra recevoir des messages Fax internes.

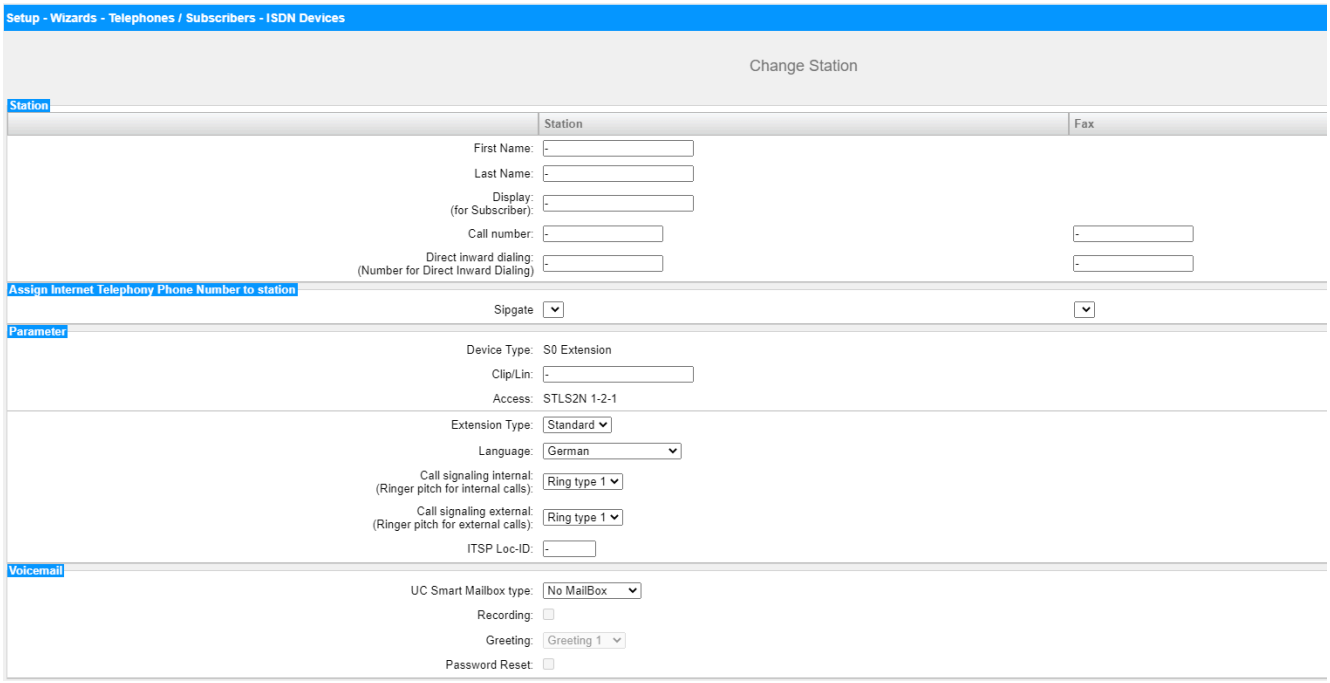
b) Si un numéro SDA doit être configuré pour la boîte Fax, saisissez dans la ligne de l'abonné souhaité, champ **SDA Fax**, le numéro de fax externe sous lequel l'abonné pourra recevoir des messages Fax externes.

6) Dans la liste déroulante **Classe de service** de la ligne de l'abonné concerné, sélectionnez le groupe de classe de service souhaité.

7) Pour intégrer l'abonné à un groupe d'interception, sélectionnez un groupe dans la liste déroulante **Interception** de la ligne de l'abonné souhaité.

8) N'effectuez les paramétrages décrits dans ce point qu'en cas de besoin ou pour un téléphone SIP :

a) Sur la ligne de l'abonné souhaité, cliquez sur l'icône **Modifier**.



b) Uniquement pour les téléphones SIP : Si ce téléphone SIP doit être utilisé en même temps qu'un téléphone mobile dual mode, saisissez dans la zone **Mobilité**, `Numéro de mobile` l'indicatif réseau suivi du numéro du téléphone mobile (par ex. **0016012345678**). Sélectionnez en plus dans la liste déroulante **Web Feature ID** ce client SIP. (Voir Téléphonie dual mode).

c) Dans le champ **Clip/Lin**, saisissez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant, et le numéro interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

---

d) Sélectionnez dans la liste déroulante **Langue** la langue des menus du téléphone.

e) Dans la liste déroulante **Signalisation des appels internes**, affectez à l'abonné l'une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres abonnés internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

f) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

g) Pour les téléphones SIP uniquement : Entrez le mot de passe d'authentification dans les champs **Mot de passe** et **Valider mot de passe**.
h) Pour les téléphones SIP uniquement : indiquez dans le champ **Identifiant utilisateur SIP/Nom d'utilisateur** l'identifiant utilisateur pour l'authentification.
i) Pour les téléphones SIP uniquement : indiquez dans **Realm** la zone correspondante pour l'authentification.
j) Cliquez sur **OK & Suivant**.
k) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonné, voir Abonnés > Abonnés > Paramètres d'abonné.
l) Cliquez sur **OK & Suivant**.

9) Si vous souhaitez paramétrer un autre abonné IP, cliquez sur **Enregistrer les données** et répétez les points 1 à 8.

10) Cliquez sur **OK & Suivant**. Le système affiche une liste de tous les abonnés paramétrés. Cette liste correspond à un plan de numérotation.

11) Si besoin est, cliquez sur **Imprimer** pour imprimer les données de l'abonné paramétré.

12) Pour terminer, cliquez sur **OK & Suivant**

Concepts associés

Texte en plusieurs langues à la page 1173

6.7.7 Configuration de UC Suite

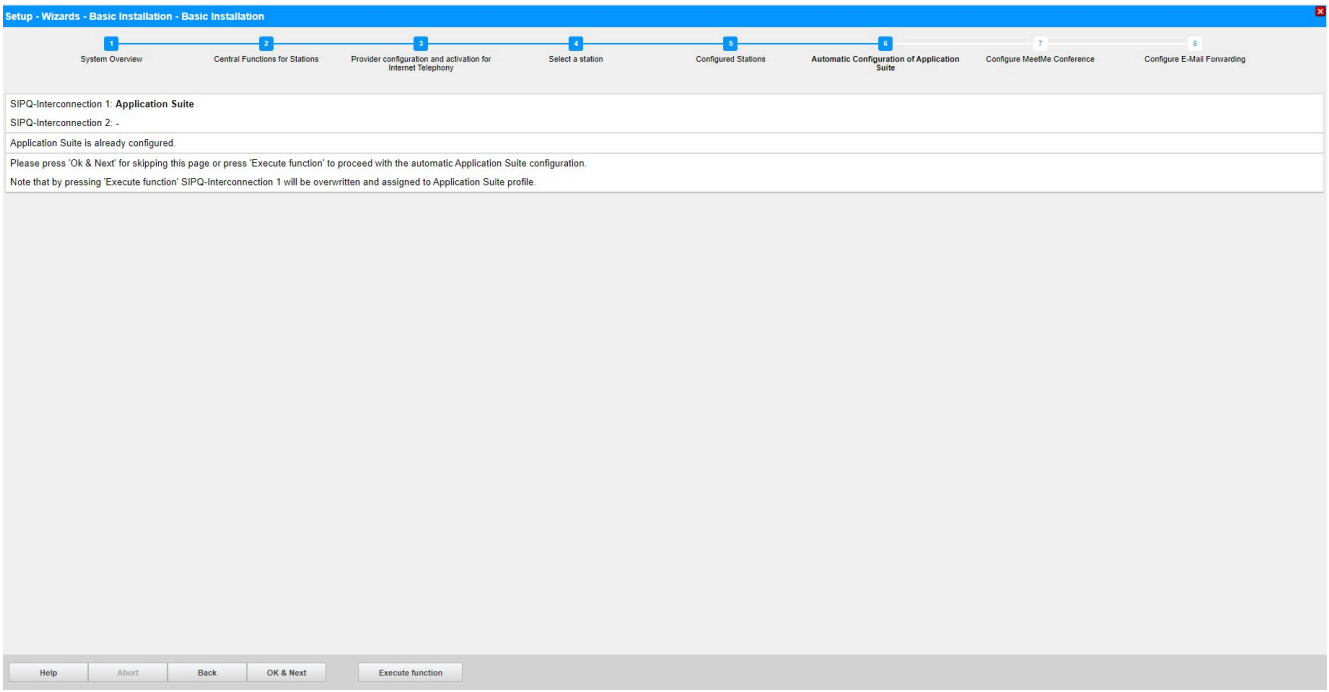
Dans la fenêtre **Configuration automatique de la suite d'application**, vous pouvez effectuer la configuration automatique de la solution UC Suite.

Remarque : Cette fenêtre apparaît uniquement si, dans l'assistant **Première installation**, il a été sélectionné **Pack avec UC Suite** lors de la sélection de l'application.

6.7.7.1 Comment configurer la UC Suite

Conditions préalables

Vous êtes dans la fenêtre **Configuration automatique de la suite d'applications**.



Étape par étape

Cliquez sur **Exécuter la fonction**. L'UC Suite est configuré automatiquement. Dès que la barre de progression indique 100%, cliquez sur **OK & Suivant**.

Remarque :

Pour OpenScape Business S, l'assistant génère automatiquement 60 canaux multimédias dans UC Suite. En parallèle, 16 canaux peuvent être utilisés pour les annonces sans configuration de canaux multimédias supplémentaires.

6.7.8 Configuration des boîtes de messagerie vocale de UC Smart

Dans la fenêtre **Configuration automatique de Smart VM**, vous pouvez effectuer la configuration automatique des boîtes de messagerie vocale UC Smart(Smart VM, Smart VoiceMail) si vous utilisez la solution UC Smart.

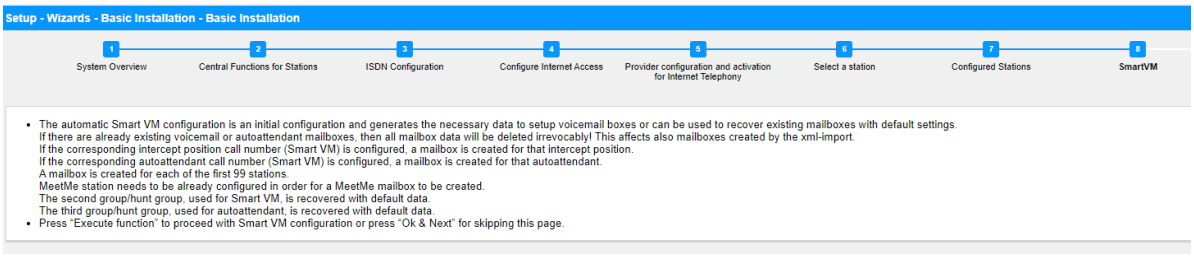
Remarque :

Cette fenêtre ne s'affiche que si, dans l'assistant **Première installation**, il a été choisi **Pack avec UC Smart** lors de la sélection de l'application.

6.7.8.1 Comment configurer les boîtes vocales UC Smart

Conditions préalables

Vous êtes dans la fenêtre **Configuration automatique de Smart VM**.



Étape par étape

1) Si les boîtes vocales UC Smart ne doivent pas être utilisées, cliquez sur **OK&Suivant**. La configuration des boîtes de messagerie vocale est sautée.
2) Si les boîtes vocales UC Smart doivent être utilisées, cliquez sur **Exécuter la fonction**. Les boîtes de messagerie vocale sont automatiquement configurées pour les 100 premiers abonnés. Dès que la barre de progression indique 100%, cliquez sur **OK&Suivant**.

Remarque : Les boîtes vocales UC Smart ou les boîtes vocales UC Smart AutoAttendant existantes sont supprimées définitivement dans ce cas.

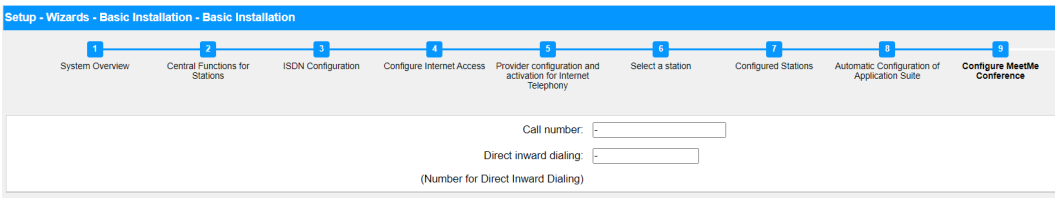
6.7.9 Paramètres du serveur de conférence

Dans la fenêtre **Conférence "Rendez-vous" - Modifier les paramètres** vous pouvez définir le numéro d'appel et le numéro de sélection d'une conférence.

6.7.9.1 Comment modifier la configuration du serveur de conférence

Conditions préalables

Vous vous trouvez dans la fenêtre **Configurer la conférence MeetMe** de l'assistant **Installation de base**.



Étape par étape

1) Dans **Numéro de téléphone**, indiquez un numéro pour la conférence.
2) Dans le champ **N° SDA**, définissez le numéro de sélection de la conférence (SDA conférence), afin de permettre aux abonnés d'entrer dans une conférence en place.
3) Cliquez sur **OK & Suivant**.

6.7.10 Envoi d'e-mails (option)

Dans la fenêtre **Modifier les renvois E-Mail**, vous pouvez configurer l'envoi d'e-mails. Les abonnés sont ainsi informés des nouveaux messages vocaux et fax et l'administrateur reçoit les messages système.

Vous disposez des possibilités suivantes :

- Configurer l'envoi d'e-mails

  Vous pouvez définir un serveur e-mail externe à l'aide duquel OpenScape Business va envoyer les e-mails. Les messages Voix et Fax ou messages système internes sont renvoyés via ce serveur d'e-mails à une ou différentes adresses e-mail configurables.

Remarque : Le paramétrage d'un serveur e-mail est important lorsqu'il doit être envoyé automatiquement aux utilisateurs de la suite UC, par e-mail, un lien vers le(s) fichier(s) d'installation.

6.7.10.1 Comment configurer l'envoi d'e-mails

Conditions préalables

Si le serveur de messagerie externe a été configuré pour utiliser l'authentification de base, assurez-vous qu'un compte e-mail avec mot de passe existe auprès d'un fournisseur d'e-mail et que vous connaissez les données d'accès à ce compte.

Si le serveur de messagerie externe a été configuré pour utiliser une authentification moderne (basée sur un jeton Microsoft OAuth 2.0), comme dans le cas d'Exchange Online, vérifiez les éléments suivants :

- Le compte de messagerie de l'expéditeur doit être autorisé à utiliser le protocole SMTP authentifié (par défaut, cette option est désactivée dans le client Microsoft 365). Une fois que le protocole SMTP authentifié est activé, le renvoi d'e-mail OAUTH 2.0 fonctionne normalement avec toutes les cartes mères OpenScape Business.
- Une application dotée des autorisations requises a été enregistrée dans Microsoft Azure Active Directory (Azure AD) pour permettre à votre système OpenScape Business d'envoyer des e-mails.
- Vous connaissez l'ID d'application (ou client) et l'ID de répertoire (ou locataire) de l'application enregistrée.

  Demandez à votre administrateur Azure AD de vous fournir ces valeurs, si nécessaire.
- L'adresse e-mail qui apparaîtra comme adresse d'expédition des e-mails appartient au même répertoire Azure AD (ou locataire) que l'application enregistrée.

Vous vous trouvez dans la fenêtre **Configurer le renvoi E-Mail** de l'assistant **Installation de base**.

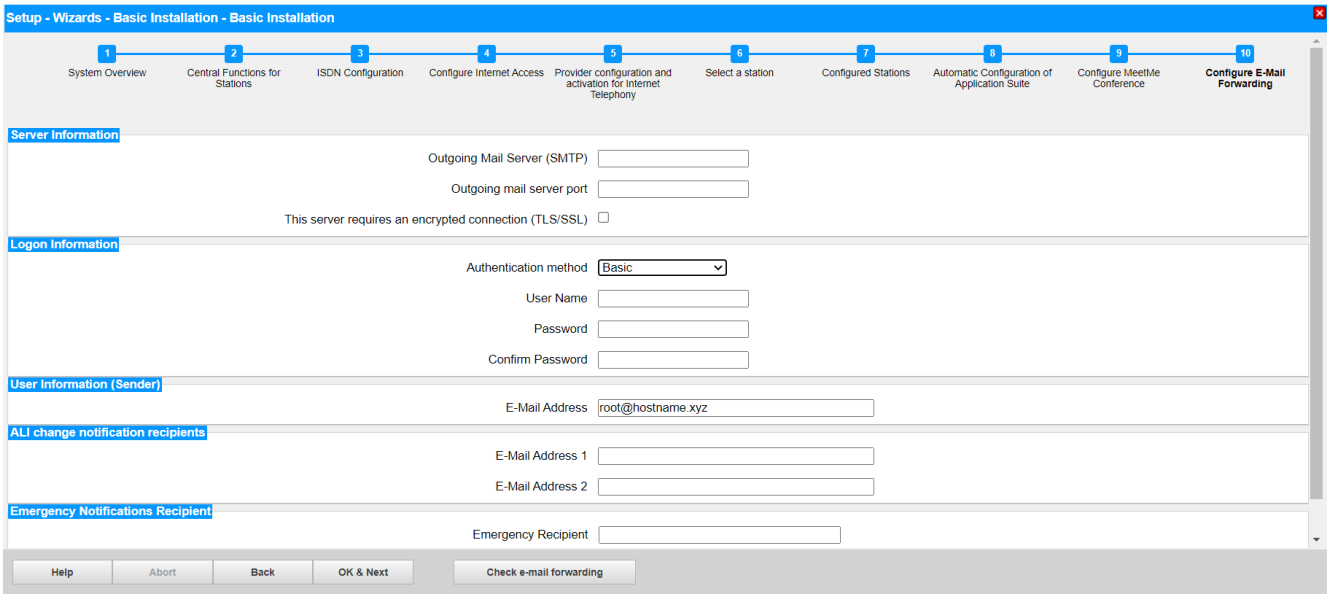


Illustration 6 : Options de renvoi d'e-mail lorsque la méthode d'authentification de base est sélectionnée

Étape par étape

1) Saisissez le **serveur de messagerie sortant (SMTP)** pour le serveur de messagerie qui doit être utilisé pour l'envoi d'e-mails, par ex. `smtp.web.fr`. Si nécessaire, interrogez le serveur de la boîte d'envoi ou bien votre fournisseur e-mail.

Remarque : Veillez à ce que le nom du serveur de messagerie sortant puisse être résolu. Si ce n'est pas le cas, vous devez démarrer la fonction d'envoi d'e-mails via **Centre de service** > **Renvoi e-Mail** et saisir l'adresse IP du serveur de courrier sortant (au lieu de son nom).

---

2) Pour le port de serveur qui doit être utilisé pour envoyer les e-mails, saisissez le **port du serveur de courrier sortant**. Si nécessaire, interrogez le serveur de la boîte d'envoi ou bien votre fournisseur e-mail.

3) Si une connexion sécurisée est requise, cochez la case **Ce serveur nécessite une connexion cryptée (TLS/SSL)**. Demandez le cas échéant à votre fournisseur d'e-mail, si cette option doit être activée.

4) Si le serveur de messagerie externe a été configuré pour utiliser l'authentification de base, procédez comme suit :

a) Dans la liste déroulante **Méthode d'authentification**, sélectionnez **Basique**.

b) Saisissez le **nom d'utilisateur** du compte e-mail, par ex. `jean.exemple`.

c) Dans **Mot de passe** et **Valider mot de passe**, saisissez le mot de passe du compte e-mail.

5) Si le serveur de messagerie externe a été configuré pour utiliser l'authentification moderne, procédez comme suit :

a) Dans la liste déroulante **Méthode d'authentification**, sélectionnez **Microsoft OAuth 2.0**.

b) Dans le champ **ID d'application**, saisissez l'ID d'application (client) obtenu à partir du portail Microsoft Azure.

c) Dans le champ **Locataire**, saisissez l'ID de répertoire (locataire) obtenu à partir du portail Microsoft Azure.

6) Saisissez l'**adresse e-mail** qui apparaîtra comme adresse d'expédition des e-mails, par exemple `john.doe@web.de`.

7) Saisissez l'**adresse e-mail 1** pour obtenir un e-mail de notification lorsque la tolérance ALI a été utilisée. Vous pouvez également saisir une deuxième adresse e-mail dans le champ **Adresse e-mail 2**.

8) Dans le champ **Destinataire d'urgence**, saisissez l'adresse e-mail d'un agent de sécurité sur site à laquelle un e-mail est envoyé lorsqu'un numéro d'urgence est composé.

L'objet de l'e-mail sera « Nouvel appel d'urgence ». Le numéro d'appel et le nom de l'appelant (s'ils sont configurés) sont inclus dans l'e-mail et récupérés auprès de la base de données du système.

9) Si vous avez sélectionné **Microsoft OAuth 2.0** comme méthode d'authentification, procédez comme suit :

a) Cliquez sur **OK & Suivant**.

b) Attendez qu'un lien d'autorisation et un code d'utilisateur apparaissent.

Le code d'autorisation expire après quelques minutes.

c) Ouvrez le lien d'autorisation et saisissez le code d'utilisateur dans la fenêtre contextuelle.

d) Connectez-vous avec l'adresse e-mail que vous avez saisie à l'étape 6 à la page 230 (**Adresse e-mail**).

L'adresse e-mail doit se trouver dans le même répertoire Azure AD (ou locataire) que l'application enregistrée.

e) Une fois l'authentification réussie, la fenêtre contextuelle affiche le message suivant :

```
Vous vous êtes connecté à <nom de l'application> sur
votre appareil. Vous pouvez maintenant fermer cette
fenêtre.
```

f) Fermez la fenêtre contextuelle et retournez dans la WBM.
Si l'authentification a réussi, le message suivant s'affiche :
`L'authentification est réussie !.`

10) Si vous souhaitez vérifier les paramètres d'e-mail saisis, procédez comme suit :

a) Cliquez sur **Contrôler le renvoi d'e-mail**.
b) Dans **Envoyer à l'adresse e-mail**, saisissez l'adresse e-mail de la messagerie e-mail à laquelle vous avez accès. L'e-mail de test est envoyé à cette adresse e-mail.
c) Dans **Objet de l'e-mail**, saisissez un texte descriptif permettant d'identifier l'e-mail dans votre messagerie e-mail.
d) Cliquez sur **Envoyer un e-mail de test**. Les paramètres e-mail sont contrôlés et l'e-mail est envoyé à la messagerie e-mail indiquée.
e) Vérifiez si l'e-mail est bien arrivée dans votre messagerie e-mail.
f) Si l'envoi de l'e-mail s'est bien déroulé, cliquez sur **Retour** et passez à l'étape suivante.
g) Si l'envoi d'e-mails n'a pas abouti, cliquez sur **Retour** et corrigez vos paramètres e-mail.

11) Cliquez sur **OK & Suivant**, puis sur **Quitter**. L'installation de base est terminée. Avant d'effectuer la sauvegarde de données mentionnées dans l'Assistant, vous devez activer les licences.

6.8 Activités finales

Une fois terminées la première installation et l'installation de base avec WBM, il faut encore procéder à certains paramétrages essentiels pour l'utilisation d'OpenScape Business.

Pour cela, suivez les étapes suivantes :

1) Activer et affecter les licences

Les licences acquises avec OpenScape Business doivent être activées dans un délai de 30 jours. La période de temps débute avec la première connexion au WBM. Une fois ce délai écoulé, le système de communication ne peut être utilisé que dans une version restreinte. Après l'activation, les licences doivent être affectées aux abonnés et aux lignes. Les fonctionnalités sur l'ensemble du système sont déjà validées lors de l'activation.

2) Comment préparer le client UC Smart pour l'installation (Uniquement pour UC Smart)

Le client UC Smart myPortal Smart fait partie de UC Smart. Le fichier d'installation de myPortal est accessible par la WBM et peuvent être mis à disposition des abonnés IP, automatiquement ou manuellement. Pour des informations supplémentaires, voir UC Smart Clients.

3) Préparer les clients UC pour l'installation

Les clients UC font partie intégrante de la UC Suite. Les fichiers d'installation des clients UC sont accessible par le WBM et peuvent être mis à disposition des clients IP, automatiquement ou manuellement.

En plus, l'administrateur dispose de la possibilité Silent Installation. C'est une méthode basée sur des lignes de commande permettant l'installation, la désinstallation et la modification automatiques des clients UC Suite, sans avoir à effectuer d'autres entrées. Pour des informations supplémentaires, voir Installation/Désinstallation silencieuse pour PC client UC Suite.

4) Réaliser la sauvegarde des données

Les modifications apportées à OpenScape Business doivent être enregistrées. La sauvegarde peut être enregistrée comme jeu de sauvegarde par ex. dans le réseau interne.

6.8.1 Comment activer et affecter les licences

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Vous connaissez le code LAC (code d'autorisation de licence) pour la validation de la licence et vous disposez d'un identifiant et d'un mot de passe pour accéder au serveur de licence.

Pour accéder au serveur de licence il faut disposer d'un accès Internet.

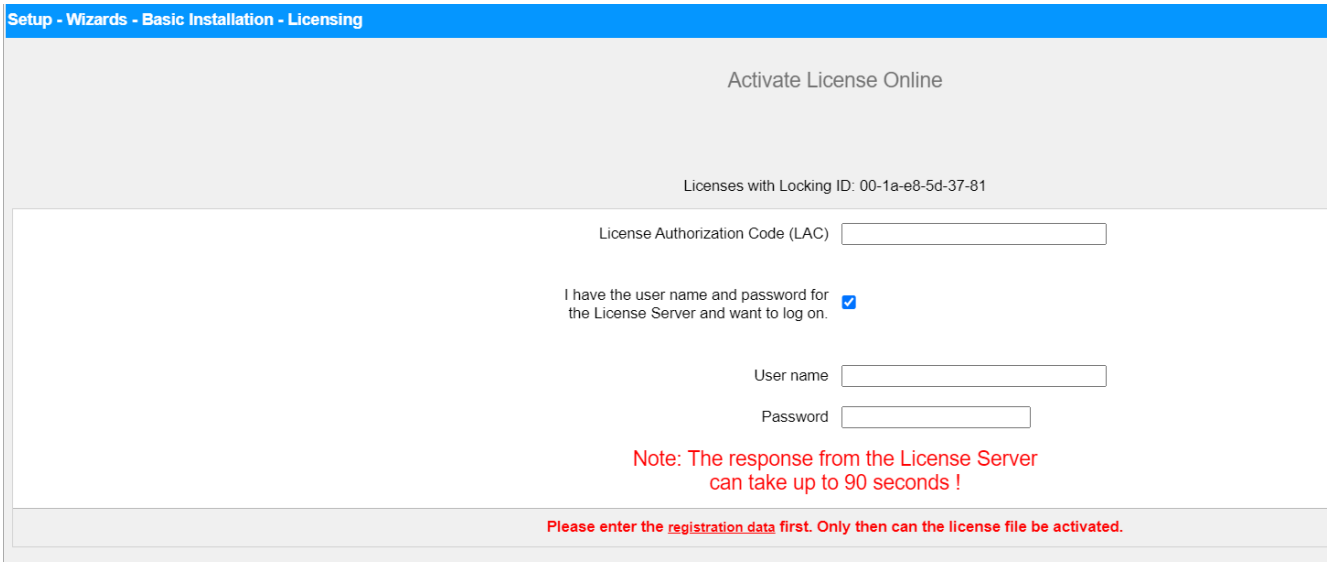
Étape par étape

1) Activer la licence en ligne :

a) Cliquez dans la barre de navigation sur **Configuration**.

b) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.

c) Cliquez sur **Modifier** pour lancer l'Assistant **Procédure de licence**.



d) Dans **Code d'autorisation de licence (LAC)**, entrez le code LAC.

e) Cochez la case **J'ai un nom d'utilisateur et un mot de passe pour le serveur de licence et souhaite ouvrir une connexion**.

f) Entrez le **Nom utilisateur** et le **Mot de passe** pour la connexion au serveur de licences.

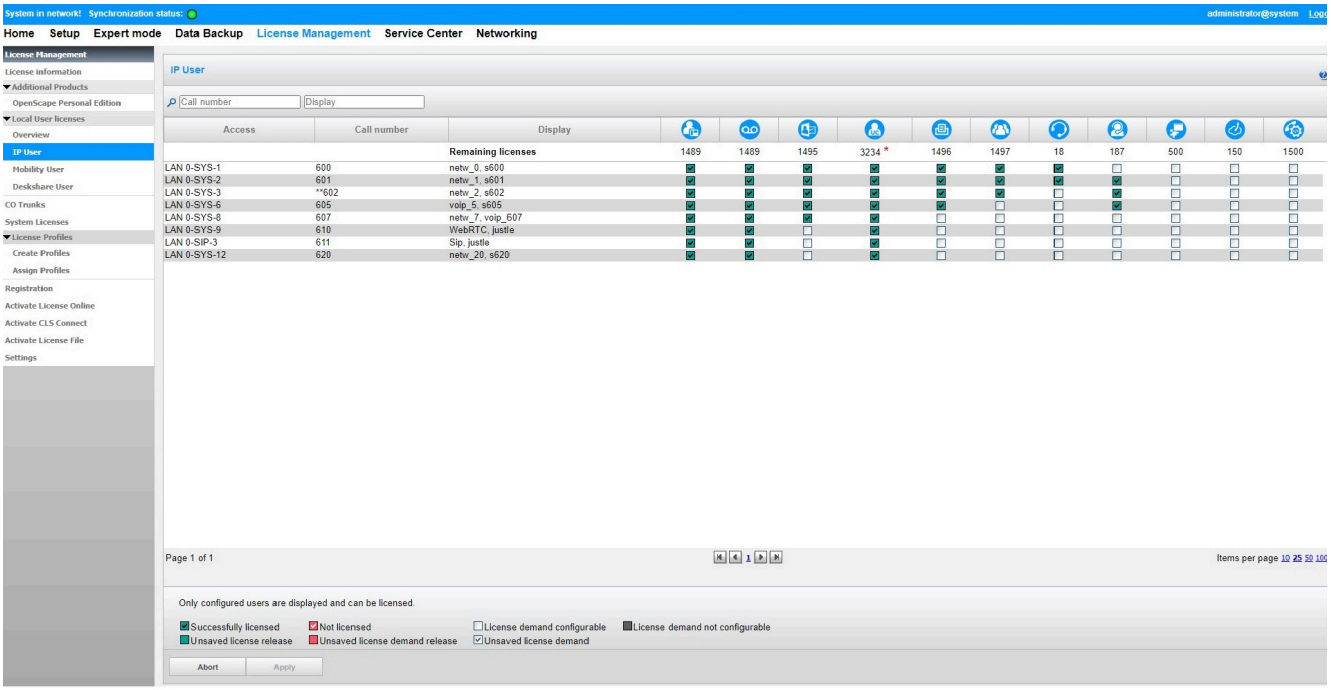
g) Cliquez sur **OK & Suivant**. La connexion avec le serveur de licences est établie et les licences sont validées.

2) Affecter les licences aux abonnés :

a) Cliquez sur **Gestion des licences** dans la barre de navigation.

b) Dans l'arborescence de navigation, accédez au type d'abonné souhaité sous **Licences d'utilisateur local** > **...**. Une liste de tous les abonnés du type d'abonné sélectionné s'affichera.

c) Dans la ligne de l'abonné souhaité, cochez la case figurant dans la colonne **Licences utilisateur** (première colonne avec case à cocher).



d) Dans la ligne de l'abonné souhaité, activez les licences orientées utilisateur en cochant les cases correspondantes.

Remarque : Il ne peut être attribué à un abonné une licence orientée utilisateur que si l'abonné précédent s'est vu attribuer une licence d'abonné (licences utilisateur) (Etape c).

---

e) Cliquez sur **OK & Suivant**. Une vérification est effectuée pour déterminer s'il y a suffisamment de licences pour votre affectation.

S'il y a suffisamment de licences, la procédure de licence des abonnés est terminée.

f) S'il manque des licences, les erreurs sont indiquées dans une case à fond rouge. Corrigez ces erreurs et répétez l'étape e.

3) Affecter les licences aux lignes

a) Dans l'arborescence de navigation, cliquez sur **Lignes réseau**. Dans la plage **Lignes réseau** il vous est présenté le nombre des licences de ligne acquises.

b) Pour les lignes SIP : dans la plage Demande de licence pour le nombre d'appels Internet simultanés dans ce nœud entrez le nombre des communications Internet qui peuvent se dérouler simultanément via un ITSP.

c) Cliquez sur **OK & Suivant**.

6.8.2 Comment préparer le clients UC Smart pour l'installation

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Le matériel et le logiciel nécessaires à l'utilisation de UC Smart sont disponibles.

Remarque : Pour l'utilisation du client UC Smart myPortal Smart, des licences sont nécessaires.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Logicielle**.
3) Cliquez sur l'icône de téléchargement de **myPortal Smart** et enregistrez le fichier d'installation dans un lecteur réseau validé.
4) Cliquez sur l'icône de lien d'**Adobe AIR** et chargez le fichier d'installation sur un lecteur réseau validé.
5) Envoyez aux utilisateurs de myPortal Smart les deux fichiers d'installation.
6) Vous pouvez également envoyer aux utilisateurs de myPortal Smart deux liens qui leur permettent d'accéder directement aux fichiers d'installation.

   `https://<Adresse IP du système de communication>/management/downloads/SmartClient.air`

   `http://www.adobe.com/air`

6.8.3 Comment préparer les clients UC Suite pour l'installation

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Le matériel et le logiciel nécessaires à l'utilisation de UC Suite sont disponibles.

Remarque : Pour l'utilisation des clients UC Suite, des licences sont nécessaires.

Étape par étape

1) Afin que les fichiers d'installation soient mis automatiquement à disposition de l'abonné, assurez-vous que les opérations suivantes ont bien été respectées.
   a) Les adresses e-mail des abonnés doivent avoir été importées en même temps que les données d'abonné à l'aide d'un fichier XML ou bien être inscrits dans **Configuration** > **UC Suite** > **Répertoire utilisateur**.
   b) Un serveur Mail doit être inscrit.

   Remarque : Vous pouvez aussi inscrire a posteriori un serveur e-mail dans **Centre de service** > **Renvoi E-Mail**.

   Tous les clients dont les adresses e-mail sont connues reçoivent un e-mail avec le lien pour l'installation des clients UC et des instructions concernant les premières étapes. Dans le répertoire Installation figure en outre un fichier Readme avec des informations sur l'installation du logiciel sur les PC client.
2) Si les étapes nécessaires pour une information automatique ne sont pas réalisées, vous pouvez aussi mettre à disposition manuellement les fichiers d'installation. Pour cela, procédez comme indiqué ci-après.
   a) Cliquez dans la barre de navigation sur **Centre de service**.
   b) Dans l'arborescence de navigation, cliquez sur **Logicielle**.
   c) Cliquez sur le client UC souhaité et enregistrez le fichier d'installation zippé sur un lecteur réseau partagé.
   d) Dans l'arborescence de navigation, cliquez sur **Documents** et sélectionnez la liste déroulante **Mode d'emploi**.
   e) Cliquez sur la documentation du client UC souhaité et enregistrez le fichier de documentation sur un lecteur réseau validé.
   f) Envoyez par e-mail aux utilisateurs de la suite UC le fichier d'installation zippé et le fichier de documentation zippé ou indiquez aux utilisateurs où les fichiers sont enregistrés.
   g) Le fichier ZIP qui contient les fichiers d'installation comprend aussi un fichier Readme. Précisez aux utilisateurs que l'installation des clients UC doit être effectuée conformément aux conseils d'installation figurant dans le fichier Readme.
3) Vous pouvez également envoyer aux utilisateurs UC des liens qui leur permettent d'accéder directement aux fichiers d'installation des UC Clients.
   a) Cliquez dans la barre de navigation sur **Centre de service**.
   b) Dans l'arborescence de navigation, cliquez sur **Logicielle**.
   c) Cliquez sur le bouton **Afficher les liens d'application**. Il vous est présenté plusieurs liens en fonction du système d'exploitation utilisé et du client UC souhaité. Par exemple :

   ```
   https://<Adresse IP du système de communication>/
   management/downloads/install-common.zip
   ```

6.8.4 Comment réaliser la sauvegarde des données

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Remarque : Informations supplémentaires sur la sauvegarde des données voir Sauvegarde immédiate .

Étape par étape

1) Cliquez dans la barre de navigation sur **Sauvegarde et restauration**.
2) Dans l'arborescence de navigation, cliquez sur **Sauvegarde - immédiate**.
3) Dans la plage **Nom** dans le champ **Commentaire**, entrez un commentaire pour le jeu de sauvegarde afin de pouvoir plus facilement identifier le jeu de sauvegarde lors d'une éventuelle restauration. Lors de la saisie, évitez les inflexions et les caractères spéciaux.
4) Dans la zone **Equipements** activez le lecteur de destination où le jeu de sauvegarde doit être enregistré. (par ex. sur un lecteur réseau).
5) Cliquez sur **OK&Suivant**. Dans une autre fenêtre, le système affiche la progression de la sauvegarde.
6) La sauvegarde a été effectuée lorsque le message **Sauvegarde effectuée !** s'affiche. Cliquez sur **Terminer**.
7) La première mise en service avec la WBM est maintenant terminée. Pour quitter WBM, cliquez en haut à droite sur le lien **Déconnexion** puis refermez la fenêtre.

6.9 Mise en service des téléphones IP

Une mise en service confortable des téléphones IP nécessite un serveur DHCP qui fournit au téléphone IP les données importantes pour l'inscription dans le système de communication (données spécifiques du réseau).

Données spécifiques du réseau

Pour l'inscription sur le système de communication, un téléphone IP a besoin de données spécifiques du réseau. Ces données peuvent soit être enregistrées dans le serveur DHCP, soit avoir été entrées directement dans le téléphone IP. L'avantage d'un serveur DHCP est que tous les téléphones IP raccordés sont automatiquement alimentés avec ces données.

Les données suivantes sont nécessaire pour le téléphone IP :

- Adresse IP du système de communication
- Adresse IP du serveur DLS

En plus, le téléphone IP a besoin de son propre numéro. Celui-ci doit être inscrit manuellement sur le téléphone durant l'inscription.

Enregistrement des téléphones SIP

Pour des raisons de sécurité, il est recommandé d'enregistrer les téléphones SIP sur le système de communication. Pour cela, les données d'enregistrement du téléphone IP et du système de communication doivent correspondre.

Les données suivantes sont nécessires pour la connexion :

- ID utilisateur SIP
- Mot de passe SIP
- Realm SIP (option)

Utilisez un mot de passe SIP hors du commun, qui répond aux règles suivantes :

- Au moins 8 positions
- Au moins une majuscule (A - Z)
- Au moins une minuscule (a - z)
- Au moins un chiffre (0-9)
- Au moins un caractère spécial

Utilisez un ID utilisateur SIP qui ne contient pas le n° de téléphone.

Remarque : Vous trouverez des informations supplémentaires sur la configuration des téléphones SIP dans `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Utilisation du serveur DHCP interne

Si l'on utilise le serveur DHCP interne du système de communication, celui-ci contient déjà les données spécifiques réseau. Afin qu'un téléphone IP puisse s'enregistrer sur le système de communication, il ne enregistrer sur le téléphone IP que le numéro de téléphone défini. Pour un téléphone SIP, il faut en plus que les données d'enregistrement SIP sur le téléphone SIP et sur le système de communication correspondent.

Utilisation d'un serveur DHCP externe avec données spécifiques du réseau

Si l'on utilise un serveur DHCP externe, il faut y entrer les données spécifiques réseau. Afin qu'un téléphone IP puisse s'enregistrer sur le système de communication, il ne enregistrer sur le téléphone IP que le numéro de téléphone défini. Pour un téléphone SIP, il faut en plus que les données d'enregistrement SIP sur le téléphone SIP et sur le système de communication correspondent.

Utilisation d'un serveur DHCP externe sans données spécifiques du réseau

Si l'on utilise un serveur DHCP externe sur lequel il est impossible d'entrer les données spécifique réseau, celles-ci doivent alors être entrées sur le téléphone IP. Pour qu'un téléphone IP puisse s'enregistrer sur le système de communication, il faut inscrire sur le téléphone IP le numéro et l'adresse IP du système de communication et éventuellement modifier les paramètres du service de déploiement. Pour un téléphone SIP, il faut en plus que les données d'enregistrement SIP sur le téléphone SIP et sur le système de communication correspondent.

6.9.1 Comment configurer le téléphone IP

Conditions préalables

Le téléphone IP est raccordé au réseau interne et il est opérationnel.

Remarque : Il est décrit ici la configuration à l'exemple d'un téléphone système IP OpenStage 40/60/80. Ce paramétrage doit être effectué par analogie pour un autre téléphone IP. Consultez à ce sujet de mode d'emploi de votre téléphone IP.

Étape par étape

1) Pour accéder au mode Administration du téléphone système IP, appuyez sur la touche du téléphone correspondant au menu Paramètres / Applications.

2) Dans l'onglet `Paramètres` à `Admin` et confirmez avec la touche OK.

3) Entrez le mot de passe Administrateur (par défaut : `123456` et confirmez avec la touche OK.

4) Si vous utilisez dans le réseau interne le serveur DHCP du système de communication, sautez le point suivant.

5) Si vous n'utilisez pas dans le réseau interne le serveur DHCP du système de communication, vous devez entrer l'adresse IP du Deployment Server (DLS) et du système de communication de manière à ce que le logiciel du téléphone système IP puisse être actualisé automatiquement. Cela s'applique uniquement aux téléphones système IP. Pour cela, suivez les étapes suivantes :

a) Recherchez `Network` (réseau) et confirmez avec la touche OK.

b) Recherchez `Update service (DLS)` (service de mise à jour DLS) et confirmez avec la touche OK.

c) Recherchez `DLS address` (adresse DLS) et confirmez avec la touche OK.

d) Entrez comme Deployment Server l'adresse IP du système de communication `(par défaut :` 192.168.1.2) et confirmez avec la touche OK.

e) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

f) Recherchez `IPv4 configuration` (configuration IPv4) et confirmez avec la touche OK.

g) Recherchez `Route (default)` (route par défaut) et confirmez avec la touche OK.

h) Entrez l'adresse IP du système de communication (par défaut `192.168.1.2`) et confirmez avec la touche OK.

i) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

j) Utilisez la touche Retour pour revenir au niveau de menu précédent.

6) Fixez le numéro de téléphone du téléphone :

a) Recherchez `System` (système) et confirmez avec la touche OK.

b) Recherchez `Identity` (identité) et confirmez avec la touche OK.

c) Recherchez `Terminal number` (numéro du terminal) et confirmez avec la touche OK.

d) Entrez le numéro de téléphone défini (par ex. `120` et confirmez avec la touche OK.

e) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

7) Utilisez la touche Retour pour revenir au niveau de menu précédent.

8) Si, en raison des modifications, le téléphone système doit effectuer un redémarrage, il apparaît dans le menu `Admin` l'option de menu `Redémarrage`. Confirmez `Redémarrage` avec le touche OK puis `Oui` ainsi que la touche OK. Le téléphone système effectue un redémarrage et se connecte au système de communication.

6.9.2 Comment configurer un téléphone SIP

Conditions préalables

Le téléphone IP est raccordé au LAN client et il est opérationnel.

Remarque : Il est décrit ici la configuration à l'exemple d'un téléphone système OpenStage 40/60/80 SIP. Ce paramétrage doit être effectué par analogie pour un autre téléphone SIP. Consultez à ce sujet de mode d'emploi du téléphone SIP.

Étape par étape

1) Pour accéder au mode Administration du téléphone système SIP, appuyez sur la touche du téléphone correspondant au menu Paramètres / Applications.

2) Dans l'onglet `Paramètres` à `Administrateur (Admin)` et confirmez avec la touche OK.

3) Entrez le mot de passe Administrateur (par défaut : `123456` et confirmez avec la touche OK.

4) Si vous utilisez dans le réseau interne le serveur DHCP du système de communication, sautez le point suivant.

5) Si vous n'utilisez pas dans le réseau interne le serveur DHCP du système de communication, vous devez entrer l'adresse IP du Deployment Server (DLS) et du système de communication de manière à ce que le logiciel du téléphone système SIP puisse être actualisé automatiquement. Cela s'applique uniquement aux téléphones système SIP. Pour cela, suivez les étapes suivantes :

a) Recherchez `Network` (réseau) et confirmez avec la touche OK.

b) Recherchez `Update service (DLS)` (service de mise à jour DLS) et confirmez avec la touche OK.

c) Recherchez `DLS address` (adresse DLS) et confirmez avec la touche OK.

d) Entrez comme Deployment Server l'adresse IP du système de communication `(par défaut :` 192.168.1.2) et confirmez avec la touche OK.

e) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

f) Recherchez `IPv4 configuration` (configuration IPv4) et confirmez avec la touche OK.

g) Recherchez `Route (default)` (route par défaut) et confirmez avec la touche OK.

h) Entrez l'adresse IP du système de communication (par défaut `192.168.1.2`) et confirmez avec la touche OK.

i) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.
j) Utilisez la touche Retour pour revenir au niveau de menu précédent.

6) Définissez les paramètres de temps SNTP :
a) Recherchez `Date and Time` (date et heure) et confirmez avec la touche OK.
b) Recherchez `Time source` (source de temps) et confirmez avec la touche OK.
c) Recherchez `SNTP IP address` (adresse IP SNTP) et confirmez avec la touche OK.
d) Entrez l'adresse IP du système de communication (par défaut `192.168.1.2`) et confirmez avec la touche OK.
e) Recherchez `Timezone offset` (décalage horaire) et confirmez avec la touche OK.
f) Indiquez l'écart entre l'heure locale et l'heure universelle (Universal Time Coordinated) en heures (Allemagne : `1`) et confirmez avec OK.
g) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.
h) Utilisez la touche Retour pour revenir au niveau de menu précédent.

7) Fixez le numéro de téléphone du téléphone :
a) Recherchez `System` (système) et confirmez avec la touche OK.
b) Recherchez `Identity` (identité) et confirmez avec la touche OK.
c) Recherchez `Terminal number` (numéro du terminal) et confirmez avec la touche OK.
d) Entrez le numéro de téléphone défini (par ex. `120` et confirmez avec la touche OK.
e) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

8) Définissez les données d'authentification SIP :
a) Recherchez `Registration` et confirmez avec la touche OK.
b) Recherchez `SIP session` (session SIP) et confirmez avec la touche OK.
c) Notez le `Realm` ou entrez si nécessaire un nouveau Realm (par ex. `OSBIZ-SIP`).
d) Notez le `User ID` ou indiquez si nécessaire un nouvel User ID (par ex. `SIP-120`) un.
e) Attribuez un `Mot de passe` pour l'enregistrement sur le serveur SIP.
f) Recherchez `Save & Exit` (enregistrer et quitter) et confirmez avec la touche OK.

9) A l'aide de la touche Précédent, revenir au menu `Admin`.

10) Si, en raison des modifications, le téléphone système doit effectuer un redémarrage, il apparaît dans le menu `Admin` l'option de menu `Redémarrage`. Confirmez `Redémarrage` avec le touche OK puis `Oui` ainsi que la touche OK. Le téléphone système effectue un redémarrage et se connecte au système de communication.

6.10 Désinstallation du logiciel de communication

La désinstallation du logiciel de communication est possible à l'aide d'une console de texte.

6.10.1 Comment désinstaller le logiciel de communication

Étape par étape

1) Ouvrez un terminal (par ex. terminal GNOME).
2) Dans l'interface shell, entrez l'instruction `su` (pour superuser = root) et validez avec la touche Entrée.
3) Dans l'interface shell, entrez le mot de passe pour l'utilisateur "root" et validez avec la touche Entrée.
4) Dans l'interface shell, entrez l'instruction `oso_deinstall.sh` et validez avec la touche Entrée. Conformez-vous aux instructions du programme de désinstallation.

6.11 Ports utilisés

Les composantes système d'OpenScape Business utilisent différents ports qui doivent, si nécessaire, être validés dans le pare-feu. Pour les ports des clients basés sur le Web (par ex. myPortal to go), il faut paramétrer un renvoi de port dans le routeur.

Une liste complète de tous les ports utilisés de OpenScape Business est disponible dans la « base de données de gestion d'interface » (IFMD) accessible depuis le portail partenaire de Unify (https://unify.com/en/partners/partner-portal.

Remarque : Les ports identifiés par O dans la liste ci-dessous sont facultatifs, c'est-à-dire qu'ils ne sont pas ouverts en permanence dans le pare-feu.

Description	TCP	UDP	Numéro de port	OpenScape E	OpenScape Business S
Composants du système					
Portail Admin (https)	X		443	X	X
Contrôles CAR Alive	X		12062	X	X
CLA	X		61740	O	O
Découverte auto CLA		X	23232	X	X
CLS	X		7780, 7790 (jusqu'au V3R3) 7780, 7791 (V3R3.1 et supérieur)	O	O
Programme d'installation Communications Client	X		8101	X	X
CSTA Message Dispatcher (CMD)	X		8900		X
CSTA Protocol Handler (CPH)	X		7004	X	X

Description	TCP	UDP	Numéro de port	OpenScape E	OpenScape Business S
Fournisseur de services CSTA (CSP)	X		8800		X
DHCP		X	67	X	
DLI	X		18443	X	X
DLSC	X		8084	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
Messagerie instantanée (http)	X		8101	X	X
JSFT	X		8771		X
JSFT	X		8772		X
Service de Cloud LAS	X		8602	X	
Serveur LDAP	X		389		X
Manager E	X		7000	X	
MEB SIP	X		15060		
Traversée de NAT (NAT-T)		X	4500	X	
NTP		X	123	X	
Openfire Admin (HTTPS)	X		9091		X
Utilitaire de mise à jour automatique OpenScape Business (http)	X		8101	X	X
OpenScape Business Multisite	X		8778		X
OpenScape Business myReports (http)	X		8101		X
Serveur d'état OpenScape Business	X		8808	X	X
Portail utilisateur OpenScape Business	X	X	8779		X
Postgres	X		5432	X	X
RTP (intégré)		X	29100-30530	X	X
RTP (serveur)		X	29100-30888	X	X
SIP (serveur)	X	X	5060	X	X
SIP TLS SIPQ (serveur)	X		5061	X	X

Description	TCP	UDP	Numéro de port	OpenScape E	OpenScape Business S
Abonné SIP TLS (serveur)	X		5062	X	X
SNMP (Get/Set)		X	161	X	X
SNMP (Traps)		X	162	X	X
VSL	X		8770-8780		X
Webadmin pour les clients	X		8803	X	X
Clients basés sur le Web					
Webbased Clients (http)	X		8801	X	X
Webbased Clients (https)	X		8802	X	X

Remarque : Pour des raisons de sécurité, il est recommandé d'utiliser exclusivement https pour les clients basés sur le Web et de configurer un renvoi de port (Port Forwarding) de TCP/443 externe vers TCP/8802 interne.

Certificat CLS

A partir de V3R3.1, un nouveau certificat CLS avec un nom commun (CN) mis à jour est fourni via un port nouvellement introduit. Il offre un algorithme de résumé amélioré et plus fort, ainsi que des entités légales mises à jour. Les systèmes sous licence en ligne via le mode CLS Connect nécessitent les deux conditions préalables suivantes :

- L'adresse IP 188.64.16.4 est activée pour le trafic sortant dans le pare-feu.
- Les ports 7780 et 7791 sont activés pour le trafic sortant dans le pare-feu.

Le port 7790 précédemment utilisé peut être supprimé de la configuration du pare-feu après la mise à niveau vers V3R3.1 pour augmenter la sécurité.

6.12 Comment collecter les traces de diagnostic pour les incidents de type erreur

Vous pouvez automatiquement collecter les données de traces de diagnostic nécessaires pour un incident de type erreur. L'assistant **Gestion des erreurs** vous guidera tout au long du processus.

Vous devez exécuter deux fois l'assistant **Gestion des erreurs** : avant et après l'exécution du scénario problématique. Durant la première exécution (phase 1), vous activez l'ensemble des traces de diagnostics. Après l'exécution du scénario problématique, exécutez de nouveau l'assistant pour collecter les données de trace de diagnostic (phase 2). Une fois la phase 2 terminée, vous pouvez télécharger le fichier de trace pour l'inclure dans le système de tickets.

Procédez comme suit pour collecter les données de traces de diagnostic pour l'incident de type erreur :

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** à côté de **Gestion des erreurs**.
3) Cliquez sur **OK & Suivant**.
4) Si vous souhaitez collecter les traces par défaut, cochez la case **Traces par défaut**.
5) Si vous souhaitez définir les types de traces à collecter, sélectionnez les traces souhaitées dans la liste. Plusieurs sélections sont possibles.

   Pour plus d'informations sur les traces, consultez le guide de résolution des problèmes.
6) Cliquez sur **OK & Suivant**.
7) Une liste d'informations supplémentaires, de documents pertinents et d'astuces s'affiche. Cliquez sur **OK & Suivant**.
8) Les scénarios et les types de trace que vous allez collecter s'affichent. Cliquez sur **Terminer**.
9) Continuez en exécutant le scénario problématique.
10) Une fois le scénario terminé, accédez de nouveau à **Configuration > Gestion des erreurs** et cliquez sur **Modifier**.

    Vous êtes redirigé vers l'étape 2 de la collecte des traces de diagnostic. Si vous souhaitez interrompre le processus et le recommander, cliquez sur le bouton **Annuler**.
11) Cliquez sur **OK & Suivant**.
12) Saisissez les informations requises et cliquez sur **OK & Suivant**.
13) Une liste répertoriant les informations requises et certaines actions supplémentaires s'affiche.
14) Cliquez sur **OK & Suivant**.
15) Cliquez sur **Terminer** pour commencer à télécharger les données de traces de diagnostic.

6.13 Refaire le flashage

En suivant les étapes ci-dessous, vous pouvez facilement changer le type de logiciel d'un périphérique.

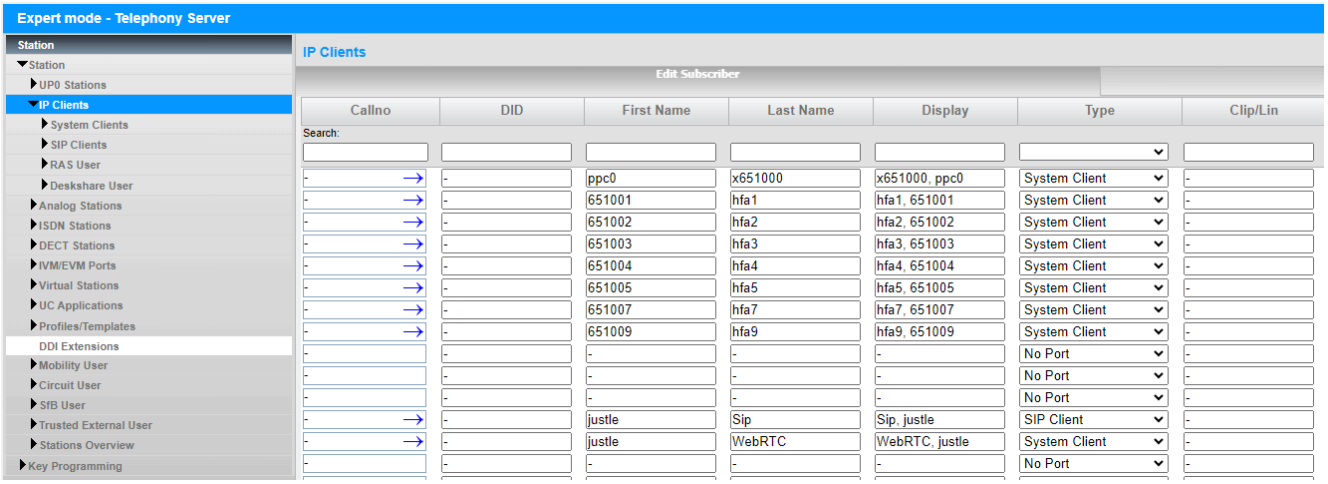
Le concept derrière cette fonction est de simplifier la façon d'obtenir un périphérique SIP (prêt à l'emploi) et de l'enregistrer dans le système OSBiz en tant que périphérique HFA. Les seules exigences sont les suivantes :

- le téléphone doit obtenir l'adresse DLI (soit à partir d'un serveur DHCP, soit manuellement)
- l'administrateur doit entrer le numéro du téléphone (qui doit être préconfiguré en tant que client du système)

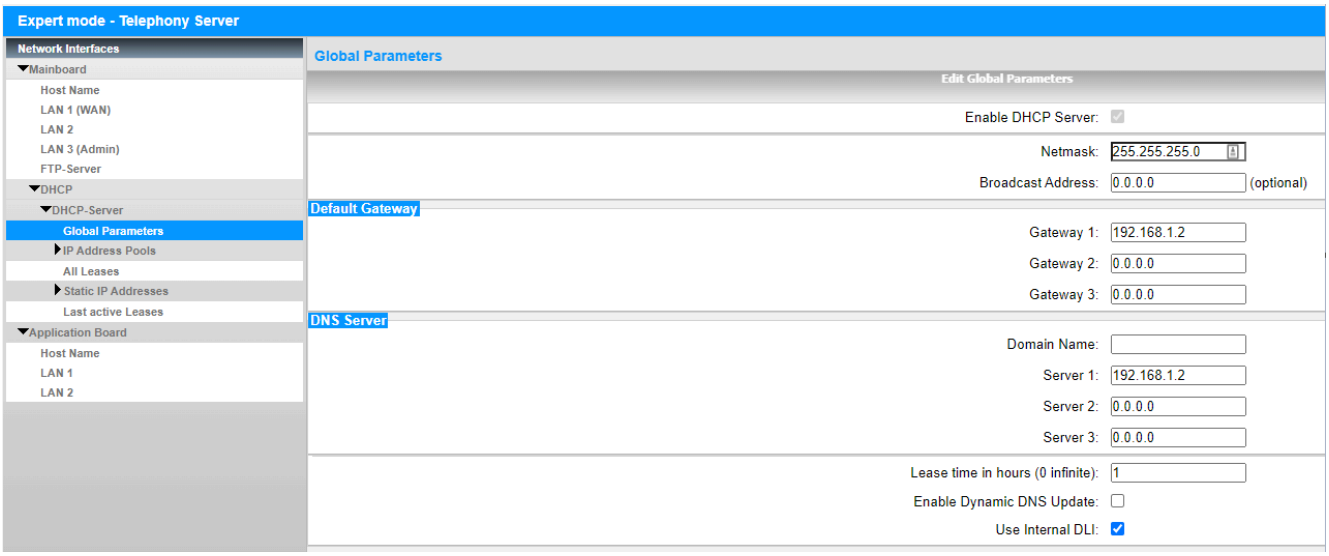
Lorsque le client reçoit un nouveau périphérique, il est préconfiguré en tant que périphérique SIP (paramètres d'usine). Les étapes pour reconfigurer ce périphérique en périphérique HFA sont les suivantes :

Étape par étape

1) Configurer dans la base de données OSBIZ le numéro de téléphone souhaité en tant que client système (HFA).



2) Configurer le serveur DHCP pour qu'il envoie l'adresse IP de DLI. Cette opération peut être effectuée soit sur le serveur DHCP externe, soit sur le serveur DHCP interne.



3) Si aucun serveur DHCP n'est utilisé, vous devez configurer manuellement l'adresse IP de DLI sur le téléphone.

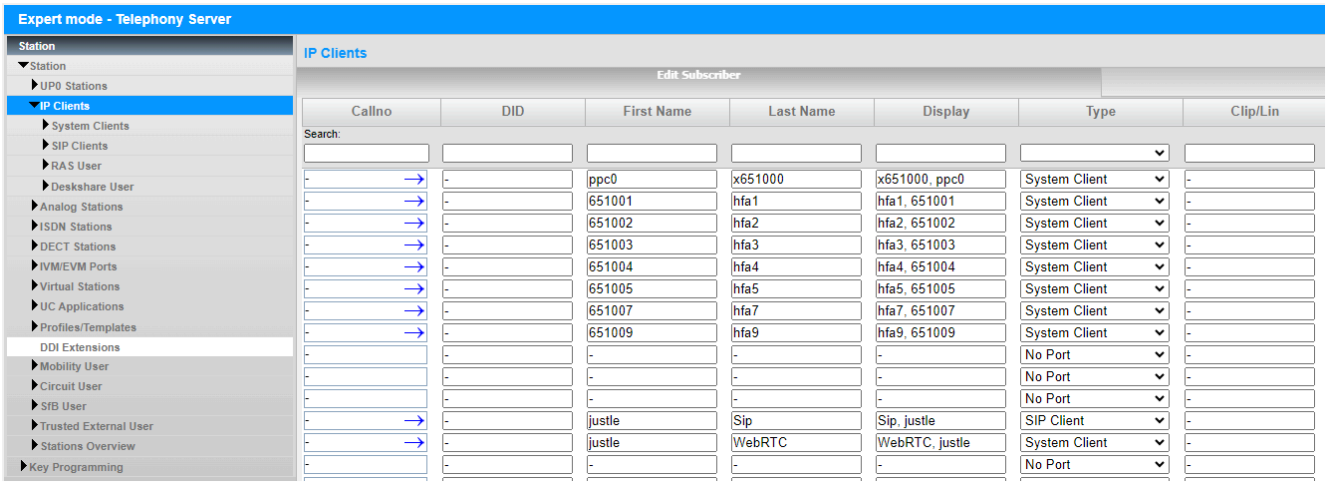
4) Une fois que le téléphone SIP obtient une IP et l'IP DLI, l'appareil téléphonique sera enregistré dans la base de données DLI et une invite s'affichera pour entrer le numéro de poste.

5) Saisissez le numéro de terminal sur le téléphone (le numéro doit être le même que celui configuré lors de la première étape, par exemple 4111).

6) Le reflash démarre et la nouvelle image HFA est téléchargée sur le téléphone. Lorsque le téléphone redémarre, il est enregistré en tant que téléphone HFA et les données « plug and play » sont envoyées par le système au téléphone.

7) **Pour reflasher un téléphone SIP déjà enregistré :**

8) Changez le type d'appareil SIP de travail en « Client système ».



9) Redémarrez le téléphone.

10) Le reflash démarre et la nouvelle image HFA est téléchargée sur le téléphone. Lorsque le téléphone redémarre, il est enregistré en tant que téléphone HFA et les données « plug and play » sont envoyées par le système au téléphone.

7 Licences

Le concept de licence flexible d'OpenScape Business permet aux clients d'adapter le périmètre fonctionnel à leurs propres besoins. Tous les systèmes de communication OpenScape Business X et OpenScape Business S sont soumis à ce concept de licence. Les téléphones, clients UC, fonctions UC et fonctionnalités concernant l'ensemble du système peuvent ainsi être déverrouillés en fonction des besoins individuels du client. Des licences unifiées sont utilisées pour tous les systèmes de communication OpenScape Business.

OpenScape Business peut être développé ou équipé de fonctionnalités supplémentaires ultérieurement via l'achat d'autres licences.

Toutes les licences sont liées en permanence à la licence de base du système de communication et permettent l'utilisation des fonctionnalités acquises pour la version correspondante d'OpenScape Business.

Des licences d'évaluation peuvent être commandées pour une durée de 90 jours pour permettre aux clients de tester et d'évaluer les fonctionnalités spécifiques.

Remarque : Il est conseillé de ne pas installer les fichiers de licence ni d'exécuter d'assistant si le système est actif, car les appels actifs risquent de disparaître.

Période d'activation

Durant la période d'activation (période de 30 jours), il faut procéder à l'activation de la licence. La période d'activation démarre lorsque la date actuelle est entrée dans WBM. Ainsi, la date de fin de période d'activation est sauvegardée.

Durant la période d'activation, le produit est entièrement fonctionnel et le nombre maximum de licences peut être utilisé.

Si, au cours de la période d'activation, le système perd la date actuelle (suite à la décharge de la batterie de la carte mère par exemple), la date doit être rapidement mise à jour dans WBM afin que le système puisse continuer à être utilisé sans restriction durant cette période d'activation.

S'il n'y a pas de prise de licence à l'issue de la période d'activation, l'utilisation du système de communication sera extrêmement restreinte. Une communication interne entre les abonnés est possible mais seuls les deux premiers téléphones actifs sont en mesure de passer des appels externes (pour des appels d'urgence par exemple). L'accès à distance au système de communication demeure possible. Le système se trouve également dans cet état d'utilisation restreint lorsque la première installation a été réalisée uniquement avec Manager E car cela ne permet pas de démarrer la période d'activation.

Structure des licences

Les licences du système de communication sont structurées comme suit :

- Une licence de base active définitivement le logiciel du système de communication. Elle est requise pour l'activation des autres licences.
- Les licences d'abonné activent la communication vocale externe des téléphones.

- Les licences orientées utilisateur activent des fonctionnalités spécifiques pour les utilisateurs.
- Les licences système activent les fonctionnalités générales concernant l'ensemble du système.

Migration

Pour les clients HiPath 3000 V9 existants, une migration de licence via une licence de mise à jour est proposée. La migration de licence garantit la protection des investissements pour le client et permet de continuer à utiliser les téléphones et les fonctionnalités vocales.

Remarque : Pour plus d'informations sur les licences et la mise à niveau ou la migration des systèmes dans un réseau, voir la section **Réseau - Licences** du chapitre Mises à jour .

Concepts associés

Abonnés à la page 378

7.1 Procédure d'activation des licences

Les licences sont gérées et activées par l'intermédiaire d'une procédure de gestion centralisée (OpenScape License Management). C'est la garantie qu'un client utilise exactement la configuration système ou les fonctionnalités pour lesquelles il a acquis les licences correspondantes (droits d'utilisation).

Les licences des systèmes de communication OpenScape Business sont liées à l'ID de verrouillage ou à l'ID de verrouillage avancé du système de communication (voir ID de verrouillage et ID de verrouillage avancé).

Le client commande les fonctionnalités souhaitées et reçoit un code d'activation de licence (LAC). Une fois la première installation du système de communication effectuée, le client active les licences acquises à l'aide du fichier de licence. Le fichier de licence met à la disposition du système un groupe comprenant toutes les licences acquises pour l'affectation de licence effectuée ensuite.

La WBM propose, dans le cadre d'une gestion par un assistant, les fonctions d'enregistrement de client, l'activation de la licence et l'attribution de la licence pour les systèmes indépendants et pour les systèmes qui sont situés dans une interconnexion de réseaux OpenScape Business. La procédure de licence avec Manager E n'est pas possible.

Etapes pour réussir la procédure de licence

1) Configuration du système durant la période d'activation
2) Enregistrement des données client
3) Activation des licences
4) Affectation de licence

Enregistrement du client

Dans le cadre de la procédure de licence, il faut nécessairement indiquer les données client du système correspondant pour l'enregistrement du client. Les données client sont nécessaires pour être en mesure de fournir rapidement

des informations en cas de questions touchant la sécurité, en particulier les rappels de produits. De plus, les clients reçoivent des informations permettant d'empêcher l'utilisation frauduleuse des licences par des tiers, par ex. au sujet de la reconnexion des informations sur la licence.

Activation des licences

Lors de l'activation des licences, à l'aide de la gestion des licences de WBM, les licences acquises sont liées au système de communication. Pour cela, on dispose de 2 méthodes.

- Activation en ligne

  Lors de l'activation en ligne, après l'entrée du code LAC, il est établi via Internet une liaison avec le serveur de licence central (Central License Server, CLS) ; le fichier de licence est automatiquement transmis à l'agent de licence intégré au système de communication (Customer License Agent, CLA). Ensuite, les licences sont automatiquement activées.
- Activation hors ligne

  Lors de l'activation hors ligne, il n'existe aucune liaison entre le système de communication et le serveur de licence central (Central License Server, CLS). Le fichier de licence est généré par un partenaire autorisé au niveau du CLS et, lors de l'activation de la licence, il doit être transmis manuellement à l'agent de licence intégré dans le système de communication (Customer License Agent, CLA).

Affectation de licence

Toutes les licences acquises sont attribuées de manière fixe par la gestion des licences de WBM.

Afin de pouvoir affecter les licences d'abonné, il faut tout d'abord créer les abonnés avec WBM, par ex. lors de la première installation. Chaque configuration système peut être créée, indépendamment des licences disponibles. C'est seulement une fois que la licence a été attribuée qu'il est possible d'utiliser la fonctionnalité correspondante.

Lors de l'affectation de licence, on fait la distinction entre configuration et attribution de licences. Pour les licences d'abonné et les licences orientées utilisateur, des demandes de licence sont configurées. S'il existe une licence correspondant à la demande de licence dans le groupe de licences, la fonctionnalité correspondante est validée. S'il n'existe aucune licence dans le groupe de licences, la demande de licence est conservée, mais la fonctionnalité correspondante n'est pas validée. Si nécessaire, les licences manquantes doivent être achetées.

Procédure de licence dans l'interconnexion de réseaux

Pour une interconnexion de réseaux OpenScape Business, un partenaire autorisé génère un fichier de licence pour l'ensemble du réseau (fichier de licence réseau) au niveau du serveur de licences central (CLS). Ce fichier de licence pour l'ensemble du réseau est géré par l'agent de licences central (CLA) du noeud maître et fournit les licences aux différents noeuds. L'affectation des licences est réalisé à l'aide du WBM de chaque noeud. A l'intérieur d'une interconnexion de réseau, les licences peuvent être distribuées à l'aide de WBM.

Pour la procédure de licence d'une interconnexion de réseaux, l'activation online n'est pas possible.

Paiement à l'utilisation

Outre le système de licences classique, OpenScape Business prend en charge le modèle de licence par abonnement (ou de « paiement à l'utilisation »). Le modèle de paiement à l'utilisation permet de facturer uniquement les licences utilisées pour chaque période de facturation et d'utiliser des licences supplémentaires sans étendre le fichier de licence. Il n'est pas nécessaire de définir le nombre de licences en amont.

Le système OpenScape Business doit être connecté au serveur de licences central (CLS) à l'aide d'une connexion Internet permanente. Celle-ci peut être activée en ligne à l'aide d'un code d'activation de licence ou via le chargement d'un fichier. Après l'installation et la configuration de la solution en fonction des besoins spécifiques, et l'activation du modèle de paiement à l'utilisation, un rapport périodique des licences utilisées est envoyé au serveur de licences central (CLS) où il est analysé. Une fois par mois, un rapport final est créé sur le site du serveur de licences central (CLS) et le contenu des licences utilisées de ce rapport final est utilisé dans le cadre de la comptabilité des licences.

Les licences par abonnement utilisent quant à elles des périodes de qualification. La période de qualification démarre lors du démarrage du système ou de l'activation d'un fichier de licence de paiement à l'utilisation. La période démarre immédiatement et durant cette période, une configuration de licence effectuée dans WBM n'entraîne pas la mise à jour des données d'utilisation des licences. La durée maximale de la période de qualification est de 2 heures.

Remarque : Pour que le pare-feu ait accès au CLS, la configuration suivante est requise :

- Le port 7790 est autorisé pour le trafic IP sortant

- L'adresse IP 188.64.16.4 est autorisée pour le trafic IP sortant

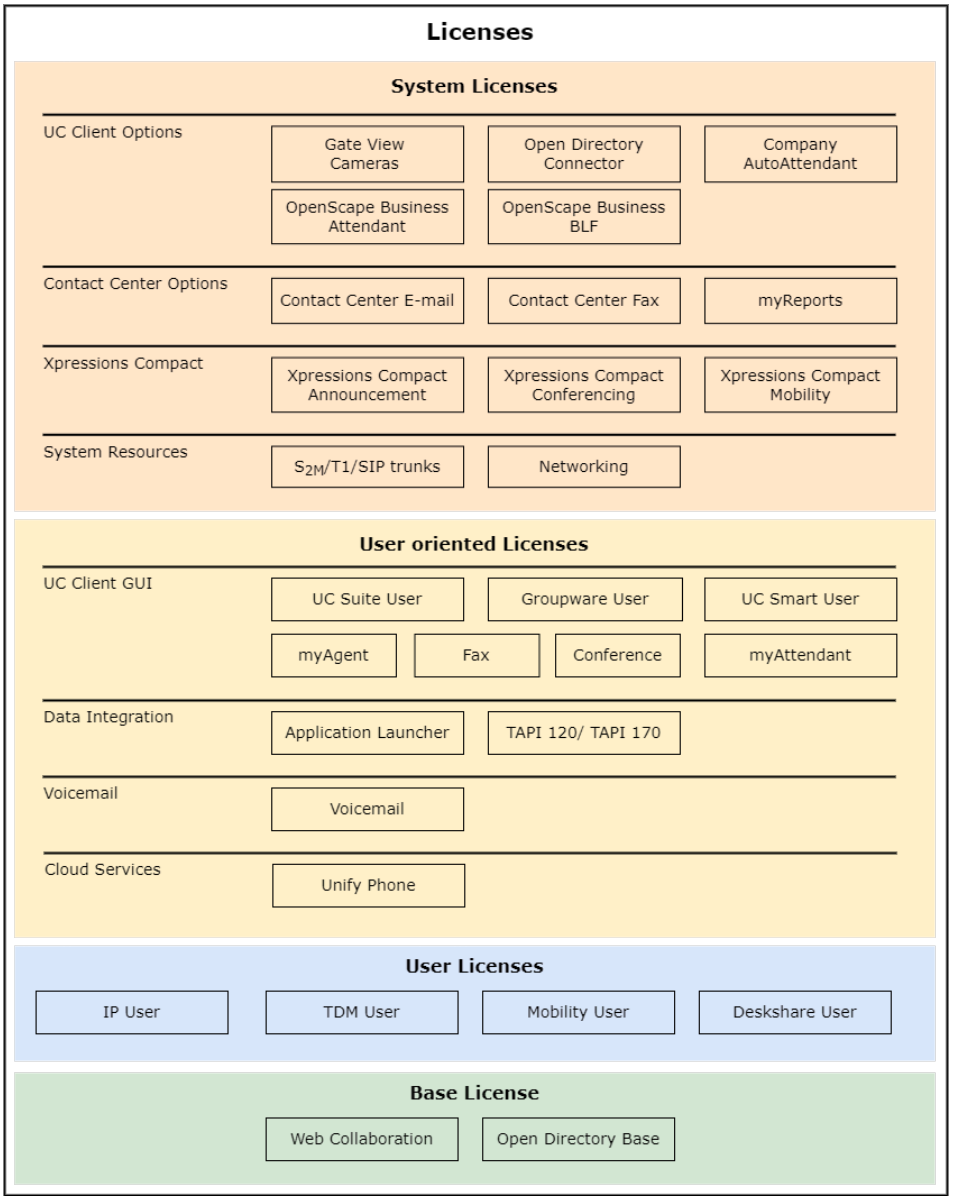
Les systèmes logiciels V3R3 plus récents utilisent le port 7791 pour l'activation de la licence en ligne.

7.2 Licences

Pour utiliser les fonctionnalités du système de communication, des licences doivent être achetées. Les licences achetées doivent être activées dans un délai déterminé (délai d'activation).

Les licences sont classées par thèmes en groupes de licences. Les groupes de licences suivants sont disponibles :

- Licences de base
- Licences de station
- Licences orientées utilisateur
- Licences système



Les licences mentionnées ci-dessus peuvent être utilisées pour OpenScape Business X et OpenScape Business S. Elles couvrent toutes les fonctionnalités et peuvent être combinées selon les souhaits du client. Les combinaisons possibles de licences sont expliquées plus en détail dans la section « Attribution des licences et des profils de licences ».

Les licences de station et les licences orientées utilisateur sont attribuées de manière permanente aux abonnés.

7.2.1 Licence de base

Une licence de base permet l'utilisation de base du système de communication. Elle est également nécessaire pour activer toutes les autres licences.

La téléphonie par Internet et les opérations d'urgence sont également possibles sans licence de base.

Les licences de base suivantes sont disponibles :

- **Base OpenScape Business V2 X1**

  pour débloquer la fonctionnalité V2 de

  – OpenScape Business X1

  La licence de base inclut en outre les licences OpenDirectory Base pour l'utilisation du service Open Directory (ODS). Cela permet à la solution de communications unifiées UC Smart d'être connectée à une base de données externe.
- **Base OpenScape Business V2**

  pour débloquer la fonctionnalité V2 de

  – OpenScape Business X5/X8 ou
  – OpenScape Business S

  La licence de base inclut en plus la licence OpenDirectory Base pour l'utilisation du service Open Directory (ODS). Cela permet de connecter les solutions UC Suite ou UC Smart à une base de données externe.

7.2.2 Licences utilisateur

Chaque abonné connecté au système de communication a besoin d'une licence utilisateur pour passer des appels externes. Cette licence est liée de manière permanente au numéro d'appel de l'abonné via le WBM.

Les licences utilisateur incluent les fonctionnalités vocales complètes d'OpenScape Business. Des licences supplémentaires sont nécessaires pour utiliser les solutions UC UC Smart ou UC Suite (voir Licences orientées utilisateur).

Les licences de station suivantes sont disponibles :

- **Utilisateur IP**

  Pour l'utilisation des téléphones à système IP (HFA) et des téléphones SIP.
- **Utilisateur TDM**

  Pour l'utilisation des téléphones système UP0, des téléphones analogiques, des télécopieurs analogiques, des terminaux RNIS, des télécopieurs RNIS et des équipements Dect.
- **Utilisateur mobile**

  Pour l'utilisation des téléphones GSM/mobiles, des smartphones et des tablettes comme extension du système de communication. Pour l'utilisation de l'entrée par mobilité. L'attribution d'un téléphone de bureau supplémentaire n'est pas requise. Pour l'utilisation du client Unify Phone en combinaison avec OpenScape Business.
- **Utilisateur DeskShare**

  Pour utiliser la fonction de partage de bureau. Seul un numéro de téléphone, et aucun téléphone physique, n'est attribué de façon permanente à ces utilisateurs. Les utilisateurs de DeskShare peuvent utiliser des téléphones spécifiques du système IP en utilisant leur numéro de téléphone permanent et accéder aux paramètres personnels de leur téléphone sur ces téléphones.
- **Utilisateur de secours**

  Pour une utilisation téléphonique de base en cas de défaillance d'un nœud du système. La licence est proposée sous forme de licence à paiement

à l'utilisation basée sur le temps. Le temps d'utilisation est donc calculé en fonction des jours où le système héberge des utilisateurs provenant d'autres nœuds. Les licences ne sont valables que pendant cette période d'hébergement. En mode de fonctionnement normal, les utilisateurs de secours sont assimilés à des utilisateurs sans licence.

Licences utilisateur flexibles

Grâce à la flexibilité des licences utilisateur, les utilisateurs TDM, Mobility et Deskshare peuvent également bénéficier de licences utilisateur IP. Si toutes les licences utilisateur TDM, DeskShare et Mobility acquises ont déjà été attribuées à des abonnés, et que d'autres utilisateurs TDM, DeskShare et Mobility sont nécessaires, alors toutes les licences utilisateur IP restantes peuvent être utilisées pour répondre à cette demande.

L'utilisation d'une licence utilisateur flexible nécessite la version logicielle V1R3.3 et un fichier de licence nouvellement généré sur le CLS, qui doit être importé dans OpenScape Business et activé.

Licence utilisateur flexible UC-Suite

Grâce au système de licences utilisateur flexible UC-Suite, les utilisateurs de myPortal pour ordinateur de bureau peuvent également bénéficier de licences utilisateur myPortal pour Outlook. Si toutes les licences myPortal for Desktop acquises ont déjà été attribuées et que d'autres utilisateurs sont nécessaires, les licences myPortal for Outlook User peuvent être utilisées pour répondre à cette demande.

L'utilisation d'une licence utilisateur flexible nécessite la version logicielle V2 et un fichier de licence nouvellement généré au niveau du CLS, qui doit être importé dans OpenScape Business et activé.

7.2.3 Licences orientées utilisateur

Les licences orientées utilisateur sont basées sur la station et autorisent l'utilisation des fonctionnalités de communications unifiées et des applications d'intégration de données. Une licence orientée utilisateur nécessite également une licence de station et est attribuée de manière permanente au numéro de téléphone de l'abonné.

Les licences suivantes, destinées aux utilisateurs, sont disponibles :

Messagerie vocale

- **Messagerie vocale**

  Pour l’utilisation d’une boîte vocale personnelle via le téléphone (TUI) et via l’interface utilisateur des solutions UC UC Smart ou UC Suite.

  Remarque : Si la solution UC Smart est étendue à UC Suite, les licences de messagerie vocale existantes et les affectations aux postes sont conservées.

  Remarque : Lors de l'attribution d'une licence de messagerie vocale à un poste, un utilisateur UC Suite est créé et tous les renvois d'appels actifs sont réinitialisés.

Services cloud

- **Téléphone Unify**

  Pour l'utilisation du client Unify Phone en combinaison avec OpenScape Business.

Interface utilisateur du client UC

- **Utilisateur intelligent UC**

  Pour l'utilisation des fonctions UC Smart des clients de communication myPortal @work et autres clients de services Web.
- **Utilisateur de UC Suite**

  Pour l'utilisation des fonctions UC Suite des clients de communication myPortal @work, myPortal for Desktop et autres clients de services Web.
- **utilisateur de logiciels de groupe**

  Pour l'utilisation des fonctions UC Suite des clients de communication myPortal @work, myPortal for Outlook et autres clients de services Web.
- **Fax**

  Pour l'utilisation d'un boîtier fax au sein de la suite UC. En prérequis, une licence utilisateur UC ou Groupware est également requise.
- **Conférence**

  Pour l'utilisation des fonctionnalités de gestion de conférences de UC Suite, telles que la gestion et le lancement de conférences permanentes et récurrentes. En outre, une licence utilisateur UC ou une licence utilisateur Groupware est requise au préalable.

  Aucune licence n'est requise pour participer aux conférences.
- **mon assistant**

  Pour l'utilisation des fonctionnalités de l'assistant UC Suite.
- **monAgent**

  Pour l'utilisation des fonctions du centre de contact telles que les informations sur les files d'attente, les fenêtres contextuelles avec les informations client sur les appels entrants et l'accès à l'historique des appels.

Intégration des données

- **Lanceur d'applications**

  Pour le contrôle des applications sur un PC client pendant les appels entrants et sortants, par exemple, le lancement d'une application ou l'affichage des informations de l'appelant. Application Launcher peut être utilisé avec UC Smart, UC Suite ou myAgent et nécessite en outre une licence utilisateur UC / utilisateur Groupware ou une licence myAgent. Il peut utiliser, en option, le service Open Directory.
- **OpenScape Business TAPI**

  Pour l'utilisation d'applications compatibles TAPI et pour la téléphonie sur PC avec les applications propres du client provenant de différents fournisseurs de logiciels.

7.2.4 Licences système

Les licences système ne sont pas spécifiques à un abonné et débloquent les fonctionnalités à l'échelle du système. Ces fonctionnalités peuvent être utilisées par tous les abonnés du système de communication.

Aperçu des exigences de licence système

Type de tronc	Licence SSP	licences de tronc/canal	Licence de réseau
ITSP	Oui	Oui	Non
Trunk SIP natif	Oui	Non	Oui
Skype Entreprise	Oui	Oui	Non
Téléphone Unify	Oui	Non	Non
Interconnexion SIPQ	Non	Non	Oui

Les licences système suivantes sont disponibles :

Ressources système

- **Liaisons S $_{2M}$ /T1/SIP**

  Pour l'utilisation des canaux S $_{2M}$ /T1 et ITSP. Les chaînes $_{S0}$ n'ont pas besoin de licence. Cela inclut également les connexions aux serveurs de fax $_{S0}$ en mode PP. Pour les connexions multiplex primaires S $_{2M}$ ou T1 (USA), les canaux vocaux individuels sont sous licence. Pour les connexions ITSP, le nombre de connexions simultanées à un ou plusieurs fournisseurs ITSP (fournisseurs SIP) est autorisé. Le nombre de connexions simultanées possibles dépend de la bande passante de la connexion.
- **Réseautage**

  Pour la mise en réseau IP via SIP-Q/SIP natif et/ou la mise en réseau TDM via CorNet-NQ ou QSIG. Pour la mise en réseau des applications UC Suite. Une licence est requise par nœud.

  Remarque : La licence réseau débloque les lignes pour le réseau vocal et le réseau UC Suite pour un nœud. Aucune licence S $_{2M}$ /T1/SIP trunk n'est requise pour les trunks réseau.

Tableau 3 : Aperçu des licences de ressources système (S $_{2M}$ /ITSP)

Protocole	Licences			
	Aucune licence	Réseau d'entreprise OpenScape (1x par système)	OpenScape Business S $_{2M}$ / ITSP (1x par canal)	Utilisateur TDM
S $_0$ interne				
Serveur de télécopie (DSS1/ QSIG)	X			

Protocole	Licences			
	Aucune licence	**Réseau d'entreprise OpenScape (1x par système)**	**OpenScape Business S $_{2M}$ / ITSP (1x par canal)**	**Utilisateur TDM**
Autobus européen				par station S $_0$
S $_0$ - Troncs CO				
EURO CO PP	X			
Euro CO PMP	X			
S $_{2M}$ - Trottoirs CO				
EURO CO PP			X	
Fournisseur de services informatiques (ITSP)				
ITSP 1 à 8			X	
Réseau S $_0$				
QSIG		X		
CorNet-NQ		X		
S $_{2M}$ - Réseautage				
Réseau QSIG		X		
CorNet-NQ		X		
Réseau SIP				
SIP-Q		X		
SIP natif		X		

Options du centre de contact

- **Courrier du centre de contact**

  Pour configurer une ou plusieurs boîtes mail afin d'envoyer et de recevoir des emails pour les agents du centre de contact. Une licence de station et une licence myAgent sont requises pour cela. Une licence est requise par nœud.
- **Fax du centre de contact**

  Pour configurer une ou plusieurs boîtes fax afin d'envoyer et de recevoir des fax pour les agents du centre de contact. Une licence de station et une licence myAgent sont requises pour cela. Une licence est requise par nœud.
- **mes rapports**

  Pour l'établissement de statistiques sur l'utilisation des ressources des centres de contact selon différents critères. Grâce au Gestionnaire de planification, il est possible de créer des rapports à partir de plus de 100 modèles de rapports prédéfinis pour les contacts téléphoniques, électroniques et par fax. Les modèles de rapports sont gérés via le Gestionnaire de rapports, avec des fonctions permettant de regrouper ainsi que d'ajouter et de supprimer des modèles de rapports nouvellement créés.

Options du client UC

- **Connecteur Open Directory**

  Pour se connecter au service Open Directory (ODS) afin de permettre l'accès à une base de données externe ou à un répertoire externe, un maximum de quatre bases de données peuvent être connectées par nœud.
- **Répondeur automatique de l'entreprise**

  Pour l'utilisation d'un standard automatique centralisé basé sur UC Smart ou UC Suite afin de transférer automatiquement les appels. Une licence est requise par nœud.

  Les annonces de type « musique d'attente » (boucle infinie) ne sont diffusées qu'avec cette licence.

7.2.5 Licences d'évaluation

Une licence d'évaluation peut être utilisée pour tester gratuitement des fonctionnalités spécifiques avec toutes leurs fonctionnalités pendant une période déterminée (appelée période d'évaluation). Si une licence standard pour cette fonctionnalité est activée pendant la période d'évaluation, la licence d'évaluation sera désactivée.

Les licences d'évaluation suivantes sont disponibles :

- **Évaluation du service OpenScape Business V3**

  Cette licence d'évaluation est destinée aux partenaires qui souhaitent d'abord préconfigurer le système de communication au sein de leur propre entreprise et le mettre en service ultérieurement chez le client. La période d'activation de 30 jours commence lors de la préconfiguration. Pour relancer la période d'activation de 30 jours après la mise en service du système, cette licence d'évaluation doit être activée depuis le site du client après le démarrage du système.

  L'activation n'est possible qu'une seule fois par système et uniquement pendant la période d'activation. Si la période d'activation a expiré, le système doit être licencié au moyen de licences permanentes.

  Remarque : Lorsque l'évaluation du service est activée, la connexion CLS ne peut pas être activée.
- **Évaluation intelligente d'OpenScape Business V3 UC**

  Cette licence d'évaluation est destinée aux clients qui souhaitent tester les fonctionnalités UC de UC Smart. Toutes les fonctionnalités de UC Smart peuvent être utilisées avec cette licence d'évaluation.

  Remarque : Cette licence d'évaluation ne peut pas être utilisée si le système de communication est situé dans un réseau et que la licence « Réseau » est active. Si des licences de messagerie vocale sont déjà disponibles, elles sont utilisées en combinaison avec les nouvelles licences d'évaluation UC.

- **Évaluation commerciale d'OpenScape UC Suite V3**

  Cette licence d'évaluation est destinée aux clients qui souhaitent tester les fonctionnalités de communications unifiées de UC Suite. Toutes les fonctionnalités de UC Suite sont utilisables avec cette licence d'évaluation.

  Remarque : Cette licence d'évaluation ne peut pas être utilisée si le système de communication est situé dans un réseau et que la licence « Réseau » est active. Si des licences de messagerie vocale sont déjà disponibles, elles sont utilisées en combinaison avec les nouvelles licences d'évaluation UC.

- **Évaluation du centre de contact OpenScape Business V3 UC Suite**

  Cette licence d'évaluation est destinée aux clients qui souhaitent tester le centre de contact multimédia. Toutes les fonctionnalités des centres de contact multimédias sont accessibles avec la licence d'évaluation.

  Remarque : Si le centre de contact multimédia n'est pas sous licence pendant la période d'évaluation, l'administrateur doit annuler les paramètres du centre de contact (par exemple, supprimer les planifications et les files d'attente, désactiver les agents, etc.) avant l'expiration de la licence d'évaluation. Sinon, des erreurs peuvent survenir dans OpenScape Business.

- **Évaluation du CRM OpenScape Business V3**

  Cette licence d'évaluation est destinée aux clients qui souhaitent tester Application Launcher, Open Directory Service et TAPI.

Règles

- L'activation d'une licence d'évaluation se produit sur le serveur de licences client (CLS) et ne peut être effectuée qu'une seule fois.
- La période d'évaluation est de 90 jours. Au bout de 60 jours, le temps restant en jours est décompté à rebours sur l'écran des téléphones du système.
- À l'expiration de la période d'évaluation, la fonctionnalité est automatiquement désactivée.
- Plusieurs licences d'évaluation peuvent être actives simultanément dans le système, mais peuvent ensuite expirer à des moments différents.
- Si une licence perpétuelle est active, la licence d'évaluation n'est pas démarrée ou, si elle est déjà présente, elle est arrêtée.

7.2.6 Licences de mise à niveau

Des licences de mise à niveau sont nécessaires pour mettre à niveau les systèmes HiPath 3000 V9, OpenScape Office V3 et OpenScape Business V1 vers les systèmes OpenScape Business V2.

La migration de licence des systèmes HiPath 3000 nécessite un système HiPath 3000 V9 en fonctionnement et éventuellement sous licence. Les étapes de la migration du matériel et des licences doivent être soigneusement observées (voir également la Migration). Les systèmes Pure HiPath 3000 TDM

sans licence doivent d'abord être mis à niveau vers la version 9 et peuvent ensuite être migrés vers OpenScape Business avec une licence de mise à niveau.

Les licences de mise à niveau suivantes sont disponibles :

- **Mise à niveau de HiPath 3000 V9 vers OpenScape Business V2**

  Pour la migration de HiPath 3000 V9 vers OpenScape Business V2 X5/X8.
- **Mise à niveau de HiPath 3000 V8 vers OpenScape Business V2**

  Pour la migration de HiPath 3000 V8 vers HiPath 3000 V9 puis vers OpenScape Business V2 X5/X8.
- **Mise à niveau de HiPath 3000 V7 vers OpenScape Business V2**

  Pour la migration de HiPath 3000 V7 vers HiPath 3000 V9 puis vers OpenScape Business V2 X5/X8.
- **Mise à niveau d'OpenScape Office V3 MX/LX vers OpenScape Business V2**

  Pour la migration d'OpenScape Office V3 MX/LX vers OpenScape Business V2.

7.2.7 Combinaisons de licences possibles

Les licences peuvent être combinées à volonté. Cette section contient quelques suggestions de combinaisons de licences possibles qui vous permettront d'utiliser les fonctions souhaitées.

Veuillez noter que plusieurs licences sont requises pour certaines fonctions.

Téléphonie

- Requis : Licence de poste utilisateur IP, TDM ou DeskShare

> **Remarque :** Sans licence valide, le téléphone ne peut être utilisé que pour les connexions internes.

Téléphonie avec UC Smart

- Téléphonie avec messagerie vocale (UC Smart)
  - Requis : Licence de poste utilisateur IP, TDM ou DeskShare
  - Requis : licence de messagerie vocale orientée utilisateur
- Téléphonie avec entrée mobile (mobilité basée sur DISA)
  - Obligatoire : Licence de station utilisateur mobile
- Téléphonie avec myPortal @work
  - Obligatoire : adresse IP de l’utilisateur
  - Requis : licence utilisateur UC orientée utilisateur
  - Optionnel : licence de messagerie vocale orientée utilisateur
  - Facultatif : licence de conférence orientée utilisateur

- Téléphonie avec myPortal @work VoIP
  - Obligatoire : adresse IP de l'utilisateur
  - Requis : licence utilisateur UC orientée utilisateur
  - Optionnel : licence de messagerie vocale orientée utilisateur
  - Facultatif : licence de conférence orientée utilisateur

Téléphonie avec UC Suite

- Téléphonie avec messagerie vocale (suite UC)
  - Requis : Licence de poste utilisateur IP, TDM ou DeskShare
  - Requis : licence de messagerie vocale orientée utilisateur
- Téléphonie avec myPortal pour ordinateur
  - Requis : Licence de poste utilisateur IP, TDM ou DeskShare
  - Requis : licence utilisateur UC orientée utilisateur
  - Optionnel : licence de messagerie vocale orientée utilisateur
  - Optionnel : licence de télécopieur orientée utilisateur
  - Facultatif : licence de conférence orientée utilisateur
- Téléphonie avec myPortal pour Outlook
  - Requis : Licence de poste utilisateur IP, TDM ou DeskShare
  - Requis : licence utilisateur de logiciel de travail collaboratif orientée utilisateur
  - Optionnel : licence de messagerie vocale orientée utilisateur
  - Optionnel : licence de télécopieur orientée utilisateur
  - Facultatif : licence de conférence orientée utilisateur
- Téléphonie avec myPortal @work
  - Obligatoire : adresse IP de l'utilisateur
  - Requis : licence utilisateur Groupware orientée utilisateur ou licence utilisateur UC
  - Optionnel : licence de messagerie vocale orientée utilisateur
  - Facultatif : licence de conférence orientée utilisateur
- Téléphonie avec myPortal @work VoIP
  - Obligatoire : adresse IP de l'utilisateur
  - Requis : licence utilisateur Groupware orientée utilisateur ou licence utilisateur UC
  - Optionnel : licence de messagerie vocale orientée utilisateur
  - Facultatif : licence de conférence orientée utilisateur
- Téléphone avec mon assistant
  - Requis : Licence de poste utilisateur IP, TDM ou DeskShare
  - Requis : licence d'assistant orientée utilisateur
  - Optionnel : licence de messagerie vocale orientée utilisateur

Téléphonie avec Unify Phone

- Obligatoire : adresse IP de l'utilisateur
- Requis : licence Unify Phone orientée utilisateur

- En option : licence de messagerie vocale orientée utilisateur et licence utilisateur IP supplémentaire pour la configuration d'équipe

Utilisation du centre de contact

- Requis : Licence de poste utilisateur IP, TDM, DeskShare ou Mobility
- Requis : licence myAgent orientée utilisateur

  Au moins une licence myAgent doit être active pour que le système puisse acheminer et traiter les appels du centre de contact.
- Optionnel : Licence du système de messagerie du centre de contact
- Optionnel : Licence pour le système de télécopie du centre de contact
- Facultatif : licence du système myReports

Utilisation du standard automatique de l'entreprise

- Requis : Licence du système de standard automatique de l'entreprise

  La licence du système de standard automatique de l'entreprise doit être active pour que le système puisse acheminer et traiter les appels du standard automatique.

7.3 Procédure de licence d'un système de communication (Standalone)

La procédure de licence d'un système Standalone doit être effectuée selon un ordre défini. Cet ordre est représenté à l'exemple de l'un des systèmes de communication OpenScape Business X.

Comment effectuer l'étape 3 et l'étape 4 avec l'aide de la WBM - voir dans les sous-chapitres ci-après.

1) **Code d'autorisation de licence (LAC)**

   A l'achat des licenses, le client reçoit un code d'autorisation de licence (LAC, License Authorization Code). Les données concernant les licences obtenues sont enregistrées dans la base de données du serveur central de licences (CLS).
2) **Installation et configuration**

   Le client ou le technicien SAV installe et configure le système de communication avec l'aide de l'assistant WBM (notamment abonnés et lignes). Lors du premier démarrage de la WBM, il faut entrer la date actuelle. A partir de ce moment-là débute la période d'activation (délai de 30 jours durant lequel la procédure de licence du système de communication doit être effectuée).
3) **Activation des licences**

   Le client ou le technicien SAV active les licences avec WBM soit en ligne avec le code d'autorisation de licence (activation de licence en ligne) soit hors ligne directement à l'aide du fichier de licence (activation de licence hors ligne).
4) **Affectation de licence**

   Le client ou le technicien SAV utilise la WBM pour attribuer aux abonnés et aux lignes les licences acquises. Une fois l'attribution effectuée, les fonctionnalités concernées par les licences sont validées.

7.3.1 CLS Connect

CLS Connect vous permet d'effectuer des ré-hébergements illimités de vos systèmes OpenScape Business. Pour ce faire, le marqueur **CLS Connect** doit être activé.

Remarque : Après activation, ce marqueur ne peut pas être désactivé.

Si le système perd la connexion à CLS, la période de basculement commence. Si la connexion n'est pas rétablie après 30 jours, le système passe en mode urgence et est considéré comme sans licence.

Remarque : Lorsqu'il convient de reprogrammer un système OpenScape Business avec CLS Connect actif, vous ne pourrez pas créer un fichier de sauvegarde. Vous devrez effectuer un rechargement avec le même ID MAC et un ID SIEL. Vous ne pouvez pas activer CLS Connect sans licence de base active. Vous pouvez charger manuellement le fichier de licence existant de CLS dans le système à l'aide de WBM.

7.3.1.1 Comment activer CLS Connect

CLS Connect vous permet d'effectuer des ré-hébergements illimités de vos systèmes OpenScape Business.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**

Vous devez disposer d'un accès Internet pour vous connecter au CLS

Les paramètres suivants sont en place pour le pare-feu :

a) Le port 7790 est ouvert pour le trafic IP sortant

Les systèmes logiciels V3R3 plus récents utilisent le port 7791 pour l'activation de la licence en ligne.

b) L'IP 188.64.16.4 est autorisée pour le trafic sortant

Remarque : Pour rendre les règles du pare-feu plus sûres, il est recommandé de n'autoriser que les communications sortantes.

La connexion à CLS est possible, voir Comment vérifier la connexion au Serveur de licence central (CLS)

Remarque : Lorsque vous activez CLS Connect, il est impossible de le désactiver.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Activer CLS Connect**.
3) Activez le **CLS Connect** en cochant la case.
4) Cliquez sur **Activer**.

Remarque : Dans la zone de notification de la page de destination, le message suivant s'affiche si le contrôle de licence en ligne est activé :

« Mode licence : « CLS Connect ». »

7.3.1.2 Abandon de CLS Connect

Abandonnez CLS Connect au profit d'une licence permanente ou PAYGO.

Si vous utilisez actuellement un système de licence CLS Connect et que vous souhaitez passer à une licence permanente ou PAYGO, suivez quelques étapes pour assurer une transition en douceur :

Étape par étape

1) Activez la fonction CLS Connect Stop pour le fichier de licence du système. Pour ce faire, il suffit de créer un ticket d'assistance CLS.
2) Activez un nouveau fichier de licence pour OSBiz afin de réinitialiser le bit sécurisé. Une fois cela fait, vous pouvez activer PAYGO ou la licence locale permanente pour le système sur CLS. Vous recevrez alors un nouveau fichier que vous pourrez activer sur le système.

Remarque : Si vous disposez d'un environnement OSBiz en réseau sous licence CLS Connect, les nœuds esclaves disposeront également du bit sécurisé. Si, à un moment donné, vous prévoyez d'utiliser un nœud esclave comme système autonome séparé avec une licence non-CLS Connect, veuillez créer un ticket d'assistance pour les étapes requises.

7.3.2 Activation des licences (Standalone)

Une fois que vous avez acheté un produit ou une fonctionnalité, vous devez activer les licences fournies avec le produit/la fonctionnalité. Après activation a lieu ensuite l'affectation de la licence.

Il existe deux possibilités pour activer les licences :

- **Activation des licences en ligne** (avec le code d'autorisation de licence)

  Le client ou le technicien de maintenance transmet, à l'aide de la WBM, le code d'autorisation de licence via Internet au serveur de licence central (CLS). En liaison avec le LAC, l'ID de verrouillage du système de communication est utilisée pour l'activation des licences. A partir des

données, CLS génère un fichier de licence et le renvoie au système qui ensuite active les licences acquises.

Pour l'accès à CLS, vous avez besoin d'une connexion Internet. L'adresse IP du serveur CLS figure dans WBM, **Gestion des licences** > **Paramètres** et peut si nécessaire être modifiée par un administrateur de profil **Expert**.

Remarque : Pour l'activation en ligne, le port 7790 est utilisé par défaut. Ce port doit être validé dans le pare-feu du réseau client.

Les systèmes logiciels V3R3 plus récents utilisent le port 7791 pour l'activation de la licence en ligne.

Remarque : Avant que la procédure de licence en ligne puisse être effectuée, il faut d'abord établir correctement les données d'inscription.

- **Activation de licence hors ligne** (directement avec le fichier de licence)

  Le client ou le technicien SAV se connecte au serveur de licences central (CLS) et entre le code d'autorisation de licence en même temps que les ID de verrouillage du système de communication. CLS génère un fichier de licence à partir des données. Le client ou le technicien SAV charge le fichier de licence et et intègre celui-ci dans la WBM. Le système active ensuite les licences acquises.

  L'adresse IP du serveur CLS figure dans WBM, **Gestion des licences** > **Paramètres** et peut si nécessaire être modifiée par un administrateur de profil **Expert**.

Si le système de communication doit être élargi, il est possible de faire l'acquisition d'autres licences. Lors de l'acquisition de licences supplémentaires, un autre code LAC (code d'autorisation) est fourni ; il permet d'activer les licences nouvellement achetées.

Remarque : Les licences acquises en supplément peuvent aussi être activées à distance.

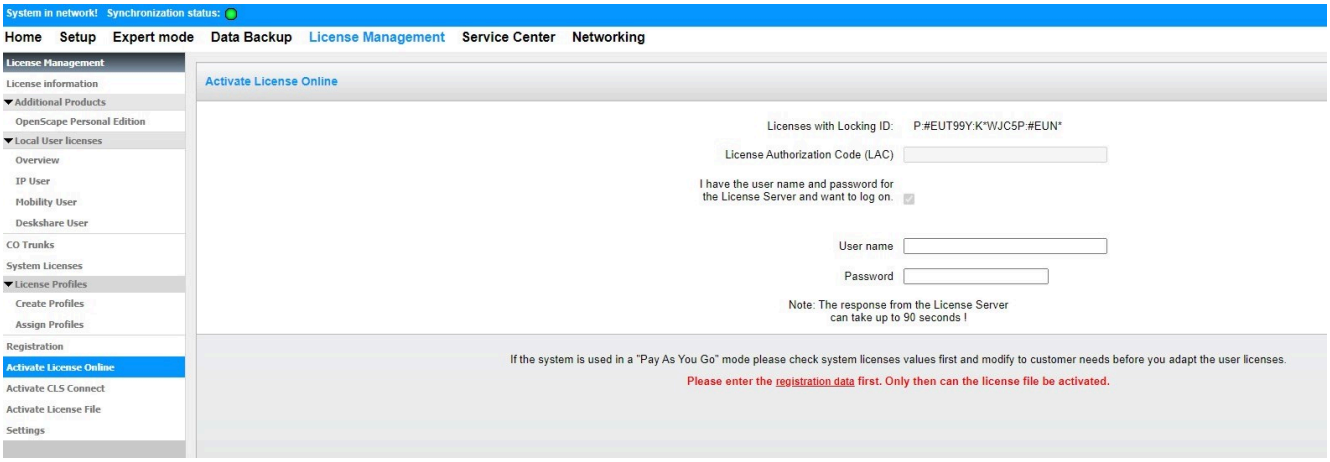
7.3.2.1 Comment activer les licences en ligne (standalone)

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Vous connaissez le code d'autorisation de licence (LAC) pour l'activation de la licence.

Pour la connexion au serveur de licences, le système de communication doit avoir une liaison Internet.



Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Enregistrement**.
3) Saisissez vos données et cliquez sur **OK**.
4) Dans l'arborescence de navigation, cliquez sur **Activer la licence en ligne**.
5) Dans **Code d'autorisation de licence (LAC)**, entrez le code LAC.
6) Cochez la case **J'ai un nom d'utilisateur et un mot de passe pour le serveur de licence et souhaite ouvrir une connexion**.
7) Entrez le **Nom utilisateur** et le **Mot de passe** pour la connexion au serveur de licences.
8) Cliquez sur **Activer**. La connexion avec le serveur de licences est établie et les licences sont transmises au système de communication. Une fois l'activation réalisée avec succès, la liaison est automatiquement déconnectée.

7.3.2.2 Comment activer les licences hors ligne (standalone)

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Le fichier de licence a été généré sur le serveur de licences central et a été sauvegardé. Vous connaissez l'emplacement de stockage du fichier de licence.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Activer le fichier de licence**.
3) Sous **Fichier de licence**, cliquez sur **Rechercher** et sélectionnez l'emplacement de stockage du fichier de licence.
4) Cliquez sur **Activer**.

7.3.3 Attribution de licences (autonome)

Une fois les licences achetées activées avec succès, elles doivent être attribuées aux stations et aux lignes. Dans un système autonome, les fonctionnalités système sont activées automatiquement dès l'activation.

Attribution des licences utilisateur et des licences orientées utilisateur

Les abonnés peuvent se voir attribuer des licences utilisateur et des licences orientées utilisateur.

Les licences utilisateur peuvent être attribuées aux types d'abonnés suivants :

Icône	Licence utilisateur	Description
	Utilisateur IP	Pour l'utilisation des téléphones à système IP (HFA ou SIP) et des téléphones SIP
	Utilisateur TDM	Pour utiliser des téléphones système UP0, des téléphones RNIS, des téléphones analogiques et des équipements Dect
	Utilisateur mobile	Pour l'utilisation de Mobility Entry et du service DISA (One Number Service)
	Utilisateur Deskshare	Pour l'utilisation du partage de bureau par stations IP

Les licences utilisateur sont attribuées de manière permanente aux numéros des abonnés. Si un abonné est supprimé ou si un autre type d'abonné est attribué à un numéro d'appel, la licence utilisateur associée est libérée.

Un astérisque rouge figure à côté de certaines licences. Cet astérisque rouge indique que ces licences peuvent également être couvertes par l'attribution d'une autre licence.

Grâce à la flexibilité des licences, les utilisateurs TDM, Mobility et Deskshare peuvent également bénéficier de licences utilisateur IP. Si toutes les licences utilisateur TDM, DeskShare et Mobility acquises ont déjà été attribuées à des abonnés, et que d'autres utilisateurs TDM, DeskShare et Mobility sont nécessaires, alors toutes les licences utilisateur IP restantes peuvent être utilisées pour répondre à cette demande.

Une fois qu'une licence utilisateur a été attribuée à l'abonné, une licence orientée utilisateur peut également lui être attribuée.

Les licences suivantes, orientées utilisateur, peuvent être attribuées aux stations :

Icône	Licence orientée utilisateur	Description
	Messagerie vocale	Pour l'utilisation de la messagerie vocale.
	utilisateur de logiciels de groupe	Pour l'utilisation des fonctionnalités de UC Suite via myPortal pour Outlook.
	Utilisateur UC	Pour l'utilisation des fonctionnalités de UC Suite via myPortal pour ordinateur.

Icône	Licence orientée utilisateur	Description
	Fax	Pour l'utilisation d'un boîtier fax au sein de la suite UC. Une licence utilisateur UC ou Groupware est requise au préalable.
	Conférence	Pour utiliser les fonctionnalités de conférence de la suite UC. Une licence utilisateur UC ou Groupware est requise au préalable.
	mon assistant	Pour l'utilisation des fonctionnalités de l'assistant UC Suite.
	monAgent	Pour l'utilisation des fonctions du centre de contact.
	Lanceur d'applications	Pour le contrôle des applications sur un PC client pendant les appels entrants et sortants, par exemple, le lancement d'une application ou l'affichage des informations de l'appelant.
	Téléphone Unify	Pour l'utilisation du client Unify Phone en combinaison avec OpenScape Business.
	TAPI	Pour l'utilisation d'applications compatibles TAPI et pour la téléphonie sur PC avec les applications propres du client provenant de différents fournisseurs de logiciels.

Vous pouvez obtenir un aperçu de toutes les licences utilisateur et des licences orientées utilisateur affichées (via **des licences utilisateur locales** > **)** .

Ce tableau récapitulatif présente également le statut des licences pour chaque abonné.

États de licence possibles :

Attribution des licences système

Les licences système comprennent des licences pour les liaisons principales et pour les fonctionnalités à l'échelle du système.

Des licences peuvent être attribuées aux types de trunks suivants :

- Liaisons S $_{2M}$ /T1 : nombre de canaux B
- Lignes ITSP : nombre d'appels simultanés effectués via un seul ITSP

Dans un système autonome, les licences pour les fonctionnalités système auront déjà été déverrouillées par défaut lors de l'activation de la licence. Par conséquent, aucune autre tâche n'est requise.

procédure d'attribution de licence

Prérequis : Le fichier de licence est activé et les stations sont configurées.

- Comment obtenir une licence pour les stations-service

  1) Attribuer une licence utilisateur à un abonné. Cette attribution déclenche la génération d'une demande de licence pour l'abonné tout en permettant l'attribution des licences orientées utilisateur.

  2) Attribuer les licences orientées utilisateur à un abonné. Ces attributions entraînent la génération de demandes de licence supplémentaires pour l'abonné. Veuillez noter que certaines licences nécessitent d'autres licences (voir Combinaisons de licences possibles).

  3) Vérifier et déverrouiller les demandes de licence.

  4) S'il n'y a pas assez de licences à déverrouiller, les attributions invalides seront affichées via les statuts de licence (en rouge). Corrigez les attributions de licences, puis vérifiez et déverrouillez à nouveau les licences.

  Remarque : Pour obtenir une meilleure vue d'ensemble, vous pouvez imprimer les affectations de licences pour tous les abonnés (via **Licences d'utilisateur local** > **Vue d'ensemble** > **Imprimer**). À la fin du document imprimé, toutes les affectations invalides sont répertoriées dans un tableau séparé.

- Attribuer des licences de tronc

  Les licences de jonction doivent être distribuées aux jonctions S $_{2M}$ /T1 et ITSP requises.

7.3.3.1 Comment obtenir des licences d'abonné (autonome)

Distribuer les licences d'abonné disponibles et les licences orientées utilisateur entre les abonnés. Une fois que les licences ont été attribuées, les abonnés sont sous licence.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Avancé**.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.

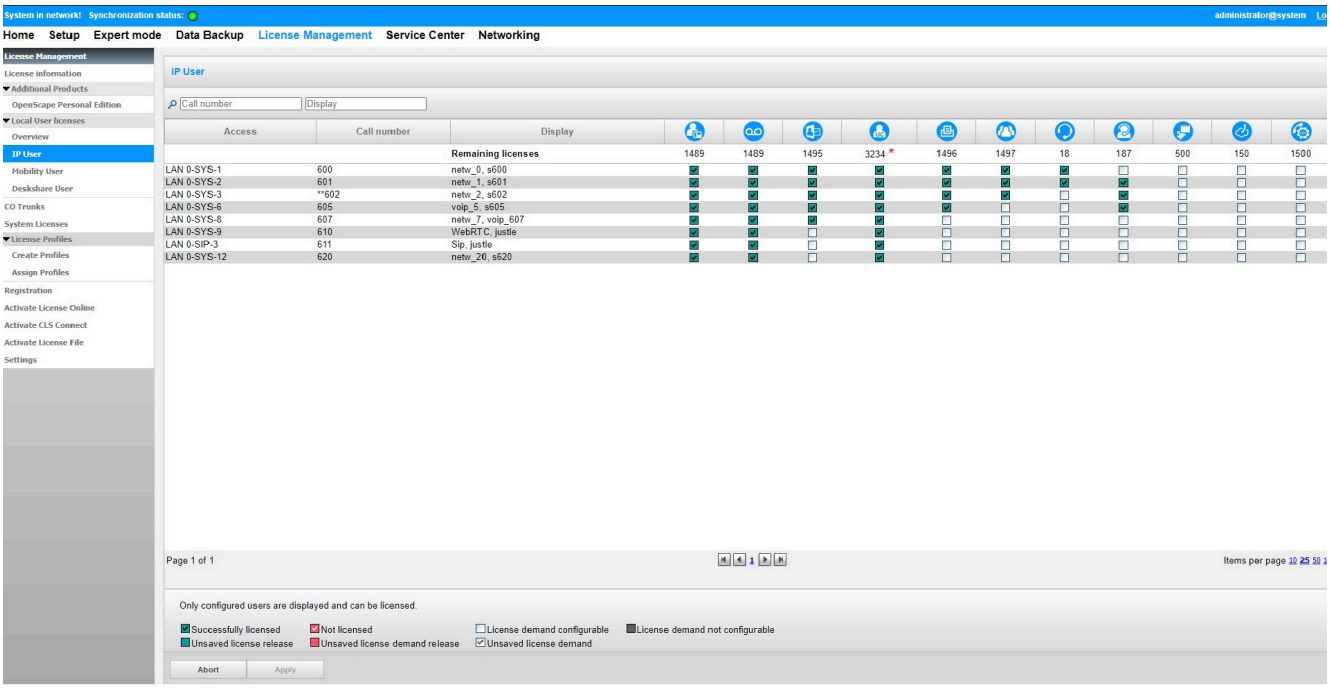
2) Dans l'arborescence de navigation, accédez au type d'abonné souhaité sous **Licences d'utilisateur local** > **...**. Une liste de tous les abonnés du type d'abonné sélectionné s'affichera.

Sous **Licences restantes**, le nombre de licences restantes à attribuer aux abonnés s'affiche. Pour les abonnés TDM, Mobility et DeskShare, l'affichage comprend aussi toutes les autres licences utilisateur IP restantes étant donné que ces licences peuvent être utilisées pour l'attribution de licences aux abonnés TDM, Mobility et DeskShare (licence flexible des abonnés).

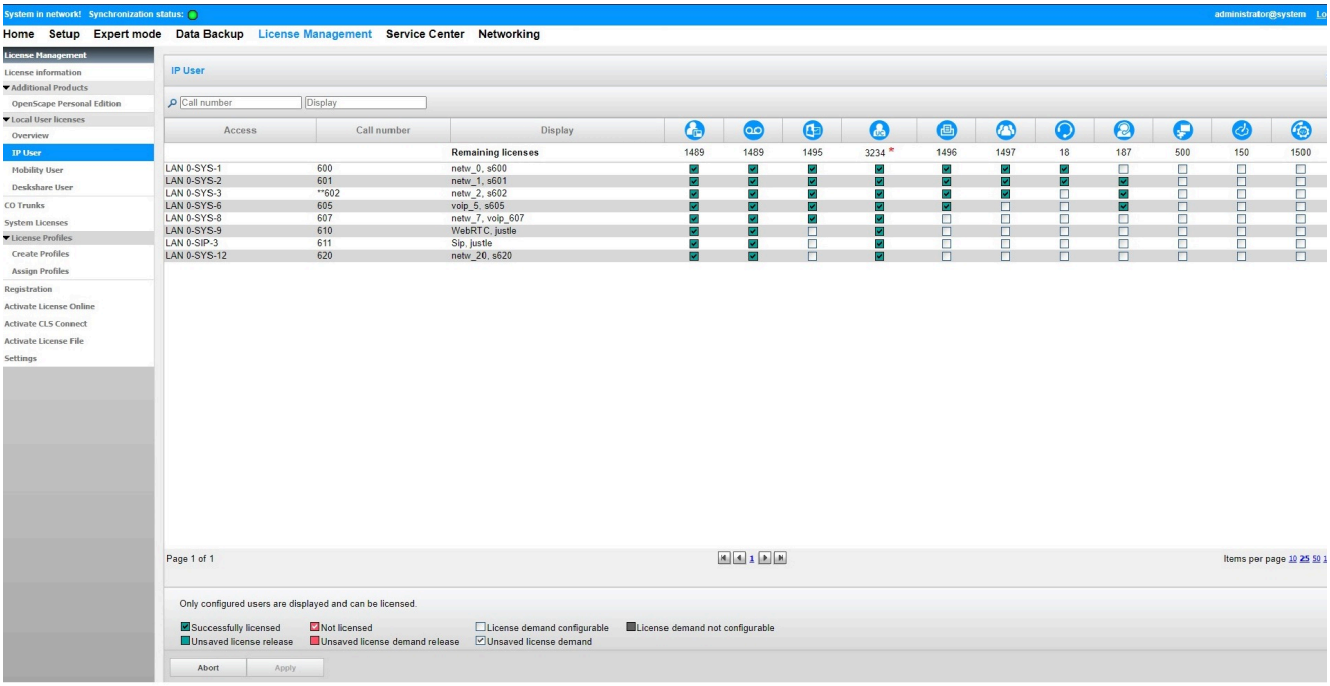
Si le type d'abonné sélectionné est "Utilisateur Mobility", vous verrez également le nombre total de licences Unify Phone disponibles et leur date d'expiration.

3) Dans la ligne de l'abonné souhaité, activez la licence d'abonné en cochant la case à fond clair (première colonne avec case à cocher). Les cases des autres colonnes sont cochées.

Remarque : Vous pouvez également afficher un abonné sélectionné en saisissant un terme de recherche dans les champs de recherche **Numéro d'abonné** ou **Nom**, puis en cliquant sur la touche Entrée ou sur l'icône en forme de loupe. Lorsque les deux champs de recherche sont vides et que vous appuyez sur la touche Retour ou cliquez sur l'icône en forme de loupe, tous les abonnés sont affichés.



4) Dans la ligne de l’abonné souhaité, activez les licences orientées utilisateur en cochant les cases correspondantes.



Remarque : Une licence orientée utilisateur peut uniquement être attribuée à un abonné qui a déjà obtenu une licence d’abonné (étape 3).

Remarque : Lors de l'attribution d'une licence de messagerie vocale à un poste, un utilisateur UC Suite est créé et tous les renvois d'appels actifs sont réinitialisés.

Remarque : En cas de "Paiement à l’utilisation", la licence de messagerie vocale est cochée/décochée automatiquement chaque fois qu’une licence utilisateur vocale est accordée/non accordée, mais il est toujours possible de décocher une licence de messagerie vocale.

Les fonctions de licence Groupware, UC User, Fax, myAttendant et myAgent ne peuvent pas être configurées en mode UC Smart.

Les licences Groupware et UC User sont incompatibles avec le mode UC Suite.

---

5) Cliquez sur **OK & Suivant**. Une vérification est effectuée pour déterminer s'il y a suffisamment de licences pour votre affectation.

   S'il y a suffisamment de licences, la procédure d'attribution de licence de l'abonné est terminée.

   Remarque : En cas de "Paiement à l'utilisation", une fenêtre contextuelle s'affiche. Cliquez sur **OK** pour confirmer votre choix.

6) S'il manque des licences, les erreurs sont indiquées dans une case à fond rouge. Corrigez ces erreur et répétez l'étape 5.

   Remarque : Si vous voulez supprimer une licence d'abonné vous devez confirmer le message d'avertissement. Une nouvelle case à cocher **Avertissements activés** s'affiche ensuite. Si vous désactivez cette case, vous pouvez supprimer d'autres licences d'abonné sans message d'avertissement.

7.3.3.2 Comment effectuer la procédure de licence pour les lignes (standalone)

Distribuez les licences de ligne acquises entre les lignes SIP et S_{2M}/T1.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Lignes réseau**. La plage **Lignes réseau** vous présente le nombre des licences disponibles pour les lignes réseau SIP et S_{2M}/T1.
3) Pour les lignes SIP : dans la plage **Lignes SIP**, **Demande de licence pour le nombre d'appels Internet simultanés dans ce noeud**, entrez le nombre des communications Internet qui peuvent se dérouler simultanément via un ITSP.
4) Pour les lignes S_{2M} : Dans la plage **PRI (S2M/T1)**, dans la ligne de l'emplacement S_{2M} souhaité, dans la liste déroulante de la colonne **Demandes** ; sélectionnez le nombre des canaux B souhaités.
5) Pour les lignes T1 numériques (uniquement pour les Etats-Unis) : Dans la plage **PRI (S2M/T1)**, dans la ligne de l'emplacement T1 souhaité, dans la liste déroulante de la colonne **Demandes**; sélectionnez le nombre des canaux B souhaités.
6) Pour lignes réseau T1 (USA uniquement) : Activez la ligne analogique T1 en sélectionnant dans la zone **PRI (S2M/T1)** dans la ligne de la ligne analogique T1, dans la liste déroulante de la colonne **Demandes** l'entrée **1** (**0** signifie : la ligne est désactivée).

7) Cliquez sur **OK&Suivant**.

Remarque : Le nombre des lignes SIP sous licence et le nombre des lignes S_{2M}/T1 sous licence ne doit pas dépasser le nombre des licences de ligne disponibles.

7.4 Procédure de licence de plusieurs systèmes de communication (interconnexion de réseaux)

La procédure de licence de plusieurs systèmes de communication doit être effectuée selon un ordre défini. Cette séquence est représentée à l'exemple d'une interconnexion de réseaux comportant un OpenScape Business S (Maître) et deux OpenScape Business X3 (Esclave).

Si plusieurs OpenScape Business (noeuds) sont regroupés en une interconnexion de réseaux, la procédure de licence est effectuée centralement à l'aide d'un fichier de licence de réseau, activé sur le noeud maître. En plus, chaque noeud esclave de l'interconnexion de réseaux a besoin de sa propre licence système de réseau. Le noeud à la bande passante la plus importante devrait être le noeud maître.

A l'aide de l'assistant de mise en réseau du WBM, les noeuds de l'interconnexion de réseaux sont configurés en tant que noeuds maître et noeuds esclave. Le noeud Maître comprend l'agent central de licence (CLA central, central Customer License Agent). Tous les noeuds Esclave de l'interconnexion de réseaux utilisent cet agent CLA pour la procédure de licence. Pour cela, à l'aide de la WBM, il est indiqué aux noeuds Esclave l'adresse IP du noeud Maître.

Pour l'ensemble de l'interconnexion de réseaux, il n'existe qu'un fichier de licence réseau. Celle-ci est liée au noeud maître à l'aide de son ID de verrouillage. Si OpenScape Business S (commutateur logiciel) est le noeud maître, le fichier de licence réseau est associé à l'aide de l'ID de verrouillage du serveur Linux du commutateur logiciel ou à l'aide de l'ID Advanced Locking du commutateur logiciel, lorsque le commutateur logiciel est utilisé dans un environnement virtuel. Le fichier de licence réseau est enregistré dans l'agent central CLA et comprend toutes les informations de licence de l'interconnexion de réseaux. Il ne peut être activé que sur le noeud maître, par WBM. Seul le noeud Maître a accès au serveur CLS ; sur tous les autres noeuds, l'accès est désactivé.

Dans l'interconnexion de réseaux, il ne doit pas être effectué de procédure de licence spécifique du noeud. S'il existe déjà pour chaque noeud un fichier réseau propre, vous pouvez effectuer un regroupement au niveau du CLS sous forme de fichier de licence réseau.

Comportement en cas de problèmes réseau (Failover)

Si la connexion avec le noeud Maître et donc avec l'agent central CLA est désactivée, "Failover Period" (période de basculement) s'affiche sur l'écran des téléphones système. A l'intérieur de cette période Failover (30 jours maxi.), tous les noeuds et leurs fonctionnalités demeurent opérationnels. Une fois les problèmes réseau éliminés et la liaison avec l'agent central CLA rétablie, tous les noeuds sont replacés dans l'état de licence régulier.

Si les problèmes de réseau ne sont pas réglés lors de la période de basculement (failover), les noeuds se placent en fonctionnement d'urgence. Ensuite, il faut effectuer une nouvelle procédure de licence pour l'interconnexion de réseaux.

Procédure de licence dans l'interconnexion de réseaux à l'exemple ci-dessus.

OpenScape Business S (Maître) et les deux OpenScape Business X3 (Esclave) sont déjà installés, configurés et regroupés dans une interconnexion de réseaux.

1) **Code d'autorisation de licence (LAC)**

   A l'achat des licenses, le client reçoit un code d'autorisation de licence (LAC, License Authorization Code). Les données concernant les licences obtenues sont enregistrées dans la base de données du serveur central de licences (CLS).

2) **OpenScape Business S comme noeud maître**

   Le client ou le technicien SAV se connecte à WBM d'OpenScape Business S et, à l'aide de l'assistant de mise en réseau, installe OpenScape Business S comme noeud maître.

   Le système a déjà été installé et configuré et fonctionne en période d'activation (intervalle de 30 jours au cours duquel la procédure de licence doit intervenir).

3) **ID de verrouillage du noeud maître**

   Le client ou le technicien SAV note l'ID de verrouillage ou l'ID Advanced Locking de OpenScape Business S.

   Description voir Comment interroger le Locking ID (identifiant de verrouillage) du système de communication

4) **OpenScape Business X3 comme noeud esclave**

   Le client ou le technicien SAV se connecte tout d'abord sur la WBM du premier OpenScape Business X3 et, à l'aide de l'assistant de mise en réseau, installe le premier OpenScape Business X3 comme noeud esclave puis répète cette procédure dans WBM pour le deuxième OpenScape Business X3.

   Les systèmes ont déjà été installés et configurés et fonctionne en période d'activation.

5) **ID de verrouillage de OpenScape Business X3**

   Le client ou le technicien SAV notent les ID de verrouillage des deux OpenScape Business X3.

   Description voir Comment interroger le Locking ID (identifiant de verrouillage) du système de communication

6) **Activation des licences**

   Le client ou le technicien SAV se connecte sur le CLS et, à partir du code d'autorisation de licence et des ID de verrouillage, génère un fichier de licence réseau. A l'aide de la WBM, il charge ce fichier dans le noeud maître.

   Description voir Comment activer les licences hors ligne (interconnexion de réseaux)

   Le système active ensuite les licences acquises.

7) **Affectation de licence**

Le client ou le technicien SAV distribue maintenant les licences dans les noeuds. Pour cela, il se connecte au WBM de chaque mois noeud et affecte au noeud le nombre souhaité de licences. Il est important d'attribuer à chaque noeud une licences système de réseau car sinon le noeud n'est pas intégré dans l'interconnexion de réseaux.

Description voir Comment affecter des licences système à un noeud

7.4.1 Activation des licences (interconnexion de réseaux)

Une fois que vous avez acheté un produit ou une fonctionnalité, vous devez activer les licences fournies avec le produit/la fonctionnalité. Pour cela, vous avez besoin du fichier de licence. Après activation a lieu ensuite l'affectation de la licence.

Il existe les possibilités suivantes pour activer les licences.

- **Activation de licence hors ligne** (directement avec le fichier de licence)

  Le client ou le technicien SAV se connecte au serveur de licences central (CLS) et entre le code d'autorisation de licence en même temps que les ID de verrouillage des systèmes de communication. CLS génère un fichier de licence à partir des données. Le client ou le technicien SAV charge le fichier de licence et et intègre celui-ci dans la WBM du noeud maître.

  Sur le noeud maître, on contrôle si les ID de verrouillage enregistrés dans le fichier de licence correspondent à ceux des systèmes. Si le contrôle est positif, les licences sont activées et les systèmes sont placés en mode licence régulier. Si le contrôle est négatif, les systèmes continuent à fonctionner dans le cadre de la période d'activation puis, une fois celle-ci terminée, seulement en fonctionnement d'urgence.

  L'adresse IP du serveur CLS figure dans WBM, **Gestion des licences** > **Paramètres**.

Pour regrouper des fichiers de licence, on dispose des possibilités ci-après.

- **Comment regrouper les fichiers de licence dans un fichier de licences réseau**

  Si un ou plusieurs noeuds font l'objet de licences qui doivent être regroupées dans une interconnexion de réseaux, l'administrateur doit alors, à l'aide du serveur CLS, regrouper les différents fichiers de licence individuels en un fichier de licence réseau et charger celui-ci dans l'agent CLA central. Sur tous les autre noeuds, l'adresse IP du noeud Maître doit être entrée avec l'agent de licence central, à l'aide de l'assistant réseau de la WBM.

7.4.1.1 Comment activer les licences hors ligne (interconnexion de réseaux)

A l'exemple d'un OpenScape Business S comme noeud maître (Noeud 1) et de deux autres OpenScape Business X3 (Noeud 2 et Noeud 3), il est décrit la génération et l'activation di fichier de licence réseau commun.

Conditions préalables

Il existe un accès au serveur CLS.

Tous les noeuds sont installés et mis en réseau les uns avec les autres, voir Mise en réseau de Open Scape Business X et OpenScape Business S (Multi-passerelle).

Étape par étape

1) Ouvrez une session sur le serveur CLS avec votre nom d'utilisateur et le mot de passe.
2) Dans **Licences**, sélectionnez l'entrée **Générer et télécharger la clé de licence**.
3) Dans **LAC**, entrez le code LAC (code d'autorisation de licence) et cliquez sur **Rechercher**.
4) Ouvrez le produit OpenScape Business S et sélectionnez les fonctionnalités qui doivent être attribuées au noeud 1.
5) Cliquez sur **Clé de licence**.
6) Dans **Adresse MAC** entrez l'adresse MAC ou l'Advanced Locking ID d'OpenScape Business S (noeud 1) et dans **Adresse MAC du CLA réseau**, entrez une nouvelle fois l'adresse MAC ou l'Advanced Locking ID d'OpenScape Business S (noeud Maître).

   Remarque : L'adresse MAC d'OpenScape Business S est l'adresse MAC de la carte réseau du serveur Linux d'OpenScape Business S, utilisée lors de l'installation du système d'exploitation Linux. L'identifiant Advanced Locking ID d'OpenScape Business S est utilisé à la place de l'adresse MAC lorsque OpenScape Business S est exploité dans un environnement virtualisé.

7) Indiquez le nombre souhaité pour les fonctionnalités et cliquez sur **Suivant**.
8) Contrôlez les données client et cliquez sur **Suivant**.
9) Lisez soigneusement les conditions juridiques puis cliquez sur **J'accepte ces conditions**.
10) Cliquez sur **Exécuter** pour générer la clé de licence.
11) Sélectionnez pour le noeud 2, dans **Licences**, l'entrée **Générer et télécharger la clé de licence**.
12) Dans **LAC** entrez de nouveau le code d'autorisation de licence (LAC) et cliquez sur **Rechercher**.
13) Ouvrez le produit OpenScape Business X3 et sélectionnez les fonctionnalités qui doivent être attribuées au noeud 2.
14) Cliquez sur **Clé de licence**.
15) Dans **Adresse MAC** entrez l'adresse MAC du noeud 2 et dans **Adresse MAC du CLA réseau** l'adresse MAC du noeud 1 (noeud maître).
16) Indiquez le nombre souhaité pour les fonctionnalités et cliquez sur **Suivant**.
17) Cliquez sur **Suivant**.
18) Confirmer la remarque de caractère juridique en cochant la case **J'accepte ces conditions**.
19) Cliquez sur **Exécuter** pour générer la clé de licence.

20) Répétez les étapes 11 à 19 pour le noeud 3.
21) Cliquez sur **Clé de licence** et ensuite sur **Téléchargement** pour télécharger le fichier de licence réseau.
22) Sauvegardez le fichier de licence réseau.
23) Ouvrez une session sur WBM du noeud Maître ; pour cela, entrez sur votre navigateur l'adresse `https://<Adresse IP du noeud Maître>` et ensuite le nom d'utilisateur et le mot de passe.
24) Cliquez dans la barre de navigation sur **Gestion des licences**.
25) Dans l'arborescence de navigation, cliquez sur **Activer le fichier de licence**.
26) Dans **Fichier de licence**, cliquez sur **Rechercher** et sélectionnez l'emplacement de stockage du fichier de licence réseau.
27) Cliquez sur **Activer**.

7.4.1.2 Comment regrouper les fichiers de licence dans un fichier de licences réseau

Si plusieurs noeuds qui n'étaient pas jusqu'ici en réseau sont intégrés dans une interconnexion de réseaux, il faut, en utilisant le serveur CLS, regrouper les fichiers de licence des différents noeuds dans un fichier de licences réseau commun.

Conditions préalables

Il existe un accès au serveur CLS et vous disposez des droits d'accès pour les paquets de licence des différents noeuds.

Tous les noeuds sont installés et mis en réseau les uns avec les autres, voir Mise en réseau de Open Scape Business X et OpenScape Business S (Multi-passerelle).

Étape par étape

1) Ouvrez une session sur le serveur CLS avec votre nom d'utilisateur et le mot de passe.
2) Dans **Procédure de licence réseau** sélectionnez l'entrée **Système ajouter/supprimer**.
3) Sélectionnez l'adresse MAC du noeud qui doit être intégré dans l'interconnexion de réseaux.
4) Cliquez sur**Rehost**.
5) Dans **Adresse MAC**, entrez l'adresse MAC du noeud.
6) Dans **Adresse MAC de l'agent CLA réseau**, entrez l'adresse MAC du noeud Maître. En général, OpenScape Business S est le noeud Maître.

Remarque : L'adresse MAC d'OpenScape Business S est l'adresse MAC de la carte réseau du serveur Linux d'OpenScape Business S, utilisée lors de l'installation du système d'exploitation Linux.

---

7) Cliquez sur **Suivant**.
8) Contrôlez les données client et cliquez sur **Suivant**.
9) Lisez soigneusement les conditions juridiques puis cliquez sur **J'accepte ces conditions**.

10) Cliquez sur **Exécuter** pour générer la clé de licence.
11) Répéter les étapes 2 à 10 pour les autres noeuds.
12) Cliquez sur **Clé de licence** et ensuite sur **Téléchargement** pour télécharger le fichier de licence réseau.
13) Sauvegardez le fichier de licence réseau.
14) Ouvrez une session sur WBM du noeud Maître ; pour cela, entrez sur votre navigateur l'adresse `https://<Adresse IP du noeud Maître>` et ensuite le nom d'utilisateur et le mot de passe.
15) Cliquez dans la barre de navigation sur **Gestion des licences**.
16) Dans l'arborescence de navigation, cliquez sur **Activer le fichier de licence**.
17) Dans **Fichier de licence**, cliquez sur **Rechercher** et sélectionnez l'emplacement de stockage du fichier de licence réseau.
18) Cliquez sur **Activer**.

7.4.2 Attribution de licences (interconnexion de réseaux)

Une fois les licences achetées activées avec succès, elles doivent être attribuées aux stations et aux lignes. L'attribution des licences doit être effectuée séparément sur chaque nœud.

Attribution des licences utilisateur et des licences orientées utilisateur

Les abonnés peuvent se voir attribuer des licences utilisateur et des licences orientées utilisateur.

Les licences utilisateur peuvent être attribuées aux types d'abonnés suivants :

Icône	Licence utilisateur	Description
	Stations IP	Pour l'utilisation des téléphones à système IP (HFA ou SIP) et des téléphones SIP
	Stations TDM	Pour utiliser des téléphones système UP0, des téléphones RNIS, des téléphones analogiques et des téléphones DECT
	Stations mobiles	Pour l'utilisation de Mobility Entry et du service DISA (One Number Service)
	Postes de travail partagés	Pour l'utilisation du partage de bureau par stations IP
	Utilisateur de secours	Pour une utilisation téléphonique de base en cas de panne.

Les licences utilisateur sont attribuées de manière permanente aux numéros des abonnés. Si un abonné est supprimé ou si un autre type d'abonné est attribué à un numéro d'appel, la licence utilisateur associée est libérée.

Grâce à la flexibilité des licences, les utilisateurs TDM, Mobility et Deskshare peuvent également bénéficier de licences utilisateur IP. Si toutes les licences utilisateur TDM, DeskShare et Mobility acquises ont déjà été attribuées à des abonnés, et que d'autres utilisateurs TDM, DeskShare et Mobility sont

nécessaires, alors toutes les licences utilisateur IP restantes peuvent être utilisées pour répondre à cette demande.

Une fois qu'une licence utilisateur a été attribuée à l'abonné, une licence orientée utilisateur peut également lui être attribuée.

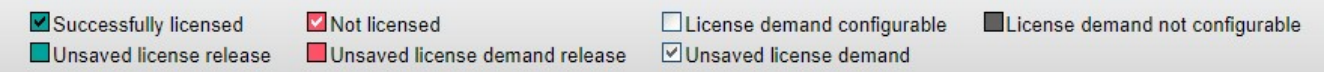
Les licences suivantes, orientées utilisateur, peuvent être attribuées aux stations :

Icône	Licence orientée utilisateur	Description
	Messagerie vocale	Pour l'utilisation de la messagerie vocale.
	utilisateur de logiciels de groupe	Pour l'utilisation des fonctionnalités de UC Suite via myPortal pour Outlook.
	Suite UC	Pour l'utilisation des fonctionnalités de UC Suite via myPortal pour ordinateur.
	Fax	Pour l'utilisation d'un boîtier fax au sein de la suite UC. Une licence utilisateur UC ou Groupware est requise au préalable.
	Conférence	Pour utiliser les fonctionnalités de conférence de la suite UC. Une licence utilisateur UC ou Groupware est requise au préalable.
	mon assistant	Pour l'utilisation des fonctionnalités de l'assistant UC Suite.
	monAgent	Pour l'utilisation des fonctions du centre de contact.
	Lanceur d'applications	Pour le contrôle des applications sur un PC client pendant les appels entrants et sortants, par exemple, le lancement d'une application ou l'affichage des informations de l'appelant.
	Téléphone Unify	Pour l'utilisation du client Unify Phone en combinaison avec OpenScape Business.
	TAPI 120/170	Pour l'utilisation d'applications compatibles TAPI et pour la téléphonie sur PC avec les applications propres du client provenant de différents fournisseurs de logiciels.

Vous pouvez obtenir un aperçu de toutes les licences utilisateur et des licences orientées utilisateur affichées (via **des licences utilisateur locales** > **)** .

Ce tableau récapitulatif présente également le statut des licences pour chaque abonné.

États de licence possibles :



Attribution des licences système

Les licences système comprennent des licences pour les liaisons principales et pour les fonctionnalités à l'échelle du système.

Des licences peuvent être attribuées aux types de trunks suivants :

- Liaisons S $_{2M}$ /T1 : nombre de canaux B
- Lignes ITSP : nombre d'appels simultanés effectués via un seul ITSP

Des licences système sont attribuées à chaque système (nœud) du réseau. Cette configuration doit être effectuée successivement (c'est-à-dire l'une après l'autre) sur chaque nœud. Le nombre total de licences système stockées dans le fichier de licences réseau sur le nœud maître est réduit du nombre configuré sur le nœud.

procédure d'attribution de licence

Prérequis : Le fichier de licence est activé et les stations sont configurées.

- Comment obtenir une licence pour les stations

  1) Attribuer une licence utilisateur à un abonné. Cette attribution déclenche la génération d'une demande de licence pour l'abonné tout en permettant l'attribution des licences orientées utilisateur.
  2) Attribuer les licences orientées utilisateur à un abonné. Ces attributions entraînent la génération de demandes de licence supplémentaires pour l'abonné. Veuillez noter que certaines licences nécessitent d'autres licences (voir Combinaisons de licences possibles).
  3) Vérifier et déverrouiller les demandes de licence.
  4) S'il n'y a pas assez de licences à déverrouiller, les attributions invalides seront affichées via les statuts de licence (en rouge). Corrigez les attributions de licences, puis vérifiez et déverrouillez à nouveau les licences.

  Remarque : Pour obtenir une meilleure vue d'ensemble, vous pouvez imprimer les affectations de licences pour tous les abonnés (via **Licences d'utilisateur local** > **Vue d'ensemble** > **Imprimer**). À la fin du document imprimé, toutes les affectations invalides sont répertoriées dans un tableau séparé.

- Attribuer des licences de tronc

  Les licences de jonction doivent être distribuées aux jonctions S $_{2M}$ /T1 et ITSP requises.

7.4.2.1 Comment effectuer la procédure de licence pour les abonnés (interconnexion de réseaux)

Distribuer les licences d'abonné disponibles et les licences orientées utilisateur entre les abonnés. Une fois que les licences ont été attribuées, les abonnés sont sous licence.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

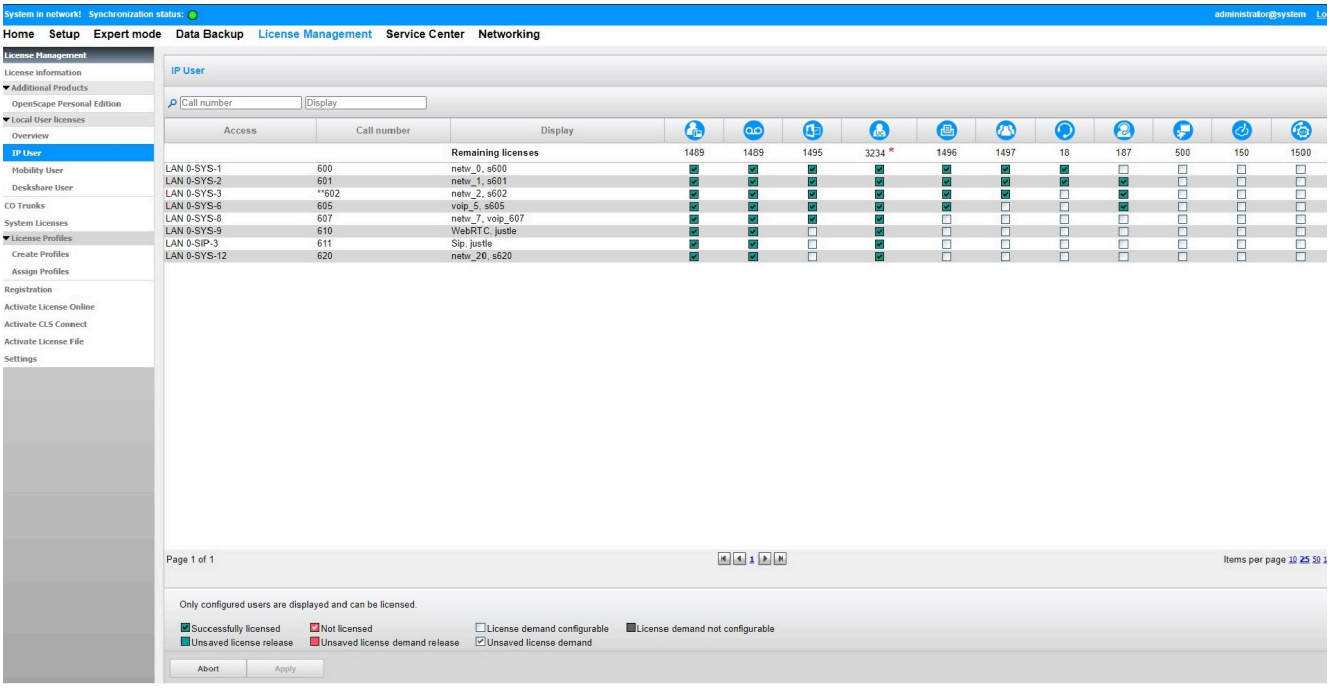
Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, accédez au type d'abonné souhaité sous **Licences d'utilisateur local** > **...**. Une liste de tous les abonnés du type d'abonné sélectionné s'affichera.

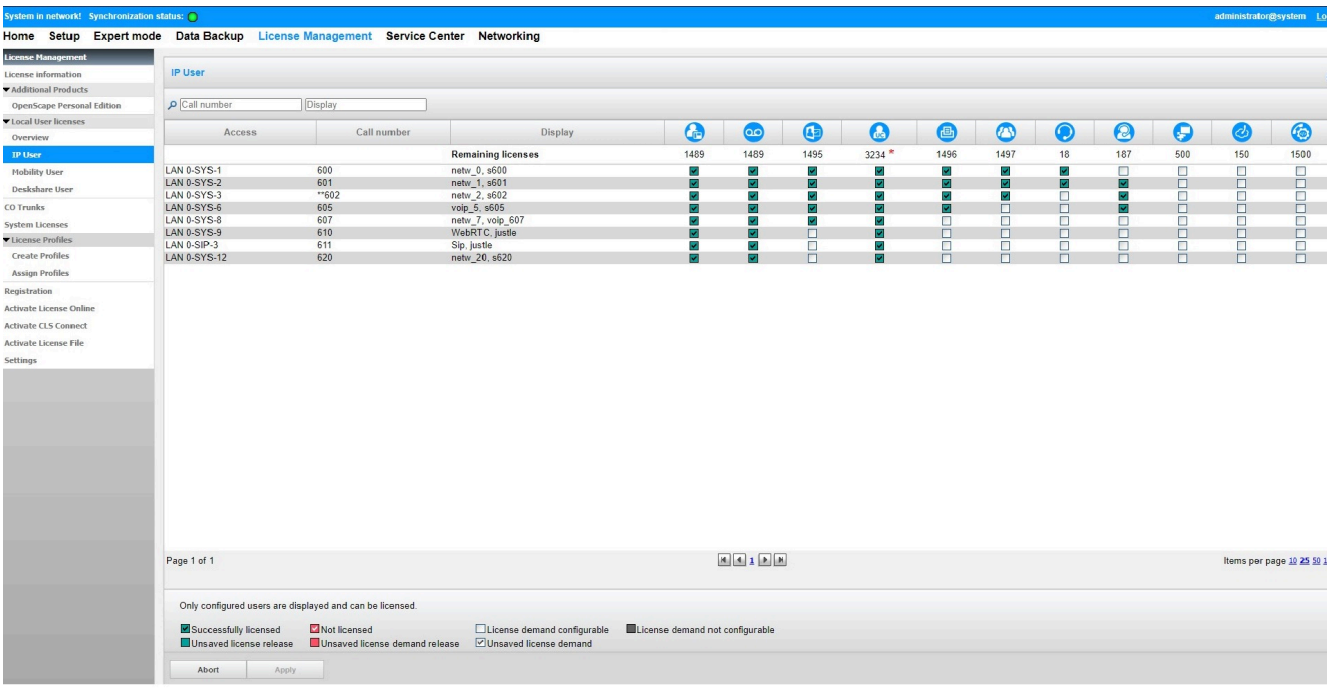
   Sous **Licences restantes**, le nombre de licences restantes à attribuer aux abonnés s'affiche. Pour les abonnés TDM, Mobility et DeskShare, l'affichage comprend aussi toutes les autres licences utilisateur IP restantes étant donné que ces licences peuvent être utilisées pour l'attribution de licences aux abonnés TDM, Mobility et DeskShare (licence flexible des abonnés).

   Si le type d'abonné sélectionné est "Utilisateur Mobility", vous verrez également le nombre total de licences Unify Phone disponibles et leur date d'expiration.
3) Dans la ligne de l'abonné souhaité, activez la licence d'abonné en cochant la case à fond clair (première colonne avec case à cocher). Les cases des autres colonnes sont cochées.

Remarque : Vous pouvez également afficher un abonné sélectionné en saisissant un terme de recherche dans les champs de recherche **Numéro d'abonné** ou **Nom**, puis en cliquant sur la touche Entrée ou sur l'icône en forme de loupe. Lorsque les deux champs de recherche sont vides et que vous appuyez sur la touche Retour ou cliquez sur l'icône en forme de loupe, tous les abonnés sont affichés.



4) Dans la ligne de l'abonné souhaité, activez les licences orientées utilisateur en cochant les cases correspondantes.



Remarque : Une licence orientée utilisateur peut uniquement être attribuée à un abonné qui a déjà obtenu une licence d'abonné (étape 3).

Remarque : Le modèle de paiement à l'utilisation n'est pas disponible dans le cas d'un fichier de licence réseau.

Dans le cas d'un réseau de systèmes OpenScape Business, n'importe lequel des systèmes peut utiliser ce modèle de paiement via l'agent de licences central local (CLA).

5) Cliquez sur **OK & Suivant**. Une vérification est effectuée pour déterminer s'il y a suffisamment de licences pour votre affectation.

   S'il y a suffisamment de licences, la procédure d'attribution de licence de l'abonné est terminée.

6) S'il manque des licences, les erreurs sont indiquées dans une case à fond rouge. Corrigez ces erreur et répétez l'étape 5.

Remarque : Si vous voulez supprimer une licence d'abonné vous devez confirmer le message d'avertissement. Une nouvelle case à cocher **Avertissements activés** s'affiche ensuite. Si vous désactivez cette case, vous pouvez supprimer d'autres licences d'abonné sans message d'avertissement.

7.4.2.2 Comment effectuer la procédure de licence pour les lignes (interconnexion de réseaux)

Distribuez les licences de ligne acquises entre les lignes SIP et S_{2M}/T1.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Lignes réseau**. La plage Lignes réseau vous présente le nombre des licences disponibles pour les lignes réseau SIP et S**2M**/T1.
3) Pour les lignes SIP : dans la plage **Lignes SIP**, **Demande de licence pour le nombre d'appels Internet simultanés dans ce noeud**, entrez le nombre des communications Internet qui peuvent se dérouler simultanément via un ITSP.
4) Pour les lignes S_{2M}- : Dans la plage **S2M**, dans la ligne de l'emplacement souhaité, dans la liste déroulante de la colonne **Demandes**; sélectionnez le nombre des canaux B souhaités.
5) Pour les lignes T1 (uniquement pour les Etats-Unis) : Dans la plage **T1**, dans la ligne de l'emplacement souhaité, dans la liste déroulante de la colonne **Demandes**; sélectionnez le nombre des canaux B souhaités.
6) Cliquez sur **OK&Suivant**.

Remarque : Le nombre des lignes SIP sous licence et le nombre des lignes S_{2M}/T1 sous licence ne doit pas dépasser le nombre des licences de ligne disponibles.

7.4.2.3 Comment affecter des licences système à un noeud

Conditions préalables

Vous êtes inscrit sur la WBM du noeud souhaité.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Licences système**. Toutes les licences système disponibles vous sont montrées.
3) Dans la colonne **Licences utilisées**sélectionnez pour les licences système désirées le nombre de licences système qui peut être attribué au noeud.

   Dans la colonne **Disponible pour la distribution**, il vous est montré le nombre de licences disponibles pour l'ensemble de l'interconnexion de réseaux.

Remarque : Veillez à ce qu'il soit attribué au noeud la licence système "Mise en réseau", sinon le compte n'est pas intégré dans l'interconnexion de réseaux.

---

4) Cliquez sur **Sauvegarder**.

7.4.2.4 Comment affecter la licence système "Networking" à un noeud

Conditions préalables

Vous êtes inscrit sur la WBM du noeud souhaité.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Licences système**. Toutes les licences système disponibles vous sont montrées.
3) Dans licence système **Mise en réseau**, colonne **Licences utilisées**, sélectionnez l'entrée **1** dans la liste déroulante.

   Dans la colonne **Disponible pour la distribution**, il vous est montré le nombre de licences disponibles pour l'ensemble de l'interconnexion de réseaux.
4) Cliquez sur **Sauvegarder**.

7.5 Information sur la licence

Les informations sur les licences, produits et fonctionnalités disponibles et attribués sont présentées par WBM. Dans une interconnexion de réseaux, il est possible de consulter les informations de licence de tous les nœuds disponibles dans le réseau.

Il est possible d'afficher les informations suivantes.

- **Adresse MAC** : adresse MAC de la plate-forme matérielle ou du serveur Linux de commutateur logiciel auxquels les licences sont associées.

  Remarque : Si le système de communication est dans la période d'activation, il peut être affiché une adresse MAC erronée dans les informations de licence. L'adresse MAC correcte peut être demandée dans **Centre de service** , dans **Inventory** (Inventory).

- **Advanced Locking ID** : Advanced Locking ID du commutateur logiciel dans un environnement virtuel auquel les licences sont liées.
- **Locking ID** : ID de verrouillage du serveur d'application auquel les licences sont associées.
- **Nœuds** : nom du système de communication auquel les licences sont liées.
- **Nom du produit** : nom du produit auquel la licence est attribuée.
- **Fonctionnalité** : fonctionnalité associée à la licence.
- **Licences utilisées** : nombre de licences utilisées et disponibles.
- **Licences distribuables** : affichage des licences encore disponibles dans l'interconnexion de réseaux.
- **Etat** : état de la licence.

Le produit OpenScape Personal Edition est licencié à l'aide d'un fichier de licence propre. Les informations sur la licence sont présentées dans **Produits supplémentaires**.

7.5.1 Information sur les licences sans interconnexion de réseaux (Standalone)

Il est possible d'afficher toutes les licences d'un système de communication et les informations à ce sujet.

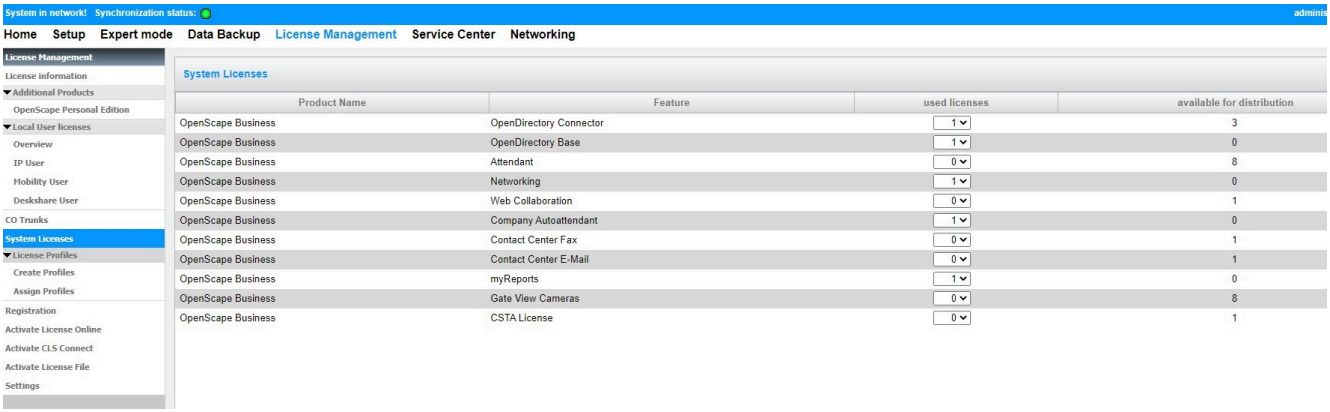
7.5.1.1 Comment afficher des informations sur les licences

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

Cliquez sur **Gestion des licences** dans la barre de navigation. Il est affiché les informations de licence concernant votre système de communication.



Remarque : En cas de modèle de paiement à l'utilisation, les licences utilisées sont configurables sauf pour le centre d'appels fax, le centre d'appels e-mail et myReports en mode UC Smart.

7.5.2 Information sur la licence dans une interconnexion de réseaux

Dans une interconnexion de réseaux, toutes les licences et les informations les concernant sont affichées. Ces informations sont lues dans le fichier de licence réseau.

Les licences dans une interconnexion de réseaux sont, sauf les licences de base, de type "floating" et se trouvent dans un groupe de licences. Si une licence n'est plus nécessaire et validée sur un noeud (système de communication), elle peut être utilisée sur un autre noeud.

Dans une interconnexion de réseaux, toutes les licences de l'intercoonexion ainsi que les licences utilisés en commun (floating) ou encore les licences liées spécialement à un noeud sont affichées.

En plus, les licences d'abonné et les licences orientées utilisateur peuvent être triées par noeud et affichées dans un aperçu.

7.5.2.1 Comment afficher toutes les licences de l'interconnexion de réseaux

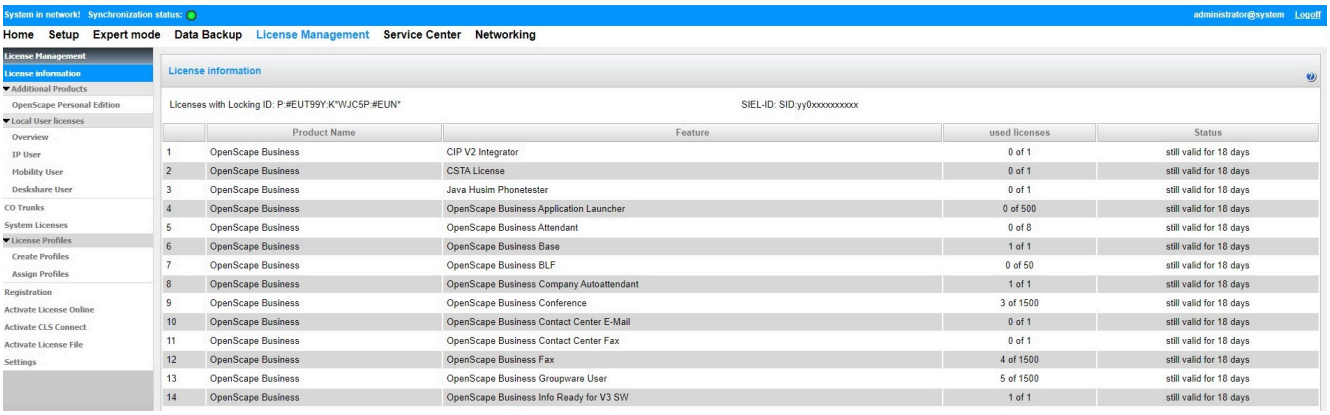
Conditions préalables

Le système de communication se trouve dans une interconnexion de réseaux.

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Information sur la licence**. Le système affiche toutes les licences de l'interconnexion de réseaux.



	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

7.5.2.2 Comment afficher les licences liées à un noeud

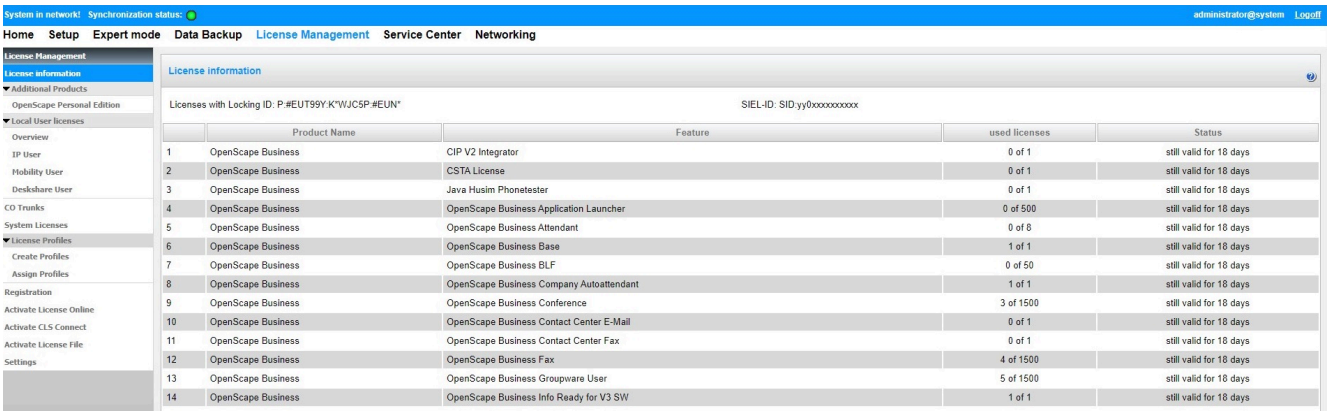
Conditions préalables

Le système de communication se trouve dans une interconnexion de réseaux.

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Information sur la licence**.
3) Dans l'arborescence de navigation, cliquez sur le nom du système ou l'ID de verrouillage du noeud souhaité. Il vous est présenté les licence liées spécialement à ce noeud, par ex. la Licence de base.



	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

7.5.2.3 Comment afficher toutes les licences utilisées en commun dans une interconnexion de réseaux

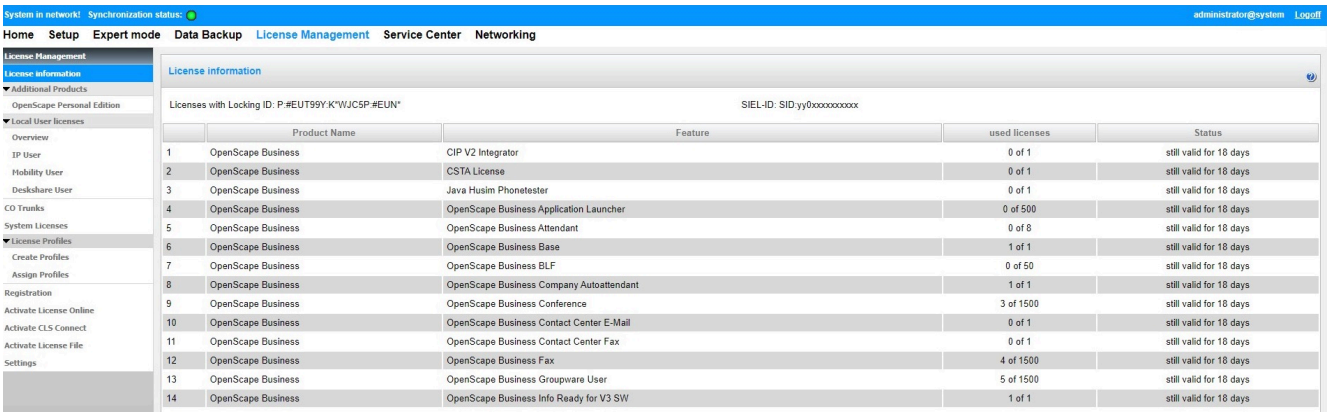
Conditions préalables

Le système de communication se trouve dans une interconnexion de réseaux.

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Information sur la licence**.
3) Dans l'arborescence de navigation, cliquez sur **Flottant**. Il est affiché toutes les licences utilisées en commun dans l'interconnexion de réseaux.



	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

7.5.2.4 Comment afficher les licences abonnés et les licences orientées utilisateur en fonction du noeud

Conditions préalables

Le système de communication se trouve dans une interconnexion de réseaux.

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Aperçu de licence pour l'ensemble du réseau**. Il est affiché toutes les licences d'abonné et les licences orientées utilisateur dans l'interconnexion de réseaux, avec un tri par noeud.

7.6 Affectation des profils de licence

Les profils de licence comprennent des affectations de licence prédéfinies et peuvent être affectés à un ou plusieurs abonnés. Les profils de licence sont utiles lorsque plusieurs abonnés doivent recevoir les mêmes licences.

Il est possible d'utiliser des profils de licence prédéfinis ou de créer de nouveaux profils de licence.

Un profil de licence s'applique toujours à un type d'abonné et ne peut être affecté qu'aux abonnés de ce type. Il est possible de créer et désigner plusieurs profils de licence pour un type d'abonné.

On créer des profils de licence pour les types d'abonné suivants :

- Abonnés IP (téléphones système IP, téléphones SIP)
- Abonnés TDM (téléphones UP0, téléphones RNIS, téléphones analogiques, téléphones DECT)
- Abonnés DeskSharing
- Abonnés mobiles

A l'intérieur d'un profil de licence vous pouvez attribuer au type d'abonné des licences orientées utilisateur, en fonction des souhaits.

Si l'affectation de licence d'un abonné disposant d'un profil de licence est modifiée séparément, l'affectation de l'abonné au profil de licence est supprimée automatiquement.

7.6.1 Comment ajouter un profil de licence

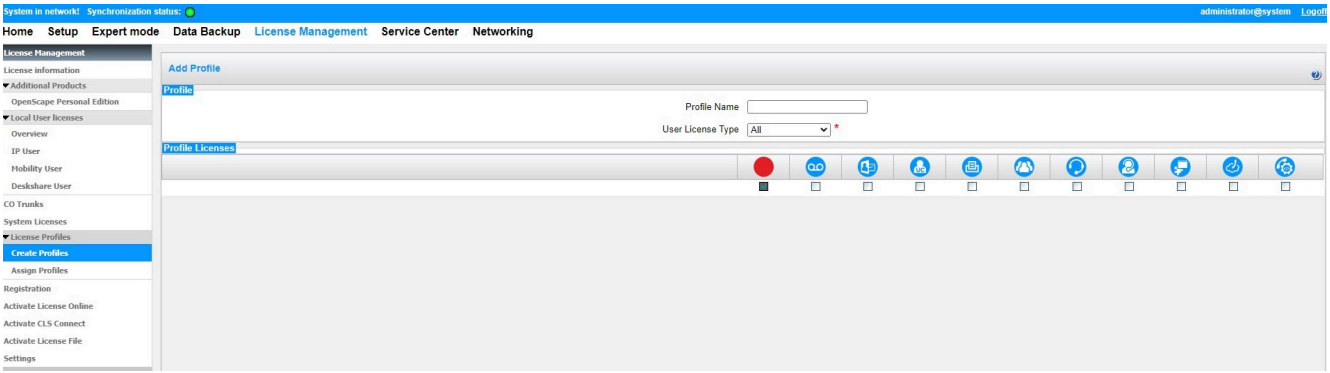
Créez un nouveau profil de licence.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Profils de licence** > **Créer des profils**. Tous les profils de licence disponibles vous sont montrés.
3) Cliquez sur **Ajouter**.



4) Dans le champ **Nom du profil**, saisissez un nom de votre choix pour le nouveau profil.
5) Dans la liste déroulante **Type de licence utilisateur**, sélectionnez le type d'abonné auquel le profil doit s'appliquer.
6) Sélectionnez les licences orientées utilisateur en cochant les case désirées.
7) Cliquez sur **OK & Suivant**. La validité de leur affectation est contrôlée.

   En cas d'erreur d'affectation, la procédure de licence des abonnés est arrêtée.

8) En cas d'erreur d'affectation, les erreurs sont signalées par une case à fond rouge. Corrigez ces erreurs et répétez l'étape 7.

7.6.2 Comment modifier un profil de licence

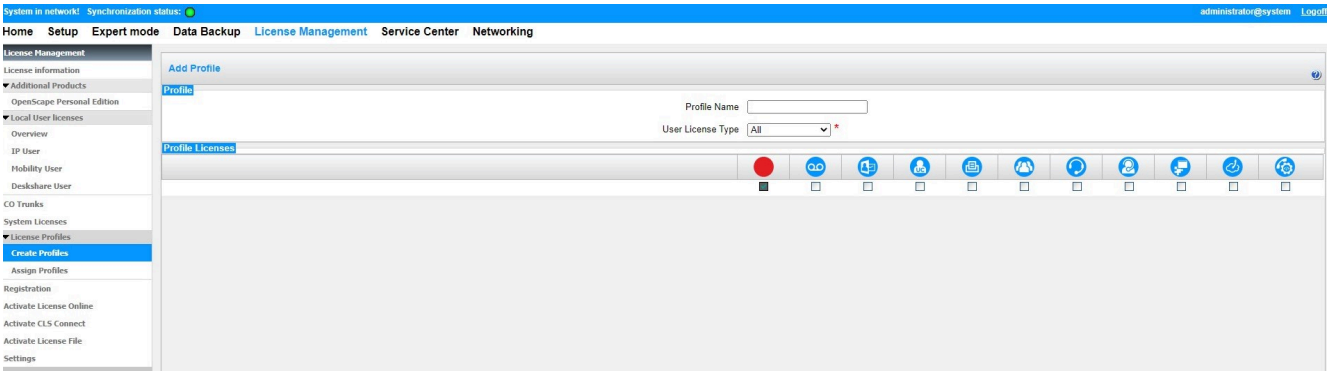
Modifier un profil de licence existant.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Profils de licence** > **Créer des profils**. Tous les profils de licence disponibles vous sont montrés.



3) Activez le bouton radio figurant en face du profil de licence souhaité et cliquez sur **Modifier**.
4) Modifiez le profil de licence comme souhaité.
5) Cliquez sur **OK & Suivant**. La validité de leur affectation est contrôlée.

   Si l'affectation est incorrecte, le traitement du profil de licence est arrêté.
6) En cas d'erreur d'affectation, les erreurs sont signalées par une case à fond rouge. Corrigez ces erreur et répétez l'étape 5.

7.6.3 Comment affecter un profil de licence aux abonnés

Attribuez un profil de licence aux abonnés disponibles.

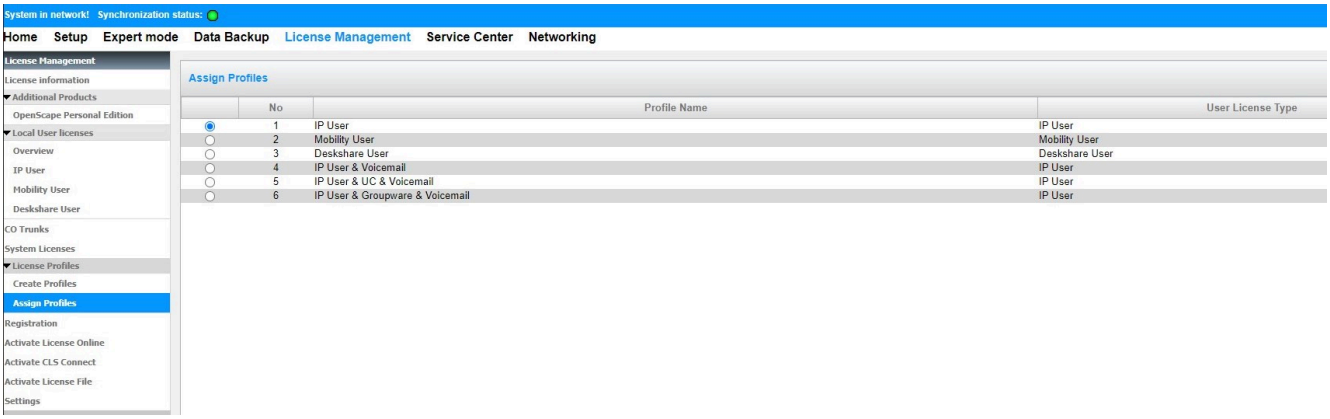
Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.

2) Dans l'arborescence de navigation, cliquez sur **Profils de licence** > **Attribuer des profils**. Tous les profils de licence disponibles vous sont montrés.



3) Activez le bouton radio figurant en face du profil de licence souhaité et cliquez sur **OK et suivant**.
4) Dans le champ **Sélection** à gauche, sélectionnez tous les abonnés auxquels le profil de licence doit être attribué.
5) Cliquez sur **Ajouter**. Les abonnés sélectionnés apparaissent dans la fenêtre **Membres** à droite.
6) Cliquez sur **OK & Suivant**. Les licences sélectionnées dans le profil de licence sont attribuées aux abonnés.

Remarque : En cas de "Paiement à l'utilisation", une fenêtre contextuelle s'affiche. Cliquez sur **OK** pour confirmer votre choix.

Remarque : Les abonnés peuvent ultérieurement sortir d'un profil de licence ou ajouter de nouveaux abonnés.

7.6.4 Comment effacer un profil de licence

Effacez un profil de licence existant.

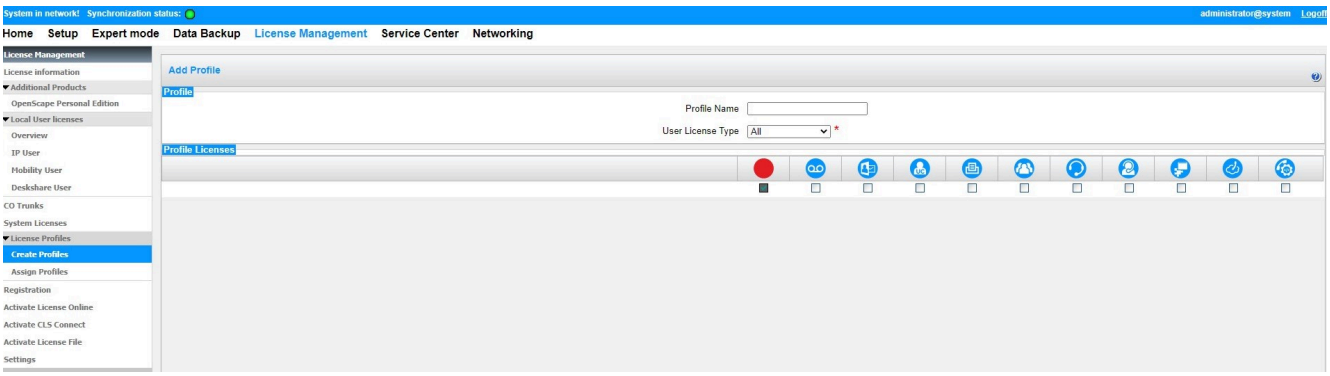
Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.

2) Dans l'arborescence de navigation, cliquez sur **Profils de licence** > **Créer des profils**. Tous les profils de licence disponibles vous sont montrés.



3) Activez le bouton radio figurant en face du profil de licence souhaité et cliquez sur **Supprimer**.
4) Confirmez la remarque avec **OK**. Le prodil de licence est effacé.

7.7 Ré-hébergement après remplacement du matériel

Il faut actualiser les licences lorsque il est nécessaire de remplacer dans le système de communication la carte mère de la plate-forme matérielle ou la carte réseau du serveur Linux. Pour le ré-hébergement, on a besoin de l'adresse MAC de l'ancien matériel, de l'adresse MAC du nouveau matériel et des données de connexion pour le serveur de licences central (CLS).

Après remplacement du matériel, les données de configuration doivent être rétablies à l'aide du jeux de sauvegarde à jour (voir Rétablir).

Comme les licences sont liées à l'adresse MAC du matériel, une fois le matériel changé, l'adresse MAC est modifiée ; ainsi les licences ne sont plus valides. Après remplacement du matériel, le système de communication est de nouveau en période d'activation. Une fois que l'ancienne adresse MAC et la nouvelle ont été inscrites dans le CLS, il est possible de générer le nouveau fichier de licence. Celui-ci est chargé dans le système de communication par actualisation hors ligne ; ensuite, toutes les licences disponibles sont automatiquement activées.

Pour le commutateur logiciel, on utilise l'adresse MAC de la carte réseau du serveur Linux qui a été sélectionnée lors de l'installation du système d'exploitation Linux (visible avec YaST). L'adresse MAC peut aussi être lue à l'aide de la WBM.

Remarque : Chaque Ré-hébergement est consigné dans CLS. Une licence peut être utilisée au maximum trois fois pour une procédure de rehost.

Remarque : L'adresse IP de CLS peut être interrogée par la WBM dans **Gestion des licences** > **Paramètres** et, si nécessaire, modifiée.

7.7.1 Comment effectuer un ré-hébergement après un remplacement de matériel

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Le matériel a été remplacé et vous avez exécuté une procédure de rehost sur le CLS.

Les données de configuration ont été rétablies à l'aide du jeux de sauvegarde actuel.

Vous connaissez le code d'autorisation de licence (LAC) pour l'activation de la licence.

Pour la connexion au serveur de licences, le système de communication doit avoir une liaison Internet.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Activer la licence en ligne**.
3) Dans **Code d'autorisation de licence (LAC)**, entrez le code LAC.
4) Laissez non cochée la case pour l'accès au serveur de licences par nom d'utilisateur et mot de passe. L'accès au serveur de licence est automatique. (L'entrée du nom d'utilisateur et du mot de passe est uniquement nécessaire pour les partenaires).
5) Cliquez sur **Activer**. La connexion au serveur de licences est établie et les licences sont mises à jour. Une fois la mise à jour réalisée avec succès, la liaison est automatiquement déconnectée.
6) Redémarrez le système de communication.

Étapes suivantes

Sauvegardez vos données de configuration dans un nouveau jeu de sauvegarde (voir Sauvegarde immédiate).

7.8 Serveur de licences (serveur de licence central, CLS)

Le serveur de licences (CLS) génère et gère les fichiers de licences.

Un fichier de licence est généré lorsque le client envoie à l'aide de la WBM le code d'autorisation de licence à CLS. La transmission du fichier de licence au système de communication s'effectue automatiquement, via Internet. Si la transmission automatique ne s'effectue pas, le fichier de licence peut également être chargé manuellement dans le système de communication.

7.8.1 Comment consulter ou modifier l'adresse IP du serveur de licences

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Si l'adresse IP du serveur de licences central a été modifiée, vous devez connaître l'adresse IP actuelle.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Paramètres**. Le champ **Adresse IP du serveur de licence central** indique l'adresse IP du serveur de licence central (serveur CLS). L'adresse IP actuellement valide est `188.64.16.4`.
3) Si vous devez modifier l'adresse IP du serveur de licence central, entrez dans le champ **Adresse IP du serveur central de licences** la nouvelle adresse IP du serveur de licence central sous la forme `123.124.125.126`.
4) Cliquez sur **Activer**.

7.8.2 Comment vérifier la connexion au Serveur de licence central (CLS)

Étape par étape

1) Cliquez sur **Gestion des licences** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Paramètres**.
3) Dans la zone **Serveur de licence central**, cliquez sur **Test de connexion CLS**.

S'il existe une connexion Internet active, le message **Connexion à CLS réussie !** s'affiche.

S'il n'existe aucune connexion Internet, le message **Aucune connexion à CLS !** s'affiche.

7.9 Agent de licence (Customer License Agent, CLA)

L'agent de licence (CLA) fait partie du logiciel de communication OpenScape Business et tourne automatiquement en arrière-plan. Il assure la gestion du fichier de licence et des licences qui y figurent. CLA contrôle les exigences de licence et, si un nombre suffisant de licence est disponible, il active les licences. Il n'y a qu'un seul CLA (CLA local) par système de communication. Si plusieurs systèmes de communication (noeuds) se trouvent dans une interconnexion de réseaux, il convient de l'utiliser qu'un CLA (CLA central) sur le noeud maître.

Les configurations suivantes sont possibles :

- **Comment configurer la connexion avec l'agent de licence local**

  Si un noeud est retiré de l'interconnexion de réseaux, il faut supprimer la liaison avec l'agent central CLA. L'agent CLA local installé sur le noeud est automatiquement utilisé. Si cet automatisme ne fonctionn pas, la connexion avec le CLA local peut être établie manuellement.
- **Comment modifier la connexion à l'agent de licence central**

  Chaque noeud de l'interconnexion de réseaux a besoin d'une connexion avec l'agent central CLA sur le noeud Maître. Cette connexion est établie automatiquement par l'assistant WBM **Mise en réseau**. Si l'adresse IP du noeud Maître est modifiée, il faut reconfigurer sur tous les noeuds esclave la connexion avec l'agent central CLA.

7.9.1 Comment configurer la connexion avec l'agent de licence local

Conditions préalables

Vous êtes inscrit sur la WBM du noeud souhaité.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Paramètres**.
3) Activez le champ d'option **Agent de licence local (CLA)**.
4) Cliquez sur **Activer**.

7.9.2 Comment modifier la connexion à l'agent de licence central

Conditions préalables

Le système de communication se trouve dans une interconnexion de réseaux.

Vous êtes inscrit sur la WBM du noeud souhaité.

Étape par étape

1) Cliquez dans la barre de navigation sur **Gestion des licences**.
2) Dans l'arborescence de navigation, cliquez sur **Paramètres**.
3) Activez le champ d'option **Agent de licence central** et, dans **Adresse IP de l'agent de licence central**, entrez l'adresse IP du noeud maître (noeud 1) sous la forme `123.124.125.126`.
4) Cliquez sur **Activer**.

7.10 ID de verrouillage (Locking ID et Advanced Locking ID)

Il est attribué à chaque système de communication un ID de verrouillage ou un ID de verrouillage évolué. Pour que les licences soient univoques, elle sont associées à ces ID de verrouillage.

ID de verrouillage

Pour les plates-formes matérielles, l'ID de verouillage est l'adresse MAC du système de communication.

Dans un commutateur logiciel, l'ID de verrouillage est l'adresse MAC de la carte réseau du serveur Linux. Si le serveur Linux contient plusieurs cartes réseau, il faut choisir la carte réseau qui a été utilisée lors de la première mise en service du serveur Linux.

Si le système de communication se trouve durant la période d'activation, il peut être affiché dans les informations de licence une adresse MAC erronée. L'adresse MAC correcte peut être demandée dans **Centre de service** , dans **Inventory**.

Identifiant Advanced Locking

Si le commutateur logiciel se trouve dans un environnement virtuel, on utilise à la place de l'ID de verrouillage l'ID de verrouillage avancée (ALI - Advanced

Locking ID). L'identifiant Advanced Locking ID est généré sur CLS à l'aide du ALI-Calculator.

Il est nécessaire de configurer les paramètres Système et Réseau suivants pour être en mesure de générer l'identifiant Advanced Locking ID de 24 caractères.

- Adresse IP de la passerelle par défaut (serveur Linux)
- Nom d'hôte du serveur Linux
- Adresse IP du serveur Linux
- Adresse IP du serveur DNS (configurée dans le serveur Linux)
- Fuseau horaire (serveur Linux)

Si un ou plusieurs de ces paramètres Système et Réseau ne sont pas définis, il est impossible de générer l'identifiant Advanced Locking ID.

L'identifiant Advanced Locking ID est affiché dans WBM. Dans certains cas, il est possible que l'identifiant ALI qui a été généré pour le fichier de licence sur le CLS, soit différent de l'ALI qui est affiché dans WBM durant la période d'activation. Le fichier de licence avec ALI différent est toutefois accepté par le système.

Si l'un des paramètres système et réseau indiqués ci-dessus est modifié, le commutateur logiciel revient sur l'état non licencié et un nouvel identifiant (ID) Advanced Locking est généré. Pour être en mesure d'utiliser de nouveau le fichier de licence acheté, il faut, sur le serveur de licence central (CLS), effectuer un ré-hébergement de l'ancien au nouvel identifiant Advanced Locking ID.

Si le système détecte une modification dans ALI, un message est affiché sur la page d'accueil de WBM dans la zone de licence pour informer l'utilisateur que ALI a été modifié. L'utilisateur doit cliquer sur Confimer pour indiquer qu'il doit être informé de la modification. Le message sera supprimé de la page d'accueil de WBM, jusqu'à ce qu'une nouvelle instance de changement ALI ait été détectée. Si l'utilisateur ne clique pas sur Confirmer, le message sera affiché de manière permanente sur la page d'accueil.

Important : En cas de modification des paramètres de l'ID de verrouillage (adresse IP, adresse de passerelle, adresse DNS, nom d'hôte pour les systèmes S, adresse MAC pour les systèmes X), la licence du système devient invalide. Vous devez contacter un partenaire agréé du serveur de licence Central pour générer un nouveau fichier de licence à installer dans le système.

Important : Si un utilisateur appuie sur le bouton de confirmation, aucun message électronique ne sera ensuite envoyé. Un message électronique ne sera envoyé que si l'utilisateur n'a pas confirmé les modifications via la page d'accueil. Le mécanisme de messagerie électronique est activé tous les jours avec un intervalle de 24h, à partir du dernier redémarrage du système.

7.10.1 Comment interroger le Locking ID (identifiant de verrouillage) du système de communication

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Inventory**. Il vous est présenté une vue des composantes qui font partie du système de communication.
3) Cliquez sur **OK&Suivant**. Le système affiche des informations sur le matériel et le logiciel. Dans **MAC-ID pour licence** vous trouverez l'ID de verrouillage du système de communication.

7.10.2 Comment interroger l'ID de verrouillage du commutateur logiciel

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Inventory**. Il est affiché des informations sur le logiciel du commutateur logiciel, sur la capacité mémoire disponible et occupée sur les disques dur et sur l'état de l'application. Dans **MAC-ID pour licence** vous trouverez l'ID de verrouillage du commutateur logiciel.

7.10.3 Comment interroger l'ID Advanced Locking du commutateur logiciel

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

Cliquez dans la barre de navigation sur **Gestion des licences**. Les licences disponibles vous sont montrées. Dans **Locking ID**, vous trouverez l'identifiant Advanced Locking ID du commutateur logiciel lorsque celui-ci est exploité dans un environnement virtualisé.

7.11 Comment migrer d’une carte mère V2 vers une carte mère V3 (système autonome)

Conditions préalables

- Effectuez une mise à jour vers la version la plus récente du système.
- Retirez les cartes IVM, nettoyez les emplacements de carte et retirez la configuration IVM du système.

- Vérifiez que les ports 511 à 532 ne sont pas utilisés. Ces ports seront réservés à SmartVM sur la carte mère V3. Cela est uniquement nécessaire pour les systèmes s'exécutant en mode UC Smart.

  Pour résoudre les problèmes liés à la fonctionnalité UC Fax lors de la migration vers le système avec carte mère V3, il est recommandé de configurer le mode de fonctionnement du système avant la migration. Si le système fonctionne en mode UC Smart, l'administrateur doit supprimer la configuration des ports 511-532 avant la migration. Si le système fonctionne en mode UC Suite, les ports SmartVM supplémentaires ne sont pas créés, et la configuration Fax n'est donc pas affectée. Par exemple, si le jeu de sauvegarde provient d'un système UC Suite, le mode de fonctionnement du système avec carte mère V3 doit passer en mode UC Suite avant de migrer le jeu de sauvegarde.

  Remarque : Lorsque vous mettez à niveau un système PAYGO OpenScape Business, mettez d'abord à niveau le système Open Scape Business vers V3 puis utilisez la fonction **Régénérer une clé de licence** sur le CLS pour recevoir un fichier de licence valide pour V3 et contenant la licence "Informations OpenScape Business prêtes pour V3 SW F31505-K158-D129". Ensuite, le fichier de licence nouvellement généré doit être activé manuellement au sein de la WBM d'OpenScape Business System, sous **Gestion des licences**.

Remarque : Lorsque vous mettez à niveau un système PAYGO OpenScape Business, mettez d'abord à niveau le système Open Scape Business vers V3 puis utilisez la fonction **Régénérer une clé de licence** sur le CLS pour recevoir un fichier de licence valide pour V3 et contenant la licence "Informations OpenScape Business prêtes pour V3 SW F31505-K158-D129". Ensuite, le fichier de licence nouvellement généré doit être activé manuellement au sein de la WBM d'OpenScape Business System, sous **Gestion des licences**.

Étape par étape

1) Passez au mode de fonctionnement système approprié.

La sauvegarde du système effectuée depuis un mode de fonctionnement ne peut pas être utilisée au sein d'un autre mode. Par exemple, si vous faites une sauvegarde de votre système depuis le mode UC Suite, vous devez d'abord passer le système mis à niveau dans le mode UC Suite avant de

faire une restauration, vous ne pouvez pas restaurer la sauvegarde depuis le mode UC Smart.

Le système avec carte mère V3 s'exécute en mode UC Smart :

Les ports SmartVM supplémentaires seront créés sans délai, et l'administrateur devra supprimer la configuration de la plage de ports susmentionnée sur le système OCC avant la migration.

Le système avec carte mère V3 s'exécute en mode UC Suite :

Les ports SmartVM supplémentaires ne sont pas créés, et la configuration Fax n'est donc pas affectée.

2) Activez la licence du système.

CLS Connect	Action
Activés	Générez de nouveau la licence vers l'adresse MAC V3 sur CLS.
Non activé	Importez la nouvelle licence et activez-la sur le système OpenScape Business V2. La demande d'accès du code de confirmation se déclenche, affichant le code de confirmation sur la page d'accueil de WBM.

3) Faites une sauvegarde du système V2 incluant la configuration du système.

Si l'OCC est connecté à un serveur Booster, un jeu de sauvegarde complet depuis le serveur Booster doit être téléchargé et enregistré.

4) Changez la carte mère.

5) Importez la nouvelle licence

CLS Connect	Action
Activés	Importez le fichier de licence V3 depuis CLS dans OpenScape Business. La fonctionnalité **CLS Connect** sera activée sur la carte mère V3.
Non activé	Générez une nouvelle licence V3 à l'aide du code de confirmation sur CLS avec l'adresse MAC de la carte mère V3, puis importez le nouveau fichier de licence V3 dans OpenScape Business.

6) Restaurez la sauvegarde V2 sur la carte mère V3.

7) Modifiez la configuration des adresses IP des clients UC.

Lors de la première connexion des clients UC (après la migration), veuillez utiliser la nouvelle adresse IP de la carte mère V3.

Seul le mode Duplex intégral est compatible avec les cartes mères V3.

Les équipements OptiPoint 4xx/5xx ne sont plus pris en charge avec les cartes mères V3.

7.12 Comment migrer le nœud maître d'un système en réseau d'une carte mère V2 vers une carte mère V3

Conditions préalables

Le système possède une licence de mise en réseau.

Étape par étape

1) Mettre à jour tous les nœuds esclaves OpenScape Business vers V3.

Scénario	Procédure à suivre
Mettre à jour avec CLS Connect	Mise à niveau de V2 vers V3 avec CLS Connect à la page 299
Mettre à jour sans CLS Connect	Mise à niveau de V2 vers V3 sans CLS Connect à la page 299

2) Migrer le nœud maître du système.

Suivre les instructions Comment migrer d'une carte mère V2 vers une carte mère V3 (système autonome) à la page 295

Les nœuds esclaves sont en mode basculement jusqu'à la migration du nœud maître. La migration du nœud maître leur permet d'être à nouveau pleinement fonctionnels.

7.13 Comment migrer le nœud esclave d'un système en réseau d'une carte mère V2 vers une carte mère V3

Conditions préalables

Le système possède une licence de mise en réseau.

Remarque : Si CLS Connect n'est pas activé, retirez d'abord le système esclave du réseau sur CLS.

Étape par étape

1) Migrez le système esclave.

Suivre les instructions Comment migrer d'une carte mère V2 vers une carte mère V3 (système autonome) à la page 295

2) Mettre à jour ou migrer le nœud maître.

Scénario	Procédure à suivre
Migration de la carte mère V2 vers la carte mère V3	Comment migrer d'une carte mère V2 vers une carte mère V3 (système autonome) à la page 295
Mise à jour du logiciel avec CLS Connect	Mise à niveau de V2 vers V3 avec CLS Connect à la page 299
Mise à jour du logiciel sans CLS Connect	Mise à niveau de V2 vers V3 sans CLS Connect à la page 299

7.14 Migration des systèmes HiPath 3000 vers le logiciel OSBiz V3 avec la carte mère V3

Le processus normal de migration de HiPath 3000 vers OSBiz à l'aide de l'outil Manager E effectue la migration logicielle. Les licences HiPath 3000 ComScendo et S2m existantes sont mises à niveau vers l'adresse MAC de la carte mère OCCe. Le CLS génère les licences TDM et l'indicateur de logiciel V3 sur la base des informations du fichier XML créé à partir de Manager E au cours de cette procédure.

Dans le cas d'une carte mère OCC réutilisée lors d'une migration précédente d'OSBiz vers OCCe, aucune migration de licence n'est possible. Toutes les licences doivent être achetées.

Dans le cas d'une carte mère OCC provenant d'un stock de pièces de rechange ou nouvellement achetée (l'adresse MAC n'est pas bloquée dans le CLS), une mise à niveau d'HiPath 3000 vers cette adresse MAC est possible et un nouveau fichier de licence est généré (comme pour la migration vers OSBiz V2).

7.15 Mise à niveau de V2 vers V3 avec CLS Connect

La dernière version V2R7 doit être mise à niveau et **CLS Connect** est actif. Les licences OpenScape Business V2 existantes liées à l'adresse MAC de la carte mère OCC sont également valables pour la V3.

Au démarrage après la mise à niveau du logiciel, le logiciel OpenScape Business V3 indique sur le CLS que les licences fonctionnent en association avec le logiciel V3. Les informations de la V3 sont ajoutées au fichier de licence et automatiquement retransférées dans le système via une connexion CLS durant le démarrage. Aucune action manuelle n'est exigée.

Aucune action n'est exigée en cas de mise à niveau du logiciel sans migration pour les systèmes esclaves disposant d'une licence de mise en réseau. Dans un tel cas, les systèmes esclaves peuvent être mis à niveau et leurs licences seront automatiquement mises à jour après la mise à niveau/migration du système maître.

7.16 Mise à niveau de V2 vers V3 sans CLS Connect

Conditions préalables

- CLS Connect n'est pas activé
- OpenScape Business S nécessite un accès Internet
- En cas de mise à niveau d'un nœud esclave au sein d'un système en réseau, retirez d'abord l'esclave de CLS.

Étape par étape

1) Activez la licence SW-Upgrade sur CLS comme une licence normale pour le système OpenScape Business. L'activation de la licence SW-Upgrade sur CLS génère un nouveau fichier de licence contenant :

- La nouvelle licence V3
- L'ID (augmenté) du nouveau fichier de licence
- Si le système est OSBiz S, CLS Connect Start est ajouté au certificat.

2) Importez ce nouveau fichier de licence et activez-le dans le système OpenScape Business V2.

3) Exécutez la mise à niveau logicielle de V2 à V3.

Durant le démarrage, après la mise à niveau logicielle vers V3, le système OpenScape Business vérifie le fichier de licence et autorise la fonctionnalité de procédure de licence uniquement si le composant de licence V3 est disponible au sein du fichier de licence.

8 Intégration au réseau de données interne (LAN)

L'intégration du système de communication dans le réseau interne existant (LAN) permet l'utilisation de solutions UC et l'administration du système de communication sur les PC du réseau interne.

Les paramètres réseau suivants doivent être configurés dans le WBM :

- Plateforme matérielle OpenScape Business X : adresse IP et masque de réseau de la carte mère. Ces paramètres sont définis lors de l'installation initiale, mais peuvent être modifiés ultérieurement.

  Softswitch OpenScape Business S : Adresse IP et masque de sous-réseau du serveur Linux sur lequel le logiciel de communication est exécuté. Ces paramètres sont définis lors de l'installation de Linux, mais peuvent être modifiés ultérieurement.
- Le système de communication peut être configuré en option comme serveur DHCP (doté de paramètres spécifiques au réseau tels que le masque de sous-réseau, la passerelle par défaut et le serveur DNS) ou comme agent de relais DHCP. La configuration en tant que serveur DHCP est effectuée lors de l'installation initiale, mais peut être modifiée ultérieurement. La configuration en tant qu'agent de relais DHCP s'effectue en mode Expert.
- Adresse IP du routeur par défaut et du serveur DNS (externe) pour l'accès aux autres réseaux IP (par exemple, Internet). Ces paramètres sont définis lors de l'installation initiale, mais peuvent être modifiés ultérieurement.

8.1 Interface LAN

Pour intégrer le système de communication dans l'infrastructure LAN, il faut harmoniser l'adresse IP et la plage d'adresses IP interne du système de communication avec le schéma des adresses IP du réseau interne (LAN).

8.1.1 Adresse IP et masque de sous-réseau de l'interface LAN

L'adresse IP et le masque de sous-réseau du système de communication sont définis lors de l'installation initiale, mais peuvent également être modifiés ultérieurement. Vous devrez peut-être adapter l'adresse IP et/ou le masque de sous-réseau à la plage d'adresses IP du réseau local.

Plateforme matérielle

Par défaut, la plateforme matérielle se voit attribuer une adresse IP et un masque de sous-réseau.

La plateforme matérielle utilise l'interface « LAN » de la carte mère pour son intégration au réseau local.

Pour que les modifications apportées à l'adresse IP ou au masque de sous-réseau soient prises en compte, un redémarrage de la plateforme matérielle est nécessaire.

Les modifications apportées à l'adresse IP et au masque de sous-réseau restent effectives après une mise à jour logicielle, mais seront réinitialisées aux valeurs par défaut en cas de réinstallation de la plateforme matérielle. Ces modifications ne peuvent pas être enregistrées dans un jeu de sauvegarde.

Interrupteur logiciel

Dans le cas d'un commutateur logiciel, le serveur Linux sur lequel s'exécute le logiciel de communication est intégré au réseau local via sa carte réseau.

Le changement d'adresse IP ou de masque de sous-réseau prend effet après un redémarrage de l'application (voir Redémarrage, Rechargement, Arrêt).

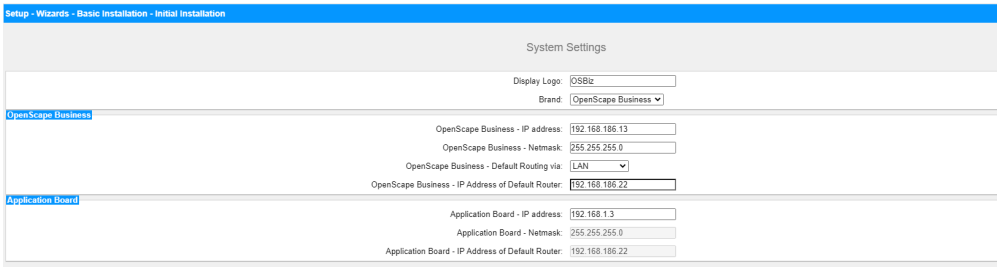
8.1.1.1 Comment modifier l'adresse IP et le masque réseau de la plate-forme matérielle

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** pour lancer l'Assistant **Première installation**.



3) Dans **OpenScape Business - Adresse IP**, modifiez l'adresse IP de la plate-forme matérielle. L'adresse IP doit être conforme au schéma des adresses IP du réseau interne et ne doit pas être affectée à un client réseau existant car cela provoque sinon un conflit d'adresses. Par défaut, l'adresse IP `192.168.1.2` est inscrite.
4) Dans **OpenScape Business - Masque de réseau**, modifiez le masque de réseau de la plate-forme matérielle. Le masque de réseau doit être adapté au schéma d'adresses IP du réseau interne. Par défaut, le masque de sous-réseau inscrit est `255.255.255.0`.
5) Cliquez sur **OK&Suivant**.
6) Cliquez autant de fois que nécessaire sur **OK&Suivant** pour afficher le message indiquant que la fonctionnalité a été configurée.
7) Cliquez sur **Terminer**. La plate-forme matérielle effectue automatiquement un redémarrage.

8.1.1.2 Comment modifier l'adresse IP et le masque réseau du commutateur logiciel

Étape par étape

1) Dans la barre des tâches, cliquez sur **Computer**.
2) Dans l'arborescence du menu, cliquez sur **System** > **YaST**.
3) Entrez le mot de passe pour l'utilisateur root et cliquez sur **Continue** (poursuivre). Le YaST Control Center s'ouvre.
4) Dans l'arborescence du menu, cliquez sur **Network Services** (équipements réseau).

5) Dans la zone **Network Equipements** cliquez sur **Network Settings** (paramètres réseau).
6) Dans l'onglet **Overview** (Présentation), sélectionnez la carte réseau souhaitée et cliquez sur **Edit** (modifier).
7) Activez le champ d'option **Statically assigned IP Address** (adresse IP affectée de manière statique).
8) Dans **Adresse IP**, modifiez l'adresse IP du serveur Linux, où le logiciel du commutateur logiciel tourne. L'adresse IP doit être conforme au schéma des adresses IP du réseau interne et ne doit pas être affectée à un client réseau existant car cela provoque sinon un conflit d'adresses.
9) Dans **Masque du sous-réseau**, modifiez le masque de sous-réseau du serveur Linux. Le masque de sous-réseau doit être conforme au schéma d'adresses IP du réseau interne.
10) Cliquez sur**Next** (suivant) et ensuite sur **OK**.
11) Fermez le **YaST Control Center**.

8.1.2 Plage d'adresses IP interne de l'interface LAN

La plage d'adresses IP interne de l'interface LAN, utilisée par la plate-forme matérielle pour la communication interne de ses modules peut être modifiée si nécessaire.

La plate-forme matérielle utilise par défaut la plage d'adresses IP interne 192.168.3.xxx. Elle peut être modifiée en faveur d'une plage d'adresse différente. Le masque de sous-réseau interne est 255.255.255.0 et ne peut pas être modifié.

Pour activer les modifications de la plage d'adresses IP interne, il faut redémarrer la plate-forme matérielle.

Les modifications de la plage d'adresses IP internes sont conservées lors d'une actualisation du logiciel, mais elles sont replacées sur les valeurs par défaut en cas de rechargement. Ces modifications ne peuvent pas être conservées dans un jeu de sauvegarde.

8.1.2.1 Comment modifier la plage d'adresses IP interne de la plate-forme matérielle

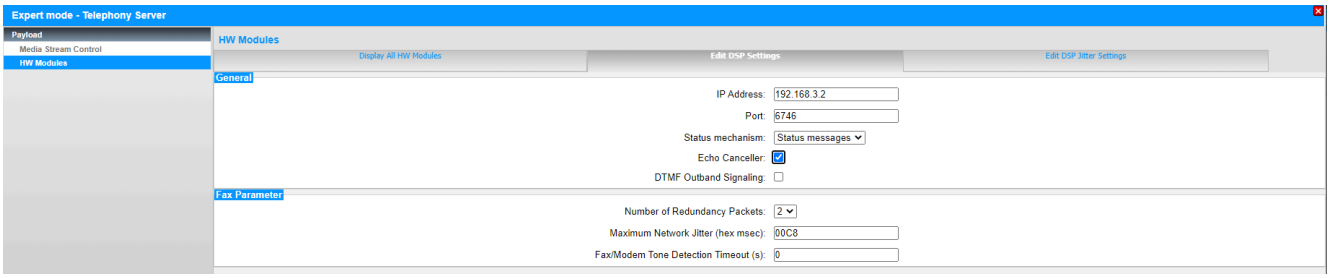
Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l’arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Charge utile**.
3) Dans l’arborescence du menu, cliquez sur **Modules matériels**.

4) Cliquez sur l'onglet **Modifier les paramètres DSP**.



5) Dans la zone **Général** sous **Adresse IP**, saisissez une adresse IP pour le système de communication qui se trouve dans la nouvelle plage interne souhaitée, par ex. `192.168.40.2`. La plage d'adresses IP complète (dans notre exemple `192.168.40.xxx`) est désormais bloquée pour les autres clients du LAN.
6) Cliquez sur **Appliquer** et confirmez avec **OK**.

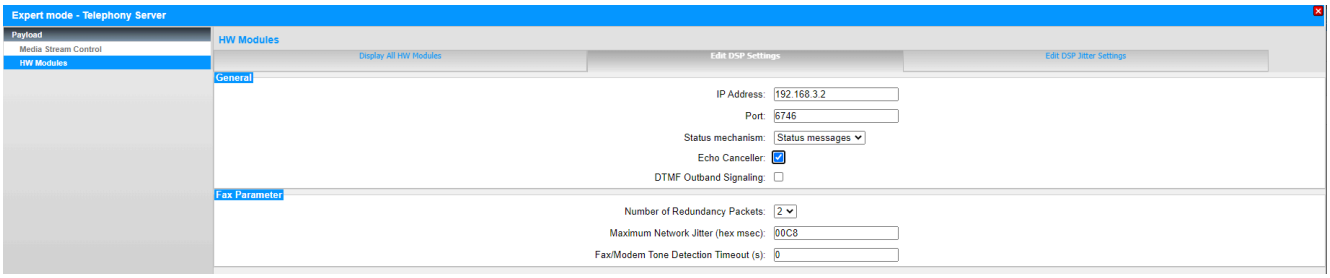
8.1.2.2 Comment réinitialiser la plage d'adresses IP interne de la plate-forme matérielle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Charge utile**.
3) Dans l'arborescence du menu, cliquez sur **Modules matériels**.
4) Cliquez sur l'onglet **Modifier les paramètres DSP**.



5) Dans la zone **Général** sous **Adresse IP**, saisissez l'adresse IP `192.168.3.2`. La plage d'adresses IP complète `192.168.3.xxx` est désormais bloquée pour les autres client du LAN.
6) Cliquez sur **Appliquer** et confirmez avec **OK**.

8.2 DHCP

DHCP (Dynamic Host Configuration Protocol) permet, avec l'aide d'un serveur DHCP, l'affectation dynamique de données spécifiques réseau aux abonnés IP d'un réseau (par ex. LAN).

DHCP permet l'intégration automatique d'un abonné IP (par ex. téléphones IP ou PC) dans un LAN existant. L'abonné IP doit être paramétré pour la réception

automatique des données réseau et il est donc un client DHCP. Le serveur DHCP fournit sur demande à l'abonné IP les données spécifiques réseau.

8.2.1 Agent relais DHCP

Lorsque l'on utilise le serveur DHCP interne de la plate-forme matérielle, le serveur DHCP interne et les clients DHCP doivent se trouver dans le même segment de réseau. Si ce n'est pas le cas, la plate-forme matérielle doit être configurée comme agent relais DHCP. Les demandes DHCP des abonnés IP sont transmises de la plate-forme matérielle au serveur DHCP proprement dit.

8.2.1.1 Comment configurer la plateforme matérielle en tant qu'agent relais DHCP

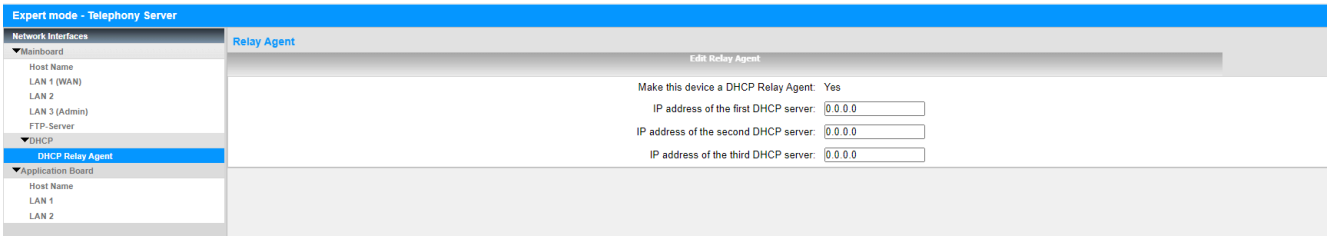
Si la plateforme matérielle est configurée comme agent de relais DHCP, elle relaie les demandes DHCP au serveur DHCP externe.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Cliquez sur **Serveur de téléphonie** > **Interfaces de réseau** dans l'arborescence de navigation.
3) Dans l'arborescence du menu, cliquez sur **Carte mère** > **DHCP**.
4) Activez le bouton radio **Agent Relais DHCP**.
5) Cliquez sur **Appliquer** et confirmer avec **OK**.
6) Cliquez sur **Agent relais DHCP** dans l'arborescence de navigation.



7) Entrez l' **adresse IP du premier serveur DHCP**.
8) Entrez l' **adresse IP du deuxième serveur DHCP**.
9) Entrez l' **adresse IP du troisième serveur DHCP**.

Conseil : Vous pouvez saisir jusqu'à trois serveurs DHCP. L'entrée du premier serveur DHCP est obligatoire.

10) Cliquez sur **Appliquer**, puis sur **OK**.

8.2.2 Serveur DHCP

Le serveur DHCP transmet de manière dynamique les données spécifiques réseau aux abonnés IP (téléphones IP, téléphones SIP, PC, points d'accès

WLAN, etc.) comme l'adresse IP et le masque réseau de l'abonnés IP, l'adresse IP de la passerelle par défaut, l'adresse IP du serveur SNTP, etc.

On peut utiliser comme serveur DHCP le serveur DHCP interne du système de communication ou u, serveur DHCP externe (par ex. le serveur DHCP du routeur Internet).

Dans la plate-forme matérielle, le serveur DHCP intégré est activé par défaut. Si l'on doit utiliser un serveur DHCP externe, le serveur DHCP interne doit être désactivé. Sinon, cela provoque des conflits avec leserveur DHCP externe.

Avec le commutater logiciel, le serveur Linux peut être configuré comme serveur DHCP interne.

Lors de la première mise en service il faut décider si l'on va utiliser le serveur DHCP interne du système de communication ou un serveur DHCP externe. Le serveur DHCP interne peut aussi être activé ou désactivé a posteriori. Il est également possible de configurer ultérieurement les données spécifiques réseau.

Serveur DHCP interne

Si le serveur DHCP interne est utilisé, les abonnés IP reçoivent automatiquement les données réseau suivantes :

- Adresse IP et masque de réseau de l'abonné IP
- Adresse IP du système de communication (passerelle par défaut)
- Adresse IP du serveur SNTP (pour la date et l'heure)
- Adresse IP du serveur DNS (pour la définition du nom)
- Adresse IP du serveur SIP (pour l'authentification des abonnés SIP)
- Adresse IP de la fonction DLI interne ou du serveur DLS externe (pour actualisation du logiciel des téléphones système IP)
- Règles de routage

Serveur DHCP externe

Si l'on utilise un serveur DHCP externe, celui-ci doit supporter pour cela un Vendor Specific Option Space qui permet de fournir des paramètres spécifiques constructeur. Les données spécifiques au réseau suivantes devraient être entrées dans le serveur SHCP externe :

- Adresse IP et masque de réseau de l'abonné IP
- Adresse IP du routeur par défaut = option 3
- Adresse IP du système de communication (passerelle par défaut) = option 33
- Adresse IP du serveur DNS (pour la définition du nom) = Option 6
- Adresse IP de la fonction DLI interne ou du serveur DLS externe (pour actualisation du logiciel des téléphones système IP) = option 43
- Pour les téléphones SIP uniquement : adresse IP du serveur SIP (SIP-Registrar, pour l'authentification des abonnés SIP) = option 120
- Pour les téléphones SIP uniquement : adresse IP du serveur SNTP (pour la fourniture aux téléphones SIP de la date & heure) = option 42

Remarque : Des informations complémentaires sur le serveur DHCP en environnement Windows figurent ici : http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment.

Si une entrée n'est pas possible sur le serveur DHCP externe, ces données doivent être entrées directement sur les téléphones système IP. C'est seulement ensuite que les téléphones système IP reçoivent automatiquement la date et l'heure, par exemple, ainsi que les nouvelles mises à jours du logiciel.

Pour plus d'informations, consultez la page Unify Experts Wiki suivante : http://wiki.unify.com/wiki/DHCP

Plage d'adresses DHCP (plage d'adresses IP)

Lorsqu'un abonnés IP se connecte sur le serveur DHCP, il lui est entre autres attribué une adresse IP dynamique. L'administrateur peut déterminer une plage d'adresses IP à partir de laquelle le serveur DHCP affecte les adresses IP aux abonnés IP. Par ex. il ne faut pas affecter toutes les adresses de la plage 192.168.1.x, mais uniquement celles de 192.168.1.50 à 192.168.1.254, étant donné que les adresses inférieures jusqu'à 192.168.1.49 sont réservées aux abonnés IP avec adresses statiques IP.

En mode Expert, il est possible de paramétrer plusieurs plages d'adresses IP pour le serveur DHCP interne, dans **Interfaces réseau**.

8.2.2.1 Comment activer et configurer le serveur DHCP de la plateforme matérielle

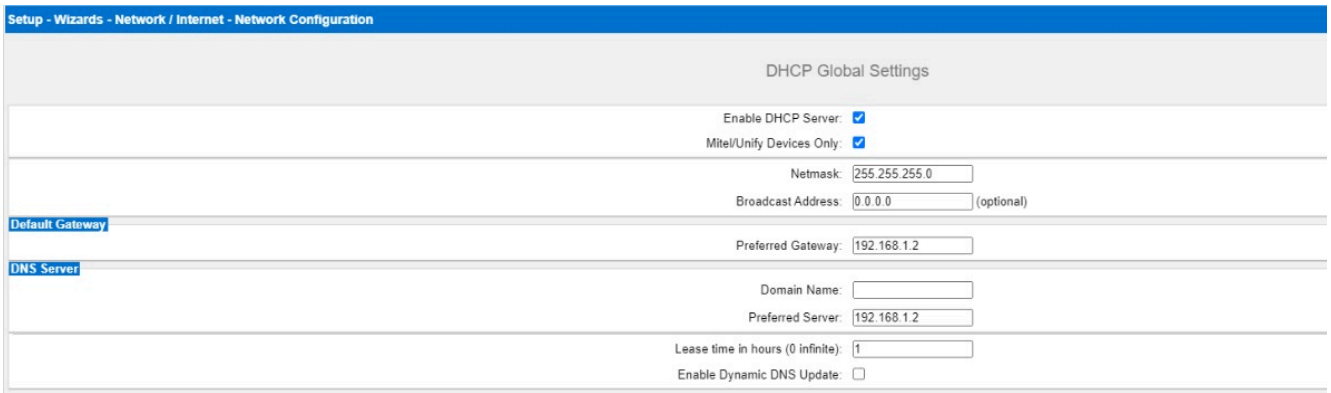
L'**assistant de configuration** du réseau peut être utilisé pour activer et configurer le serveur DHCP de la plateforme matérielle.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseaux/ Internet**.
3) Cliquez sur **Modifier** pour lancer l'Assistant de **Configuration du réseau**.



4) Cochez la case **Activer le serveur DHCP**.
5) Si nécessaire, activez la case à cocher **Appareils Mitel/Unify uniquement**.

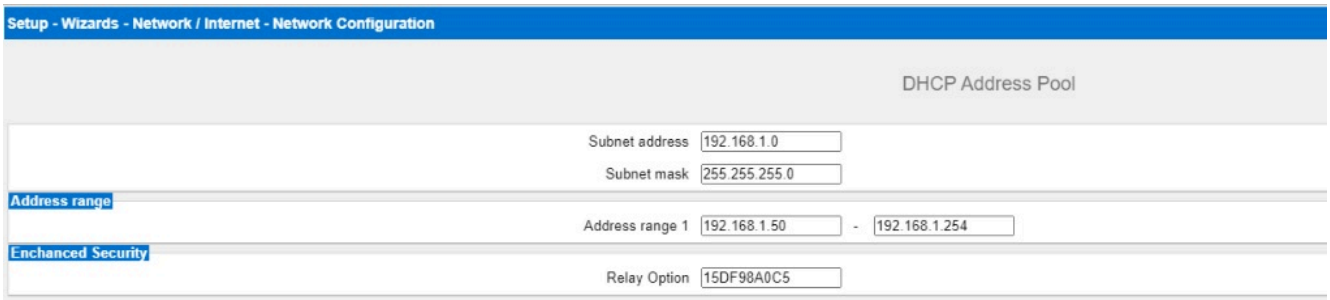
Remarque : Cette option n'est disponible que pour les cartes mères V3.

6) Entrez le masque de sous-réseau de votre réseau dans le champ **Masque de sous-réseau** field (par ex., `255.255.255.0`).
7) Dans le champ **Adresse de diffusion**, entrez l'adresse de diffusion (la « dernière » adresse IP du réseau ou du sous-réseau, par défaut : `0.0.0.0`) si nécessaire.
8) Dans le champ **Passerelle préférée**, entrez l'adresse IP de la Passerelle par défaut. En règle générale, l'adresse IP du routeur Internet est `192.168.1.1`.
9) Si vous avez besoin d'un nom de domaine complet pour le serveur DHCP, indiquez-le dans le champ **Nom de domaine** (80 caractères max.).
10) Dans le champ **Serveur préféré**, entrez l'adresse IP d'un serveur DNS disponible, par exemple, l'adresse IP du routeur Internet, `192.168.1.1`.
11) Si nécessaire, entrez la durée maximale du bail en heures (par défaut : 1 h, 0 = durée de bail infinie) dans le champ **Durée de bail en heures (0 = infinie)**.
12) Si vous souhaitez autoriser les mises à jour dynamiques du serveur DNS, activez l'option **Activer la mise à jour dynamique du DNS** (par défaut : désactivée).

Remarque : Si l'option Mise à jour dynamique du DNS est activée, il est obligatoire de configurer le nom de domaine dans le champ **Nom de domaine** respectif du pool d'adresses IP.

---

13) Cliquez sur **OK & Suivant**. Les paramètres du pool d'adresses DHCP s'affichent.



14) Dans le champ **Adresse de sous-réseau**, entrez l'adresse IP la plus basse du sous-réseau dans lequel se trouve la plage d'adresses IP souhaitée (dans notre exemple, `192.168.1.0`).
15) Dans le champ Masque de sous-réseau, entrez le **Masque de sous-réseau** de la plage d'adresses IP souhaitée (par exemple, `255.255.255.0`).
16) Saisissez les seuils supérieur et inférieur de la plage d'adresses IP souhaitée dans le champ **Plage d'adresses 1** (par exemple, `192.168.1.50` à `192.168.1.254`).
17) Si nécessaire, spécifiez la valeur du champ **Relay Option**.

Remarque : Cette option n'est disponible que pour les cartes mères V3.

---

18) Cliquez sur **OK & Suivant**. La fenêtre **Paramètres de routage** s'affiche.

19) Dans le champ **Adresse IP du serveur DNS**, entrez l'adresse IP d'un serveur DNS disponible, par exemple, l'adresse IP du routeur Internet, `192.168.1.1`.
20) Sélectionnez l'élément **LAN** dans la liste déroulante **Routage par défaut via**.
21) Si l'accès à Internet se fait via un routeur Internet, entrez l'adresse IP du routeur Internet (par exemple, `192.168.1.1`) dans le champ **Adresse IP du routeur par défaut**.
22) Cliquez sur **OK & Suivant**, puis sur **Terminer**.

8.2.2.2 Comment désactiver le serveur DHCP de la plateforme matérielle

L'assistant de **configuration de réseau** peut être utilisé pour désactiver le serveur DHCP de la plateforme matérielle.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseaux/ Internet**.
3) Cliquez sur **Modifier** pour lancer l'Assistant de **Configuration du réseau**.
4) Laissez la case **Activer le serveur DHCP**.
5) Continuez à cliquer sur **OK & Suivant** jusqu'à ce que vous receviez un message indiquant que la fonctionnalité a été installée.
6) Cliquez sur **Terminer**.

8.2.2.3 Comment activer et configurer le serveur DHCP du commutateur logiciel

Étape par étape

1) Dans la barre des tâches, cliquez sur **Computer**.
2) Dans l'arborescence du menu, cliquez sur **System** > **YaST**.
3) Entrez le mot de passe pour l'utilisateur root et cliquez sur **Continue** (poursuivre). Le YaST Control Center s'ouvre.
4) Dans l'arborescence du menu, cliquez sur **Network Services** (services réseau).
5) Dans la zone **Network Services**, cliquez sur **DHCP Server** (serveur DHCP).
6) Sélectionnez la carte réseau souhaitée et cliquez sur **Select** (sélectionner).
7) Cochez la case **Open Firewall for Selected Interfaces** (Ouvrir le pare-feu pour les interfaces sélectionnées).
8) Cliquez sur **Suivant**.
9) Si vous avez besoin d'un nom de domaine entièrement qualifié pour le serveur DHCP, entrez-le dans **Domain Name** (Nom du domaine - 80 caractères maxi.).

10) Dans le champ **Primary Name Server IP** (nom primaire serveur IP), entrez l'adresse IP d'un serveur DNS disponible, par ex. l'adresse IP du routeur Internet, `192.168.1.1`.
11) Dans le champ **Passerelle par défaut (routeur)**, entrez l'adresse IP de la passerelle par défaut. En règle générale, il s'agit de l'adresse IP du routeur Internet, par ex. `192.168.1.1`.
12) Dans le champ **NTP Time Server** (serveur NTP), entrez le serveur NTP défini lors de la première mise en service.
13) Cliquez sur **Suivant**.
14) Dans le champ **First IP Address** (première adresse IP) entrez la limite inférieure de la plage d'adresses IP souhaitée et dans le champ **Last IP Address** (dernière adresse IP) la limite supérieure (par ex. `192.168.1.50` à `192.168.1.254`).
15) Cochez la case **Allow Dynamic BOOTP**.
16) Cliquez sur **Suivant**.
17) Activez le champ d'option **When Booting** (lors de l'initialisation).
18) Cliquez sur **Terminer**.
19) Fermez le **YaST Control Center**.

8.2.2.4 Comment désactiver le serveur DHCP du commutateur logiciel

Étape par étape

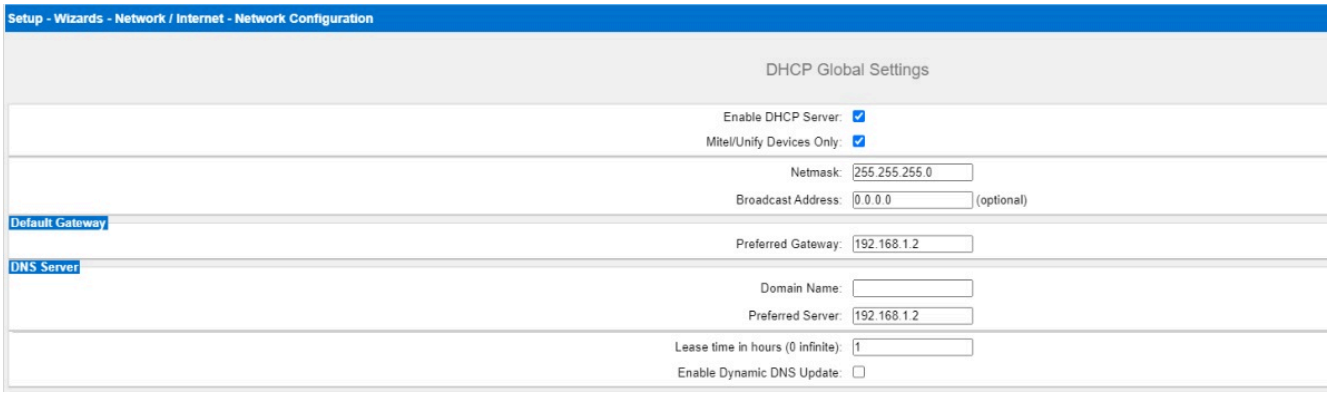
1) Dans la barre des tâches, cliquez sur **Computer**.
2) Dans l'arborescence du menu, cliquez sur **System** > **YaST**.
3) Entrez le mot de passe pour l'utilisateur root et cliquez sur **Continue** (poursuivre). Le YaST Control Center s'ouvre.
4) Dans l'arborescence du menu, cliquez sur **Network Services** (services réseau).
5) Dans la zone **Network Services**, cliquez sur **DHCP Server** (serveur DHCP).
6) Décochez la case **Start DHCP Server** (démarrer serveur DHCP).
7) Cliquez sur **Terminer**.
8) Fermez le **YaST Control Center**.

8.2.2.5 Comment activer DHCP pour les appareils Mitel/Unify uniquement

Cette option permet à l'administrateur système d'activer le service DHCP Unify OpenScape Business exclusivement pour les appareils Mitel et Unify.

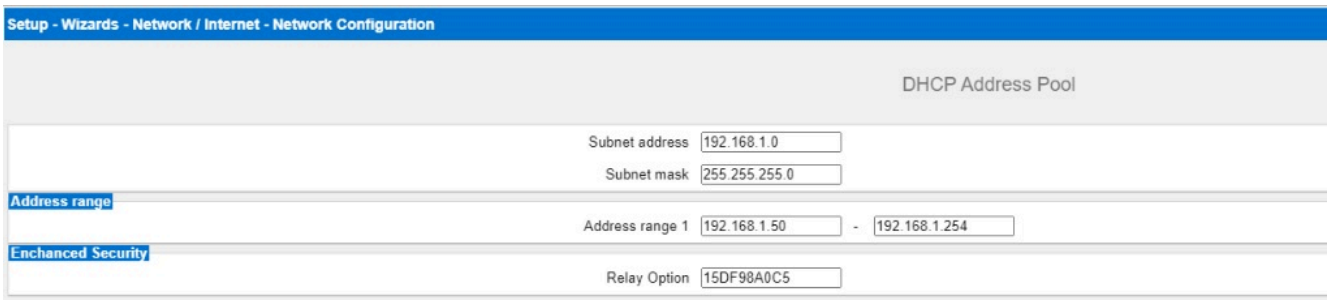
Conditions préalables

Vous êtes dans la fenêtre **Paramètres globaux DHCP**.



Étape par étape

1) Laissez la case à cocher **Activer le serveur DHCP** activée.
2) Cliquez pour activer la case à cocher **Mitel/Unify Devices Only**. Voir Serveur DHCP > Paramètres globaux pour plus d'informations sur cette option.
3) Accédez au champ **Netmask** et ajustez le masque de sous-réseau à votre plage d'adresses IP (par exemple, `255.255.255.0`).
4) Entrez dans le champ **Passerelle par défaut** l'adresse IP du routeur Internet (par ex., `192.168.1.1`).
5) Dans le champ **Serveur par défaut**, entrez l'adresse IP du serveur DNS (par ex., l'adresse IP du routeur Internet, `192.168.1.1`).
6) Cliquez sur **OK & Suivant**. La fenêtre **Pool d'adresses DHCP** apparaît.



7) Spécifiez les valeurs pour **l'adresse de sous-réseau**, **le masque de sous-réseau** et **la plage d'adresses 1** pour définir la plage d'adresses IP à gérer par le serveur DHCP interne.

   Si le réseau interne utilise des adresses IP statiques (par exemple, pour un serveur d'imprimante), la plage d'adresses IP (pool d'adresses DHCP) doit être sélectionnée de sorte que les adresses IP fixes ne soient pas incluses dans cette plage.

   Exemple:

   Routeur Internet : `192.168.1.1`

   Unify OpenScape Business : `192.168.1.2`

   Adresse du sous-réseau : `192.168.1.0`

   Masque de sous-réseau : `255.255.255.0`

   Serveur d'imprimante : `192.168.1.10`

   Pool d'adresses DHCP : `192.168.1.50` à `192.168.1.254`

8) Spécifiez la valeur du champ **Option de relais**.

9) Cliquez sur **OK & Suivant**.

Étapes suivantes

Paramètres de pays et d'heure

8.3 DNS - Résolution du nom

Le Domain Name Service (DNS) sert à convertir les noms en adresses numériques. Cela permet de traduire le nom de l'ordinateur ou le nom de domaine en Adresses IP et inversement.

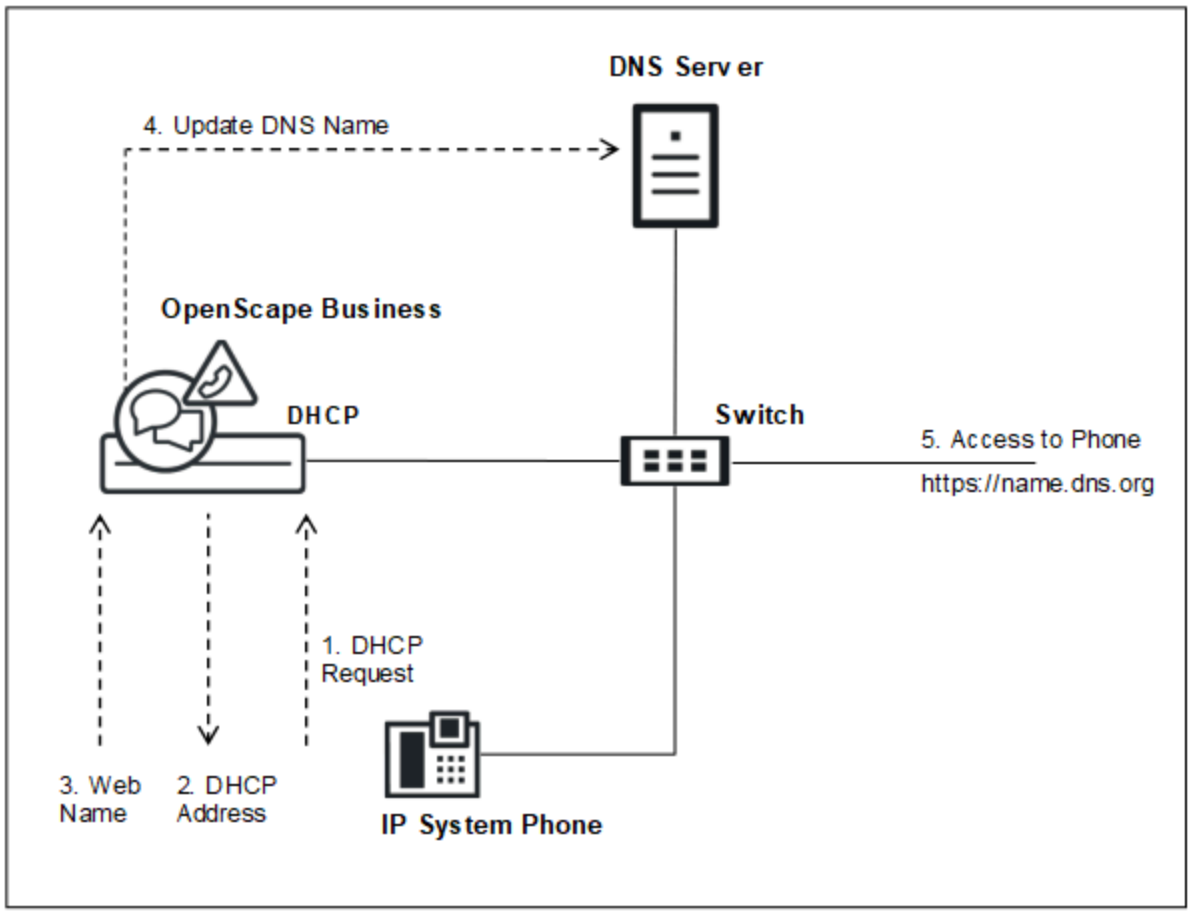
DNS utilise une base de données hiérarchique distribuée entre les serveurs à l'échelle mondiale qui gère la plage de noms d'Internet. Cette plage de nom est subdivisée en zones (domaines). Pour les demandes locales - au sein d'un réseau d'entreprise, ce sont en règle générale des serveurs DNS propres qui sont utilisés, indépendamment d'Internet.

Résolution du nom avec les téléphones système IP

Les conditions suivantes doivent être satisfaites.

- Windows 2008 DNS-Server (avec niveau de patch actuel et activation nécessaire de "autoriser une mise à jour non sécurisée")
- Serveur DHCP interne activé
- La fonctionnalité "Actualiser le DNS dynamique" est activée dans le serveur DHCP (voir Serveur DHCP)
- Dans le téléphone système IP, le nom Web est inscrit.

Le téléphones système IP envoie une DHCP-Request (1) et reçoit du serveur DHCP interne une adresse IP valide et les autres données spécifiques réseau (2). Après réception de ces données, le téléphone système IP envoie le nom du web réglé au serveur DHCP interne (3) qui transmet automatiquement le nom au serveur DNS (4) configuré. Le serveur DNS connaît maintenant le nom correspondant à l'adresse IP du téléphone système IP. Le téléphone système IP peut maintenant être contacté via la WBM avec son nom Web (5).



Serveur DNS

Le serveur DNS, également appelé serveur de noms, est un programme qui répond aux demandes concernant les noms de domaine ou les noms de calculateur. Le PC où ce programme fonctionne peut aussi être désigné par serveur DNS.

En cas de demande d'un nom de domaine ou d'un nom d'ordinateur, le serveur DNS envoie l'adresse IP correspondante.

Exemple : pour `www.wikipedia.org` les serveur DNS sur Internet renvoient l'adresse IP `91.198.174.2`.

Si le serveur DNS préféré ne peut pas répondre à la demande, il la transmet à un autre serveur DNS.

Dans un commutateur logiciel, le serveur Linux où tourne le logiciel de communication peut être configuré comme serveur DNS. La plate-forme matérielle ne peut pas être utilisée comme serveur DNS. On peut désigner un serveur DNS externe comme commutateur logiciel ou comme plate-forme matérielle.

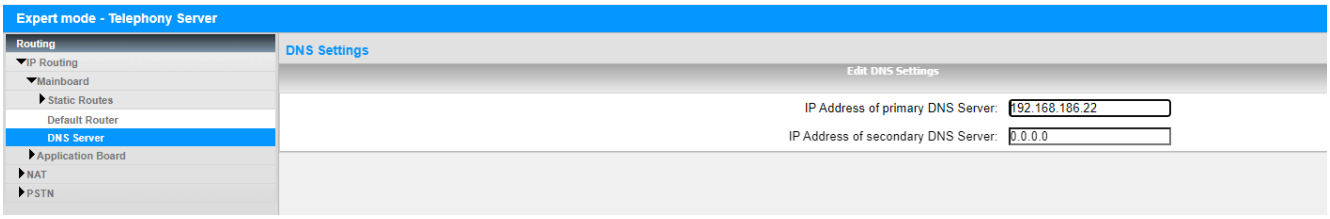
8.3.1 Comment définir un serveur DNS externe

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Routage**.
3) Dans l'arborescence du menu, allez à **Routage IP** > **Carte mère** > **Serveur DNS**. La fenêtre **Modifier les paramètres DNS** apparaît.



4) Entrez dans le champ **Adresse IP du serveur DNS** l'adresse IP du serveur DNS externe souhaité.
5) Cliquez sur **Appliquer**, puis sur **OK**.

Remarque : S'il s'agit d'un système OpenScape Business S, un redémarrage du système est nécessaire pour que les modifications soient applicables.

8.4 Routage IP

En technologie des données, le terme Routage IP désigne le choix de chemins (routes) pour les flux de données à l'intérieur des réseaux. Routage IP est nécessaire lorsque l'expéditeur et les destinataire sont dans des réseaux différents.

Routeur par défaut

Pour garantir que les abonnés IP parviennent aux destinations situées en dehors de leur propre réseau, qui ne figurent pas explicitement dans une table de routage, il faut indiquer une passerelle pour le transport de ces paquets (routeur par défaut). Le routeur par défaut transfère alors les données au réseau supérieur.

Vous pouvez activer ou désactiver Routage IP à l'aide du routeur par défaut pour la carte mère comme pour la carte d'application.

Itinéraires statiques

Les itinéraires statiques sont utilisés pour indiquer aux données la voie vers un réseau qui ne peut pas être joint par le routeur par défaut.

Vous pouvez créer des itinéraires statiques pour la carte mère comme pour la carte d'application.

8.4.1 Comment activer ou désactiver le routeur par défaut

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Routage**.
3) Dans l'arborescence du menu, sélectionnez **Routage IP** > **Carte mère/ Carte d'application** > **Routeur par défaut**. La fenêtre **Modifier le routeur par défaut** s'affiche.

4) Si vous souhaitez activer le routage IP à l'aide d'un routeur par défaut, dans le champ de la liste **Routage par défaut via**, choisissez l'entrée **LAN**. Sous `Adresse IP du routeur par défaut`, saisissez l'adresse IP du routeur par défaut, par ex. l'adresse IP du routeur Internet **192.168.1.1**.
5) Si vous souhaitez désactiver le routage IP à l'aide d'un routeur par défaut, dans le champ de la liste **Routage par défaut via**, choisissez l'entrée **Pas d'interface**.
6) Cliquez sur **Appliquer**, puis sur **OK**.

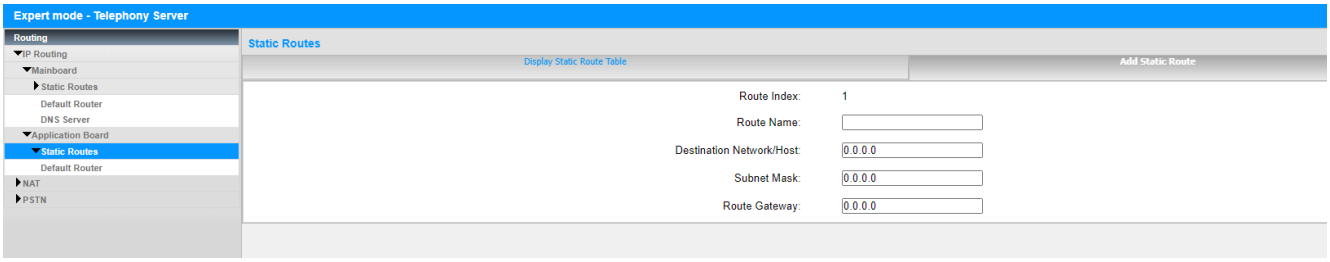
8.4.2 Comment ajouter un itinéraire statique

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Routage**.
3) Naviguez dans l'arborescence des menus jusqu'à **IP Routing** > **Mainboard/ Application Board** > **Static Routes**. La fenêtre **Itinéraires statiques** s'affiche.
4) Cliquez sur l'onglet **Ajouter un itinéraire statique**. L'**index d'itinéraire** affiche l'itinéraire ajouté.



5) Dans le champ **Nom de l'itinéraire**, saisissez le nom souhaité pour cet itinéraire.
6) Saisissez l'adresse IP du **réseau de destination/de l'hôte**.

7) Saisissez l'adresse IP du **masque de sous-réseau de destination** (masque de sous-réseau).
8) Dans le champ **Passerelle de l'itinéraire**, saisissez l'adresse IP du routeur que vous souhaitez utiliser pour accéder au réseau de destination.
9) Cliquez sur **Appliquer**, puis sur **OK**.

8.4.3 Comment effacer les itinéraires statiques

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Routage**.
3) Dans l'arborescence du menu, allez à **Routage IP** > **Carte mère / Carte d'application** > **Itinéraires statiques**.
4) Sélectionnez l'itinéraire à effacer.
5) Passez à l'onglet **Effacer l'itinéraire statique**.
6) Cliquez sur **Effacer**.
7) Validez le message et cliquez ensuite sur **OK**.

8.5 Deployment Service (DLI et DLS)

Avec l'aide de DLI et DLS, il est possible d'administrer de manière centralisée les composantes IP et d'assurer la fourniture des logiciels. Le DLI est intégré au système de communication. il s'agit d'une appication indépendante qui doit être installée sur un PC Serveur externe.

DLI (Deployment Serveur Integrated)

DLI est une composante intégrée dans le système de communication qui fournit une fonctionnalité DLS restreinte. A l'aide du DLI interne, vous pouvez configurer de manière centralisée tous les téléphones système IP raccordés au système de communication et leur fournir automatiquement le logiciel de téléphonie le plus récent. Pour le téléphone de bureau CP 400/600/600E/700/700X/710, lorsque le DLI est activé, les paramètres suivants du serveur UC sont automatiquement configurés : Protocole UC, adresse du serveur UC, port du serveur UC.

La DLI interne fonctionne avec le serveur FTP également intégré sur lequel le logiciel de téléphonie le plus récent est enregistré.

Si le serveur DHCP connaît l'adresse IP de DLI, le serveur DHCP envoie ces données au téléphone système IP (HFA, SIP) dès qu'il se connecte au réseau interne. Ainsi, le téléphone peut aller charger le logiciel actuel à partir du serveur FTP du système de communication. DLI est configuré par défaut dans le serveur DHCP interne. Si l'on doit par contre utiliser un serveur DLS externe, il faut configurer son adresse IP dans le serveur DHCP interne.

DLS (Deployment Service)

DLS est une application client/serveur pour administrer de manière centralisée les composantes IP. Le serveur DLS n'est pas intégré dans le système de communication et doit être installé séparément sur une PC-serveur. Le Client DLS fonctionne sur les composantes IP. L'administration a lieu avec un navigateur Web.

Les composantes IP sont les téléphones système IP, les téléphones SIP, les clients SIP et les passerelles IP.

Remarque : Les propriétés et fonctionnalités de DLS sont indiquées dans la Description du produit DLS et ne sont donc pas décrites dans la présente documentation.

DLI ou DLS avec serveur DHCP externe

Pour que le logiciel des téléphones système IP (HFA, SIP) soit automatiquement actualisé, même lorsque vous utilisez un serveur DHCP externe, vous disposez des possibilités suivantes.

- Configurer l'adresse IP du DLI ou DLS dans le serveur DHCP externe

  Dans le serveur DHCP externe, les données spécifique réseau doivent être inscrites ainsi que l'adresse IP du Deployment-Serveur utilisé (DLI ou serveur DLS externe). De plus, il faut enregistrer le logiciel de téléphonie sur le serveur DLS externe.
- configurer tous les téléphones système IP

  sur chaque téléphone système IP, il faut inscrire comme adresse DLS l'adresse IP du Deployment-server utilisé (adresse IP du système de communication pour le DLI interne ou adresse IP du serveur DLS externe).

Fonctions et restrictions

Fonction	DLI	DLS
Configuration centrale des paramètres des composantes IP Les paramètres des composantes IP sont configurables à l'aide de modèles XML adaptables.	oui	oui
Mise en service Plug&Play des composantes IP A l'aide du serveur DHCP, les composantes IP peuvent s'inscrire automatiquement au système, par ex. en cas de nouveau raccordement ou du remplacement d'une composante IP.	Oui	Oui
Actualisation logicielle centrale et automatique des composantes IP Les composantes IP reçoivent automatiquement la version logicielle la plus actuelle lors de la première connexion ou lorsqu'une nouvelle version logicielle est disponible. L'adresse IP de DLI/DLS doit être configurée dans la composante IP.	Oui	Oui sur DLS il faut enregistrer le logiciel de téléphonie le plus actuel.

Fonction	DLI	DLS
Gestion Inventory centrale des composantes IP Les données relatives aux configurations matérielles des composantes IP peuvent être appelées centralement.	non	Oui
Support de IP Mobility (DeskSharing) Les données de téléphonie d'un utilisateur sont enregistrées de manière centrale et peuvent être appelées sur d'autres téléphones (par ex. programmation des touches, inscriptions dans le répertoire, journaux).	Oui pas pour téléphones SIP, impossible dans une interconnexion de réseaux.	Oui pas pour téléphones SIP, dans réseaux homogènes (uniquement systèmes OpenScape Business), seulement avec numérotation fermée, pas dans les réseaux non homogènes (avec OpenScape 4000 ou OpenScape Voice).
Support de SPE en réseaux	SPE est possible dans les réseaux. Utiliser DLS (pas DLI).	Oui Les clés et les certificats à déployer doivent être disponibles sur le DLS.
Alimentation centrale de plusieurs plates-formes différentes	non	Oui
Validation de la 2e interface LAN des téléphones système IP (mode PC Ethernet). Voir Configuration de base > Déploiement des paramètres du téléphone	Oui	Oui

Client de développement et licence (DLSC)

Pour être en mesure d'utiliser les fonctions DSL, par exemple le gestionnaire d'éléments, le système de communication doit accorder au DLS externe l'accès aux données de configuration. Le système de communication est ensuite exploité comme un Deployment et Licensing Client.

8.5.1 Comment configurer un serveur DLS externe dans le serveur DHCP interne

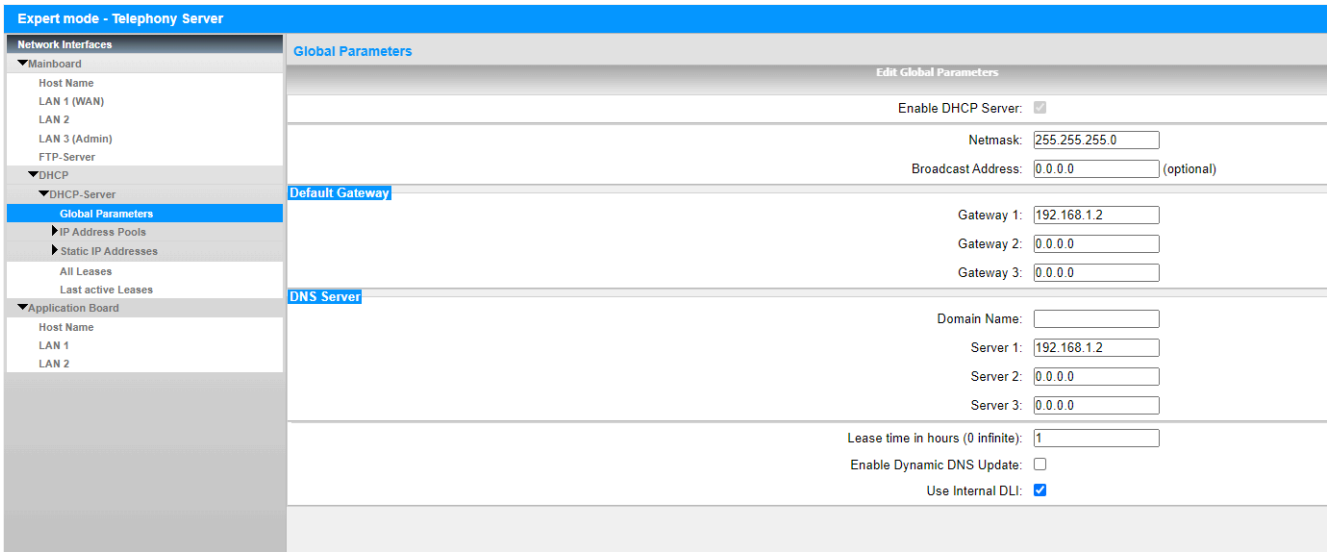
Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Interfaces réseau**.

3) Dans l'arborescence du menu, sélectionnez **Carte mère** > **DHCP** > **Serveur DHCP** > **Paramètres globaux**. La fenêtre **Modifier les paramètres généraux** s'affiche.



4) Décochez la case **Utiliser le DLI interne**.
5) Dans le champ **Adresse IP**, saisissez l'adresse IP permettant d'accéder au serveur.
6) Dans le champ **Port**, saisissez le port utilisé par le serveur DLS. Ce port doit être validé dans le pare-feu.
7) Cliquez sur **Appliquer**, puis sur **OK**.

8.5.2 Comment activer DLI interne

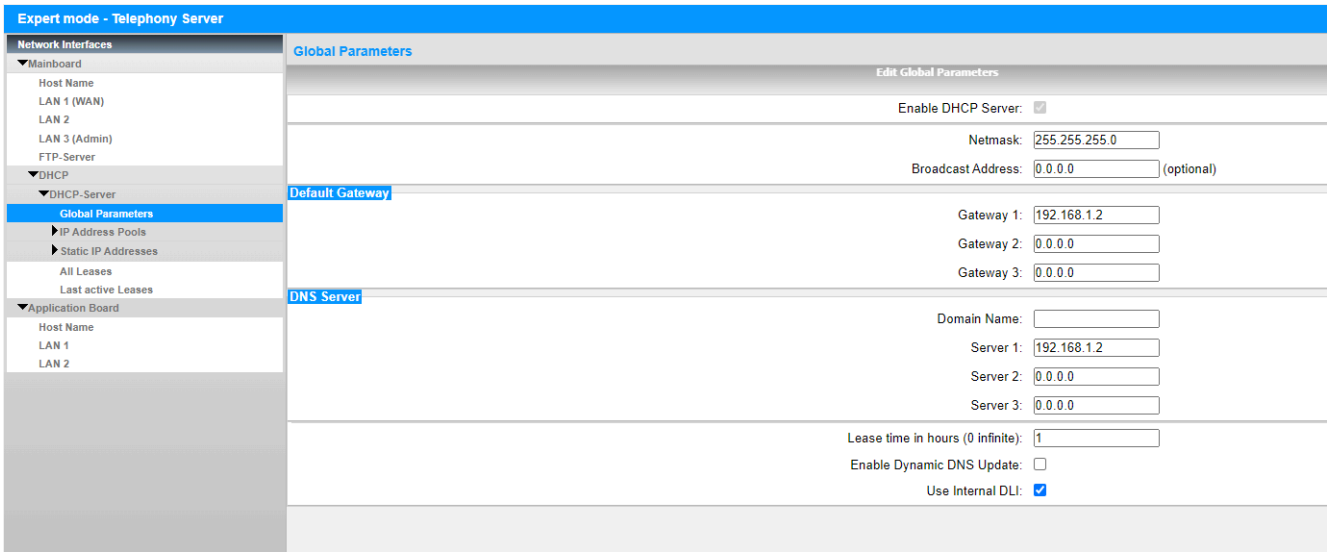
Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Interfaces réseau**.

3) Dans l'arborescence du menu, sélectionnez **Carte mère** > **DHCP** > **Serveur DHCP** > **Paramètres globaux**. La fenêtre **Modifier les paramètres généraux** s'affiche.



4) Cochez la case **Utiliser le DLI interne**. La case est cochée par défaut.
5) Cliquez sur **Appliquer**, puis sur **OK**.

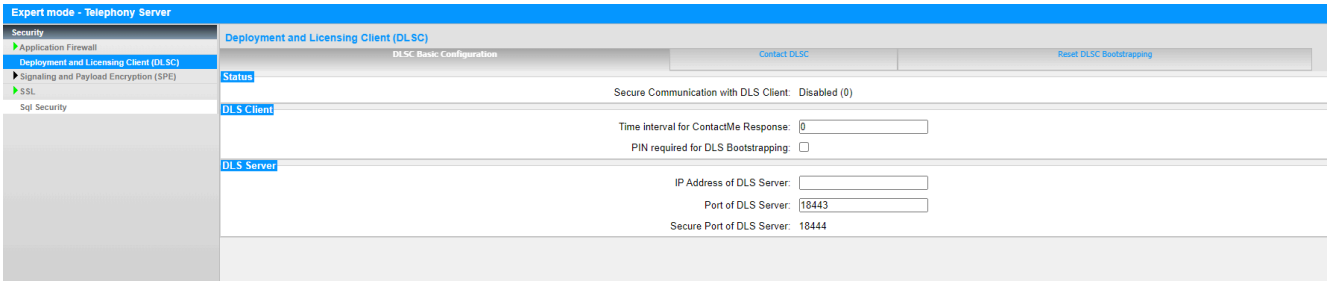
8.5.3 Comment configurer le système de communication comme client Deployment et Licensing

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, cliquez sur **Deployment and Licensing Client (DLSC)**.



4) Dans l'onglet **Configuration de base DLSC** de la zone **Serveur DLS**, saisissez l'adresse IP à laquelle le serveur DLS externe peut être joint dans le champ **Adresse IP du serveur DLS**.
5) Dans le champ **Port du serveur DLS**, saisissez le port utilisé par le serveur DLS. Les deux ports indiqués doivent être validés dans le pare-feu.
6) Cliquez sur **Appliquer**, puis sur **OK**.

9 Connexion à fournisseur de services

Le système de communication supporte la connexion aux réseaux de communication publics. Le raccordement au réseau IP permet l'accès à Internet et à la téléphonie Internet, l'accès réseau permet l'accès au réseau RNIS et au réseau analogique.

L'accès Internet est réalisé à l'aide d'un modem Internet ou d'un routeur Internet.

L'accès réseau RNIS est réalisé, pour les plates-formes matérielles, via la carte mère ou via des modules supplémentaires insérés. Sur un commutateur logiciel, l'accès réseau RNIS n'est pas possible.

L'accès réseau analogique nécessite sur les plates-formes matérielles un module enfichable supplémentaire. Sur un commutateur logiciel, l'accès réseau analogique n'est pas possible.

9.1 Accès Internet

Pour l'accès à Internet, une liaison large bande (raccordement DSL ou raccordement par câble) est nécessaire. Cela permet une transmission rapide de données dans le cadre de la bande passante disponible.

Accès Internet par connexion DSL

La liaison à large bande à Internet par DSL (Digital Subscriber Line) se fait par la ligne téléphonique classique. L'accès Internet peut être utilisé parallèlement au téléphone normal. Fax, téléphone analogique ou RNIS restent disponibles pendant la liaison DSL. Vous pouvez ainsi réaliser un accès Internet qui est disponible en permanence comme pour une ligne fixe (Flatrate).

Pour un accès Internet par DSL, vous avez besoin d'un raccordement téléphonique (analogique ou RNIS) et d'un fournisseur d'accès à Internet (FAI). Le FAI fournit un éclateur et un modem Internet ou un routeur Internet avec modem Internet intégré. L'éclateur répartit le signal en une partie DSL et une partie Téléphonie et restitue les signaux DSL au modem Internet.

Le système de communication peut être directement raccordé au modem Internet ou au routeur Internet avec modem Internet intégré. Dans le premier cas, les données d'accès du FAI doivent être entrées dans le système de communication ; dans le deuxième cas, le routeur Internet doit être connu du système de communication. Les données d'accès du ITSP sont enregistrées dans le routeur Internet.

Pour pouvoir utiliser la téléphonie Internet, vous avez besoin également d'un fournisseur de services de téléphonie sur Internet (ITSP, fournisseur SIP).

Accès Internet par câble

La liaison large bande à Internet par le câble se fait par le raccordement du câble TV. En plus du transfert des signaux TV, le raccordement de câble TV peut être utilisé pour l'accès à Internet et pour la téléphonie. Il est ainsi possible de surfer et téléphoner sans ligne téléphonique.

Pour un accès Internet par câble, vous avez besoin d'un câblo-opérateur qui offre cette fonctionnalité. Il est aussi également votre fournisseur d'accès à

Internet (FAI). Ce câblo-opérateur vous fournit un raccordement de câble avec un canal vers l'arrière et un modem câble qui transfère les données par le réseau câblé TV. Le raccordement de câble et le système de communication sont raccordés par Ethernet au modem câble. Le filtrage des données Internet est réalisé dans le modem câble lui-même.

Le système de communication peut être raccordé directement au modem câble ou bien à un routeur Internet qui est lui-même raccordé au modem câble. Dans les deux cas, le modem câble ou le routeur Internet doit être connu du système de communication.

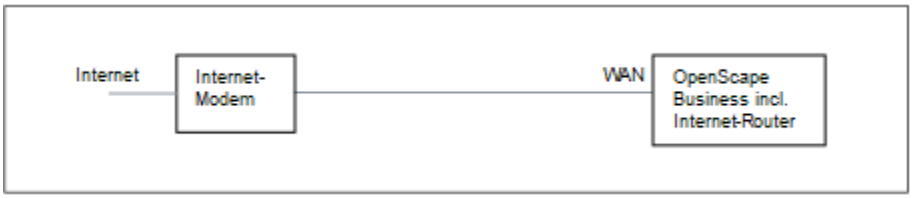
Pour pouvoir utiliser la téléphonie Internet, vous avez besoin également d'un fournisseur de services de téléphonie sur Internet (ITSP, fournisseur SIP).

Configuration de l'accès Internet

La configuration de l'accès Internet dans WBM est différente selon que l'accès Internet a déjà été paramétré dans un routeur extene ou qu'il passe par un modem Internet, ce qui nécessite le paramétrage au niveau de la WBM.

- **Accès Internet par un modem Internet** (**DSL sur port WAN directement**)

  Vous souhaitez exploiter directement le système de communication sur un modem Internet (DSL, Câble, UMTS, …). OpenScape Business a intégré le routeur Internet. Entrez directement dans le système de communication les données d'accès du fournisseur d'accès Internet (FAI) et utilisez le raccordement WAN du système de communication. Cette possibilité n'existe pas avec le commutateur logiciel.

  Vous disposez des possibilités suivantes :

  – Accès Internet par le FAI préconfiguré
  – Accès Internet par le FAI PPPoE par défaut
  – Accès Internet par le FAI PPTP par défaut

  Si votre FAI ne figure pas parmi les FAI préconfigurés, utilisez le FAI PPPoE ou PPTP par défaut.

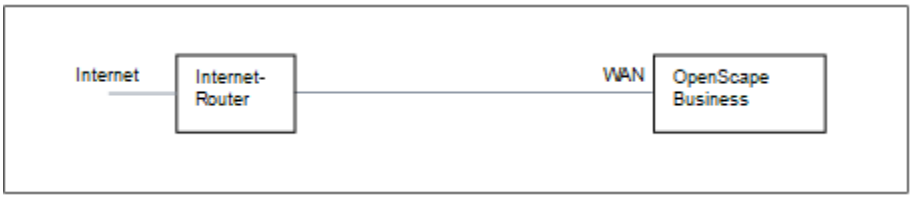
- **Accès Internet par un routeur Internet externe**

  Vous voulez exploiter le système de communication sur un routeur Internet externe. Le fournisseur de services Internet est déjà configuré sur le routeur Internet.

  Vous disposez des possibilités suivantes :

  – **Accès Internet par routeur Internet externe sur raccordement WAN**

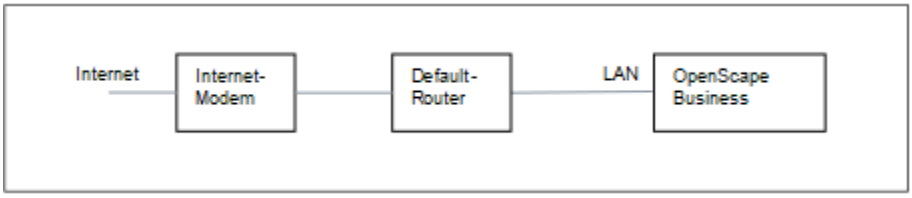
    (**TCP/IP sur port WAN via un routeur externe**)

    Pour cela, utilisez le raccordement WAN du système de communication. OpenScape Business utilise le routeur Internet ou bien fonctionne comme client DHCP. Cette possibilité est utilisable lorsque le routeur Internet se trouve sur un autre segment du réseau et dispose de son propre serveur DHCP.

  – **Accès Internet par routeur Internet externe sur raccordement LAN**

    (**TCP/IP sur port LAN via un routeur externe**)

    Pour cela, utilisez le raccordement LAN du système de communication. OpenScape Business connaît uniquement le routeur par défaut et pas l'infrastructure en arrière-plan. Pour activer la connexion avec le routeur Internet il faut indiquer au système de communication l'adresse IP du routeur par défaut et du serveur DNS.

- **Désactiver l'accès Internet** (Paramètre par défaut)

  Vous ne souhaitez pas utiliser Internet. Puis laissez l'accès Internet désactivé.

9.1.1 Accès Internet par routeur Internet externe

L'Assistant **Configuration Internet** vous permet de configurer votre accès Internet par un routeur Internet supplémentaire.

Pour configurer l'accès Internet, vous disposez des possibilités suivantes :

- **Accès Internet par routeur Internet externe sur raccordement LAN**

  Pour cela, utilisez le raccordement LAN du système de communication. Pour activer la connexion avec le routeur Internet il faut indiquer au système de communication l'adresse IP du routeur par défaut et du serveur DNS.

- **Accès Internet par routeur Internet externe sur raccordement WAN**

  Pour cela, utilisez le raccordement WAN du système de communication. Cette possibilité est utilisable lorsque le routeur Internet se trouve sur un autre segment du réseau et dispose de son propre serveur DHCP.

9.1.1.1 Comment configurer l'accès Internet par un routeur Internet externe avec raccordement LAN

Avec l'Assistant **Configuration Internet**, vous pouvez, en tant qu'administrateur, configurer l'accès Internet si le système de communication se trouve derrière un routeur Internet supplémentaire. Le système de communication et le routeur Internet se trouvent dans le même segment LAN. Pour cela, vous devez entrer l'adresse IP du routeur Internet et du serveur DNS.

Conditions préalables

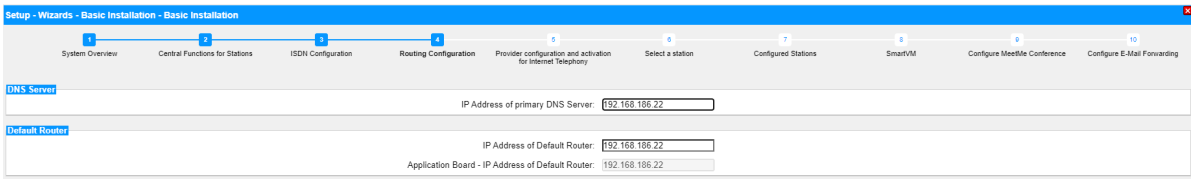
Vous êtes connecté à WBM avec le profil **Advanced**.

Pour OpenScape Business X : le système de communication est relié au réseau client via l'interface "LAN". La connexion ne doit pas être réalisée via l'interface "WAN".

Pour OpenScape Business S : le serveur Linux est connecté au réseau client via l'interface LAN de la carte réseau.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration Internet**.
4) Décochez la case **Pas d'accès Internet**.
5) Cochez **TCP/IP sur port LAN via un routeur externe** et cliquez sur **OK & Suivant**.



6) Dans le champ **Adresse IP du serveur DNS** entrez l'adresse IP du serveur DNS local (par ex. Routeur Internet) ou du serveur DNS Internet (par ex. pour la téléphonie Internet).
7) Dans **Adresse IP du routeur par défaut** entrez l'adresse IP du routeur Internet externe.
8) Cliquez sur **OK & Suivant** puis sur **Quitter**.

9.1.1.2 Comment configurer l'accès Internet par un routeur Internet externe par le raccordement WAN

Avec l'Assistant **Configuration Internet**, vous pouvez, en tant qu'administrateur, configurer l'accès Internet si le système de communication se trouve derrière un routeur Internet supplémentaire. Le système de communication et le routeur Internet doivent se trouver dans le même segment LAN.

Conditions préalables

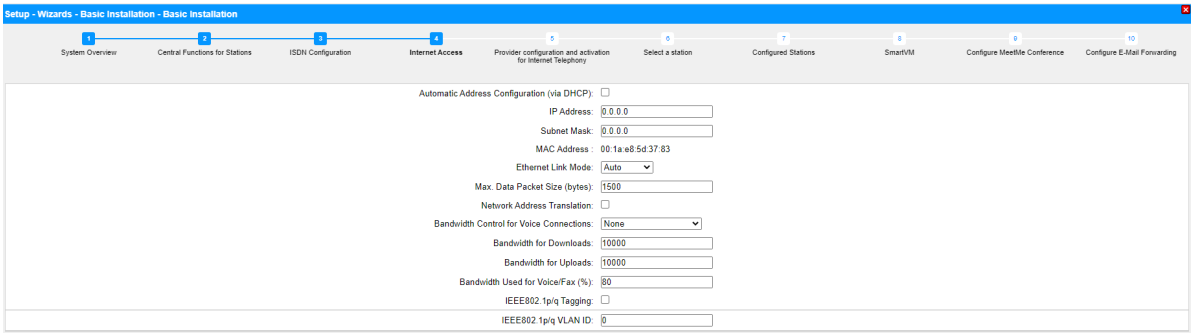
Vous êtes connecté à WBM avec le profil **Advanced**.

Le système de communication doit être connecté au segment LAN du réseau client où se trouve le routeur Internet, au moyen de l'interface "WAN".

Vous êtes dans la fenêtre **Configuration de l'accès Internet**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration Internet**.
4) Décochez la case **Pas d'accès Internet**.
5) Cochez le bouton d'option **TCP/IP sur port WAN via un routeur externe** et cliquez sur **OK&Suite**.



6) S'il est nécessaire de récupérer pour l'interface WAN les données spécifiques réseau à partir d'un serveur DHCP déjà activé, procédez comme indiqué ci-après.
   a) Cochez la case **Configuration automatique de l'adresse (via DHCP)**.
   b) Cochez la case **Accepter l'adresse IP du routeur par défaut**.
   c) Si nécessaire, cochez la case **Accepter Adresse IP du serveur DNS**.
   d) Si nécessaire, cochez la case **Accepter Adresse IP du serveur SNTP**.
7) S'il faut affecter une adresse IPO fixe à l'interface WAN :
   a) Décochez la case **Configuration automatique de l'adresse (via DHCP)**.
   b) Indiquez l' **Adresse IP** et le **Masque de réseau IP** souhaités de l'interface WAN.
8) Cochez la case **Conversion d'adresse réseau (NAT)**.
9) Si vous voulez utiliser en plus la téléphonie Internet, sélectionnez dans la liste déroulante **Gestion de la bande passante pour les connexions vocales** l'entrée **Liaison montante seulement** ou **Liaison montante**

et descendante selon les besoins. Si la bande passante de la liaison descendante est élevée et la bande passante de la liaison montante est parallèlement nasse, la gestion de la bande passante ne doit être activée que pour la liaison montante afin que ne soit pas réservée inutilement une bande passante descendante pour la transmission de la voix.

10) Dans **Bande passante pour les liaisons descendantes** et **Bande passante pour les liaisons montantes** indiquez la bande passante en kbit/s pour le téléchargement ou le chargement que votre fournisseur d'accès à Internet vous a fourni.
11) Cliquez sur **OK & Suivant** puis sur **Quitter**.

9.1.1.3 Comment configurer l'accès à Internet via un routeur Internet externe sur le LAN avec un port WAN dédié à l'ITSP

Conditions préalables

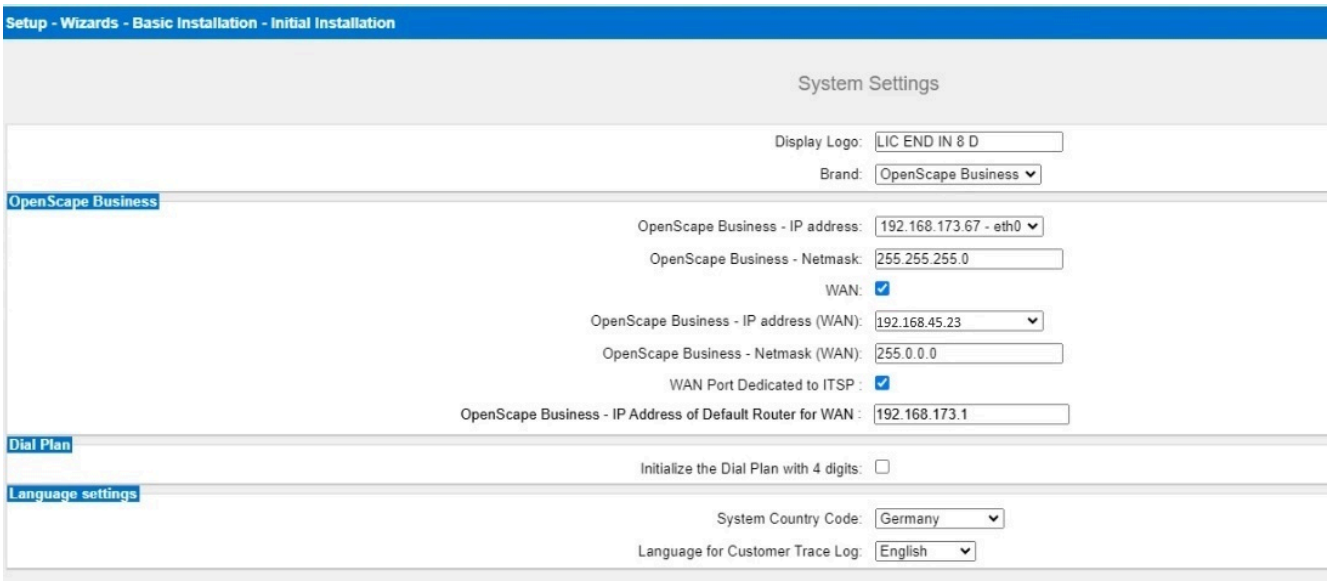
Vous avez créé une nouvelle interface réseau dans le SLES.

Vous êtes dans la fenêtre **Paramètres du système** de l'assistant d'**installation initiale**.

Veuillez noter que cette fonctionnalité ne s'applique qu'aux ITSP qui n'exigent pas l'utilisation de STUN dans les paramètres du fournisseur.

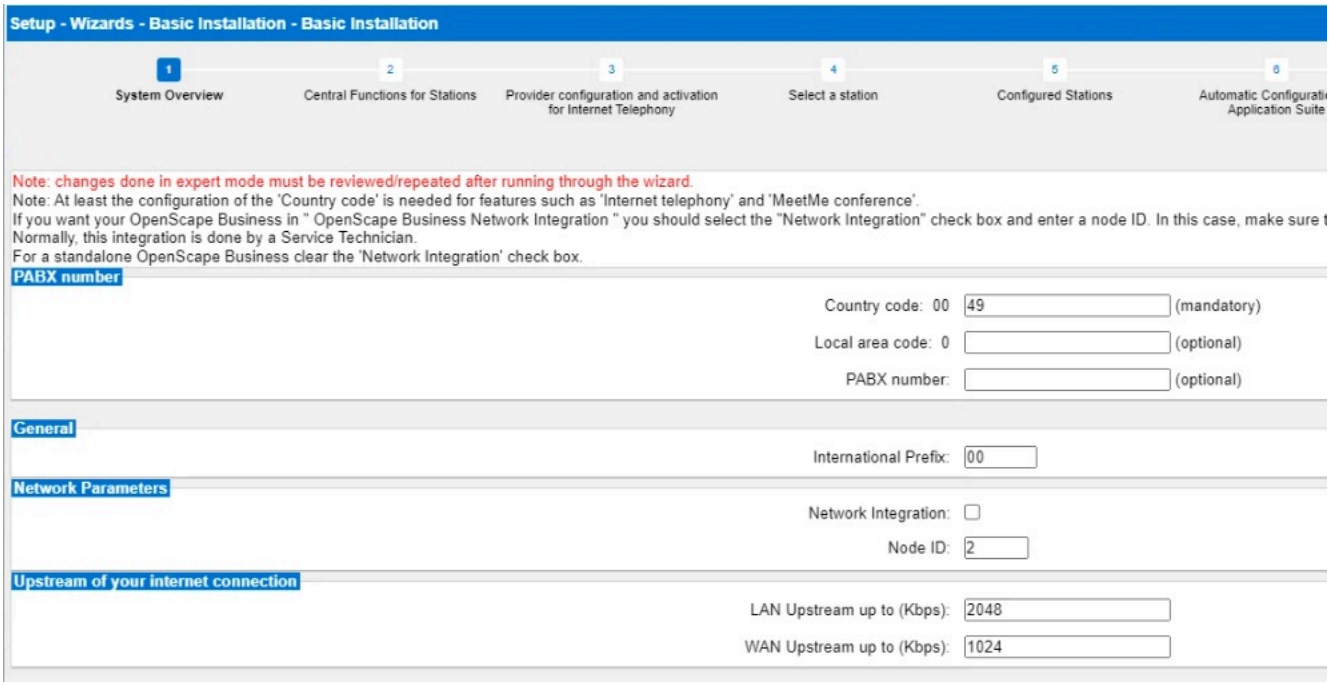
Étape par étape

1) Activez la case à cocher **WAN** et sélectionnez l'interface réseau appropriée. L'option **Interface WAN dédiée à l'ITSP** devient disponible.
2) Cliquez sur pour activer la case à cocher **Interface WAN dédiée à l'ITSP**.



3) Cliquez sur **OK & Suivant**.
4) Naviguez vers **Configuration > Installation de base** et exécutez l'assistant d'**installation de base**.

5) Configurez les valeurs maximales en amont dans les champs correspondants **LAN Upstream jusqu'à (Kbps)** et **WAN Upstream jusqu'à (Kbps)**.



6) Cliquez sur **OK & Suivant**.

7) Après avoir appliqué la configuration, un redémarrage du système est nécessaire.

9.1.2 Accès Internet par un modem Internet

Avec l'Assistant **Configuration Internet**, vous configurez votre accès Internet par un modem Internet. Pour cela, le raccordement WAN du système de communication est directement raccordé à un modem Internet. Vous pouvez utiliser un FAI préconfiguré dans le système de communication ou un type de FAI par défaut (le type doit être demandé au FAI).

Pour configurer l'accès Internet, vous disposez des possibilités suivantes :

- **Configurer l'accès Internet par le FAI préconfiguré**

  Vous utilisez un FAI préconfiguré dans le système de communication. Vous pouvez alors sélectionner dans une liste votre FAI préconfiguré.
- **Configurer l'accès Internet par le FAI par défaut PPPoE**

  Vous utilisez le type de FAI par défaut **Fournisseur PPPoE**. Demandez les paramètres nécessaires à votre FAI.
- **Configurer l'accès Internet par le FAI par défaut PPTP**

  Vous utilisez le type de FAI par défaut **Fournisseur PPTP**. Demandez les paramètres nécessaires à votre FAI.

Coupure de la liaison en fonction du modèle tarifaire

En fonction du modèle tarifaire, il est possible de définir si la liaison avec le FAI doit être conservée en cas d'inactivité ou pas.

- Avec le modèle tarifaire Illimité, aucune coupure de la liaison Internet ne doit avoir lieu en cas d'inactivité. De nombreux FAI nécessitent une coupure forcée toutes les 24 heures. L'heure à laquelle la liaison doit être coupée peut être indiquée.
- Avec le modèle tarifaire Forfait, la liaison Internet doit être coupée en cas d'inactivité. Le délai d'inactivité au bout duquel la liaison doit être coupée (par ex. 60 secondes) peut être indiquée. Lors de la prochaine demande Internet, la liaison est automatiquement rétablie. Si VPN est configuré, la connexion ne doit pas être coupée par inactivité - il faut ici sélectionner le modèle de forfait.

Remarque : Des programmes ou services du réseau peuvent établir automatiquement une liaison Internet et provoquer ainsi en cas de tarif forfaitaire des coûts de communication supplémentaires.

Bande passante

Le FAI fournit pour la liaison montant et la liaison descendante des données des bandes passantes différentes. La bande passante est indiquée en kbit/s. Si en plus la téléphonie sur Internet est utilisée, la transmission de la voix et le transfert de données se partagent la bande passante. Par conséquent, il est conseillé de réserver une bande passante suffisamment élevée pour une bonne qualité vocale de la transmission vocale. Toutefois, en cas de transfert de la voix intensif, cela peut conduire à des goulets d'étrangement pour le transfert de données (par ex. téléchargements plus lents).

Vous pouvez sélectionner si la gestion de la bande passante pour les liaisons vocales doit être active uniquement pour la liaison montante ou pour la liaison montante et descendante. Si la bande passante de la liaison descendante est élevée et la bande passante de la liaison montante est parallèlement nasse, la gestion de la bande passante ne doit être activée que pour la liaison montante afin que ne soit pas réservée inutilement une bande passante descendante pour la transmission de la voix.

Remarque : Pour une communication Internet, une bande passante d'environ 128 kbit/s est réservée.

9.1.2.1 Comment configurer l'accès Internet via un FAI préconfiguré

L'Assistant **Configuration Internet** vous permet de configurer votre accès Internet par un fournisseur d'accès à Internet FAI préconfiguré dans le système de communication.

Conditions préalables

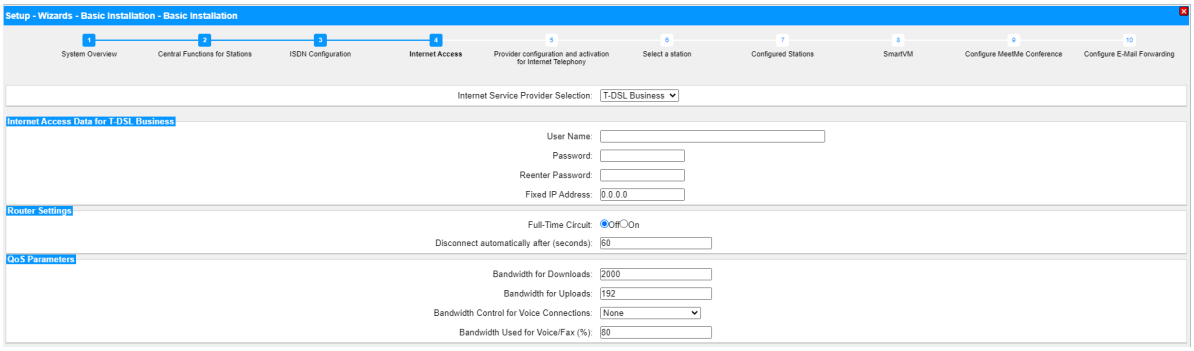
Vous êtes connecté à WBM avec le profil **Advanced**.

Vous disposez des données d'accès Internet de votre FAI (par ex. ID utilisateur, mot de passe).

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration Internet**.
4) Décochez la case **Pas d'accès Internet**.
5) Cochez **DSL sur port WAN directement** et cliquez sur **OK & Suivant**.



6) Dans la liste déroulante **Sélection de fournisseur de service** sélectionnez votre ISP.
7) Entrez dans la zone **Données d'accès Internet pour...** les données d'accès que vous avez reçues de votre FAI. Les champs de cette zone sont fonction du fournisseur. Lors de l'entrée des données, veillez à entrer correctement les majuscules et les minuscules.
8) Sélectionnez une des deux options suivantes dans la zone **Paramètres de routeur** sous **Liaison permanente**, en fonction de votre modèle tarifaire :
   - Si votre modèle de tarif correspond à un forfait, activez le champ d'option **Activé**. Dans **Coupure forcée à (h:mn)**, définissez l'heure à laquelle la connexion Internet doit être coupée (par ex. 04:59).
   - Si votre modèle de tarif correspond à un tarif en fonction du temps, activez le champ d'option **Désactivé**. Dans le champ **Couper automatiquement au bout de (secondes)**, entrez la durée d'inactivité au bout de laquelle la liaison doit être coupée (par ex. 60 secondes).
9) Paramétrez dans la zone **Paramètres QoS** les valeurs suivantes :
   a) Dans **Bande passante pour les liaisons descendantes** et **Bande passante pour les liaisons montantes** indiquez la bande passante en kbit/s pour le téléchargement ou le chargement que votre FAI vous a fournie.
   b) Si vous voulez utiliser en plus la téléphonie Internet, sélectionnez dans la liste déroulante **Gestion de la bande passante pour les connexions vocales** l'entrée **Liaison montante seulement** ou **Liaison montante et descendante** selon les besoins. Dans **Bande passante pour les connexions voix/fax (%)**, entrez en pourcentage quelle bande passante doit être réservée pour les liaisons voix et fax (valeur par défaut : 80%).
10) Cliquez sur **OK&Suivant**. Le système ouvre la fenêtre **Configurer le compte DynDNS**.

11) Si vous voulez utiliser VPN ou l'accès distant et que vous ne disposez pas d'une adresse IP publique statique, vous devez avoir demandé un compte DynDNS (par ex. auprès de dyndns.org) et le configurer.

a) Si le fournisseur DynDNS de votre choix figure dans la liste déroulante **Nom de domaine**, sélectionnez-le à partir de la liste (par ex. dyndns.org).

b) Si le fournisseur DynDNS de votre choix ne figure pas dans la liste déroulante **Nom de domaine**, cochez la case **Domaine défini par l'utilisateur**. Dans le champ **Nom de domaine**, indiquez le fournisseur DynDNS souhaité et dans le champ **Mise à jour-URL** l'URL de mise à jour du fournisseur DynDNS. La configuration de cette URL dépend du fournisseur DynDNS. En plus, les paramètres spécifiques client (en *caractères italiques* dans l'exemple) doivent être complétés.

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Entrez le **Nom utilisateur** et le **Mot de passe** de votre compte DynDNS.

d) Dans le champ **Nom d'hôte**, entrez le nom d'hôte que vous a attribué votre fournisseur DynDNS sans le nom de domaine, par ex. myhost. Votre nom de domaine complet est alors par ex. myhost.dyndns.org.

e) Testez le compte DynDNS avec **Test connexion**.

f) Une fois le test effectué avec succès, cliquez sur **OK**.

g) Cliquez sur **OK&Suivant**.

12) Si vous disposez d'une adresse IP publiques statique ou que vous ne voulez pas utiliser VPN ou l'accès distant, cliquez sur **Pas de DynDNS**.

13) Cliquez sur **Quitter**. Le système de communication effectue ensuite un redémarrage.

9.1.2.2 Comment configurer l'accès Internet via un FAI PPPoE par défaut

L'Assistant **Configuration Internet** vous permet de configurer votre accès Internet par le fournisseur d'accès à Internet par défaut PPPoE.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Vous disposez des données d'accès Internet suivantes de votre FAI :

Champ	Description	Valeur du FAI
Paramètres IP (uniquement pour adresse IP fixe)		
Adresse IP partenaire de la connexion PPP	Adresse IP du serveur de votre FAI	
Adresse IP locale de la connexion PPP	Adresse IP qui vous a été communiquée par le FAI pour l'accès Internet	
Authentification (par PAP ou CHAP). PAP n'est presque plus utilisé car l'authentification n'est pas cryptée.		
Nom d'utilisateur PPP	Nom de l'utilisation de la liaison PPP qui vous a été attribuée par le FAI.	

Champ	Description	Valeur du FAI
Mode d'authentification PAP	Mode d'authentification pour la connexion PPP via PAP : **PAP Client**, **PAP Host** ou **Non utilisé**.	
Mot de passe PAP	Mot de passe pour l'authentification par PAP qui vous a été attribué par le FAI	
Mode d'authentification CHAP	Mode d'authentification pour la connexion PPP via CHAP : **CHAP Client**, **CHAP Host**, **CHAP Client et Host** ou **Non utilisé**.	
Mot de passe CHAP	Mot de passe pour l'authentification par CHAP qui vous a été attribué par le FAI	
Paramètres QoS de l'interface		
Bande passante pour les liaisons descendantes	Valeur de bande passante totale en kbit/s pour le téléchargement à partir du FAI.	
Bande passante pour les liaisons montantes	Valeur de bande passante totale en kbit/s pour le transfert au FAI.	

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration Internet**.
4) Décochez la case **Pas d'accès Internet**.
5) Activez le bouton radio **DSL sur port WAN directement** et cliquez sur **OK & Suivant**.
6) Sélectionnez dans la liste déroulante **Utiliser le WAN comme** le type de FAI par défaut **Fournisseur-PPPoE**.
7) Dans la zone **Paramètres IP**, cochez la case **Paramètres IP** uniquement si une adaptation est demandée par le FAI. Dans les champs **Adresse IP partenaire de la connexion PPP**, **Adresse IP locale de la connexion PPP** et **Longueur de paquet de données maxi. (octets)**, entrez les valeurs que vous avez reçues de votre FAI. Sélectionnez dans la liste déroulante **Négociation de l'adresse IP** l'entrée **Utiliser l'adresse IP configurée**.
8) Sélectionnez une des deux options suivantes dans la zone **Paramètres de routeur** sous **Liaison permanente**, en fonction de votre modèle tarifaire :
   - Si votre modèle de tarif correspond à un forfait, activez le champ d'option **Activé**. Dans le champ **Coupure forcée à (h:mn)**, définissez l'heure à laquelle la connexion Internet doit être coupée (par ex. 04:59).
   - Si votre modèle de tarif correspond à un tarif en fonction du temps, activez le champ d'option **Désactivé**. Dans le champ **Couper automatiquement au bout de (secondes)**, entrez la durée d'inactivité au bout de laquelle la liaison doit être coupée (par ex. 60 secondes).

9) Le paramétrage dans **Authentification** dépend de la nécessité d'authentifier ou non le FAI via PPP.

- Authentification requise par le FAI : Assurez-vous que la case à cocher **Authentification PPP** est activée. Entrez comme nom d'utilisateur PPP le nom de l'accès Internet du FAI. La norme habituelle est le mode d'authentification **Client CHAP**.
- Authentification non requise par le FAI : Assurez-vous que la case à cocher Authentification PPP est désactivée.

10) Si vous voulez utiliser NAT, vous devez, dans la zone **Traduction d'adresses** cocher la case **NAT** (cochée par défaut).

11) Dans la zone **Paramètres QoS de l'interface**, paramétrez les valeurs suivantes :

a) Dans **Bande passante pour les liaisons descendantes** et **Bande passante pour les liaisons montantes** indiquez la bande passante en kbit/s pour le téléchargement ou le chargement que votre FAI vous a fournie.

b) Si vous voulez utiliser en plus la téléphonie Internet, sélectionnez dans la liste déroulante **Gestion de la bande passante pour les connexions vocales** l'entrée **Liaison montante seulement** ou **Liaison montante et descendante** selon les besoins. Dans **Bande passante pour les connexions voix/fax (%)**, entrez en pourcentage quelle bande passante doit être réservée pour les liaisons voix et fax (valeur par défaut : 80%).

12) Cliquez sur **OK & Suivant**. Le système ouvre la fenêtre **Configurer le compte DynDNS**.

13) Si vous voulez utiliser VPN ou l'accès distant et que vous ne disposez pas d'une adresse IP publique statique, vous devez avoir demandé un compte DynDNS (par ex. auprès de dyndns.org) et le configurer.

a) Si le fournisseur DynDNS de votre choix figure dans la liste déroulante **Nom de domaine**, sélectionnez-le à partir de la liste (par ex. dyndns.org).

b) Si le fournisseur DynDNS de votre choix ne figure pas dans la liste déroulante **Nom de domaine**, cochez la case **Domaine défini par l'utilisateur**. Dans le champ **Nom de domaine**, indiquez le fournisseur DynDNS souhaité et dans le champ **Mise à jour-URL** l'URL de mise à jour du fournisseur DynDNS. La configuration de cette URL dépend du fournisseur DynDNS. En plus, les paramètres spécifiques client (en *caractères italiques* dans l'exemple) doivent être complétés.

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Entrez le **Nom utilisateur** et le **Mot de passe** de votre compte DynDNS.

d) Dans le champ **Nom d'hôte**, entrez le nom d'hôte que vous a attribué votre fournisseur DynDNS sans le nom de domaine, par ex. myhost. Votre nom de domaine complet est alors par ex. myhost.dyndns.org.

e) Testez le compte DynDNS avec **Test connexion**.

f) Une fois le test effectué avec succès, cliquez sur **OK**.

g) Cliquez sur **OK & Suivant**.

14) Si vous disposez d'une adresse IP publique statique ou si vous ne voulez pas utiliser un VPN ou l'accès distant, cliquez sur **Pas de DynDNS**.

15) Cliquez sur **Terminer**.

9.1.2.3 Comment configurer l'accès Internet via un FAI PPTP par défaut

L'Assistant **Configuration Internet** vous permet de configurer votre accès Internet par le fournisseur d'accès à Internet par défaut PPTP.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Vous disposez des données d'accès Internet suivantes de votre FAI :

Champ	Description	Valeur du FAI
Paramètres IP (uniquement pour adresse IP fixe)		
Adresse IP partenaire de la liaison PPP	Adresse IP du serveur de votre FAI	
Adresse IP locale de la connexion PPP	Adresse IP qui vous a été communiquée par le FAI pour l'accès Internet	
Paramètres PPTP		
Adresse IP locale de la connexion de contrôle	Adresse IP qui vous a été attribuée par le FAI pour la liaison PPTP. La valeur par défaut est : 10.0.0.140.	
Adresse IP partenaire de la connexion de contrôle	Adresse IP du serveur de votre FAI pour la connexion PPTP. La valeur par défaut est : 10.0.0.138.	
Masque de réseau partenaire pour la connexion de contrôle	Masque de réseau qui vous a été attribué par le FAI pour la liaison PPTP. La valeur par défaut est : 255.255.255.248.	
Authentification (par PAP ou CHAP). PAP n'est presque plus utilisé car l'authentification n'est pas cryptée.		
Nom d'utilisateur PPP	Nom de l'utilisation de la liaison PPP qui vous a été attribuée par le FAI.	
Mode d'authentification PAP	Mode d'authentification pour la liaison PPP par PAP : **Client PAP**, **Hôte PAP** ou **Non utilisé**.	
Mot de passe PAP	Mot de passe pour l'authentification par PAP qui vous a été attribué par le FAI.	
Mode d'authentification CHAP	Mode d'authentification pour la liaison PPP par CHAP : **Client CHAP**, **Hôte CHAP**, **Client et hôte CHAP** ou **Non utilisé**.	
Mot de passe CHAP	Mot de passe pour l'authentification par CHAP qui vous a été attribué par le FAI.	
Paramètres QoS de l'interface		
Bande passante pour les liaisons descendantes	Valeur de bande passante totale en kbit/s pour le téléchargement à partir du FAI.	

Champ	Description	Valeur du FAI
Bande passante pour les liaisons montantes	Valeur de bande passante totale en kbit/s pour le transfert au FAI.	

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration Internet**.
4) Décochez la case **Pas d'accès Internet**.
5) Cochez **DSL sur port WAN directement** et cliquez sur **OK & Suivant**.
6) Sélectionnez dans la liste déroulante **Utiliser le WAN comme** le type de FAI par défaut **Fournisseur-PPTP**.
7) Dans la zone **Paramètres IP**, cochez la case **Paramètres IP** uniquement si une adaptation est demandée par le FAI. Dans les champs **Adresse IP partenaire de la connexion PPP**, **Adresse IP locale de la connexion PPP** et **Longueur de paquet de données maxi. (octets)**, entrez les valeurs que vous avez reçues de votre FAI. Sélectionnez dans la liste déroulante **Négociation de l'adresse IP** l'entrée **Utiliser l'adresse IP configurée**.
8) Entrez dans la zone **Paramètres PPTP** les valeurs que vous avez reçues de votre FAI.
9) Si vous avez un forfait horaire comme modèle tarifaire, cochez la case **Mode Short-Hold**. Entrez dans **Durée Short-Hold (s)** le délai d'inactivité au bout duquel la liaison doit être coupée (par ex. 60 secondes).
10) Le paramétrage dans **Authentification** dépend de la nécessité d'authentifier ou non le FAI via PPP.
    - L'authentification est demandée par le FAI : vérifiez que la case **Authentification PPP** est bien cochée. Entrez comme nom d'utilisateur PPP le nom de l'accès Internet du FAI. Effectuez les paramétrages PAP et CHAP tels que vous les avez reçus de votre FAI.
    - L'authentification n'est pas demandée par le FAI : vérifiez que la case Authentification PPP est bien décochée.
11) Si vous voulez utiliser NAT, vous devez, dans la zone **Traduction d'adresses** cocher la case **NAT** (cochée par défaut).
12) Dans la zone **Paramètres QoS de l'interface**, paramétrez les valeurs suivantes :
    a) Dans **Bande passante pour les liaisons descendantes** et **Bande passante pour les liaisons montantes** indiquez la bande passante en kbit/s pour le téléchargement ou le chargement que votre FAI vous a fournie.
    b) Si vous voulez utiliser en plus la téléphonie Internet, sélectionnez dans la liste déroulante **Gestion de la bande passante pour les connexions vocales** l'entrée **Liaison montante seulement** ou **Liaison montante et descendante** selon les besoins. Dans **Bande passante pour les connexions voix/fax (%)**, entrez en pourcentage quelle bande passante doit être réservée pour les liaisons voix et fax (valeur par défaut : 80%).
13) Cliquez sur **OK & Suivant**. Le système ouvre la fenêtre **Configurer le compte DynDNS**.

14) Si vous voulez utiliser VPN ou l'accès distant et que vous ne disposez pas d'une adresse IP publique statique, vous devez avoir demandé un compte DynDNS (par ex. auprès de dyndns.org) et le configurer.

a) Si le fournisseur DynDNS de votre choix figure dans la liste déroulante **Nom de domaine**, sélectionnez-le à partir de la liste (par ex. dyndns.org).

b) Si le fournisseur DynDNS de votre choix ne figure pas dans la liste déroulante **Nom de domaine**, cochez la case **Domaine défini par l'utilisateur**. Dans le champ **Nom de domaine**, indiquez le fournisseur DynDNS souhaité et dans le champ **Mise à jour-URL** l'URL de mise à jour du fournisseur DynDNS. La configuration de cette URL dépend du fournisseur DynDNS. En plus, les paramètres spécifiques client (en *caractères italiques* dans l'exemple) doivent être complétés.

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Entrez le **Nom utilisateur** et le **Mot de passe** de votre compte DynDNS.

d) Dans le champ **Nom d'hôte**, entrez le nom d'hôte que vous a attribué votre fournisseur DynDNS sans le nom de domaine, par ex. myhost. Votre nom de domaine complet est alors par ex. myhost.dyndns.org.

e) Testez le compte DynDNS avec **Test connexion**.

f) Une fois le test effectué avec succès, cliquez sur **OK**.

g) Cliquez sur **OK & Suivant**.

15) Si vous disposez d'une adresse IP publiques statique ou que vous ne voulez pas utiliser VPN ou l'accès distant, cliquez sur **Pas de DynDNS**.

16) Cliquez sur **Terminer**. Le système de communication effectue ensuite un redémarrage.

9.1.3 Interface WAN

Les WAN (**W**ide **A**rea **N**etwork) sont utilisés pour mettre en réseau différents LAN (**L**ocal **A**rea **N**etwork), mais aussi des ordinateurs. Il est possible de raccorder sur l'interface WAN un modem Internet our l'accès à Internet.

L'interface WAN ne doit pas être utilisée pour la mise en réseau de noeuds de réseau et pour la connexion d'abonnés IP ou de clients IP.

9.1.4 DynDNS

DynDNS (Dynamic Domain Name Service) est un service Internet qui attribue un nom DNS fixe à une adresse IP qui change de manière dynamique.

OpenScape Business X fournit le service DynDNS lorsque un modem Internet est raccordé au port WAN d'OpenScape Business X et que le système de communication est utilisé comme routeur Internet. Si ce n'est pas le cas, DynDNS est paramétré dans le routeur Internet externe, dans l'infrastructure du client.

Nom DNS

Un client qui est raccordé à une adresse IP dynamique à Internet peut être joint grâce à DynDNS toujours par le même nom, le nom DNS. Pour cela, un compte DynDNS chez un fournisseur DynDNS (par ex. www.dyndns.org) est nécessaire. Si une nouvelle adresse IP est affectée au système de communication (par ex. par le fournisseur d'accès à Internet), cette adresse IP est automatiquement envoyée au fournisseur DynDNS et enregistrée dans le compte DynDNS. L'intervalle de temps durant lequel a lieu cette actualisation est paramétrable. Si un nom DNS est joint, il est converti par une demande au fournisseur DynDNS en l'adresse IP valide momentanément. Le nom DNS complet (également appelé nom de domaine) se compose du nom d'hôte choisi librement (par ex. myhost) et du fournisseur DynDNS sélectionné (par ex. dyndns.org), par ex. myhost.dyndns.org. Vous trouverez plus d'informations à l'adresse Internet suivante :

`http://www.dyndns.org/services/dyndns`

Avec DynDNS, il est aussi possible d'établir un réseau privé virtuel (VPN) par un fournisseur d'accès à Internet qui fournit des adresses IP dynamiques. Ainsi, les télétravailleurs peuvent par ex. accéder au réseau interne par Internet. Vous trouverez des informations supplémentaires dans Virtual Private Network VPN .

Echangeur de messagerie

L'entrée d'échangeur de messagerie (enregistrement MX) indique au sein du services DNS (Domain Name Service) à quelle adresse IP les e-mails pour le nom de domaine configuré (par ex. myhost.dyndns.org) doivent être envoyés. Derrière l'adresse IP indiquée doit se trouver un serveur de messagerie (échangeur de messagerie). Une adresse e-mail pour ce nom de domaine pourrait par ex. avoir l'aspect suivant : mymail@myhost.dyndns.org.

Grâce à la fonction Sauvegarde MX, les e-mails qui n'ont pas pu être remis à l'échangeur de messagerie indiqué ci-dessus (parce que ce dernier est par ex. temporairement indisponible), sont enregistrés et ils sont remis dès que l'échangeur de messagerie est à nouveau disponible.

9.1.4.1 Comment configurer le service DynDNS

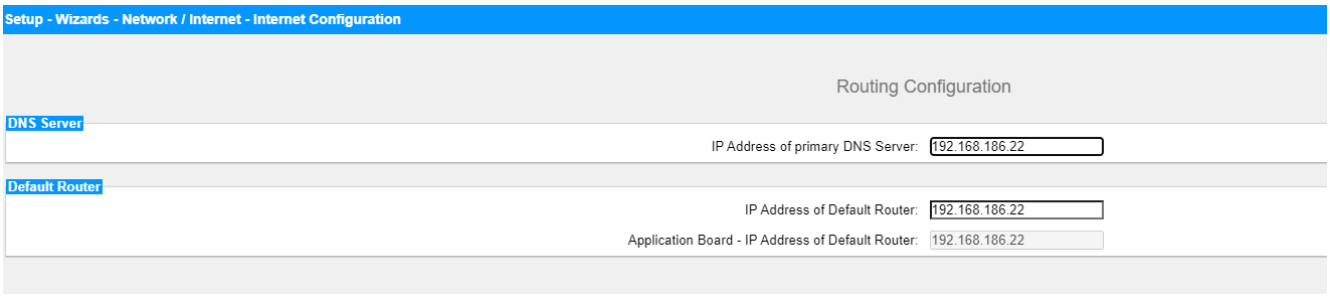
Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **DynDNS**.

4) Cliquez sur **Temporisation pour l'actualisation des noms DNS**.



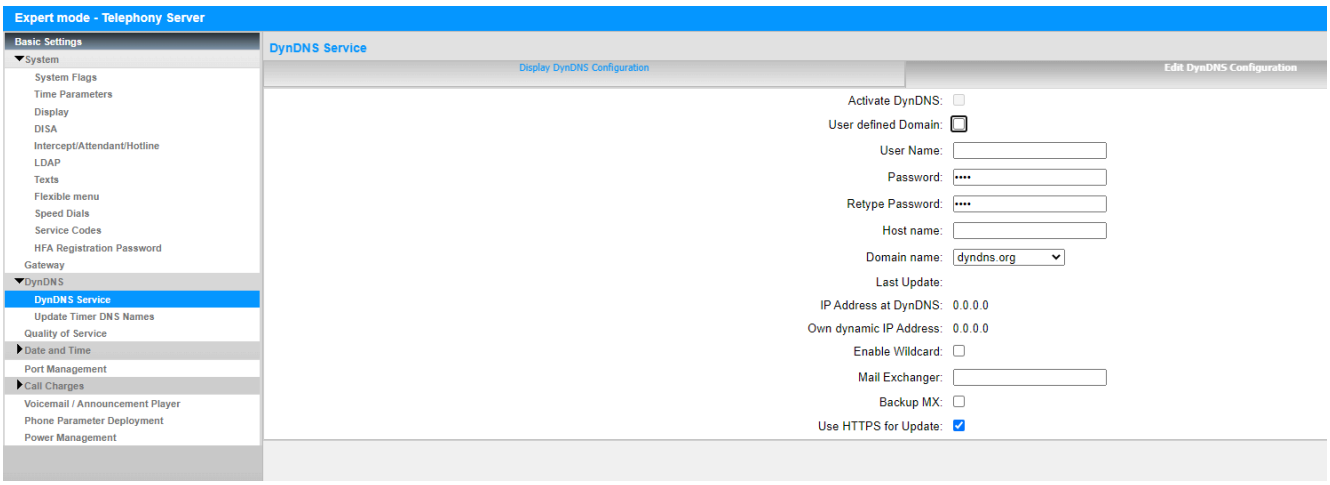
5) Activez le bouton radio **Actualiser les noms DNS**.

6) Cette valeur de temporisation n'est valable que pour le VPN : dans le champ **Valeur de temporisation pour l'actualisation des noms DNS (s)**, indiquez le temps en secondes à l'issue duquel la composante VPN vérifie si les noms DNS utilisés sont résolus en nouvelles adresses IP dans la configuration VPN (VPN avec adresses IP dynamiques). Dans ce cas, VPN est reconfiguré avec les nouvelles adresses IP.

   La valeur par défaut de ce champ est `180`, ce qui correspond à un intervalle d'actualisation de 3 minutes.

7) Dans l'arborescence du menu, cliquez sur **Service DynDNS**.

8) Cliquez sur l'onglet **Modifier la configuration DynDNS**.



9) Cochez la case **Activer DynDNS**.

10) Si le fournisseur DynDNS de votre choix figure dans la liste déroulante **Nom de domaine**, sélectionnez-le à partir de la liste (par ex. dyndns.org).

11) Si le fournisseur DynDNS de votre choix ne figure pas dans la liste déroulante **Nom de domaine**, cochez la case **Domaine défini par l'utilisateur**. Dans le champ **Nom de domaine**, indiquez le fournisseur DynDNS souhaité et dans le champ **Mise à jour-URL** l'URL de mise à jour du fournisseur DynDNS. La configuration de cette URL dépend

du fournisseur DynDNS. De plus, les paramètres propres au client (en *caractères italiques* dans l'exemple) doivent être complétés.

`http://www.anydns.info/update.php?`
`user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`

Exemple d'une URL Mise à jour avec authentification cryptée Base64 :

`https://<b64><username>:<pass></`
`b64>@members.dyndns.org/nic/update?`
`hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG&backmx=NOC`

<b64>...</b64> paramètres codés pour Base64

12) Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur de votre compte DynDNS auprès du fournisseur DynDNS.

13) Dans les champs **Mot de passe** et **Répéter le mot de passe**, saisissez le mot de passe de votre compte DynDNS auprès du fournisseur DynDNS.

14) Dans le champ **Nom d'hôte**, entrez le nom d'hôte que vous a attribué votre fournisseur DynDNS sans le nom de domaine, par ex. myhost. Votre nom de domaine complet est alors par ex. myhost.dyndns.org.

15) Il est visible uniquement pour les fournisseurs DynDNS inclus dans la liste déroulante **Nom de domaine** : Si vous souhaitez que les requêtes vers un nom de domaine subordonné tel que any.myhost.dyndns.org soient également acceptées, activez le bouton radio **Activer le joker**.

16) Il est visible uniquement pour les fournisseurs DynDNS inclus dans la liste déroulante **Nom de domaine** : Si vous souhaitez utiliser une connexion sécurisée avec le fournisseur DynDNS pour mettre à jour l'adresse IP, activez le bouton radio **Utiliser HTTPS pour l'actualisation**.

17) Cliquez sur **Appliquer**, puis sur **OK**.

9.1.4.2 Comment définir l'échangeur de messagerie

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

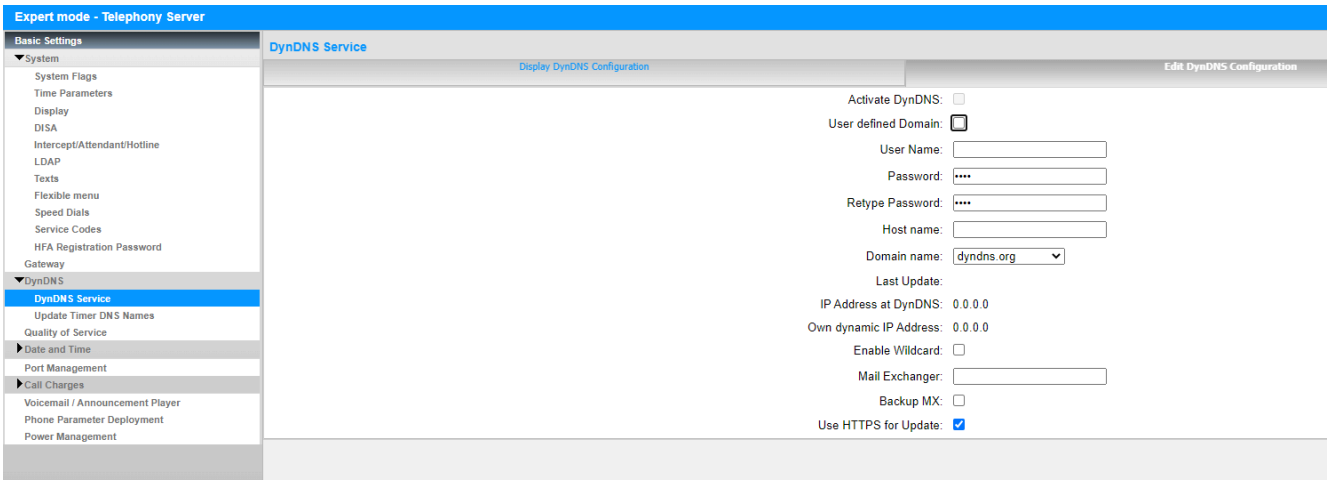
1) Dans la barre de navigation, cliquez sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.

3) Dans l'arborescence du menu, cliquez sur **DynDNS**.

4) Cliquez sur **Service DynDNS**.

5) Cliquez sur l'onglet **Modifier la configuration DynDNS**.



6) Dans le champ **Échangeur de messagerie**, saisissez l'adresse IP du serveur de messagerie (entrée de l'échangeur de messagerie ou enregistrement MX).
7) Si besoin est, activez l'option **Sauvegarde MX**.
8) Cliquez sur **Appliquer**, puis sur **OK**.

9.2 Accès au CO via ITSP

Pour passer des appels via Internet, vous aurez besoin d'un accès à un fournisseur de services de téléphonie sur Internet (ITSP, fournisseur SIP). Pour ce faire, il faut demander une connexion de téléphonie sur Internet et un compte utilisateur auprès du fournisseur de services de téléphonie sur Internet.

Connexion au fournisseur de services de téléphonie sur IP (ITSP)

Le système de communication utilise les options décrites dans la section « Accès Internet » pour atteindre le fournisseur de services de télécommunications (OpenScape Business X : via LAN ou WAN / OpenScape Business S : exclusivement via LAN).

L'accès ITSP est basé sur le protocole SIP (Session Initiation Protocol) pour la signalisation et le protocole RTP (Realtime Transport Protocol) pour la voix et les données.

Les fournisseurs de services de téléphonie sur Internet n'offrent pas toujours la même gamme de fonctionnalités SIP. Par conséquent, seuls les fournisseurs de services de télécommunications certifiés pour le système de communication doivent être utilisés. Vous trouverez une liste des fournisseurs de services de télécommunications certifiés ainsi que la procédure de certification en suivant ce lien :

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

Remarque : Les numéros spéciaux et les numéros d'urgence, qui ne sont pas pris en charge par le fournisseur de services de téléphonie sur IP, doivent être acheminés via des connexions réseau fixes.

En cas de défaillance du fournisseur de services de télécommunications (ITSP), les connexions réseau fixes via le routage à moindre coût (LCR) peuvent être utilisées comme solution de repli.

Compte utilisateur ITSP

Le compte utilisateur ITSP (compte utilisateur SIP) doit être demandé auprès de l'ITSP. Le fournisseur de services de communication (ITSP) met à disposition un serveur d'enregistrement SIP auprès duquel le système de communication doit d'abord se connecter (spécifique au fournisseur) à cette fin.

Remarque : L'enregistrement n'est pas nécessaire si l'authentification IP statique ou un tunnel VPN est utilisé par le fournisseur de services de téléphonie sur IP (ITSP).

Extension mobile (MEX)

Cette fonctionnalité est proposée par certains opérateurs de téléphonie mobile dans le cadre du service MDA (accès direct mobile). Il permet d'intégrer les téléphones mobiles/smartphones en tant qu'abonnés internes dans un système de communication.

Cette fonctionnalité ne peut être utilisée qu'avec une connexion téléphonique Internet DID. Pour ce faire, le numéro MEX fourni par le fournisseur de services de téléphonie sur IP (ITSP) doit être saisi lors de la configuration de l'ITSP. Chez le fournisseur de services de téléphonie mobile (ITSP), le numéro d'appel du téléphone portable est associé au numéro MEX. De plus, le téléphone mobile ou smartphone doit être configuré dans le système de communication en tant que poste Mobility (voir Configuration de Mobility Entry).

Description courte :

- L'opérateur de téléphonie mobile propose un forfait mobile.
- Service à numéro unique : le téléphone mobile est joignable grâce à un seul numéro de réseau fixe, qui est également communiqué à l’autre partie.
- L'état de présence et l'état de connexion des téléphones mobiles sont visibles exactement comme pour les abonnés internes normaux.
- Chaque appel téléphonique depuis ou vers le téléphone mobile est effectué exclusivement via OpenScape Business en combinaison avec un fournisseur de services de téléphonie sur IP certifié.
- Le numéro de téléphone portable n'est pas connu de l'extérieur, c'est-à-dire que le téléphone portable ne peut pas être appelé directement. Il ne peut pas non plus passer d'appels sortants directs. Tous les appels sont effectués via OpenScape Business.
- Le téléphone mobile peut être intégré aux équipes internes du système.
- Les applications de communications unifiées telles que myPortal for Desktop et myPortal for Outlook peuvent être utilisées de la même manière que pour les abonnés internes.
- Les téléphones mobiles intégrés s'identifient par leur nom lorsqu'ils appellent un abonné interne.
- L'analyse des chiffres et le routage des appels dans le système ou le réseau s'effectuent comme pour toute autre station interne (par exemple, numéros autorisés, numéros refusés, règles LCR).

- Le fournisseur de services de télécommunications (ITSP) utilise une signalisation d'appel spéciale depuis/vers OpenScape Business, qui doit être administrée en conséquence.
- Chaque téléphone mobile intégré nécessite une licence utilisateur de mobilité.
- Pour utiliser les applications UC, une licence UC Client est également requise.

9.2.1 Configuration d'un ITSP

Il est possible de configurer des fournisseurs de services de téléphonie sur Internet (ITSP) prédéfinis et nouveaux. Pour chaque fournisseur ITSP, vous pouvez configurer un ou plusieurs comptes. Au maximum 8 fournisseurs ITSP peuvent être actifs simultanément.

Vous trouverez ci-après des informations supplémentaires sur le fournisseur ITSP et ses fonctionnalités.

`http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#Overview`

Remarque : Vous trouverez des exemples de configuration sur Internet dans **Unify Experts Wiki** sous *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Affectation des numéros de téléphone ITSP

- Dans un **raccordement d'installation téléphonie Internet**, l'ITSP fournit des numéros de téléphone individuels, par ex. 70005555, 70005556, ... Ces numéros de téléphone individuels sont ensuite attribués manuellement aux numéros internes des abonnés.
- Dans un **raccordement d'installation téléphonie Internet**, l'ITSP fournit un groupe de numéros de téléphone (plage de numéros de téléphone), par ex.(+49) 89 7007-100 à (+49) 89 7007-147. Les numéros de téléphone de ce groupe de numéros sont ensuite attribués manuellement aux numéros internes des abonnés.

Les deux types de raccordement peuvent être combinés.

Autre variante : pour les deux types de raccordement, les numéros ITSP peuvent être inscrits comme numéros SDA des abonnés lors de la configuration des stations.

Numéro interne	Nom	SDA
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Les numéros de téléphone ITSP résultent donc des numéros d'installation créés (par ex. indicatif national 49) et des numéros de sélection directe à l'arrivée

au format long qui ont été inscrits. Cela a des avantages pour l'évaluation de la numérotation et la gestion des appels dans une interconnexion de réseaux. Ainsi, le raccordement ITSP permet par ex. la sélection en direction d'un autre noeud.

Un autre raccordement réseau via RNIS n'est dans ce cas possible qu'avec certaines restrictions.

Gestion Multisite

Les abonnés du système de communication peuvent se voir affecter différents sites (par ex. avec différents préfixes locaux). Chaque site est associé à une voie et chaque voie est associée à un enregistrement ITSP. Il est possible de gérer 8 enregistrements ITSP maxi. Un enregistrement par ITSP est possible ainsi que plusieurs enregistrements dans un ITSP. A chaque enregistrement ITSP il est possible d'affecter une préfixe de réseau local et ensuite plusieurs abonnés. Le raccordement des abonnés aux différents sites du système de communication est réalisé via VPN. Tous les sites doivent se trouver dans un même pays et utiliser le même indicatif réseau (voir aussi *Mise en réseau de OpenScape Business dans un environnement d'hébergement*, scénario 1b).

Utilisation des modèles ITSP

Par défaut, on utilise un modèle ITSP préconfiguré. Pour cela, on entre dans ce modèle les propres données d'accès et numéros d'appel et on les active ensuite.

En mode Expert, vous pouvez également modifier un modèle ITSP préconfiguré et l'enregistrer comme modèle.

Actualiser les modèles ITSP

Les modèles ITSP préconfigurés sont automatiquement actualisés après une mise à jour logicielle du système dans la mesure où cette mise à jour comprend des modèles ITSP nouvellement préconfigurés ou des valeurs par défaut plus actuelles pour les modèles préconfigurés déjà en place.

Si l'ITSP d'un modèle est déjà activé, l'actualisation n'est pas effectuée automatiquement car, lors de l'actualisation des valeurs standard, des adaptations importantes pourraient être écrasées. C'est pourquoi l'actualisation peut être effectuée manuellement si nécessaire, en mode Expert. Ensuite, les valeurs par défaut doivent être adaptées aux propres besoins.

Mode Direction de ligne

Les lignes individuelles d'une ligne ITSP peuvent être bloquées pour le trafic sortant et/ou entrant. Les modes de direction de ligne suivants sont possibles :

- seulement sortant
- seulement entrant
- sortant et entrant (par défaut)

La direction de la ligne est évaluée lorsque le système de communication doit réserver une ligne ITSP pour un appel entrant ou sortant.

9.2.1.1 Comment configurer un ITSP prédéfini

L'assistant **Téléphonie Internet** permet de configurer et d'activer un fournisseur de services de téléphonie Internet (ITSP) prédéfini. Vous pouvez configurer un

ou plusieurs comptes pour chaque fournisseur de services de téléphonie sur Internet (ITSP).

Conditions préalables

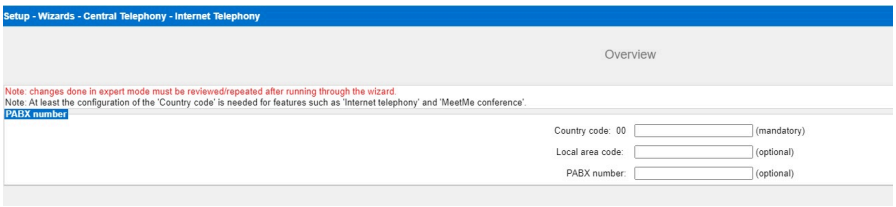
La connexion à Internet est opérationnelle.

Les données d'accès à la téléphonie sur Internet de votre fournisseur de services (ITSP) sont disponibles (par exemple, le compte d'utilisateur, le mot de passe et le numéro de téléphonie sur Internet).

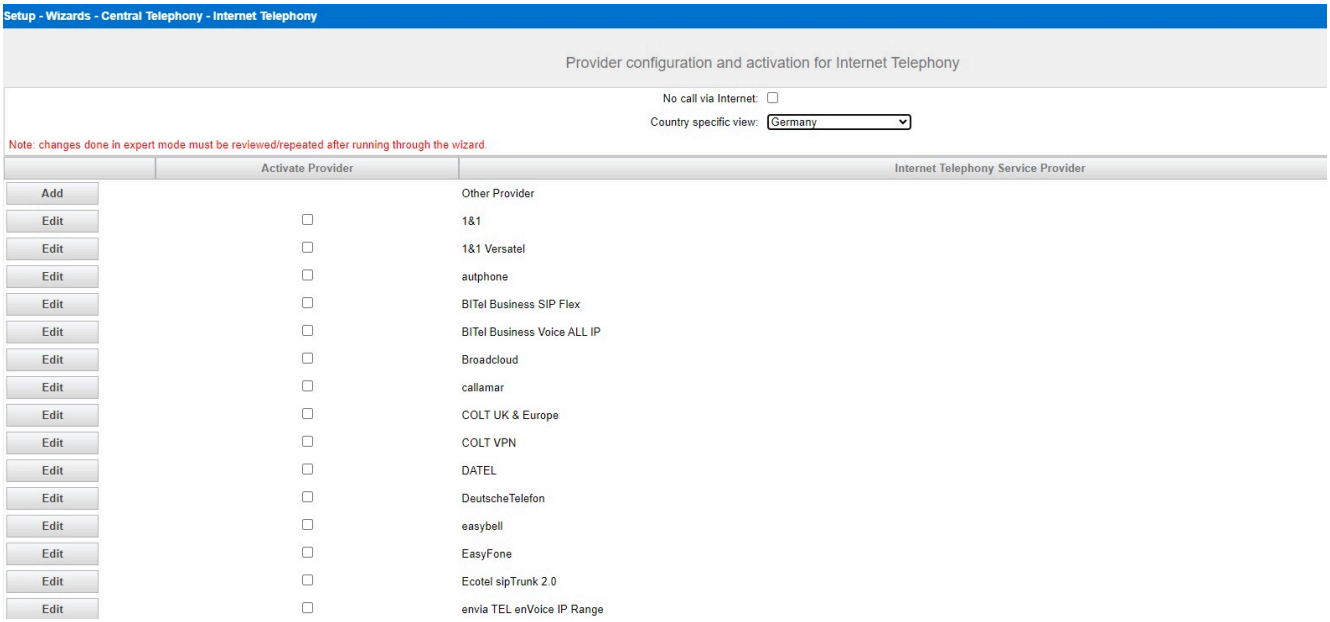
Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Téléphonie Internet**.



4) Décochez **Pas de téléphonie par Internet**. Le système affiche une liste des ITSP disponibles, en fonction du pays. La liste contient les ITSP prédéfinis pour le pays sélectionné et les ITSP que vous avez créés.



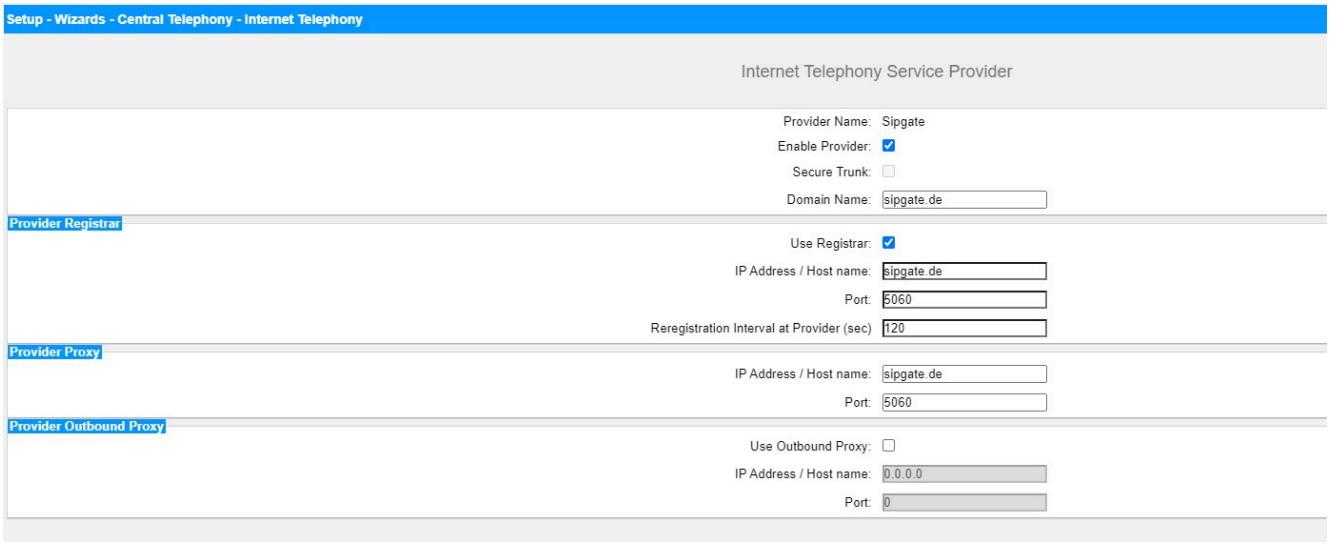
5) Si vous souhaitez modifier le pays présélectionné, sélectionnez le pays souhaité dans la liste **Affichage spécifique du pays**. Les ITSP possibles pour le pays sélectionné s'affichent.
6) Si nécessaire, cliquez sur **Afficher le statut** pour savoir quels ITSP sont déjà activés et quels abonnés téléphonie Internet sont déjà inscrits sur les ITSP. Vous pouvez activer 8 ITSP au maximum. Pour finir, cliquez sur **OK**.
7) Pour configurer l'ITSP prédéfini, cliquez sur **Modifier** dans la ligne associée à l'ITSP souhaité.

8) Cochez **Activer le fournisseur**.

9) Si le fournisseur prend en charge une connexion sécurisée, la case à cocher **Secure Trunk** peut être activée.

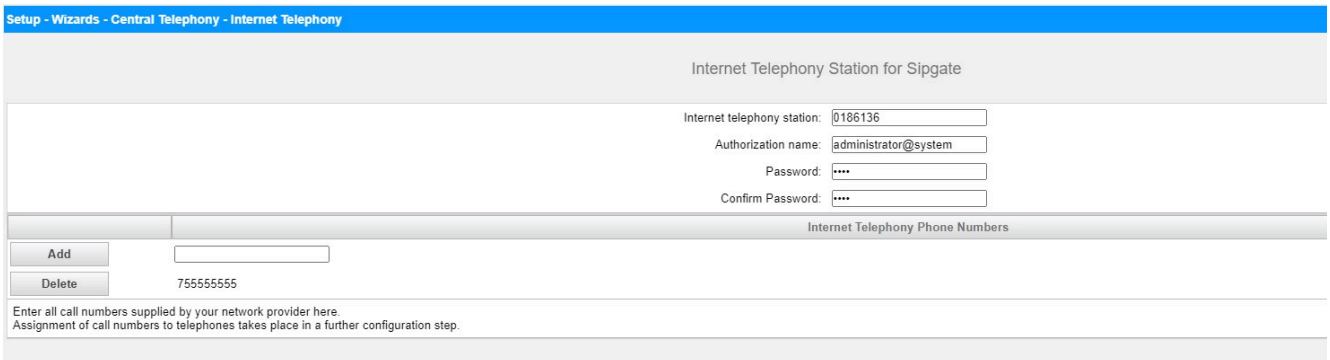
10) Les valeurs pour "**Registre du fournisseur**", "**Proxy du fournisseur**", "**Proxy sortant du fournisseur**" et "**Fonctionnalité du fournisseur**" (si elle est activée) sont prédéfinies en fonction des besoins de la plupart des ITSP. Certains ITSP utilisent des adresses de serveurs spécifiques à leurs clients. Dans ce cas, les champs qui ne sont pas grisés doivent être remplis conformément à la documentation reçue de l'ITSP.

11) Si le fournisseur prend en charge la déviation d'appel, la section Fonctionnalité du fournisseur est affichée et vous pouvez activer la fonction de déviation d'appel. Lorsque la déviation d'appel est activée, le renvoi d'appel est effectué dans le réseau du fournisseur, la gestion des appels dans le système n'est pas effective.



12) Cliquez sur **OK & Suivant**.

13) Cliquez sur **Ajouter** pour configurer vos comptes ITSP avec les numéros correspondants de téléphonie sur Internet. Les champs affichés ensuite sont fonction du fournisseur d'accès.



14) Dans le champ **Abonné de téléphonie Internet** entrez les données d'accès de votre compte. Les données ont été fournies par votre ITSP. Suivant l'ITSP, des désignations différentes sont utilisées, par ex. : Utilisateur SIP, ID SIP, etc.

Vous trouverez plus de détails à l'adresse suivante : http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

15) Entrez dans **Nom d'autorisation** le nom d'autorisation. Les données ont été fournies par votre ITSP. Si vous n'avez pas reçu de nom d'autorisation, entrez les mêmes données que dans **Abonné de téléphonie Internet**.

Remarque : Si aucun enregistrement n'est utilisé, le **Nom d'autorisation** est grisé et ne peut pas être configuré.

---

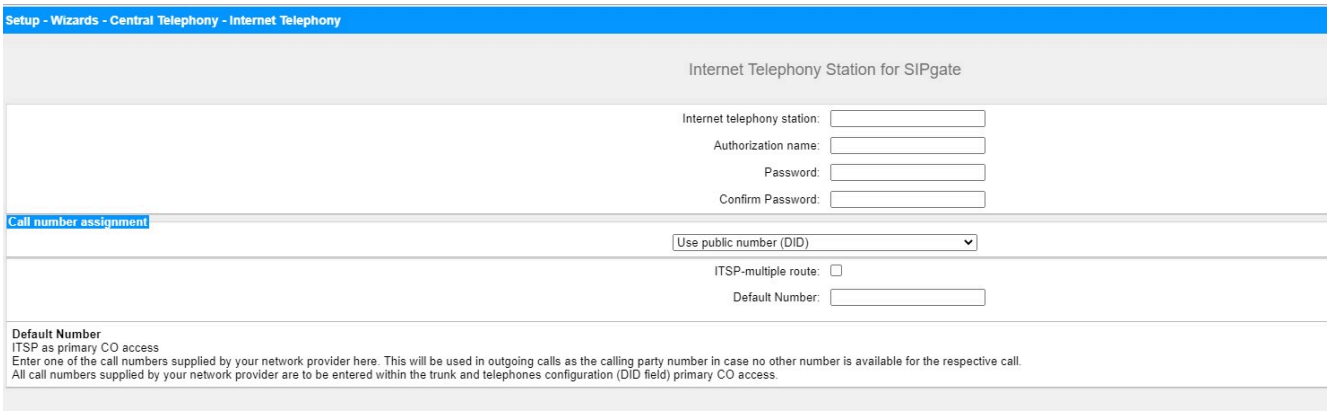
16) Dans les champs **Nouveau mot de passe** et **Répéter le mot de passe**, entrez le mot de passe que vous avez reçu du ITSP. Suivant l'ITSP, des désignations différentes sont utilisées, par ex. : Mot de passe, mot de passe SIP, etc.

Remarque : Si aucun enregistrement n'est utilisé, le **Mot de passe** est grisé et ne peut pas être configuré.

---

17) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 1 :

Utiliser le numéro public (SDA) : les numéros de téléphone Internet (SDA) de votre connexion de téléphonie Internet sont configurés dans la configuration des stations (dans les champs **SDA**). Aucune configuration de mappage n'est nécessaire lors de la configuration de l'ITSP.

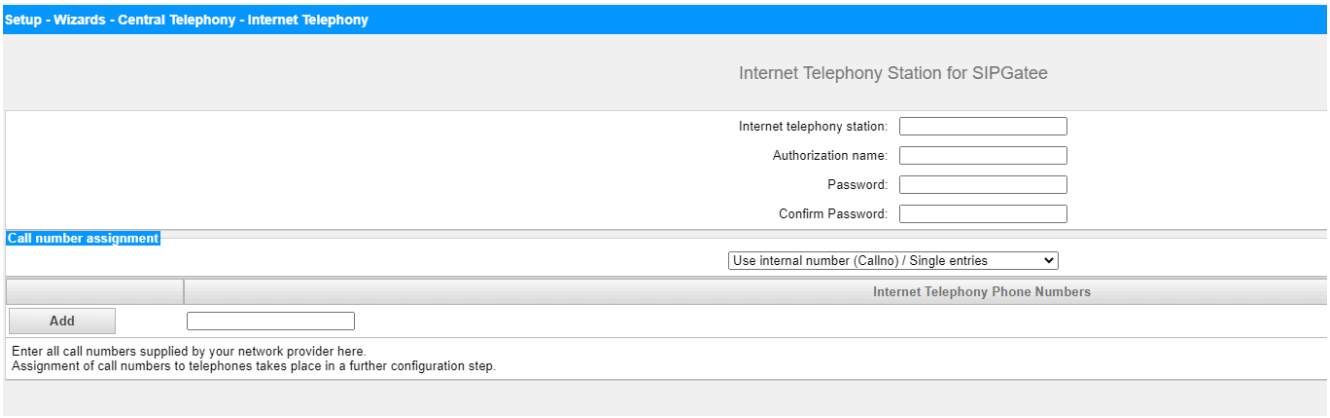


a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **N° de téléphone public (SDA)**.
b) Sous **Numéro par défaut**, entrez le numéro de téléphone à utiliser pour les appels sortants lorsqu'aucun numéro SDA n'est disponible.
c) Si votre ITSP supporte la fonctionnalité "Mobile Extension (MEX)", entrez dans **Numéro MEX** le numéro MEX fourni par l'ITSP (8 positions, chiffres uniquement). Si votre ITSP ne prend pas en charge la fonction "Poste Mobile (MEX)", le champ **Numéro MEX** n'est pas affiché.
d) Si plusieurs itinéraires doivent être configurés, activez la case à cocher **ITSP-itinéraire multiple**.
e) Saisissez les **préfixes d'itinéraire ITSP** attribués à l'itinéraire et cliquez sur **Ajouter**.

18) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 2 :

Utiliser numéro interne (n° appel) / entrées individuelles : Vous avez un ITSP qui a besoin d'un enregistrement SIP pour chaque numéro d'appel (par exemple 70005555, 70005556,...). Pour chaque numéro d'appel, une station de téléphonie Internet doit être créée et un numéro d'appel unique

doit être attribué. Si votre ITSP autorise plusieurs numéros d'appel avec un seul enregistrement, l'option 1 doit être utilisée.



a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **Utiliser le numéro interne (N° tél)/entrées individuelles**.

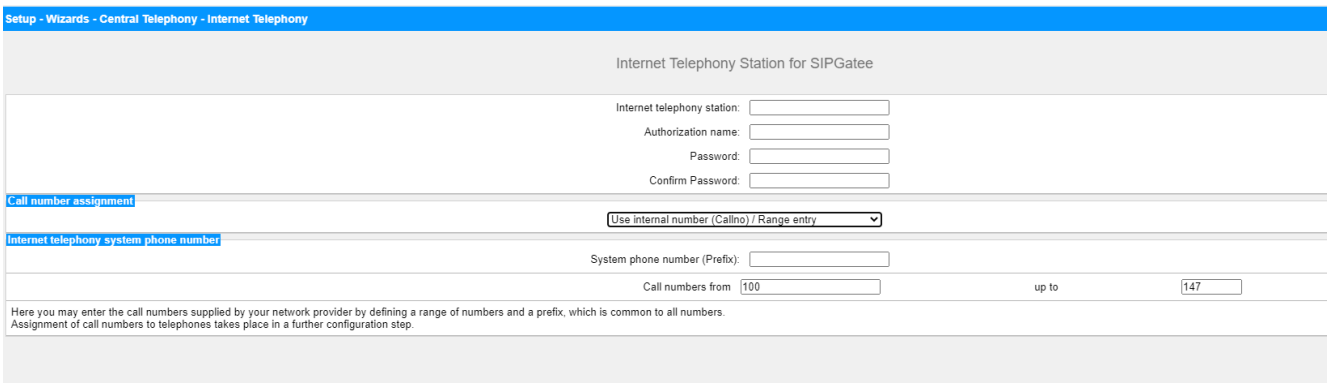
b) Dans la zone **Téléphonie Internet-Numéros des abonnés**, dans le champ situé à côté du bouton **Ajouter**, saisissez un numéro d'abonné de téléphonie Internet communiqué par le ITSP et cliquez sur **Ajouter**.

c) Si vous souhaitez attribuer d'autres numéros de téléphonie Internet au compte, répétez l'étape b).

19) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 3 :

Utiliser le numéro interne (CalIno) / Entrée de plage : l'utilisation de cette option est obsolète, pour la configuration SDA, l'option 1 doit être utilisée.

Vous disposez d'une connexion Téléphonie Internet et, comme numéros de téléphonie Internet, d'une plage de numéros, par ex. (+49) 89 7007-100 à (+49) 89 7007-147. Vous affectez ensuite les numéros de la plage aux numéros internes des abonnés.



a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **Utiliser le numéro interne (N° tél)/Entrée individuelle**.

b) Dans **Numéro de l'installation (préfixe)**, entrez le numéro de l'installation.

c) Entrez la série de numéros SDA souhaitée pour la station de téléphonie Internet dans les champs 'de' **et** 'à **' après** Bande de numérotation directe à l'arrivée. Par défaut, la valeur 100 - 147 est entrée.

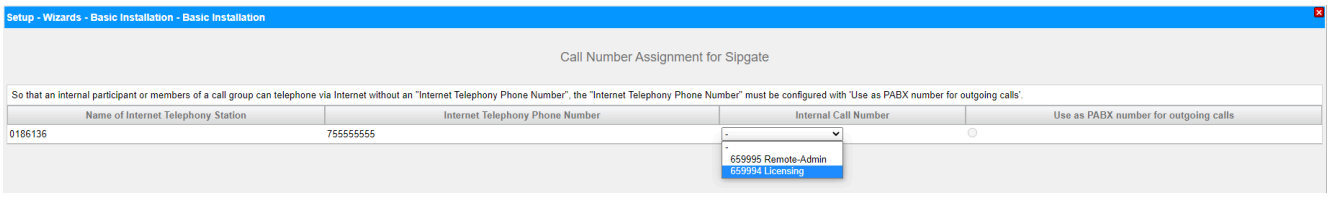
20) Cliquez sur **OK & Suivant**.

21) Si vous souhaitez configurer d'autres comptes, répétez les étapes 13 à 20.

22) Cliquez sur **OK & Suivant**. Vous visualisez une vue d'ensemble indiquant la correspondance entre les numéros de téléphonie Internet et les comptes.

23) Affectez respectivement le numéro interne d'un abonné à tous les numéros de téléphonie Internet.

Cette étape est supprimée si vous avez choisi la possibilité 1 pour l'affectation des numéros de téléphonie Internet. Dans ce cas, l'affectation est effectuée lors de la configuration des stations (c'est-à-dire des téléphones et des abonnés) dans le champ **SDA**. Dans ce cas, l'écran est également visible mais n'est pas modifiable.



a) Dans la ligne correspondante de la liste déroulante **Numéro interne**, sélectionnez un numéro de téléphone interne.

b) Si les abonnés sans numéro de téléphone Internet ou les membres d'un groupe d'appel doivent être autorisés à effectuer des appels externes via Internet, le bouton radio **Utiliser comme numéro PABX pour les appels sortants** doit être activé. La case doit être cochée uniquement pour un seul numéro de téléphonie Internet.

24) Cliquez sur **OK & Suivant**. Vous obtenez à nouveau un aperçu des ITSP possibles. Les ITSP activés sont cochés dans la colonne **Activer le fournisseur**. Avec la fonction Afficher le statut, vous pouvez vérifier le statut de la connexion. Si vous avez des problèmes de connexion avec un ITSP déjà activé, vous pouvez le réenregistrer avec **Redémarrer ITSP** sur cette page.

25) Cliquez sur **OK & Suivant**.

26) Dans le champ **Flux ascendant jusqu'à (kbit/s)** entrez la valeur de la vitesse du flux ascendant de votre connexion Internet. A ne pas confondre avec la vitesse de téléchargement !

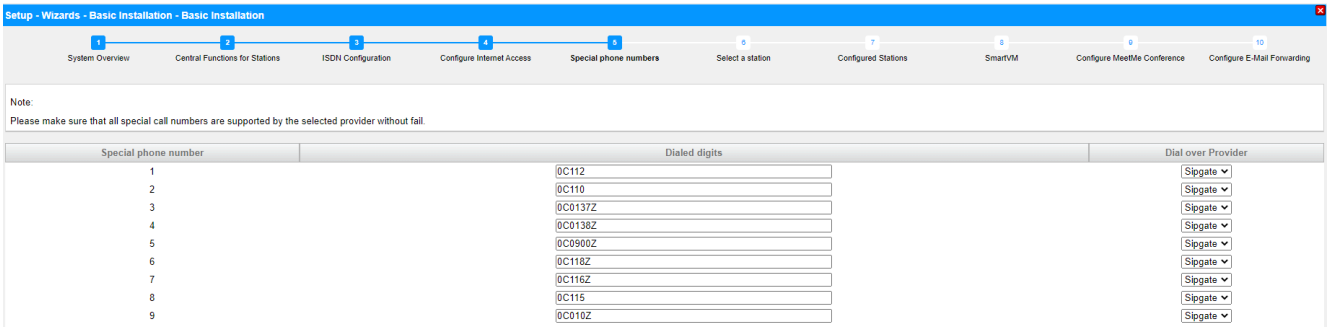
Remarque : Dans le champ **Nombre de communications téléphoniques Internet simultanées**, le système indique le nombre maximal de communications téléphoniques Internet simultanées possibles. Si la qualité de la communication se détériore en raison de la charge du réseau, vous devez réduire ce nombre.

Pour plus d'informations sur le nombre d'appels Internet simultanés, veuillez vous référer à Limitation du nombre de communications simultanées via ITSP à la page 775.

---

27) Cliquez sur **OK & Suivant**.

28) Entrez dans la colonne **Chiffres composés** les numéros spéciaux souhaités.



Les entrées de numéro de station suivantes sont valides :

- 0 à 9: chiffres autorisés
- -: Séparateur de champ
- X : Chiffre au choix entre 0 et 9
- N : Chiffre au choix entre 2 et 9
- Z : Un ou plusieurs chiffres suivent jusqu'à la fin de la numérotation
- C : Tonalité d'invitation à numéroter simulée (peut être entrée max. trois fois)

29) Choisissez dans la colonne **Appeler par le fournisseur** si le numéro spécial doit être composé par RNIS ou par un ITSP. Seuls les ITSP activés sont affichés.

Remarque : Assurez-vous que les numéros d'urgence puissent toujours être composés. S'il est nécessaire de sélectionner des numéros d'urgence via un fournisseur de téléphonie sur Internet (ITSP), le fournisseur doit supporter ce service.

---

30) Cliquez sur **OK & Suivant**. Le système vous indique l'état du ITSP.

31) Cliquez sur **Suivant** puis sur **Terminer**. Après cette étape, veuillez exécuter l'assistant **Réseau RNIS CO / Analogique / ITSP** pour définir la priorité pour la saisie de la ligne d'échange (par exemple : Saisie de la ligne d'échange d'abord par ITSP et ensuite par RNIS).

9.2.1.2 Comment ajouter un nouveau fournisseur de services de téléphonie sur internet (ITSP)

L'assistant **Téléphonie Internet** peut être utilisé pour configurer et activer un nouveau fournisseur de services de téléphonie Internet (ITSP). Vous pouvez configurer un ou plusieurs comptes pour chaque fournisseur de services de téléphonie sur Internet (ITSP).

Conditions préalables

La connexion à Internet est opérationnelle.

Vous êtes connecté à WBM avec le profil **Advanced**.

Les données d'accès à Internet suivantes, spécifiques à l'ITSP, sont disponibles :

Champ	Description	Valeur du FAI
Nom de domaine de la passerelle	Nom de domaine de la passerelle de l'ITSP Généralement identique au nom d'hôte (par exemple, sip-voice.de)	
Fournisseur Bureau d'enregistrement		
Utiliser l'enregistrement	Prédéfini par l'ITSP et généralement toujours activé (non requis pour les ITSP qui utilisent l'authentification IP statique).	
Adresse IP / Nom de l'hôte	Nom d'hôte ou adresse IP du serveur d'enregistrement (par exemple, sip-voice.de).	
Port	Numéro de port du serveur du bureau d'enregistrement (par exemple, 5060).	
Intervalle de réenregistrement chez le fournisseur (sec)	Intervalle (en secondes) auquel l'enregistrement ITSP est répété. La valeur de l'intervalle ne doit pas être égale à 0 et ne doit pas être trop élevée car, lors de la répétition de l'enregistrement à l'ITSP, une connexion interrompue peut également être détectée et une autre route (via RNIS ou un autre fournisseur) peut être sélectionnée si nécessaire. Valeur par défaut : 120 secondes.	
Proxy du fournisseur		
Adresse IP / Nom de l'hôte	Nom d'hôte ou adresse IP du serveur proxy (par exemple, sip-voice.de). Cette adresse est généralement identique à celle de l'entrée Fournisseur Bureau d'enregistrement.	
Port	Numéro de port du serveur proxy (par exemple, 5060). Il est généralement identique au numéro de port du bureau d'enregistrement du fournisseur.	
Fonctionnalité du fournisseur		
Déviation d'appel	Visible uniquement si le modèle de base sélectionné prend en charge la déviation d'appels	
Proxy sortant du fournisseur		
Utiliser un proxy sortant	Uniquement si l'ITSP utilise un proxy sortant.	
Adresse IP / Nom de l'hôte	Nom d'hôte ou adresse IP du proxy sortant	

Champ	Description	Valeur du FAI
Port	Numéro de port du proxy sortant	
Proxy entrant du fournisseur		
Utiliser le proxy entrant	Cette option n'est activée que si l'ITSP utilise un second proxy.	
Adresse IP / Nom de l'hôte	Nom d'hôte ou adresse IP du second proxy	
Port	Numéro de port du second proxy	
Fournisseur STUN		
Utiliser STUN	Utilisé uniquement si la fonctionnalité STUN est requise. Active également le mode STUN global.	
Adresse IP / Nom de l'hôte	Adresse IP STUN si l'ITSP utilise un serveur STUN.	
Port	Numéro de port STUN si l'ITSP utilise un serveur STUN.	

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Téléphonie Internet**.
4) Décochez **Pas de téléphonie par Internet**. Le système affiche une liste des ITSP disponibles, en fonction du pays. La liste contient les ITSP prédéfinis pour le pays sélectionné et éventuellement les ITSP nouvellement ajoutés.
5) Si nécessaire, cliquez sur **Afficher le statut** pour savoir quels ITSP sont déjà activés et quels abonnés téléphonie Internet sont déjà inscrits sur les ITSP. Vous pouvez activer 8 ITSP au maximum. Pour finir, cliquez sur **OK**.
6) Cliquez sur **Ajouter** pour configurer un nouvel ITSP. Une fenêtre de configuration pour le nouvel ITSP apparaît.
7) Sélectionnez un **Modèle de base** dans la liste déroulante. Cette option permet de configurer le même serveur ITSP sur plusieurs itinéraires.
8) Attribuez un nom de votre choix à l'ITSP dans le champ **Nom du fournisseur**.

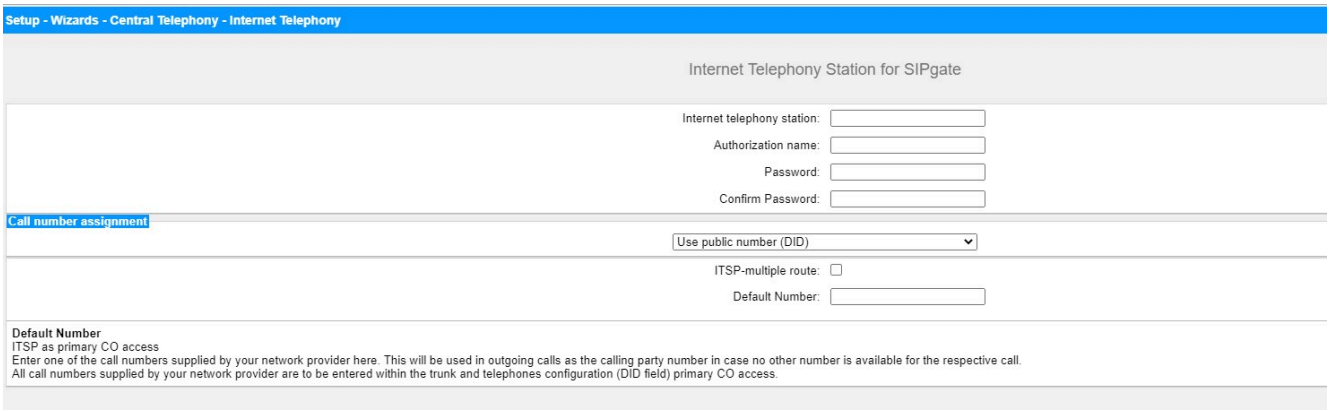
   Remarque : La limite maximale de caractères est de 10.

9) Cochez **Activer le fournisseur**.
10) Saisissez les valeurs fournies par votre ITSP dans les zones restantes (voir le tableau immédiatement après les conditions préalables).

    Remarque : Les valeurs sous « Extended SIP Provider Data » ne peuvent être modifiées que par le personnel de service autorisé, en collaboration avec le service de développement !

11) Cliquez sur **OK & Suivant**.

12) Cliquez sur **Ajouter** pour configurer vos comptes ITSP avec les numéros correspondants de téléphonie sur Internet. Les champs affichés ensuite sont fonction du fournisseur d'accès.



13) Dans le champ **Abonné de téléphonie Internet** entrez les données d'accès de votre compte. Les données ont été fournies par votre ITSP. Suivant l'ITSP, des désignations différentes sont utilisées, par ex. : Utilisateur SIP, ID SIP, etc.

    Vous trouverez plus de détails à l'adresse suivante : http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

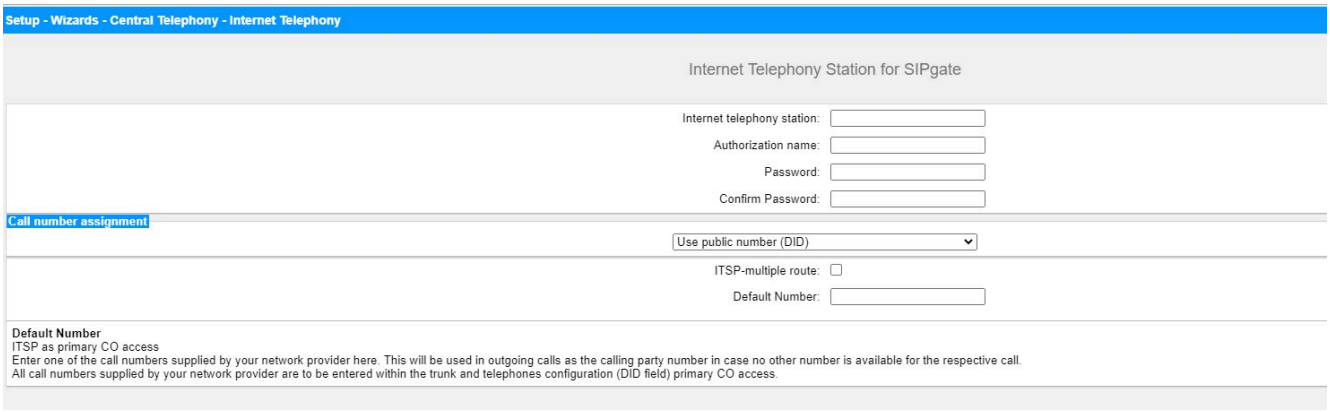
14) Entrez dans **Nom d'autorisation** le nom d'autorisation. Les données ont été fournies par votre ITSP. Si vous n'avez pas reçu de nom d'autorisation, entrez les mêmes données que dans **Abonné de téléphonie Internet**.

15) Dans les champs **Nouveau mot de passe** et **Répéter le mot de passe**, entrez le mot de passe que vous avez reçu du ITSP. Suivant l'ITSP, des désignations différentes sont utilisées, par ex. : Mot de passe, mot de passe SIP, etc.

16) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 1 :

    Utiliser le numéro public (SDA) : les numéros de téléphone Internet (SDA) de votre connexion de téléphonie Internet sont configurés dans la

configuration des stations (dans les champs **SDA**). Aucune configuration de mappage n'est nécessaire lors de la configuration de l'ITSP.



a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **N° de téléphone public (SDA)**.
b) Sous **Numéro par défaut**, entrez le numéro de téléphone à utiliser pour les appels sortants lorsqu'aucun numéro SDA n'est disponible.
c) Si votre ITSP supporte la fonctionnalité "Mobile Extension (MEX)", entrez dans **Numéro MEX** le numéro MEX fourni par l'ITSP (8 positions, chiffres uniquement).
d) Activez la case à cocher **ITSP-itinéraire multiple**.
e) Saisissez les **préfixes d'itinéraire ITSP** attribués à l'itinéraire et cliquez sur **Ajouter**.

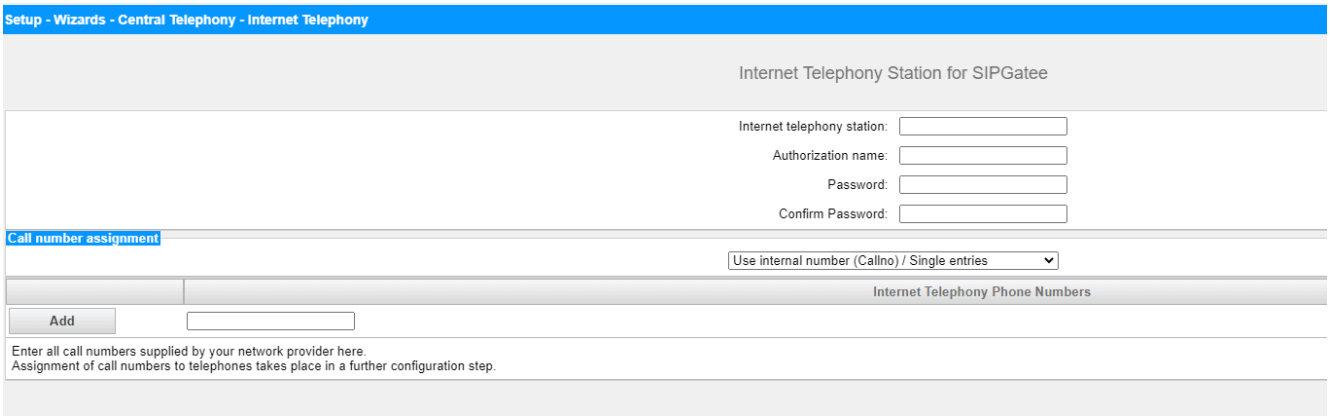
Remarque : Pour configurer plusieurs itinéraires, les étapes ci-dessus doivent être répétées. Pour plus d'informations, consultez le wiki Unify à l'adresse suivante : http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#General_Configuration_guides

---

17) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 2 :

Utiliser numéro interne (n° appel) / entrées individuelles : Vous avez un ITSP qui a besoin d'un enregistrement SIP pour chaque numéro d'appel (par exemple 70005555, 70005556,...). Pour chaque numéro d'appel, une station de téléphonie Internet doit être créée et un numéro d'appel unique

doit être attribué. Si votre ITSP autorise plusieurs numéros d'appel avec un seul enregistrement, l'option 1 doit être utilisée.



a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **Utiliser le numéro interne (N° tél)/entrées individuelles**.

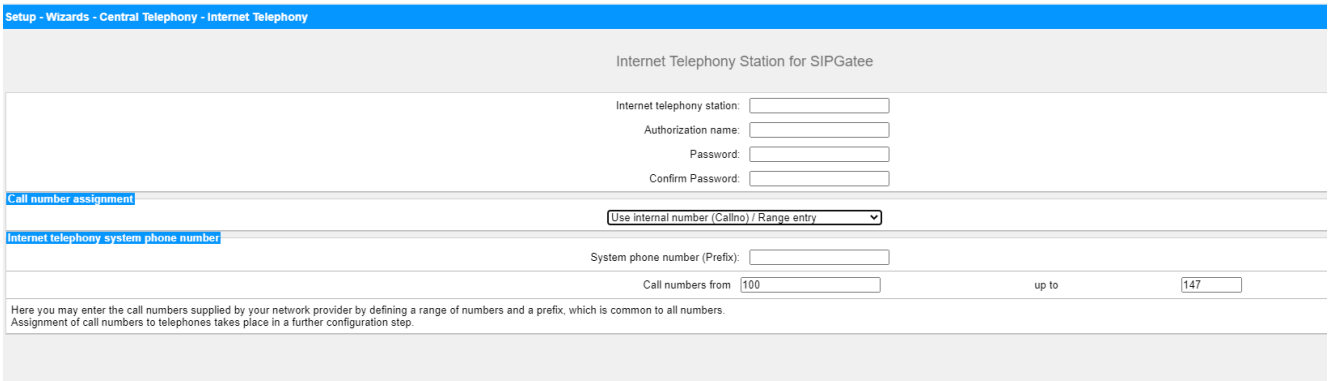
b) Dans la zone **Téléphonie Internet-Numéros des abonnés**, dans le champ situé à côté du bouton **Ajouter**, saisissez un numéro d'abonné de téléphonie Internet communiqué par le ITSP et cliquez sur **Ajouter**.

c) Si vous souhaitez attribuer d'autres numéros de téléphonie Internet au compte, répétez l'étape b).

18) Affectation du numéro de téléphone de téléphonie Internet - Possibilité 3 :

Utiliser le numéro interne (Callno) / Entrée de plage : l'utilisation de cette option est obsolète, pour la configuration SDA, l'option 1 doit être utilisée.

Vous disposez d'une connexion Téléphonie Internet et, comme numéros de téléphonie Internet, d'une plage de numéros, par ex. (+49) 89 7007-100 à (+49) 89 7007-147. Vous affectez ensuite les numéros de la plage aux numéros internes des abonnés.



a) Dans la zone **Affectation du numéro**, sélectionnez le champ d'option **Utiliser le numéro interne (N° tél)/Entrée individuelle**.

b) Dans **Numéro de l'installation (préfixe)**, entrez le numéro de l'installation.

c) Entrez la série de numéros SDA souhaitée pour la station de téléphonie Internet dans les champs 'de' **et** 'à **' après** Bande de numérotation directe à l'arrivée. Par défaut, la valeur 100 - 147 est entrée.

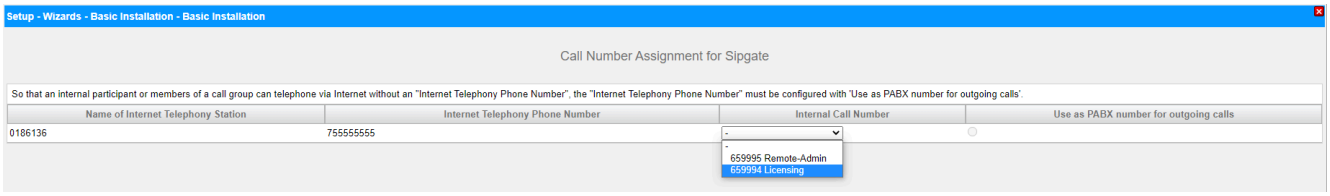
19) Cliquez sur **OK & Suivant**.

20) Si vous souhaitez configurer d'autres comptes, répétez les étapes 12 à 19.

21) Cliquez sur **OK & Suivant**. Vous visualisez une vue d'ensemble indiquant la correspondance entre les numéros de téléphonie Internet et les comptes.

22) Affectez respectivement le numéro interne d'un abonné à tous les numéros de téléphonie Internet.

    Cette étape est supprimée si vous avez choisi la possibilité 1 pour l'affectation des numéros de téléphonie Internet. Dans ce cas, l'affectation est effectuée lors de la configuration des stations (c'est-à-dire des téléphones et des abonnés) dans le champ **SDA**. Dans ce cas, l'écran est également visible mais n'est pas modifiable.



a) Dans la ligne correspondante de la liste déroulante **Numéro interne**, sélectionnez un numéro de téléphone interne.

b) Si les abonnés sans numéro de téléphone Internet ou les membres d'un groupe d'appel doivent être autorisés à effectuer des appels externes via Internet, le bouton radio **Utiliser comme numéro PABX pour les appels sortants** doit être activé. La case doit être cochée uniquement pour un seul numéro de téléphonie Internet.

23) Cliquez sur **OK & Suivant**. Vous obtenez à nouveau un aperçu des ITSP possibles. Les ITSP activés sont cochés dans la colonne **Activer le fournisseur**. Avec la fonction Afficher le statut, vous pouvez vérifier le statut de la connexion. Si vous avez des problèmes de connexion avec un ITSP déjà activé, vous pouvez le réenregistrer avec **Redémarrer ITSP** sur cette page.

24) Cliquez sur **OK & Suivant**.

25) Dans le champ **Flux ascendant jusqu'à (kbit/s)** entrez la valeur de la vitesse du flux ascendant de votre connexion Internet. A ne pas confondre avec la vitesse de téléchargement !

Remarque : Dans le champ **Nombre de communications téléphoniques Internet simultanées**, le système indique le nombre maximal de communications téléphoniques Internet simultanées possibles. Si la qualité de la communication se détériore en raison de la charge du réseau, vous devez réduire ce nombre.

Pour plus d'informations sur le nombre d'appels Internet simultanés, veuillez vous référer à Limitation du nombre de communications simultanées via ITSP à la page 775.

---

26) Cliquez sur **OK & Suivant**.

27) Entrez dans la colonne **Chiffres composés** les numéros spéciaux souhaités.

Les entrées de numéro de station suivantes sont valides :

- 0 à 9: chiffres autorisés
- -: Séparateur de champ
- X : Chiffre au choix entre 0 et 9
- N : Chiffre au choix entre 2 et 9
- Z : Un ou plusieurs chiffres suivent jusqu'à la fin de la numérotation
- C : Tonalité d'invitation à numéroter simulée (peut être entrée max. trois fois)

28) Choisissez dans la colonne **Appeler par le fournisseur** si le numéro spécial doit être composé par RNIS ou par un ITSP. Seuls les ITSP activés sont affichés.

Remarque : Assurez-vous que les numéros d'urgence puissent toujours être composés. S'il est nécessaire de sélectionner des numéros d'urgence via un fournisseur de téléphonie sur Internet (ITSP), le fournisseur doit supporter ce service.

---

29) Cliquez sur **OK & Suivant**. Le système vous indique l'état du ITSP.

30) Cliquez sur **Suivant** puis sur **Terminer**. Après cette étape, veuillez exécuter l'assistant **Réseau RNIS CO / Analogique / ITSP** pour définir la priorité pour la saisie de la ligne d'échange (par exemple : Saisie de la ligne d'échange d'abord par ITSP et ensuite par RNIS).

9.2.1.3 Comment configurer un multisite via ITSP

A l'aide de l'assistant **Gestion multisite**, vous pouvez définir pour le système de communication jusqu'à 8 sites ; à chacun d'entre eux vous pouvez attribuer un enregistrement ITSP et plusieurs abonnés.

Conditions préalables

Il est créé autant d'enregistrement pour un ou plusieurs ITSP qu'il doit être paramétré de sites.

Tous les sites se trouvent à l'intérieur d'un même pays.

Vous êtes connecté à WBM avec le profil **Avancé**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.

3) Cliquez sur **Modifier** pour lancer l'Assistant **Gestion multisite**.

4) Dans **Indicatif local**, indiqué pour chaque site un préfixe local (y compris zéro à gauche, par ex. `069` pour Francfort et `030` pour Berlin). Il est possible d'inscrire des préfixes locaux différents ou identiques.

5) Entrez dans **Plage** pour chaque site un nom (par ex. les villes `Francfort` et `Berlin` correspondant aux préfixes locaux ou, lorsque les préfixes

locaux sont les mêmes, les désignations de département `Service` et `Distribution`).

6) Dans la liste de sélection **Route dédiée**, attribuez à chaque site un faisceau. Pour chaque enregistrement ITSP, il est automatiquement réservé un faisceau (jusqu'à 8 possibles).
7) Si vous voulez effacer un ou plusieurs sites, marquez les sites dans la colonne **Effacer** et cliquez sur **Sauvegarder**.
8) Cliquez sur **OK & Suivant**.
9) Affectez aux sites les abonnés et les groupes :
   a) Marquez les abonnés et groupes souhaités.

   Remarque :

   Vous pouvez aussi effectuer une recherche par abonnés et groupes ; pour cela entrez le terme de recherche dans les champs de recherche **Numéro**, **SDA** ou **Nom** et cliquez ensuite sur l'icône de la loupe. Tous les abonnés et groupes sont listés lorsque tous les champs de recherche sont vides et que vous cliquez ensuite sur l'icône de la loupe.

   A l'aide de la sélection **Type**, il est possible d'afficher tous les types d'abonnés (par ex. **Clients SIP** ou **Clients TFA**).

   Vous pouvez sélectionner les abonnés et groupes individuellement dans la colonne **Sélection** ou bien les sélectionner tous à l'aide de la case à cocher **Sélectionner tous**.

   b) Dans **par zone**, sélectionnez le site choisi.
   c) Cliquez sur **Enregistrer**.
   d) Répétez les étapes précédentes pour les autres sites.
10) Si nécessaire, vous pouvez aussi affecter à un autre site les abonnés et les groupes d'un site.
   a) Dans **Décaler sélection de la plage**, sélectionner le site dont vous voulez affecter à un autre site les abonnés et groupes. Tous les abonnés et groupes du site sont affichés.
   b) Vous pouvez sélectionner les abonnés choisis soit individuellement dans la colonne **Sélection** soit dans leur ensemble à l'aide de la case à cocher **Sélectionner tous**.
   c) Dans **par zone**, sélectionnez le nouveau site.
   d) Cliquez sur **Enregistrer**.
   e) Répétez les étapes précédentes pour les autres sites.
11) Cliquez sur **OK & Suivant**.

9.2.1.4 Comment enregistrer un modèle ITSP préconfiguré en tant que nouveau modèle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence, cliquez sur **Fournisseur de services de téléphonie Internet**.
4) Cliquez sur l'onglet **Ajouter un fournisseur de services de téléphonie Internet**.
5) Sélectionnez le modèle ITSP souhaité dans la liste **Modèle de base**.
6) Saisissez le nom souhaité pour le nouveau modèle ITSP dans le champ **Nom du fournisseur**.
7) Modifiez les valeurs du modèle en fonction de vos besoins. Vous trouverez une explication des valeurs sous Passerelle vocale>Téléphonie InternetFournisseur de services.
8) Cliquez sur **Appliquer**, puis sur **OK**.

9.2.1.5 Comment adapter un modèle ITSP préconfiguré

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence du menu, cliquez sur **Internet Telefonie Service Provider - fournisseur de services de téléphonie sur Internet**.
4) Dans l'arborescence du menu, cliquez sur le modèle ITSP souhaité.
5) Cliquez sur l'onglet **Modifier fournisseur de services de téléphonie sur Internet**.
6) Adaptez les valeurs du modèle à vos besoins. Vous trouverez les explications sur les valeurs dans Passerelle vocale>Fournisseur de services de téléphonie sur Internet.

Remarque : Avec le Bouton **Réinitialiser les valeurs par défaut**, vous pouvez rétablir les valeurs par défaut du modèle pour les valeurs modifiées. Lorsque l'ITSP du modèle est déjà activée, tous les comptes du ITSP sont immédiatement déconnectés puis enregistrés de nouveau avec les valeurs par défaut.

Remarque : Avec le bouton **Actualiser**, vous pouvez mettre à niveau les valeurs par défaut dans la mesure où une Mise à jour logicielle a été effectuée et qu'il existe dans cette mise à jour des valeurs standard plus actuelles pour ce modèle.

---

7) Cliquez sur **Appliquer** puis sur **OK**.

9.2.1.6 Comment actualiser manuellement un modèle ITSP préconfiguré

Conditions préalables

L'ITSP de ce modèle est activé.

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence du menu, cliquez sur **Internet Telefonie Service Provider - fournisseur de services de téléphonie sur Internet**.
4) Dans l'arborescence du menu, cliquez sur le modèle ITSP souhaité.
5) Cliquez sur l'onglet **Modifier fournisseur de services de téléphonie sur Internet**.
6) Notez les valeurs du modèle que vous avez modifiées par rapport aux valeurs par défaut (par ex. à l'aide d'une instantané d'écran).
7) Cliquez sur **Mise à jour**. Les valeurs par défaut du modèle sont actualisées dans la mesure où une mise à jour logicielle du système a été effectuée et qu'il existe dans cette mise à jour des valeurs standard plus actuelles pour ce modèle.
8) Adaptez de nouveau les valeurs du modèle à vos besoins. Vous trouverez les explications sur les valeurs dans Passerelle vocale>Fournisseur de services de téléphonie sur Internet.

   Remarque : Avec le Bouton **Réinitialiser les valeurs par défaut**, vous pouvez rétablir les valeurs par défaut du modèle pour les valeurs modifiées. Dans ce cas, tous les comptes du ITSP sont immédiatement déconnectés puis enregistrés de nouveau avec les valeurs par défaut.

9) Cliquez sur **Appliquer** puis sur **OK**.

9.2.2 STUN (Simple Traversal of UDP through NAT)

Dans le cadre de l'exploitation du système de communication derrière un routeur NAT, STUN détermine l'adresse IP publique / le port nécessaire pour quelques ITSP. La fonctionnalité est fournie dans Internet sur des serveurs STUN dont les adresses doivent être enregistrées en fonction de la configuration du système de communication.

Le mode STUN nécessaire est fonction de l'infrastructure ITSP et du routeur Internet utilisé. STUN n'est pas nécessaire lorsque l'ITSP remplace NAT Traversal en utilisant des composantes d'infrastructure du réseau du fournisseur comme le Session Border Controller (SBC).

Les modes STUN suivants peuvent être réglés sur le système de communication :

- **Automatiquement (par défaut)**

  Si aucun ITSP n'est activé, STUN est entièrement arrêté dans ce mode. Si un ITSP est activé, STUN détermine le type de pare-feu utilisé (type NAT) lors du démarrage du système ; il est en mesure de reconnaître les modifications des adresses IP en cours d'exploitation. En fonction du type NAT défini, STUN modifie certains paramètres des messages SIP.

  Remarque : NAT symétrique n'est pas supportée.

- **Toujours**

  STUN est toujours activé. En fonction du type de NAT défini, certains paramètres des messages SIP sont adaptés.

- **Utiliser l'IP statique**

  Les modems DSL ou les routeurs Internet utilisent une adresse IP statique (adresse IP publique) et le fournisseur ITSP a besoin d'une authentification IP statique. L'adresse IP statique et le port utilisés par le modem ou le routeur doivent être indiqués.

- **Routeur de préservation de port**

  L'adresse IP publique est déterminée à l'aide de STUN. Le port est inscrit sans modification dans les messages SIP.

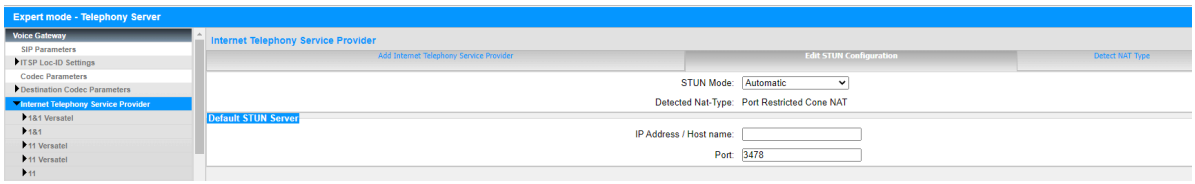
9.2.2.1 Comment déterminer le mode STUN

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence du menu, cliquez sur **Internet Telefonie Service Provider - fournisseur de services de téléphonie sur Internet**.
4) Cliquez sur l'onglet **Modifier la configuration STUN**.



5) Dans la liste déroulante **Mode STUN**, sélectionnez le mode STUN souhaité.
6) Si vous avez sélectionné le mode STUN **Utiliser l'IP statique** entrez dans **Adresse IP Publique** et **Port SIP public** l'adresse IP statique et le port du modem DSL ou du routeur Internet.
7) Cliquez sur **Appliquer** puis sur **OK**.

9.3 Accès réseau via lignes numériques et analogiques

L'accès réseau relie le système de communication au réseau public (RTC) via des lignes RNIS ou des lignes analogiques.

Les assistants facilitent la configuration d'un accès réseau RNIS ou d'un accès réseau analogique.

9.3.1 Lignes

Les lignes relient les plates-formes matérielles au réseau public (RTC). Il doit être attribué à chaque ligne un faisceau qui permet d'affecter à la ligne différentes propriétés.

Par défaut, il est attribué à toutes les lignes un indicatif de ligne et un faisceau. Ces affectations peuvent être modifiées par l'administrateur.

Avec un raccordement réseau RNIS on parle aussi pour les lignes de canaux B.

Code de ligne

À partir du code de ligne, le système de communication occupe la ligne correspondant au code de ligne. Le code de ligne sert aussi à programmer une touche de ligne ou à contrôler une ligne.

Affectation MSN

Le fournisseur de services attribue à chaque raccordement multiposte RNIS (PMP, Point-à-Multipoint) un ou plusieurs MSN (Multiple Subscriber Number, numéro d'abonné multiple). Ceux-ci peuvent être affectés directement à une ligne.

Numéros système

Les numéros système comprennent le préfixe international, les indicatifs de pays et les indicatifs locaux et le numéro de l'installation ou bien un ou plusieurs MSN.

Protocole RNIS

Le protocole RNIS utilisé est fonction de l'indicatif national. Il ne doit être modifié que dans le cas où la liaison avec le RTC exige impérativement un protocole différent. On dispose d'un grand nombre de modèles de protocole qui doivent être adaptés aux besoins spécifiques. Les informations nécessaires vous sont fournies par votre fournisseur de services.

Mode de prise du canal B

Différents canaux B d'une ligne RNIS peuvent être verrouillés pour le trafic sortant et/ou entrant.

Les modes de prise du canal B suivants sont possibles :

- seulement sortant
- seulement entrant
- sortant et entrant (par défaut)

Le mode de prise du canal B est uniquement évalué lorsque le système de communication doit proposer un banal B. C'est le cas dans les situations suivantes :

S_2 sortant :	Dans ce cas, le système de communication doit proposer un canal B.
S_2 entrant :	Le côté opposé est obligé de proposer un canal B. Ce canal B est repris par le système de communication sans contrôle du paramétrage. Le paramétrage n'a donc aucune influence.
S_0 sortant :	Comme le système de communication ne prescrit aucun canal B (any channel), le paramétrage n'a aucune influence.
S_0 entrant :	Si le côté opposé établit la communication sans prescrire de canal B, le système de communication propose un canal B. Lors de cette proposition, le mode de prise du canal B réglé est pris en compte.

Numérotation pour lignes réseau analogiques (HKZ)

Le mode de numérotation est reconnu automatiquement par le système de communication lors de la prise de ligne. Pour certains cas particuliers, il est possible de paramétrer directement la numérotation multifréquence (MF) ou la numérotation décimale (DC).

9.3.1.1 Comment configurer l'accès réseau RNIS

L'Assistant **Ligne réseau RNIS / Analogique / ITSP** vous permet de configurer l'accès réseau RNIS. Selon les ports disponibles dans le système de communication pour les lignes réseau (RNIS ou analogique), l'Assistant passe par différentes étapes.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Le système de communication est raccordé à une ligne réseau RNIS.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Ligne réseau RNIS/ analogique/ITSP**. L'Assistant présente une vue d'ensemble des boîtiers, des emplacements et des ports S_0.
4) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. `49` pour l'Allemagne ou `1` pour les Etats-Unis.
5) Dans le champ **Préfixe du réseau local**, entrez le préfixe du réseau local, par ex. 89 pour Munich.
6) Si vous avez un raccordement système, entrez dans le champ **N° installation** le numéro de l'installation de votre raccordement réseau, par ex. 7007 (votre numéro de raccordement).

7) Modifiez le champ **Préfixe international** uniquement si nécessaire. pour Allemagne on a `00`, pour les Etats-Unis `011`).

   Lors des appels téléphoniques à l'étranger, le numéro de téléphone est précédé du préfixe international et de l'indicatif national, par ex. d'Allemagne aux Etats-Unis `00-1` et des Etats-Unis à l'Allemagne `011-49`.

8) Cliquez sur **OK&Suivant**.

9) Sélectionnez un des types de connexion suivants pour le raccordement correspondant (boîtier, emplacement et port S_0) :

   - Si vous souhaitez configurer un raccordement système, cliquez sur le champ d'option **Raccordement système**.
   - Si vous souhaitez configurer un raccordement multiposte, cliquez sur le champ d'option **Raccordement multiposte**.

10) Cliquez sur **OK&Suivant**.

11) S'il s'agit d'un raccordement multiple, indiquez le MSN pour le raccordement correspondant (boîtier, emplacement et port S_0 et cliquez sur **OK&Suivant**.

12) Conservez le paramétrage de la case **Pas de téléphonie par Internet** et cliquez sur **Ignorer**.

13) Dans la liste déroulante **D´abord par**, sélectionnez la ligne extérieure préférée et cliquez sur **OK&Suivant**.

14) Cliquez sur **OK&Suivant** puis sur **Terminer**.

9.3.1.2 Comment configurer l'accès réseau analogique

L'Assistant **Ligne réseau RNIS / Analogique / ITSP** vous permet de configurer l'accès réseau analogique.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Votre système de communication est raccordé à une ligne réseau analogique.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.

3) Cliquez sur **Modifier** pour lancer l'Assistant **Ligne réseau RNIS/ analogique/ITSP**. L'Assistant présente une vue d'ensemble des boîtiers, des emplacements et des ports analogiques.

4) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. `49` pour l'Allemagne ou `1` pour les Etats-Unis.

5) Dans le champ **Préfixe du réseau local**, entrez le préfixe du réseau local, par ex. 89 pour Munich.

6) Si vous avez un raccordement système, entrez dans le champ **N° installation** le numéro de l'installation de votre raccordement réseau, par ex. 7007 (votre numéro de raccordement).

7) Modifiez le champ **Préfixe international** uniquement si nécessaire. pour Allemagne on a `00`, pour les Etats-Unis `011`).

   Lors des appels téléphoniques à l'étranger, le numéro de téléphone est précédé du préfixe international et de l'indicatif national, par ex. d'Allemagne aux Etats-Unis `00-1` et des Etats-Unis à l'Allemagne `011-49`.

8) Cliquez sur **OK&Suivant**.

9) Cliquez sur **Ignorer RNIS**.

10) Conservez le paramétrage de la case **Pas de téléphonie par Internet** et cliquez sur **Ignorer**.

11) Dans la liste déroulante **Protocole**, sélectionnez le protocole pour l'affichage du numéro de téléphone (en fonction du fournisseur de services).

    - Si vous souhaitez utiliser Frequency Shift Keying, sélectionnez **FSK**.
    - Si vous souhaitez utiliser le mode de sélection multifréquence, sélectionnez **DTMF**.
    - Si vous ne souhaitez pas utiliser l'affichage du numéro de téléphone, sélectionnez **Néant**.

12) Cliquez sur **OK&Suivant**.

13) Cliquez sur **Modifier** pour paramétrer les caractéristiques de la ligne concernée. Si nécessaire, modifiez **Numérotation**, **Détection appel**, **Flash**, **Longueur de la ligne** et **Flags** et cliquez sur **OK**.

14) Cliquez sur **OK&Suivant**.

15) Cliquez sur **Ignorer** et sur **OK&Suivant**.

16) Dans la liste déroulante **D´abord par**, sélectionnez la ligne extérieure préférée et cliquez sur **OK&Suivant**.

17) Cliquez sur **OK&Suivant** puis sur **Terminer**.

9.3.1.3 Comment afficher toutes les lignes

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.

3) Dans l'arborescence du menu, cliquez sur **Lignes/Routage** > **Lignes**. En fonction de la configuration du système de communication, il vous est présenté toutes les lignes possibles, y compris code de ligne et faisceau.

9.3.1.4 Comment afficher une ligne individuelle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Naviguez dans l'arborescence menu sous **Lignes/Routage** > **Lignes** > **…** pour accéder à la ligne souhaitée. Le système vous présente la ligne raccordée au système de communication, y compris le code de ligne.
4) Cliquez sur **OK**.

9.3.1.5 Comment modifier l'indicatif de ligne

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Naviguez dans l'arborescence menu sous **Lignes/Routage** > **Lignes** > **…** pour accéder à la ligne souhaitée.
4) Cliquez sur l'onglet **Modifier la ligne**.
5) Dans le champ **Indicatif**, entrez la valeur souhaitée.

Remarque : Si aucune valeur n'est inscrite comme indicatif, cette ligne n'a pas de code de ligne.

---

6) Cliquez sur **Appliquer** puis sur **OK**.

9.3.1.6 Comment affecter le MSN à une ligne

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes / Réseau**.
3) Dans l'arborescence du menu, cliquez sur **Lignes/Routage** > **Affecter le MSN**.
4) Dans l'arborescence du menu, cliquez dans **Affecter le MSN** sur l'entrée que vous voulez modifier.
5) Entrez le **MSN**.
6) Dans la liste déroulante **Lignes**, sélectionnez la ligne que vous voulez affecter.
7) Cliquez sur **Appliquer** puis sur **OK**.

9.3.1.7 Comment modifier le protocole RNIS

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes / Réseau**.
3) Naviguez dans l'arborescence du menu vers **Lignes/Routage** > **Lignes** > **...** jusqu'au port souhaité.
4) Cliquez sur l'onglet **Modifier les flags RNIS**.
5) Dans la zone **Protocole: Description**, sélectionnez le protocole souhaité dans la liste déroulante.
6) Cliquez sur **Appliquer** puis sur **OK**.

9.3.1.8 Comment modifier le mode de prise du canal B

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes / Réseau**.
3) Naviguez dans l'arborescence du menu vers **Lignes/Routage** > **Lignes** > **...** jusqu'au port souhaité.
4) Cliquez sur l'onglet **Modifier le canal B**.
5) En fonction de vos souhaits, décochez pour chaque canal des cases des colonnes **Sortant** et **Entrant**.
6) Cliquez sur **Appliquer** puis sur **OK**.

9.3.1.9 Comment modifier le mode de numérotation

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes / Réseau**.
3) Naviguez dans l'arborescence du menu vers **Lignes/Routage** > **Lignes** > **...** jusqu'au port souhaité.
4) Cliquez sur l'onglet **Modifier les flags analogiques**.
5) Réglez la numérotation multifréquence (MF) ou la numérotation décimale (DC).

6) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2 Faisceaux

A l'aide des faisceaux, il est possible d'associer les lignes (canaux B). Il est possible de configurer des paramètres spécifiques pour chaque faisceau de lignes (= Faisceau).

Il est possible d'affecter un faisceau à chacune ligne. Par défaut le faisceau 1 est affecté à toutes les lignes.

Il est possible d'attribuer un nom et un indicatif de faisceau à chaque faisceau.

Conseil : Les préfixes faisceaux des prises de ligne sortantes ne sont opérationnels que si LCR n'est pas activé.

Répartition du canal B

La répartition des canaux B entre différents faisceaux de lignes est également appelée répartition du canal B. Avec les connexions réseau RNIS comptant de nombreux canaux B, comme les raccordements S_{2M}, il peut être judicieux de répartir les canaux B entre différents faisceaux de lignes.

Pour les communications sortantes, seuls sont sélectionnés les canaux B qui font partie du faisceau de lignes (par ex. faisceau de lignes sélectionné à l'aide de l'indicatif de faisceau, faisceau de débordement ou faisceau de lignes sélectionné par LCR).

Les communications entrantes sont toujours acceptées, indépendamment du faisceau. En règle générale, le canal B qui est proposé par le partenaire est occupé. Pour cette raison, la répartition du canal B configurée dans le système doit être supportée également du côté partenaire (installation ou réseau public). Si ce n'est pas le cas, il est alors impossible de garantir l'affectation correcte de l'appel par rapport au faisceau de lignes correspondant.

Touche de faisceau

Un abonné peut programmer une touche de faisceau sur le téléphone. Une touche de faisceau est réservé aux appels sortants. Les appels émis à l'aide des touches de faisceau sont soumis aux niveaux et aux règles de discrimination réseau COS.

Une fois que l'abonné a appuyé sur une touche de faisceau (ou a sélectionné un indicatif de faisceau), le système de communication occupe une ligne disponible correspondant à la direction pour établir la liaison. Le téléphone indique le numéro de ligne à l'écran. Si toutes les lignes du faisceau sont occupées, la LED correspondante s'allume, y compris en cas de débordement réussi.

Débordement lorsque LCR est désactivé

L'administrateur peut pour chaque faisceau définir une direction de débordement. Lors d'une tentative de prise de ligne, si toutes les lignes d'un faisceau sont occupées, la recherche se poursuit dans le faisceau de débordement. Si toutes les lignes sont également occupées sur le faisceau de débordement, il n'y a pas d'autre débordement.

Débordement lorsque LCR est activé

Dans le cadre de la configuration LCR, l'administrateur peut configurer jusqu'à 16 entrées par table de routage, qui sont alors traitées successivement comme pour un débordement.

Prise

Pour une prise de ligne sortante, l'administrateur peut déterminer à l'aide du type de prise le critère selon lequel le système de communication va rechercher une ligne disponible sur le faisceau correspondant. Cela est réalisé en définissant le type de prise de la manière suivante :

- Cyclique:

  Après la ligne sortante occupée en dernier - la recherche débute avec le numéro de ligne suivant le plus élevé, rapportée à la ligne sortante occupée en dernier dans ce faisceau. Ainsi, toutes les lignes sont utilisées environ avec la même fréquence.
- Linéaire :

  Toujours la premier ligne libre - la recherche commence avec le numéro de ligne le plus bas qui est affecté à ce faisceau.

Numéro d'installation entrant et sortant

L'administrateur peut définir séparément le numéro de l'installation entrant et le numéro de l'installation sortant. Ainsi, le propre numéro de téléphone peut, pour les communications sortantes, être représenté différemment de ce qui est nécessaire pour permettre d'être joint par les communications entrantes. Les parties correspondant à l'indicatif national, à l'indicatif du réseau local et au numéro de l'installation doivent être inscrites séparément. Pour qu'il y ait des entrées différentes pour le numéro d'installation entrant et sortant, il faut le réseau dispose de la fonctionnalité "CLIP No Screening". S'il n'a pas été configuré de numéro d'installation sortant, le système de communication utilise toujours les données du numéro d'installation entrant.

En cas de prise d'appel entrant sur une ligne RNIS, le système de communication masque dans le numéro reçu les parties correspondant au numéro de l'installation entrant, en fonction du type de numéro reçu (Type Of Number = TON, voir tableau dans Transfert du numéro de téléphone) avec alignement à gauche et interprète la partie restante comme un numéro SDA. En cas d'information sur le numéro fournie au RTC, le système de communication utilise automatiquement les parties du numéro de l'installation sortant comme la partie initiale du numéro d'appel, en fonction du type de numéro d'appel sortant configuré. En Allemagne, la partie du numéro de l'installation doit être indiqué au niveau du raccordement réseau sans l'indicatif du réseau local et sans l'identifiant de renvoi distinct (0).

Transfert du numéro de téléphone

Le numéro de téléphone qui est envoyé au RTC et au destinataire se compose de la manière suivante :

Type Of Number (TON), sortant	numéro transmis au RTC
Inconnu(e) TON=Unknown	uniquement numéro SDA (paramètre par défaut)
Numéro de l'installation TON=Subscriber	Numéro de l'installation + numéro SDA
Indicatif du réseau local TON=National	Indicatif du réseau local + numéro de l'installation + numéro SDA
Indicatif national TON=International	Indicatif national + indicatif du réseau local + numéro de l'installation + numéro SDA
Interne TON=Intern	uniquement pour système en réseau : dans un plan de numérotation fermé, on ne peut pas compléter avec un préfixe de numéro. Ici, le complément au numéro d'appel est masqué.

De plus, il est possible d'indiquer l'information concernant le numéro d'appel envoyé par l'abonné qui effectue la sélectionné en direction de l'abonné de destination.

Type de numéro	numéro transmis au RTC
Interne	Ici, il est envoyé uniquement une information sur le numéro interne. Si l'abonné destinataire est externe, il n'est envoyé aucun numéro ou bien le numéro de téléphone du poste opérateur. Pour les abonnés destinataires, il est possible d'afficher le numéro de téléphone interne.
SDA	Il n'est envoyé ici qu'une information à propos du numéro SDA. Pour les abonnés destinataires internes dans un autre noeud, il manque le numéro interne pour l'affichage. Pour les destinations externes, l'information sur le numéro d'appel est suffisante.
Interne/SDA	Dans une mise en réseau, il est judicieux de sélectionner ce paramétrage. Il est envoyé à l'abonné destinataire aussi bien le numéro interne que le numéro SDA. Si, à l'intérieur de ce réseau, un abonné interne est appelé, il peut être affiché à cet abonné le numéro interne de l'appelant. Si l'abonné destinataire interne a activé par exemple un renvoi d'appel en direction d'une destination externe, il est dans ce cas envoyé un numéro SDA.

En plus, il est possible de configurer le traitement souhaité pour le préfixe de faisceau.

- Appels entrants

  Lors de la tranmission au bus S0, le numéro d'appel est complété par l'indicatif de faisceau (-> format au choix pour rappel) ou transmis de manière transparente. Par défaut : activé.
- Appel sortant

  La représentation du numéro composé sur le téléphone système est effectuée avec ou sans préfixe de faisceau. Par défaut : activé.

Second indicatif réseau

Un second indicatif réseau est défini si le système de communication est une sous-installation d'un autre système de communication ou est en réseau avec plusieurs autres systèmes de communication. Il ne s'applique qu'aux faisceaux de mise en réseau (type de faisceau=PABX). Dans ce cas, le second indicatif réseau sert d'indicatif de prise de ligne pour l'installation principale. A l'intérieur d'une mise en réseau, il faut configurer les indicatifs de prise de réseau, les indicatifs de faisceau et le second indicatif réseau de manière unifiée. La valeur par défaut en Allemagne est 0.

9.3.2.1 Comment modifier l'affectation de faisceau

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Naviguez dans l'arborescence menu sous **Lignes/Routage** > **Lignes** > **…** pour accéder à la ligne souhaitée.
4) Cliquez sur l'onglet **Modifier la ligne**.
5) Dans la liste déroulante **Faisceau**, sélectionnez le faisceau que vous voulez attribuer à la ligne.
6) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.2 Comment modifier le nom du faisceau

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur l'entrée que vous voulez modifier.
5) Dans le champ **Nom du faisceau**, entrez la valeur souhaitée.

6) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.3 Comment modifier l'indicatif du faisceau

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Remarque : Les indicatifs de faisceaux ne sont opérationnels que si l'acheminent LCR n'est pas actif.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur l'entrée que vous voulez modifier.
5) Dans le champ **Préfixes faisceaux**, entrez la valeur souhaitée.
6) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.4 Comment configurer un débordement lorsque LCR est désactivé

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes / Réseau**.
3) Dans l'arborescence du menu, cliquez sur **Lignes/Routage** > **Sens**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur l'entrée que vous voulez modifier.
5) Dans la liste déroulante **Débordement**, sélectionnez l'entrée souhaitée.
6) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.5 Comment configurer un débordement lorsque LCR est activé

Lorsque LCR est activé, la gestion du débordement est assurée par le traitement successif des différentes entrées de la table de routage LCR dans le cadre de la configuration LCR (voir LCR (Least Cost Routing)).

9.3.2.6 Comment configurer la prise de ligne

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur le faisceau que vous voulez modifier.
5) Cliquez sur l'onglet **Modifier les paramètres faisceaux**.
6) Dans la liste déroulante **Prise**, sélectionnez **cyclique** ou **linéaire**.
7) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.7 Comment inscrire le numéro d'installation entrant et sortant

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes / Réseau**.
3) Dans l'arborescence du menu, cliquez sur **Lignes/Routage** > **Sens**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur l'entrée que vous voulez modifier.
5) Entrez dans la zone **N° installation entrant** dans les champs **Indicatif national**, **Préfixe du réseau local** et **N° installation** les valeurs correspondantes sans zéros à gauche.
6) Entrez dans la zone **N° installation sortant** dans les champs **Indicatif national**, **Préfixe du réseau local** et **N° installation** les valeurs correspondantes sans zéros à gauche.
7) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez masquer le numéro de téléphone de l'abonné, cochez **Masquer le n° de téléphone de l'abonné**.
   - Si vous souhaitez pas masquer le numéro de téléphone de l'abonné, décochez **Masquer le n° de téléphone de l'abonné**.
8) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.8 Comment configurer le format des numéros de téléphone transmis

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur le faisceau que vous voulez modifier.
5) Cliquez sur l'onglet **Modifier les paramètres faisceaux**.
6) Dans la liste déroulante **N° type, sortant** sélectionnez le format souhait pour les numéros de téléphone transmis.
7) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.9 Comment configurer le type de numéro de téléphone transmis

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur le faisceau que vous voulez modifier.
5) Cliquez sur l'onglet **Modifier les paramètres faisceaux**.
6) Sélectionnez dans la liste déroulante **Type numéro d'appel** l'entrée **Interne**, **SDA** ou **Interne/SDA**.
7) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.10 Comment configurer le préfixe réseau

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur le faisceau que vous voulez modifier.
5) Cliquez sur l'onglet **Modifier les paramètres faisceaux**.

6) Sélectionnez une des possibilités suivantes :
   - Si vous voulez compléter par l'indicatif de faisceau l'affichage du numéro de téléphone pour les communications entrantes, dans la zone **Flags faisceaux** cochez la case **Compléter le préf.réseau entrant**.
   - Si vous voulez pas compléter par l'indicatif de faisceau l'affichage du numéro de téléphone pour les communications entrantes, dans la zone **Flags faisceaux** décochez la case **Compléter le préf.réseau entrant**.
   - Si vous voulez compléter par l'indicatif de faisceau l'affichage du numéro de téléphone pour les communications sortantes, dans la zone **Flags faisceaux** cochez la case **Compléter le préf.réseau sortant**.
   - Si vous voulez pas compléter par l'indicatif de faisceau l'affichage du numéro de téléphone pour les communications sortantes, dans la zone **Flags faisceaux** décochez la case **Compléter le préf.réseau sortant**.
7) Cliquez sur **Appliquer** puis sur **OK**.

9.3.2.11 Comment définir un faisceau pour la mise en réseau et inscrire un second indicatif réseau

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur l'entrée que vous voulez modifier.
5) Dans le champ **Indicatif réseau (2e AKZ)**, entrez la valeur souhaitée.
6) Cliquez sur l'onglet **Modifier les paramètres faisceaux**.
7) Dans la liste déroulante **Type faisceau**, sélectionnez l'entrée **PABX**.
8) Cliquez sur **Appliquer** puis sur **OK**.

9.3.3 Surveillance de la tonalité d'invitation à numéroter

Lors de l'établissement de la liaison via une ligne réseau analogique, l'émission des chiffres composés en direction du réseau ne peut avoir lieu que si la tonalité d'invitation à numéroter (acoustique) a été reconnue. Comme le temps nécessaire pour l'arrivée de la tonalité d'invitation à numéroter varie en fonction de l'opérateur du réseau et des conditions du réseau, il faut surveiller l'arrivée de la tonalité d'invitation à numéroter.

La configuration de la durée de surveillance de la tonalité d'invitation à numéroter et du délai de composition des chiffres est réalisée dans Manager E.

Temporisation de la surveillance de la tonalité d'invitation à numéroter

La surveillance de la tonalité d'invitation à numéroter peut intervenir immédiatement ou après une pause. Dans certains cas, il est diffusé des tonalités supplémentaires à l'abonné après la prise de ligne, par ex. pour lui

faire savoir qu'un renvoi est activé sur le réseau. Pour ces cas, il est possible de programmer une temporisation de la surveillance de la tonalité d'invitation à numéroter (pause avant numérotation, 1 à 9 secondes). Les chiffres numérotés ne sont envoyés au réseau qu'une fois cette pause écoulée.

Remarque : Remarque pour le Brésil :

Si la numérotation MF est émise à partir de terminaux analogiques, en liaison avec des lignes réseau analogiques (TLAx et TML8W) et en cas de numérotation décimale après la surveillance de la tonalité d'invitation à numéroter, il peut se produire des problèmes avec le contrôle de la numérotation si l'indicatif national du Brésil est paramétré. Dans ce cas, les signaux MF sont émis directement depuis les terminaux analogiques vers les lignes réseau analogiques. Tous les signaux MF qui ont été composés avant la réception de la tonalité d'invitation à numéroter sont perdus. Dans ce cas, le routage automatique (LCR) doit être activé afin que la fonction de numérotation et le contrôle de la numérotation du terminal se déroulent parfaitement.

Durée de surveillance de la tonalité d'invitation à numéroter

La durée d'attente de la tonalité d'invitation à numéroter peut être configurée. Si, à l'issue de la durée configurée aucune tonalité d'invitation à numéroter n'est reconnue, la ligne est mise hors service. Le système contrôle à intervalles cyclique si la tonalité d'invitation à numéroter est toujours disponible. Si c'est le cas, la ligne concernée est remise en service.

Délai de composition des chiffres

Il est possible de régler l'intervalle en seccondes entre la reconnaissance de la tonalité d'invitation à numéroter et l'envoi du premier chiffre au réseau (par défaut : 0 s).

Evaluation de la deuxième tonalité d'invitation à numéroter

Le système de communication est en mesure de reconnaître une tonalité d'invitation à numéroter supplémentaire (2e signal acoustique). Cela concerne les opérateurs réseau publics qui émettent une seconde tonalité d'invitation à numéroter pour les communications avec l'étranger, par ex. pour la Belgique après 00 et pour la France après 16 ou encore 19. Cette fonction ne s'applique pas à l'Allemagne.

9.3.3.1 Comment configurer la temporisation de la surveillance de la tonalité d'invitation à numéroter

Conditions préalables

Un port analogique avec accès réseau analogique est disponible.

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur le faisceau analogique que vous voulez modifier.
5) Cliquez sur l'onglet **Modifier les paramètres faisceaux**.
6) Si la surveillance de la tonalité d'invitation à numéroter doit intervenir immédiatement, dans la zone **Pause avant numérotation**, sélectionnez le champ d'option **Evaluation de la tonalité**.
7) Si la surveillance de la tonalité d'invitation à numéroter ne doit intervenir qu'après un certain délai de temporisation, sélectionnez dans le zone **Pause avant numérotation** le délai de temporisation en secondes.
8) Cliquez sur **Appliquer** puis sur **OK**.

9.3.3.2 Comment configurer la durée de surveillance de la tonalité d'invitation à numéroter

Conditions préalables

Un module réseau analogique est connecté.

Étape par étape

1) Ouvrez une session sur le PC Admin de Manager E.
2) Dans la barre de menu, cliquez sur **Fichier | Transférer**
3) Sélectionnez l'onglet **Communications**.
4) Dans la plage **Accès** activez le champ d'option en fonction du type de raccordement du PC Admin au système de communication.
5) Activez le champ d'option **Lecture/Ecriture KDS** et cliquez sur **Pièces jointes -> PC**.
6) Cliquez sur **OK**. Le KDS est transmis du système de communication à Manager E.
7) Une fois la transmission effectuée, cliquez sur **OK** puis sur **Fermer**.
8) Dans Manager E, dans l'arborescence du menu de la vue système, cliquez sur **Paramètres** > **Paramètres système** > **Temporisations**.
9) Dans la liste, dans **Durée de surveillance de la tonalité d'invitation à numéroter**, définissez la durée maximale d'attente de la tonalité d'invitation à numéroter, en agissent sur la **Base** et le **Facteur** (par défaut : Base = `1 s`, Facteur = `10`).
10) Cliquez sur **Appliquer**.
11) Dans la barre de menu, cliquez sur **Fichier | Transférer**
12) Sélectionnez l'onglet **Communications**.
13) Cliquez sur **PC > Installation** puis sur **OK**. Les paramètres sont transmis au système de communication.
14) Pour finir, cliquez sur **OK** et **Fermer**.

9.3.3.3 Comment configurer le délai de composition des chiffres

Conditions préalables

Un module réseau analogique est connecté.

Étape par étape

1) Ouvrez une session sur le PC Admin de Manager E.
2) Dans la barre de menu, cliquez sur **Fichier | Transférer**
3) Sélectionnez l'onglet **Communications**.
4) Dans la plage **Accès** activez le champ d'option en fonction du type de raccordement du PC Admin au système de communication.
5) Activez le champ d'option **Lecture/Ecriture KDS** et cliquez sur **Pièces jointes -> PC**.
6) Cliquez sur **OK**. Le KDS est transmis du système de communication à Manager E.
7) Une fois la transmission effectuée, cliquez sur **OK** puis sur **Fermer**.
8) Dans Manager E, dans l'arborescence du menu de la vue système, cliquez sur **Paramètres** > **Paramètres système** > **Temporisations**.
9) Dans la liste, dans **Délai entre la reconnaissance de tonalité et la composition du préfixe réseau** avec **Base** et **Facteur**, régler l'intervalle de temps en secondes entre la reconnaissance de la tonalité d'invitation à numéroter et l'envoi du premier chiffre de la numérotation au réseau (par défaut : base = `10 ms`, Facteur = `0`).
10) Cliquez sur **Appliquer**.
11) Dans la barre de menu, cliquez sur **Fichier | Transférer**
12) Sélectionnez l'onglet **Communications**.
13) Cliquez sur **PC > Installation** puis sur **OK**. Les paramètres sont transmis au système de communication.
14) Pour finir, cliquez sur **OK** et **Fermer**.

9.3.3.4 Comment activer ou désactiver l'évaluation de la deuxième tonalité d'invitation à numéroter

Conditions préalables

Un port analogique avec accès réseau analogique est disponible.

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes / Réseau** > **Faisceau**.
4) Dans l'arborescence du menu, dans **Sens**, cliquez sur le faisceau analogique que vous voulez modifier.
5) Cliquez sur l'onglet **Modifier les paramètres faisceaux**.

6) Pour activer l'évaluation de la deuxième tonalité d'invitation à numéroter, dans la zone **Flags faisceaux**, cochez la case **Evaluation de la 2e tonalité d'invitation à numéroter**.
7) Pour désactiver l'évaluation de la deuxième tonalité d'invitation à numéroter, dans la zone **Flags faisceaux**, décochez la case **Evaluation de la 2e tonalité d'invitation à numéroter / Surveillance de la ligne**.
8) Cliquez sur **Appliquer** puis sur **OK**.

9.4 Priorisation du réseau lorsque LCR est activé

La priorité pour l´indicatif réseau permet de définir dans quel ordre les différents fournisseurs d'accès (RNIS/Analogique ou ITSP) sont sélectionnés.

L'indicatif réseau est normalement obtenu en composant le "0". Sous cet indicatif, différents fournisseurs sont priorisés (selon le réglage par défaut). Il est ainsi possible de sélectionner un appel sortant via un ITSP dans un premier temps puis, en cas d'échec, d'utiliser le réseau RNIS.

9.4.1 Comment définir une priorité pour l'Indicatif réseau

L'assistant **Ligne réseau RNIS / Analogique / ITSP** permet de configurer l'ordre des prise de ligne via RNIS/Analogique et ITSP.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**. Plusieurs ITSP (fournisseur d'accès téléphonie Internet) sont configurés.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Ligne réseau RNIS/ analogique/ITSP**. L'Assistant présente une vue d'ensemble des boîtiers, des emplacements et des ports analogiques.
4) Cliquez sur **OK&Suivant**.
5) Cliquez plusieurs fois sur **OK&Suivant** jusqu'à ce que la fenêtre **Priorité pour l´indicatif réseau** s'affiche.
6) Dans la zone **Tentatives de prise réseau**, liste déroulante **D´abord par**, sélectionnez le fournisseur préféré qui sera utilisé en premier par le système de communication pour obtenir une ligne libre.
7) Dans la liste déroulante **Puis par**, sélectionnez un deuxième fournisseur qui sera utilisé pour effectuer la deuxième tentative pour obtenir une ligne.
8) Dans la liste déroulante suivante **Puis par**, sélectionnez un troisième fournisseur qui sera utilisé pour effectuer la tentative pour obtenir une ligne.
9) Cliquez sur **OK&Suivant** puis sur **Terminer**.

10 Abonnés

Un abonné ou une station est un partenaire de communication connecté au système de communication. En général, un terminal est attribué à chaque station (à l'exception des stations virtuelles). Un terminal est, par exemple, un téléphone, un PC ou un télécopieur. Les stations peuvent également être des utilisateurs des clients UC.

Il existe les types de stations suivants :

- les stations IP (également appelées clients IP)
- stations SIP (un sous-ensemble de stations IP)
- Stations UP0.
- Abonnés DECT
- Postes Mitel SIP-DECT
- Abonnés ISDN
- les stations analogiques
- Les stations de mobilité (stations mobiles, voir Mobilité)
- Abonnés virtuels

Les données des abonnés (nom, numéro de poste, numéro SDA, adresse e-mail, etc.) peuvent être importées sous forme de fichier XML lors de l'installation initiale (voir Plan de numérotation individuel). En outre, les données relatives aux abonnés peuvent également être exportées vers un fichier XML (voir Exportation des données relatives aux abonnés).

Procédure d'octroi de licences pour les stations

Toutes les stations sont soumises à l'obtention d'une licence. Pour commencer, les stations peuvent être configurées lors de l'installation initiale ou ultérieurement à l'aide des assistants de station. Après une installation réussie, les abonnés peuvent effectuer des appels internes. Dans l'étape suivante, les licences des stations doivent être activées et attribuées aux stations. Une fois les licences attribuées avec succès, les abonnés peuvent également effectuer des appels externes.

Concepts associés

Licences à la page 247
Mobilité à la page 888

10.1 Plan de numérotation

Le plan de numérotation est une liste de tous les numéros de téléphone et indicatifs disponibles dans le système de communication. Il contient notamment les numéros de téléphone internes, les numéros SDA et les numéros des appels de groupe. Dans le système de communication, les numéros d'appel et les indicatifs sont préconfigurés avec des valeurs par défaut. Si nécessaire, ces valeurs peuvent être adaptées.

Il se peut, lors de la configuration des numéros ou indicatifs, que des messages d'erreur s'affichent si le numéro souhaité est déjà occupé. A l'aide du plan de numérotation, vous pouvez contrôler quels numéros restent encore à attribuer.

10.1.1 Plan de numérotation par défaut

Le plan de numérotation par défaut comprend tous les numéros d'appel et les codes prédéfinis dans le système de communication avec des valeurs par défaut.

Ces valeurs par défaut peuvent être modifiées selon les besoins. Certains numéros peuvent également être complètement supprimés afin qu'ils n'apparaissent plus dans un aperçu du plan de numérotation.

Plan de numérotation par défaut pour les plateformes matérielles et le commutateur logiciel :

Type de numéros d'appel	X1	X5/X8/S	Action
Numéros de station internes	11-30	100-742	supprimable
Numéros d'appel direct entrants de l'utilisateur	11 -30	100-742	supprimable
Numéros d'appel de groupe 1-90 Numéros d'appel de groupe 91-800	31-40 -	350-439 non préréglé	supprimable
numéro de station principale	700-703	à partir de 7801	supprimable
Codes de saisie (codes externes) : Trk. Grp 1 (liaison principale : ISDN, analogique) Route 8 (Suite UC) Trk. Groupe 12-15 (tronc : ITSP) Route 16 (Réseautage)	0 = Monde / 9 = États-Unis - non préréglé non préréglé	0 = Monde / 9 = États-Unis 851 855-858 859	uniquement modifiable
Code de l'agent (position d'interception), Interne	9 = Monde 0 = ÉTATS-UNIS	9 = Monde 0 = ÉTATS-UNIS	uniquement modifiable
Code de l'opérateur (position d'interception), numérotation directe entrante	0 = LIGNE – = ÉTATS-UNIS	0 = LIGNE – = ÉTATS-UNIS	uniquement modifiable
Numéros de station pour les utilisateurs en ligne	non préréglé	749	uniquement modifiable
Numéro d'appel pour l'accès à distance	non préréglé	non préréglé	uniquement modifiable
Numéro d'appel pour la messagerie vocale UC Smart Suite UC	351 -	351 non préréglé	uniquement modifiable uniquement modifiable

Type de numéros d'appel	X1	X5/X8/S	Action
numéros de conférence téléphonique	-	non préréglé	uniquement modifiable
Numéro d'appel pour le stationnement	-	non préréglé	uniquement modifiable
Numéros de standard automatique	-	non préréglé	uniquement modifiable
Numéro de poste pour la console de l'agent de bord	9 = Monde 0 = ÉTATS-UNIS	9 = Monde 0 = ÉTATS-UNIS	uniquement modifiable
Substitution de « # » (pour les codes de service)	75	75	supprimable
Substitution de « # » (pour les codes de service)	76	76	supprimable
Codes de service			uniquement modifiable

10.1.2 Plan de numérotation individuel

Le système de communication permet la configuration d'un plan de numérotation individuel. De plus, les valeurs par défaut des numéros et des indicatifs peuvent être modifiées. Lors d'une recharge du système de communication, les valeurs sont réinitialisées à leur état par défaut.

Les actions suivantes sont alors utiles :

- Effacer les numéros par défaut : à certaines exceptions près (numéros par défaut spécifiques), les numéros par défaut peuvent être effacés. Ces numéros sont identifiés dans le tableau du plan de numérotation standard, dans la colonne "Action" par "effaçable".
- Modifier les numéros par défaut spécifiques : ces numéros ne doivent pas être effacés. Mais les valeurs de ces numéros peuvent être modifiées. Ces numéros sont identifiés dans le tableau du plan de numérotation standard, dans la colonne "Action" par "uniquement modifiable".
- Importer les numéros et les données d'abonnés : les données d'abonnés peuvent être importées par un fichier XML durant la première installation. Dans ce cas, le numéro d'appel et le numéro SDA des abonnés sont également importés. En règle générale, cela est effectué lors de la première installation.

Importation des données d'abonnés via fichier XML

Un plan de numérotation individuel peut être importé dans le système de communication à l'aide d'un fichier XML au format UTF-8, durant la première installation.

Le programmes d'administration OpenScape Business Assistant présente dans **Centre de service** > **Documents** > **Modèles CSV** le fichier `csv-templates.zip`. Ce fichier Zip comprend notamment les fichiers suivants, y compris la description.

- `portdata_xml_import_empty.xml`

  Ce modèle comprend les onglets sans exemples de données. Il est possible d'inscrire de nouveaux articles de données à l'aide de Microsoft Excel par exemple.
- `portdata_xml_import_example.xml`

  Ce modèle comprend des onglets avec exemples de données. Ils peuvent être écrasés à l'aide de Microsoft Excel par exemple. Les données non nécessaires devraient être effacées.
- `portdata_xml_import_syntax.txt`

  Description en allemand et en anglais sur la manière correcte de créer les jeux de données.

10.1.2.1 Comment effacer ou modifier les numéros par défaut

Vous pouvez effacer certains des numéros par défaut, puis les redéfinir par les Assistants. Pour les numéros par défaut spécifiques non effaçables, vous pouvez modifier les valeurs prédéfinies.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

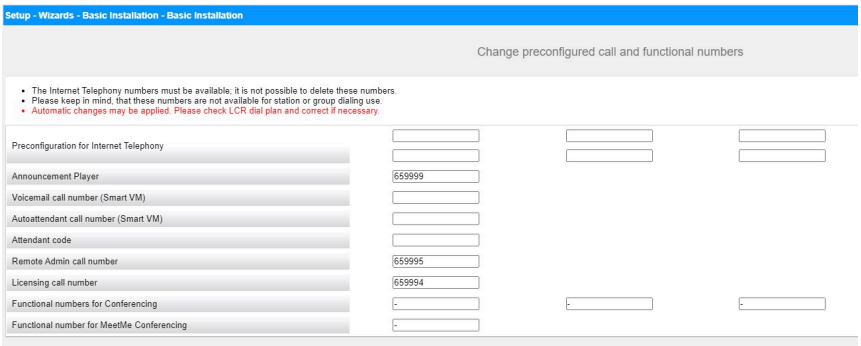
Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** pour lancer l'Assistant **Installation de base**.
3) Cliquez sur **Suivant**.

Remarque : Vous pouvez afficher une vue d'ensemble des numéros de téléphone actuellement configurés en activant le champ d'option **Afficher la configuration des abonnés** et en cliquant sur **Exécuter la fonction**.

---

4) Activez le champ d'option **Supprimer tous les numéros d'abonné**.
5) Cochez dans la demande de sécurité **Effacer tous les numéros**.
6) Cliquez sur **Exécuter la fonction**.



7) Si nécessaire, modifiez dans les champs les valeurs prédéfinies des numéros par défaut spécifiques.
8) Cliquez sur **OK**. Les numéros sont effacés et les modifications éventuelles apportées aux numéros par défaut spécifiques.

9) Cliquez sur **Annuler** pour quitter l'Assistant **Installation de base**.

10.1.2.2 Comment modifier les numéros par défaut spécifiques

Vous pouvez modifier les numéros prédéfinis pour les fonctions spéciales.

Conditions préalables

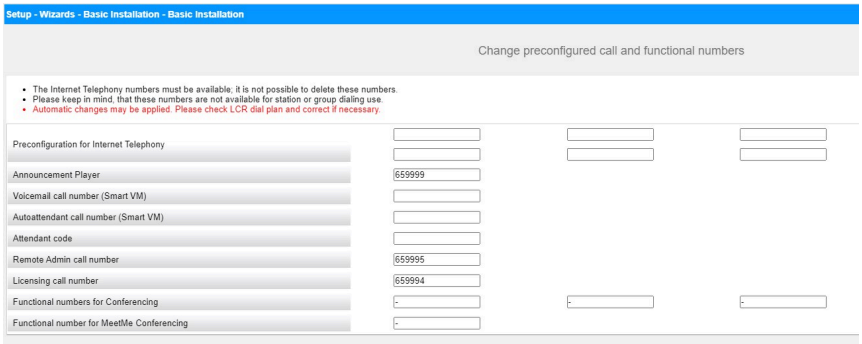
Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** pour lancer l'Assistant **Installation de base**.
3) Cliquez sur **Suivant**.

> **Remarque :** Vous pouvez afficher une vue d'ensemble des numéros de téléphone actuellement configurés en activant le champ d'option **Afficher la configuration des abonnés** et en cliquant sur **Exécuter la fonction**.

4) Cochez le champ **Modifier les numéros d'appel et les numéros fonctionnels préconfigurés**.
5) Cliquez sur **Exécuter la fonction**.



6) Entrez dans les champs les numéros et indicatifs souhaités et cliquez sur **OK**. Les nouveaux numéros et indicatifs sont enregistrés.

> **Remarque :** Les numéros configurés ici ne peuvent pas être attribués comme numéros d'abonnés, numéros SDA ou numéros de groupes.

7) Cliquez sur **Annuler** pour quitter l'Assistant **Installation de base**.

10.1.2.3 Comment importer les numéros et données d'abonnés

Grâce à un fichier XML, vous pouvez importer des données d'abonnés importées auparavant.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Un fichier XML au format UTF-8 avec les données inscrites est disponible. Vous trouverez un modèle XML dans **Centre de service** > **Documents** > **Modèles CSV**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** pour lancer l'Assistant **Installation de base**.
3) Cliquez sur **Suivant**.

Remarque : Vous pouvez afficher une vue d'ensemble des numéros de téléphone actuellement configurés en activant le champ d'option **Afficher la configuration des abonnés** et en cliquant sur **Exécuter la fonction**.

---

4) Cochez le champ d'option **Importer le fichier XML avec les données d'abonné**.
5) Cliquez sur **Exécuter la fonction**.
6) Sélectionnez avec **Parcourir** le fichier XML souhaité et cliquez sur **Ouvrir**.
7) Pour finir, cliquez sur **OK**. Les données d'abonnés sont importées.
8) Cliquez sur **Annuler** pour quitter l'Assistant **Installation de base**.

10.2 Exigences pour la téléphonie LAN.

La téléphonie LAN correspond aux communications entre abonnés IP à l'intérieur du réseau interne (LAN). Afin de garantir la qualité de la transmission de la voix en téléphonie LAN, les réseaux IP utilisés et le système de communication doivent répondre à certaines exigences. La qualité vocale et la fiabilité de la communication voix dépendent de la technologie utilisée sur le réseau.

Afin de garantir une transmission sans perte et une bonne qualité de la voix, les signaux voix sont numérisés à l'aide de codecs audio et identifiés à l'aide de procédures spéciales (Qualité de service) de manière à ce que la transmission de la voix soit traitée prioritairement par rapport à la transmission des données.

Exigences

- LAN avec au moins 100 Mbit/s et Full-Duplex (duplex intégral)
- Chaque composante du réseau IP doit se terminer sur un port propre, sur un commutateur ou un routeur ; n'utilisez pas de HUB.
- Autoriser au maximum 50 ms de retard dans une direction (One Way Delay) ; au maximum 150 ms de retard au total.
- Au maximum, 3 % de perte de paquets ; si fax/modem est utilisé via G.711, la perte de paquets ne doit pas dépasser 0,05%.
- Au maximum une gigue de 20 ms
- Support pour la qualité de service (QoS) : IEEE 802.p, DiffServ (RFC 2474) ou ToS (RFC 791)
- Charge du réseau, au maximum 40 %

10.2.1 Codecs audio

Un codec audio est un programme qui code la parole en paquets de données numériques (paquets IP) et la décode inversement. En fonction du codec audio utilisé, la compression des données est plus ou moins importante. Grâce à la compression, la transmission du paquet IP demande moins de bande passante que ce n'est le cas sans compression. Lors du décodage des paquets de données, il peut toutefois se produire une diminution de la qualité de la voix et de la continuité de la transmission.

Afin que les données soient converties correctement en voix à l'issue de la transmission, le destinataire doit utiliser le même codec que l'émetteur.

Codecs audio supportés

Les codecs audio suivants sont supportés :

- G.729A, G.729AB : codage de la voix à 8 kbit/s - bonne qualité vocale.
- G.711 (Loi A et Loi µ) : codage de la voix à 56 ou 64 kbit/s - très bonne qualité vocale. G.711 est utilisé dans le secteur du réseau fixe (RNIS).

Il est possible d'attribuer aux codecs audio des propriétés de 1 (élevée) à 4 (basse). Le système de communication essaie automatiquement, pour chaque liaison, d'utiliser un codec audio avec une priorité aussi élevée que possible. Lorsque l'on utilise un codec audio à faible compression de la voix (bonne qualité vocale), la charge pour le réseau est plus élevée. Dans le cadre d'une téléphonie IP intensive, cela peut se traduire par une détérioration de la qualité de la voix lorsque le réseau est déjà surchargé en raison du transfert de données.

Avec certains codecs, le système de communication peut activer la reconnaissance de pause vocale (VAD - Voice Activity Detection). Lors des longues pauses, il est possible de réduire ainsi charge du réseau.

Pour chaque codec il est possible de définir la taille de la trame (taille du paquet IP) entre 10 et 90 millisecondes. Vous définissez ainsi la fréquence d'échantillonnage servant à découper le signal vocal en paquets IP. Une valeur élevée (par ex. 90 ms) correspond d'une part à un meilleur rapport entre la charge utile et le surdébit de paquet IP, mais entraîne un retard plus important lors de la transmission.

Il est possible de désactiver les codecs G.729 qui ont besoin de beaucoup de ressources et de n'utiliser que les codecs G.711. Ainsi, le nombre des communications possibles, gérées en parallèles, est optimisé. Si cette fonction est activée, un redémarrage du système est nécessaire.

Dans les systèmes OSBiz X, la charge utile se termine dans le système, de sorte que les utilisateurs parlent avec un codec pris en charge par le système. Par exemple, le téléphone HFA a d'abord défini le codec G.722. Le système ne prend pas en charge le codec G.722 codec et le codec G.711 a été défini comme sa première option. Dans ce cas, les deux utilisateurs parleront avec un codec G.711. Concernant les systèmes OSBiz S, les utilisateurs parlent avec un codec G.722, tandis qu'il y a une charge utile de bout en bout.

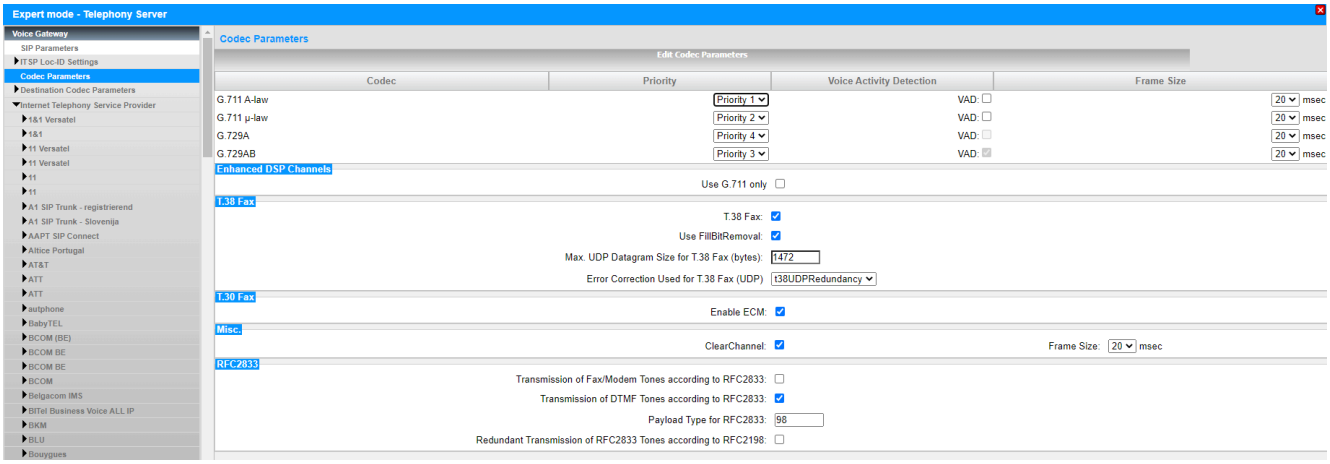
10.2.1.1 Comment configurer les paramètres du codec audio

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence du menu, cliquez sur **Paramètres du codec**.



4) À l'aide de la liste déroulante **Priorité**, affectez une priorité aux codecs audio souhaités, de 1 (élevée) à 4 (basse).
5) Dans le codecs audio souhaités, activez ou désactivez le bouton radio **Détection d'activité vocale (VAD)**.
6) Dans le champ **Taille de trame** des codecs audio souhaités, définissez la taille de trame à laquelle les codecs audio découpent les paquets voix IP.

Remarque : Vous devez saisir la même valeur pour tous les codecs, par exemple 20 ms. Il n'est pas possible de configurer des valeurs différentes pour chaque codec.

---

7) Si vous voulez utiliser uniquement les deux codecs audio G.711, dans la zone **Canaux DSP étendus**, cochez la case **Utiliser exclusivement G.711**.
8) Cliquez sur **Appliquer**, puis sur **OK**.

10.2.1.2 Comment affecter les paramètres d'un codec audio à une destination

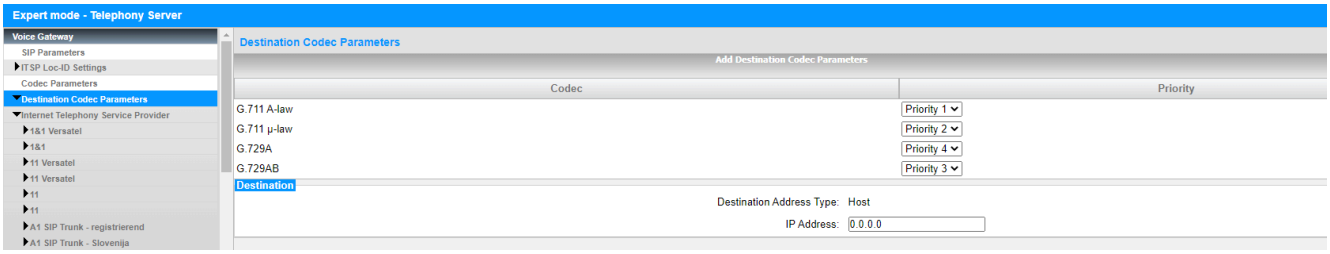
Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Passerelle vocale**.

3) Dans l'arborescence du menu, cliquez sur **Paramètres du codec de destination**.



4) À l'aide de la liste déroulante **Priorité**, affectez une priorité aux codecs audio souhaités, de 1 (élevée) à 4 (basse).
5) Dans **Adresse IP**, saisissez l'adresse IP de la destination à laquelle doivent être attribuées les priorités du codec audio définies précédemment (par `ex. 192.168.1.10`).
6) Cliquez sur **Appliquer**, puis sur **OK**.

10.2.2 Transmission de tonalités selon RFC2833

La tranmission des tonalités DTMF et des tonalité fax/modem selon RFC2833 peut être activée ou désactivée.

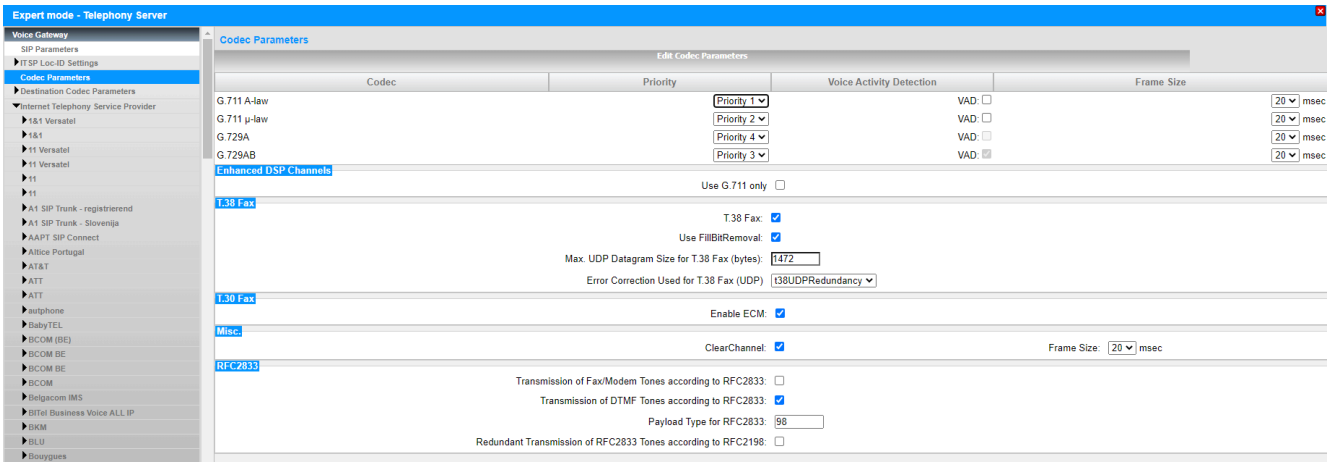
10.2.2.1 Comment activer ou désactiver les tonalités fax et modem selon RFC2833

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence du menu, cliquez sur **Paramètres du codec**.



4) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Transmission de tonalités fax/modem selon RFC2833**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Transmission de tonalités fax/modem selon RFC2833**.
5) Cliquez sur **Appliquer**, puis sur **OK**.

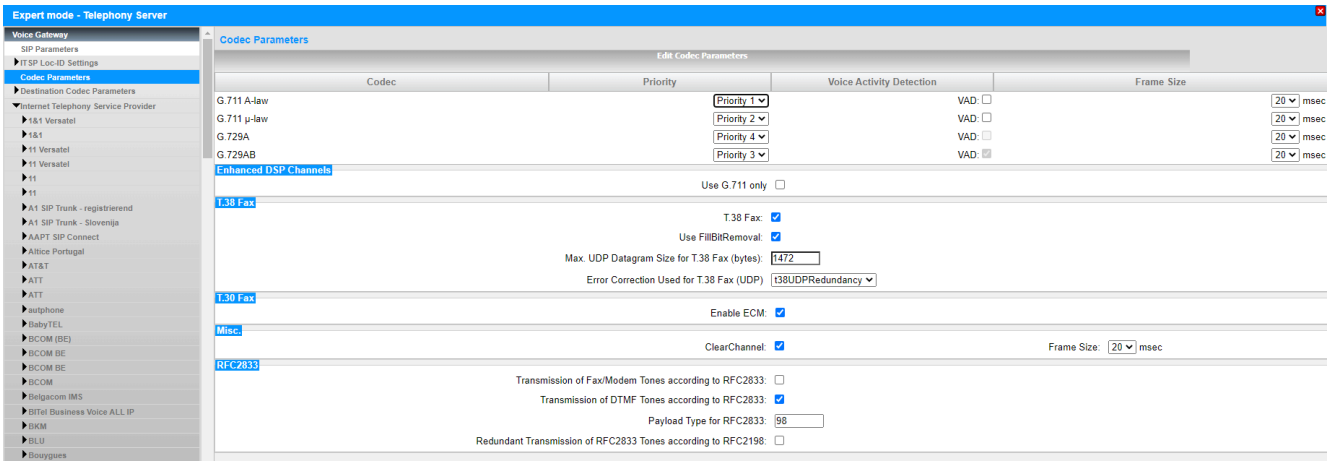
10.2.2.2 Comment activer ou désactiver la transmission MF selon RFC2833

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence du menu, cliquez sur **Paramètres du codec**.



4) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Transmission de tonalités DTMF selon RFC2833**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Transmission de tonalités DTMF selon RFC2833**.
5) Cliquez sur **Appliquer**, puis sur **OK**.

10.2.3 Qualité de service

La qualité de service (QoS) englobe différentes procédures permettant d'assurer un qualité maximale et l'absence de pertes lors de la transmission de paquets de données (paquets IP). Afin de parvenir à une bonne qualité de la voix lors de la transmission de la voix, QoS donne la priorité aux paquets voix IP par rapport aux paquets de données IP sur le réseau IP.

Les paquets IP sont pour cela identifiés par un marquage spécifique (point de code) afin d'être traités de manière prioritaire. L'information de priorisation

se traduit par l'affectation dans différentes classes. Lorsque les composantes disponibles dans le réseau IP (par ex. système de communication, abonnés SIP et routeur Internet) supportent QoS, vous pouvez affecter à ces classes différentes bandes passantes et ainsi privilégier le transport des paquets voix IP.

Classes de priorité selon DiffServ

Pour la priorité selon DiffServ, différents points de code sont définis pour le champ Type de Service (ToS) de sorte que la transmission de paquet IP peut être répartie en différentes classes.

- Le point de code Expedited Forwarding (EF) : garantit une bande passante constante. Les paquets IP identifiés par ce point de code disposent toujours de la même bande passante. Une fois la valeur définie atteinte, tous les paquets qui dépassent cette bande passante sont rejetés.
- Le point de code Assured Forwarding (AF) : garantit une bande passante minimale. Les paquets ID identifiés par ce point de code ont une priorité inférieure à EF et doivent se partager la bande passante non utilisée par EF. Une fois la valeur définie atteinte, tous les paquets IP sont dépassent cette bande passante sont rejetés.

  Quatre classes sont réservées pour AF : AF1 (basse priorité), AF2x, AF3x et AF4x (priorité élevée), x représente l'un des trois niveaux (level) de dropping : bas (1), moyen (2) et haut (3). Avec bas, les paquets sont stockés longtemps, avec haut, les paquets sont rejetés rapidement s'ils ne peuvent pas être transportés plus loin.
- Best Effort (BE) : les paquets IP non marqués (champ ToS=00) sont traités avec la priorité la plus basse.

Classes de priorité selon IP-Precedence

En dehors du mécanisme DiffServ, il existe différentes définitions plus anciennes qui effectuent la priorisation sur la base du champ ToS. Pour une adaptation optimale du système de communication aux paramétrages éventuellement nécessaires dans le réseau client, il est possible de sélectionner pour IP-Precedence les classes 3 à 7 (CS3-CS7).

Classes de priorité individuelles

Si aucune des possibilités prédéfinies n'est utilisée dans le réseau client, il est alors possible de régler directement, de manière manuelle, la valeur ToS. La valeur réglée est définie de manière décimale (0-63) et reprise dans les 6 bits supérieurs de l'octet ToS (par ex. 41 = 101-001-00 = 0xA4).

Tableau des classes de priorité possibles

Classe de priorité	Valeur ToS binaire	Valeur ToS hexadécimale
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

Classe de priorité	Valeur ToS binaire	Valeur ToS hexadécimale
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 - acheminement accéléré)		
EF	101-110-00	B8
BE (Best Effort - Meilleur effort)		
BE	000-000-00	00
CS (Class Selector - Sélecteur de classe)		
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
Entrée manuelle	xxx-xxx-00	0-63 (dezimal)

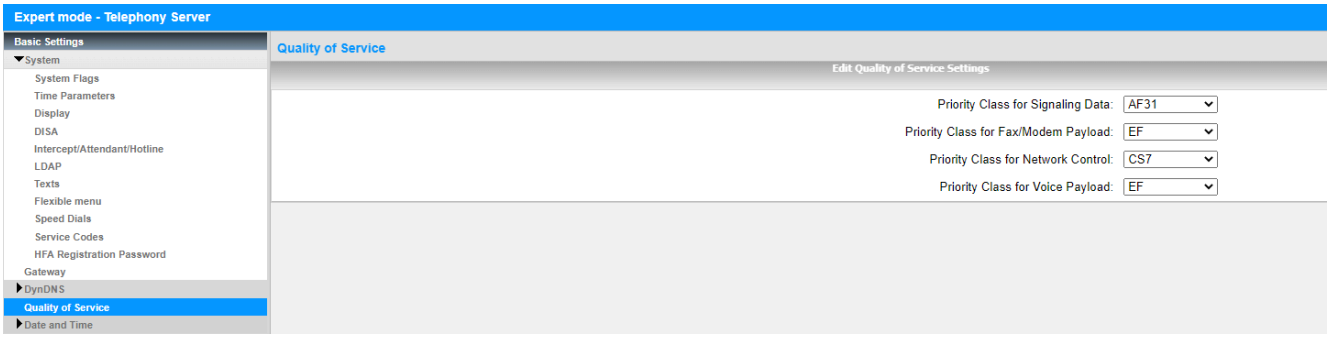
10.2.3.1 Comment configurer la Qualité de service

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Qualité de service**.



4) Dans la liste déroulante **Classe de priorité pour les données de signalisation**, sélectionnez la classe de priorité souhaitée.
5) Dans la liste déroulante **Classe de priorité pour les données utiles fax/ modem**, sélectionnez la classe de priorité souhaitée.
6) Dans la liste déroulante **Classe de priorité pour la gestion de réseau**, sélectionnez la classe de priorité souhaitée.
7) Dans la liste déroulante **Classe de priorité pour les données utiles vocales**, sélectionnez la classe de priorité souhaitée.
8) Cliquez sur **Appliquer**, puis sur **OK**.

10.3 Abonnés IP

Les abonnés sont reliés au système de communication via le LAN. En général, l'abonné IP est un téléphone LAN ou WLAN.

Les protocoles IP ci-après sont supportés.

- Protocole de communication indépendant des constructeurs

  Pour la téléphonie IP à l'intérieur du réseau interne, le système de communication utilise CorNet-IP (CorNet-Internet-Protocol). CorNet-IP est un développement de H.323. Grâce à CorNet-IP, toutes les fonctionnalités téléphoniques du système de communication peuvent être supportées.
- SIP (Session Initiation Protocol)

  SIP est généralement utilisé dans la téléphonie Internet, mais il n'est pas limité à cet usage. Il peut par ex. être utilisé également dans la téléphonie au sein des réseaux internes. Toutefois, SIP ne permet pas d'utiliser toutes les fonctionnalités téléphoniques du système de communication.

Il existe les types suivants d'abonnés IP :

- **Client système** : un client système est un abonné IP qui en mesure, via CorNet-IP, d'utiliser toutes les fonctionnalités du système de communication. Il peut s'agir d'un téléphone système IP comme le OpenStage 60 HFA ou d'un PC équipé d'un logiciel CTI comme OpenScape Personal Edition.
- **Client SIP** : un client SP est un abonné IP qui utilise le protocole SIP. Il ne peut utiliser, avec ce protocole SIP, qu'un nombre restreint de fonctionnalités du système de communication. Un client SIP est par ex. un téléphone SIP comme OpenStage 15 S.
- **Deskshare User** : un Deskshare User est un abonnné IP qui peut s'inscrire sur un autre téléphone système IP (connexion mobile) et utiliser ce téléphone comme s'il s'agissait de son propre téléphone (y compris le numéro d'abonné).
- **RAS User** : l'utilisateur RAS-User (Remote Access Service User) a accès au réseau IP via le raccordement RNIS. Cela permet d'assurer la télémaintenance du système de communication.

Pour chaque abonné IP raccordé, il faut une licence "IP User".

Deux abonnés IP sont réservés pour l'utilisateur en ligne (Online User) et pour l'accès distant via RNIS. Ces abonnés IP n'ont pas besoin de licence d'abonné. Si un ou plusieurs de ces trois abonnés réservés ne sont pas nécessaires, il est possible de les transformer en abonnés IP normaux en utilisant le mode Expert. Dans ce cas toutefois, il faut des licences d'abonné pour ces abonnés IP.

Configuration des abonnés IP

Les configurations suivantes peuvent être définies pour un abonné IP :

- Configuration des paramètres par défaut à l'aide de l'assistant **Téléphones IP** (voir Comment configurer un abonné IP).
- Configuration de tous les paramètres (paramètres par défaut et paramètres avancés) en mode Expert (voir >Abonné>Abonné>Clients IP).

Les téléphones système OpenScape Desk Phone IP sont fournis par défaut avec le logiciel SIP. Lorsque un téléphone système IP OpenScape Desk Phone est configuré dans la WBM en tant que **Client TFA**, le logiciel HFA enregistré dans le système de communication est automatiquement chargé dans le téléphone système IP.

10.4 Stations SIP

Les stations SIP sont des stations IP qui utilisent le protocole d'initiation de session (SIP) pour communiquer. Les stations SIP peuvent utiliser ce protocole pour accéder à un nombre limité de fonctions du système de communication. Les stations SIP, comme les stations IP, sont connectées au système de communication via le LAN.

Un poste SIP est un téléphone WLAN ou un téléphone LAN tel que l'OpenStage 15 S, par exemple.

Pour chaque station SIP connectée, une licence de station « Utilisateur IP » est nécessaire.

Authentification du SIP

Afin de garantir la sécurité du réseau interne, il est important que les abonnés SIP soient authentifiés sur le système de communication avec les valeurs décrites ci-dessous. Ces valeurs doivent être configurées dans le WBM du système de communication pour chaque abonné SIP ainsi que pour chaque téléphone SIP. Pour se protéger contre les attaques SIP, l'authentification est fortement recommandée !

- Mot de passe

  Mot de passe pour l'authentification : attribué librement ; au moins 8 caractères jusqu'à un maximum de 20 caractères. Le mot de passe doit contenir au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial. Un mot de passe distinct doit être attribué à chaque abonné SIP.
- SIP ID utilisateur / Nom utilisateur

  Nom d'utilisateur pour l'authentification : pré-attribué ; peut être modifié si nécessaire, maximum 20 caractères. Chaque abonné SIP dispose d'un ID utilisateur SIP différent.
- Realm

  Zone ou domaine pour l'authentification : attribué librement ; peut être modifié si nécessaire, max. 20 caractères. Le domaine de tous les abonnés SIP est prédéfini avec la même valeur. Elle peut être modifiée si nécessaire, par exemple dans le nom d'hôte ou le nom de domaine du système de communication.

Configuration des stations SIP dans le système de communication

Les configurations suivantes peuvent être effectuées dans le WBM du système de communication pour une station IP :

- Configuration des paramètres standard avec l'assistant des **téléphones IP** (voir Comment configurer les stations SIP).
- Configuration de tous les paramètres (standard et avancés) en mode expert (voir Station>Station>IPClients).

Configuration du téléphone SIP

Les données utilisées pour authentifier un abonné SIP sur le système de communication doivent être saisies directement sur le téléphone SIP.

Configuration des données d'authentification sur le téléphone SIP (voir Configuration des données d'authentification sur le téléphone SIP).

Fonctionnalités utilisables avec les téléphones SIP

Les fonctions suivantes peuvent être utilisées avec les téléphones SIP :

- Appels entrants et sortants avec affichage du numéro d'appel et du nom
- Mise en attente, basculement/connexion, consultation
- Transfert d'appel (filtré/non filtré)
- Décrocher l'appel
- Renvoi d'appel immédiat, sur occupation et après temporisation
- Conférence à trois
- Listes d'appels, indicateur de message en attente
- Coupure de la sonnerie du téléphone, rejet de l'appel, renvoi d'appel
- Appel en attente
- Appartenance à des groupes (sans affichage du numéro de groupe)
- Appels différents pour les appels internes, externes et de rappel
- DEL de la boîte aux lettres - Indication de message en attente
- Composition DTMF, par exemple pour le fonctionnement des boîtes vocales
- Utilisation des clients UC
- Mises à jour automatiques du logiciel (en cas d'utilisation du DLI)

Remarque : Le déploiement avec un Contact Center multicanal n'a pas été validé (par exemple, transfert vers des groupes UCD).

Selon le téléphone, il peut y avoir des restrictions sur les fonctions disponibles ; voir le wiki à l'adresse :

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

Les fonctions suivantes, qui sont activées à l'aide de codes de service avec * ou #, peuvent être utilisées avec les téléphones SIP :

- Réinitialiser tous les services : #0
- Renvoi d'appel : *1xf (x = 1 - tous, 2 - interne, 3 - externe) (f = numéro de renvoi)
- Renvoi d'appel désactivé : #1
- Quitter/rejoindre un groupe de recherche : #85g/*85g (g = numéro de groupe, facultatif - nécessaire en cas de participation à plusieurs groupes)

- Supprimer/activer l'ID de l'appelant (CLIR) : *86/#86
- Composition rapide : * 7nnnn (nnnn = numéro de composition rapide)
- Ouvre-porte : *61

Conseil : Il est recommandé d'utiliser les codes de substitution * ou # pour une meilleure compatibilité avec les dispositifs SIP tiers. L'utilisateur SIP doit envoyer la séquence complète du code de service sous forme de numérotation en bloc.

Conseil : Contrairement aux dispositifs HFA, il n'y a pas d'interaction avec l'utilisateur ou d'orientation pour les séquences de code de service sur les dispositifs SIP. La séquence complète du code de service doit être composée en une seule fois.

Fonctionnalités utilisables avec les téléphones SIP et myPortal/ myAttendant

Les téléphones SIP à utiliser avec myPortal et myAttendant doivent répondre aux exigences suivantes :

- 3PCC selon RFC 3725 est pris en charge.
- La fonction « appel en attente » est prise en charge.
- La fonction « Ne pas déranger » locale est désactivée.

La fonctionnalité complète des fonctions dépend du téléphone SIP utilisé et ne peut être garantie. Un test réussi des fonctions énumérées ci-dessous a été effectué avec les téléphones SIP OpenStage.

Fonctions orientées connexion/appel :

- Appeler
- Redirection d'appel
- Décrocher l'appel
- Reprendre l'appel
- Conférence contrôlée par l'application
- Mettre l'appel en attente
- Alternance (basculer/connecter)
- Consultation
- Quitter
- Transférer

Fonctions orientées vers le téléphone :

- Ne pas déranger
- Renvoi d’appel

10.5 Stations UP0

Un terminal UP0 utilise une ligne $U_{P0/E}$ pour transmettre des signaux numériques. Les terminaux UP0 sont connectés au système de communication via des interfaces UP0 et sont des téléphones système tels qu'un OpenStage 60T, par exemple. Les stations UP0 peuvent donc utiliser l'ensemble des fonctionnalités du système de communication.

Les options de connectivité suivantes sont disponibles pour les stations UP0 :

- OpenScape Business X1

  Vers les interfaces $U_{P0/E}$ de la carte mère.
- OpenScape Business X5

  Vers les interfaces $U_{P0/E}$ de la carte mère ou, si plusieurs terminaux UP0 sont impliqués, vers une carte $U_{P0/E}$ insérée en plus.
- OpenScape Business X8

  Vers des cartes $U_{P0/E}$ insérées en plus.
- OpenScape Business S

  Connexion impossible.

Pour chaque station UP0 connectée, une licence de station « Utilisateur TDM » est requise. Même les téléphones système connectés en mode esclave nécessitent une licence de poste.

Configuration des terminaux UP0

Les configurations suivantes peuvent être effectuées pour un terminal UP0 :

- Configuration des paramètres standard avec l'assistant **Équipements UP0** (voir Comment configurer les terminaux UP0).
- Configuration de tous les paramètres (paramètres standard et Advanced en mode Expert (voir Terminal>Terminal>Terminaux UP0).

10.6 Stations DECT

Une station DECT utilise une station de base sans fil pour transmettre des signaux numériques. Une station DECT est un téléphone DECT.

Les options de connexion suivantes sont disponibles pour les stations DECT :

- OpenScape Business X1R/X5R

  Station de base sans fil connectée à une interface U $_{P0/E}$ de la carte mère.
- OpenScape Business X8

  Station de base sans fil connectée à une ou plusieurs cartes SLMUC.
- OpenScape Business S

  Station de base DECT IP sur le réseau local

Le raccordement d'une station de base sans fil est appelé solution sans fil intégrée. Cela signifie que la quasi-totalité des fonctions du système de communication sont disponibles.

L'intégration d'une station de base IP DECT dans le réseau interne est appelée IP sans fil. Étant donné que seul le protocole SIP peut être utilisé dans ce cas, toutes les fonctionnalités du système de communication ne sont pas disponibles.

Pour chaque station DECT connectée, une licence de station « Utilisateur TDM » est requise.

Pour la description et la configuration de la solution sans fil intégrée, voir Solution sans fil intégrée .

Configuration des stations DECT

Les configurations suivantes peuvent être réalisées pour une station DECT :

- Configuration des paramètres standard avec l'assistant **des périphériques DECT** (voir Comment configurer les stations DECT).
- Configuration de tous les paramètres (paramètres standard et avancés en mode Expert (voir Station>Station>DECTStations>DECT Stations).

Les stations DECT IP sont configurées comme des stations SIP normales.

10.7 Stations Mitel SIP DECT

Les options de connexion suivantes sont disponibles pour les stations Mitel SIP DECT :

- Systèmes OpenScape Business S
- Matériel OpenScape Business V3 (OCCe)

Provisionnement des stations RFP Mitel SIP DECT

Le processus comprend les étapes générales suivantes :

1) Configurer le DHCP avec une adresse IP statique pour la station de base OMM.
2) La station de base recevra une adresse IP et démarrera l'application OMM.
3) Configurer la station de base via son interface web.
4) La station de base récupère automatiquement les fichiers de configuration d'OpenScape Business.
5) Lorsqu'un combiné se connecte, la station de base récupère également le fichier de configuration de l'utilisateur et configure le combiné.

Configuration des stations Mitel SIP DECT via WBM

Les étapes de configuration suivantes doivent être effectuées :

1) Activer le serveur DHCP et fournir une adresse IP statique à la station de base OMM (voir Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Adresses IP statiques).
2) Configuration des paramètres standards avec l'assistant Mitel SIP DECT Devices (voir Comment configurer les stations Mitel SIP DECT).
3) Configuration des stations SIP et de ses paramètres via le mode Expert (voir Comment configurer les stations SIP via le mode Expert).

10.8 Terminaux RNIS

Un terminal RNIS utilise le bus $_0$ pour transmettre des signaux numériques et est donc souvent référencé comme un terminal S_0. Le terminal RNIS est connecté au système de communication via les interfaces S_0

Pour un terminal S_0, il existe les possibilités de raccordement ci-après :

- OpenScape Business X1

  Vers une interface S_0 de la carte mère.

- OpenScape Business X5

  Vers une interface S_0 de la carte mère ou vers une carte S_0.
- OpenScape Business X8

  Vers une ou plusieurs cartes S_0.
- OpenScape Business S

  Aux passerelles ou adaptateurs supplémentaires requis

Les éléments suivants peuvent être connectés

- Téléphones RNIS
- Groupe Fax
- Modem RNIS
- PC avec carte RNIS

Les types de terminaux RNIS suivants peuvent être définis :

- Par défaut : pour téléphone RNIS, groupe de télécopieurs 4, modem RNIS ou PC avec carte RNIS
- Fax : prérequis pour la mise en place de la touche « Info depuis Fax/ Répondeur ». Si un PC avec une carte RNIS et un logiciel de télécopie est attaché au bus S_0 et affecté du type « Télécopie », par exemple, une touche « Info du télécopieur/répondeur » pourrait être configurée sur chaque poste. Lorsque cette touche s'allume, cela indique qu'une télécopie a été reçue.
- Répondeur : conditions préalables pour intercepter un appel lorsque le répondeur l'a déjà accepté Si un téléphone RNIS Gigaset avec un répondeur est connecté et affecté au type « Répondeur », par exemple, un appel qui a déjà été accepté par le répondeur peut être intercepté sur n'importe quel terminal. Pour cela, il faut programmer sur le terminal une touche avec le numéro interne de cet abonné analogique.

Pour chaque abonné DECT raccordé, il faut une licence d'abonné "TDM User".

Connexion des terminaux RNIS au port S_0

Pour pouvoir connecter un terminal RNIS au système de communication, vous devez configurer au moins l'un des ports S_0 utilisés pour la ligne d'abonné RNIS ou la connexion point à point RNIS en tant que bus S_0 interne (bus S_0 EURO).

Remarque : S'il y a plus d'un terminal RNIS connecté à un port S_0 (jusqu'à 8 terminaux RNIS sont possibles) dans une connexion RNIS point à multipoint, chaque terminal RNIS individuel doit être attribué à un MSN unique. Cette affectation doit être effectuée dans le menu de configuration du terminal RNIS.

Configuration des terminaux RNIS

Les configurations ci-après peuvent être définies pour un abonné DECT.

- Configuration des paramètres standard à l'aide de l'assistant **Terminaux RNIS** (voir Comment configurer les terminaux RNIS).
- Configuration de tous les paramètres (paramètres standard et Advanced en mode Expert (voir Terminal>Terminal>TerminauxRNIS).

Comment autoriser uniquement les numéros paramétrés pour MSN

L'administrateur peut spécifier que d'autres MSN au niveau d'un bus S0 ne peuvent être configurés que pour les numéros d'appel qui y existent déjà. Cela empêche les abonnés d'ajouter un MSN sans autorisation par le biais d'une saisie sortante du bus S0 avec un autre MSN. Sans cette restriction, le système de communication attribuerait normalement un numéro d'appel interne gratuit au bus S0 pour ce MSN.

Portabilité du terminal

Le système de communication prend en charge la portabilité du terminal (TP), c'est-à-dire qu'il vous permet de garer un appel sur le bus S_0, de débrancher le terminal et de le rebrancher à un nouvel emplacement pour reprendre l'appel. Le terminal stationné reçoit un message indiquant que l'utilisateur effectue un portage. Trois minutes sont disponibles pour l'ensemble de l'opération.

La fonctionnalité n'est pas prise en charge pour les services tels que le télécopieur, le télétex ou le transfert de données.

10.8.1 Comment configurer l'interface S_0 pour abonnés RNIS

Avec l'assistant **Ligne réseau RNIS / Analogique / ITSP** vous pouvez configurer une ou plusieurs interfaces S_0 afin de pouvoir leur raccorder des téléphones RNIS.

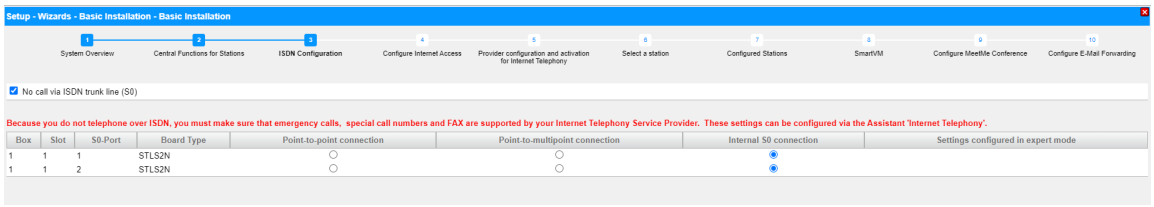
Conditions préalables

Il existe une ou plusieurs interfaces S_0 libres.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Dans l'Assistant **Ligne réseau RNIS / Analogique / ITSP**, cliquez sur **Modifier**.
4) Cliquez sur **OK&Suivant**. Le système vous présente les interfaces S_0 (ports S_0) existantes.



5) Laissez la case à cocher **Pas de téléphonie par la ligne réseau RNIS (S0)** réglée comme elle l'est.

6) Dans les interfaces S_0 souhaitées, activez le champ d'option **Connexion S0 interne**.

Remarque : Vous ne pourrez plus utiliser ces interfaces S_0 pour l'accès réseau RNIS.

---

7) Cliquez autant de fois que nécessaire sur **OK&Suivant** pour afficher le message indiquant que la modification de la fonctionnalité est terminée.
8) Cliquez sur **Terminer**.

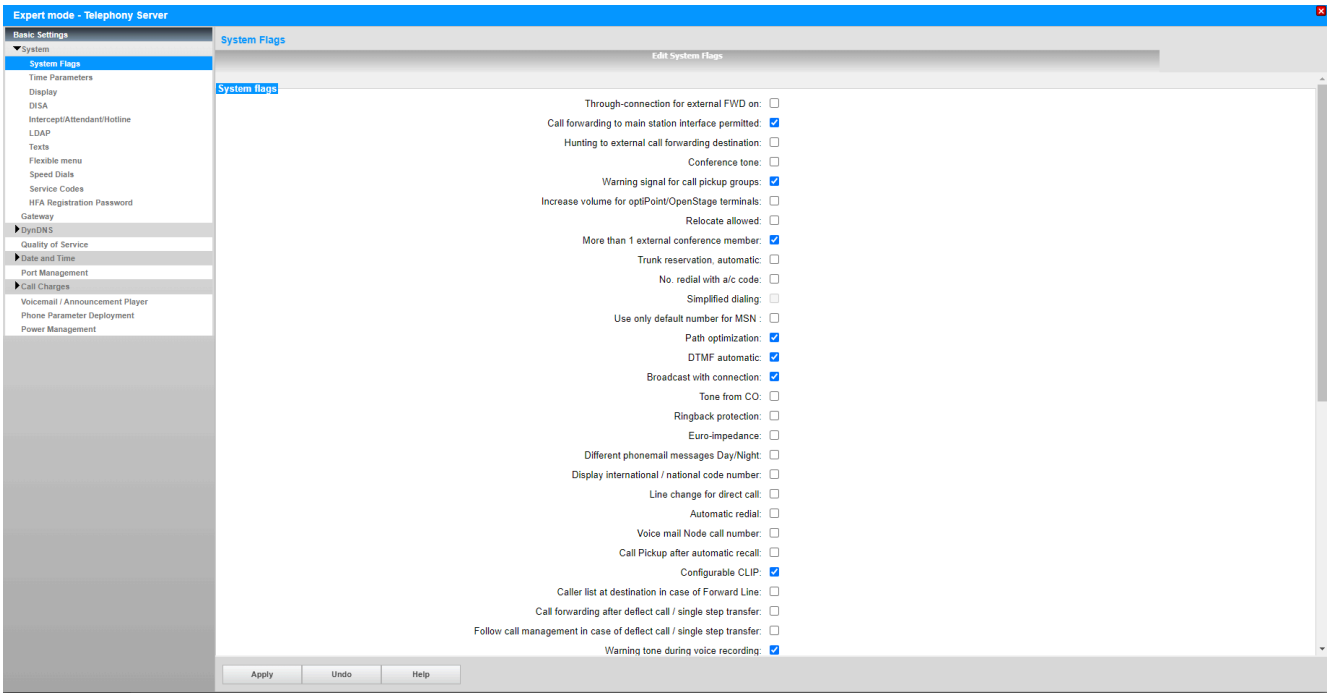
10.8.2 Comment autoriser uniquement les numéros paramétrés pour MSN

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configuration de base** > **Système** > **Indicateurs système**.



4) Si vous ne voulez autoriser que les numéros paramétrés pour MSN, cochez la case **N'utiliser que le N° configuré pour MSN**.
5) Si vous ne voulez pas autoriser uniquement les numéros paramétrés pour MSN, décochez la case **N'utiliser que le N° configuré pour MSN**.
6) Cliquez sur **Appliquer**, puis sur **OK**.

10.9 Stations analogiques

Une station analogique utilise un câble analogique à deux conducteurs pour transmettre des signaux analogiques. Le système de communication connecte la station analogique via les ports analogiques.

Les options de connectivité suivantes sont disponibles pour les stations analogiques :

- OpenScape Business X1

  À une interface analogique de la carte mère.
- OpenScape Business X5

  À une interface analogique de la carte mère ou à une carte analogique.
- OpenScape Business X8

  Sur une ou plusieurs cartes analogiques.
- OpenScape Business S

  Aux passerelles ou adaptateurs supplémentaires requis

Les stations analogiques suivantes peuvent être connectées :

- Téléphone analogique
- Télécopieur analogique (Groupe 3)
- Répondeur
- Modem, 9600 bps ou plus
- Téléphone d'entrée (ouvre-porte)
- Haut-parleur

On peut définir les types suivants de stations analogiques :

- Norme : pour téléphone analogique, télécopieur de groupe 3, répondeur ou haut-parleurs
- Fax : conditions préalables à la configuration de la touche « Informations du fax/répondeur ». Si un appareil du groupe de télécopieurs 3 est connecté et configuré comme étant de type « Fax », par exemple, une touche « Info du télécopieur/répondeur » peut être configurée sur chaque appareil. Lorsque ce voyant s'allume, cela indique qu'un fax a été reçu.
- Répondeur : conditions préalables pour répondre à un appel déjà pris en charge par le répondeur. Si un téléphone Gigaset avec répondeur est connecté et configuré comme « Répondeur », par exemple, un appel déjà pris en charge par le répondeur peut être pris en charge depuis n’importe quel terminal. Pour ce faire, le terminal doit être programmé avec le numéro d'appel interne du Gigaset.
- Modem : Les modems analogiques avec une vitesse fixe de 56 kbit/s ou plus ne sont pas pris en charge, car les vitesses de 56 kbit/s ou plus ne peuvent pas être traitées.

Pour chaque station analogique connectée, une licence de station « Utilisateur TDM » est requise.

Disponibilité d'un télécopieur analogique dans le système avec le numéro de télécopieur précédent

Comme il n'est pas possible de transférer un fax analogique vers un numéro de fax du système, la solution de contournement suivante existe : le numéro de fax précédent est configuré dans le système et reçoit les messages fax entrants.

Pour le télécopieur analogique, un port est configuré avec le numéro précédent comme CLIP. La case à cocher CLIP configurable doit être sélectionnée à cet effet. Les fax sortants affichent le numéro précédent comme expéditeur ; les destinataires internes voient le numéro interne du télécopieur.

Configuration des stations analogiques

Les configurations suivantes peuvent être réalisées pour une station analogique :

- Configuration des paramètres standard à l'aide de l'assistant **Équipements analogiques** (voir Comment configurer les terminaux analogiques).
- Configuration de tous les paramètres (paramètres standard et Advanced via le mode Expert (voir Terminal>Terminal>TerminauxAnalogiques).

10.10 Abonnés virtuels

Les abonnés virtuels se comportent comme des abonnés réels, mais il ne leur est pas attribué de terminaux physiques.

Les abonnés virtuels sont par ex. nécessaire pour l'intégration de téléphones mobiles et pour le renvoi temporisé. Ceux-ci doivent être configurés comme les abonnés réels afin de pouvoir par ex. être utilisés pour la signalisation des appels.

Configuration des abonnés virtuels

La configuration des paramètres d'un abonné virtuel est réalisée en mode Expert (voir Abonnés>Abonnés>Abonnés virtuels).

10.11 Programmation des touches

Chaque téléphone système est équipé d'un certain nombre de touches de fonction. Par défaut, certaines de ces touches sont préconfigurées avec des fonctions. Il est possible de modifier la préconfiguration et d'affecter des fonctions aux autres touches de fonction non préconfigurées.

Pour la programmation des touches, vous disposez des possibilités ci-après.

- Programmation des touches avec WBM

  Dans WBM, vous pouvez, à l'aide de l'assistant **Programmation des touches**, programmer les touches des téléphones système raccordés.

  A l'aide de cet assistant, il est également possible de programmer une configuration de touches pour un abonné, même si cet abonné n'est pas encore raccordé à un téléphone système.
- Programmation des touches via clients UC

  Les utilisateurs des clients UC **myPortal Smart**, **myPortal for Desktop**, **myPortal for Outlook** et **myAttendant** peuvent également programmer les touches du téléphone système à l'aide des clients UC (voir Mode d'emploi des clients UC).

- Programmation des touches directement sur le téléphones système

  Sur les téléphones système avec écran, il est également possible de programmer certaines touches de fonction directement sur le téléphone système.

Programmation multiple des touches de fonction

Les touches de fonction des téléphones système peuvent être configurées à deux niveaux, le 1er niveau et le 2e niveau. Le 1er niveau peut être configuré avec toutes les fonctions offertes. Le 2e niveau peut être configuré avec des numéros de téléphone externes. Pour pouvoir utiliser le 2e niveau, il faut que la touche de basculement (Shift-key) soit programmée sur le téléphone système. La LED de la touche de fonction correspond toujours au 1er niveau.

Remarque : Dans le cas d'un **utilisateur, il est impossible de copier une programmation de touches car la fonctionnalité d'assignation des touches est spécifique à MULAP et ne doit pas être copié chez un abonné. Le préfixe ** doit être retiré manuellement de ces utilisateurs pour que la copie de clé puisse être activée.

10.11.1 Comment programmer les touches de fonction des téléphones système

L'assistant **Programmation des touches** permet de configurer les touches de fonction des téléphones système.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphones/ Abonnés**.

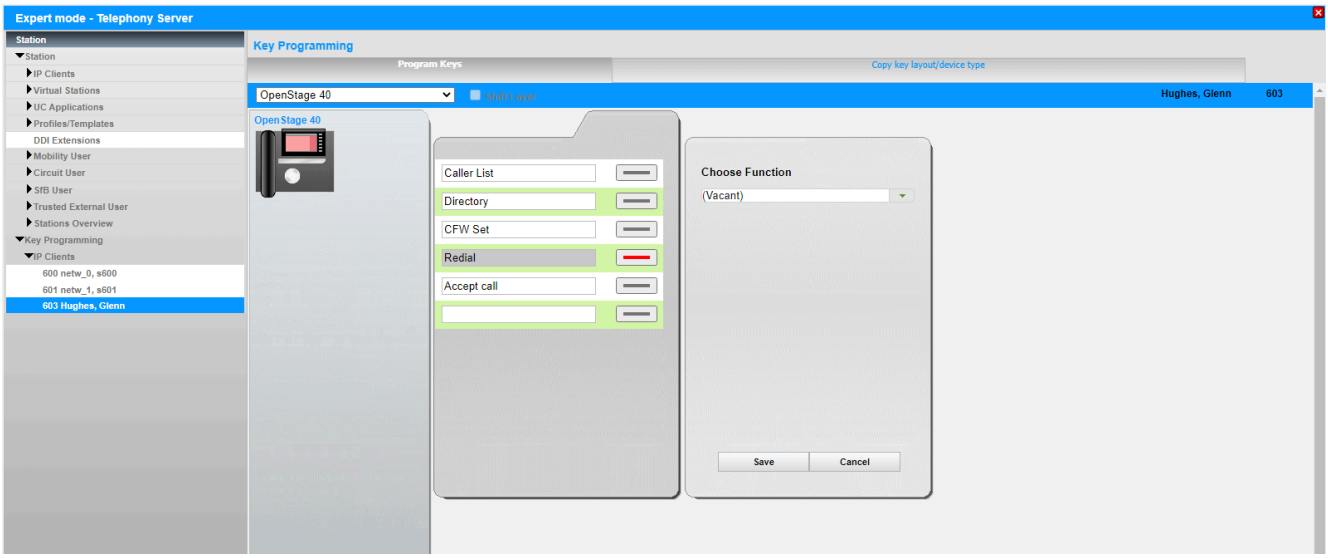
3) Pour lancer l'assistant **Programmation des touches**, cliquez sur **Modifier**. Le système ouvre la liste de tous les abonnés.

4) Sur la ligne de l'abonné souhaité, cliquez sur **Modifier**.

5) Affectez l'abonné au téléphone système :

- Si un téléphone système est déjà raccordé pour l'abonné, le système affiche une représentation simplifiée du téléphone système.
- Si aucun téléphone système n'est raccordé pour l'abonné, sélectionnez dans la liste déroulante le téléphone système à raccorder. Le système affiche une représentation simplifiée du téléphone système sélectionné.

6) Dans la représentation simplifiée du téléphone système, cliquez sur les touches souhaitées. Les touches de fonction du clavier sélectionné sont affichées avec les fonctions actuellement programmées.



7) Programmez les touches de fonction :

a) Cliquez sur le symbole de touche pour la touche de fonction à occuper. Le système affiche une liste déroulante avec les fonctions possibles.

b) Dans la liste déroulante **Sélectionner fonction**, sélectionnez l'une des possibilités suivantes.

c) Certaines fonctions nécessitent des informations supplémentaires. Sélectionnez si nécessaire ou fournissez les données nécessaires.

d) Cliquez sur **Enregistrer**.

e) Dans le champ **Modifier l'étiquette prédéfinie**, modifiez si nécessaire l'étiquette de la touche de fonction.

Remarque : Si vous disposez d'un téléphone système avec identification automatique des touches (par ex. OpenStage 60 HFA), ce texte est repris du téléphone système.

---

f) Cliquez sur **Enregistrer**.

g) Si vous voulez paramétrer d'autres touches de fonction, répétez l'étape 7.

8) Si vous avez paramétré le **changement de niveau** sur une touche de fonction, cochez la case **Changement de niveau**. Paramétrez les numéros d'appel externe sur le deuxième niveau des touches de fonction comme décrit à l'étape 7.

9) Cliquez sur **Appliquer la configuration des touches**.

10) Si vous souhaitez reprendre pour tous les téléphones système ou pour plusieurs d'entre eux la configuration des touches qui vient d'être définie, cochez la case des téléphones système concernés, puis cliquez sur **Appliquer**, sur **OK** et sur **OK et suivant**.

11) Si vous souhaitez reprendre la configuration des touches qui vient d'être définie uniquement pour le téléphone système sélectionné, cliquez par sécurité sur **Désélectionner tous les abonnés**, puis sur **OK et suivant**.

12) Cliquez sur **Suivant** puis sur **Terminer**.

10.12 Profils d'abonnés

Les valeurs et caractéristiques des abonnés sont enregistrées dans les profils. Il est possible d'affecter plusieurs membres à un profil. Les mêmes valeurs et caractéristiques s'appliquent à tous les membres de ce profil.

Il est possible d'affecter aux profils d'abonnés des abonnés avec téléphones système. Il est possible de créer jusqu'à 20 profils d'abonné. Les profils d'abonné peuvent être exportés et importés individuellement ou tous ensemble. Les fichiers sont de type `xml`.

Chaque abonné peut être membre d'exactement un profil. Si les valeurs et propriétés d'un abonné, qui est membre d'un profil, sont modifiées directement (c.-à-d. pas par l'entremise du profil) l'abonné est alors effacé du profil.

10.13 Configuration des abonnés

Il est possible de définir pour les abonnés certaines valeurs (par ex. numéro de téléphone, nom et numéro SDA) et certaines caractéristiques (par ex. type de signalisation d'appel).

La configuration des abonnés comprend une configuration standard et une configuration avancée. Les paramètres par défaut peuvent être configurés par des assistants de profil **Advanced**. Les paramètres avancés ne peuvent être configurés qu'en mode Expert avec le profil **Expert**.

Les paramètres par défaut de tous les abonnés d'un même type (par ex. abonnés IP ou abonnés analogiques) peuvent être aisément modifiés à l'aide d'une liste. Les paramètres supplémentaires (par ex. la signalisation d'appel ou les drapeaux abonnés) peuvent être modifiés individuellement pour chaque abonné.

Les abonnés virtuels sont entièrement configurés en mode Expert (les paramètres standard comme les paramètres étendus).

Le profil **de base** ne permet pas de configurer les abonnés, mais de modifier les noms des abonnés.

Pour les abonnés connectés au système de communication, il devrait exister un plan de numérotation. Les numéros de téléphone, noms et numéros de sélection directe à l'arrivée de tous les abonnés configurés peuvent être affichés à l'aide du mode Expert, dans **Abonnés** > **Numéros SDA**.

Les numéros de sélection directe à l'arrivée qui ne sont pas mis à disposition par le fournisseur de service et qui ne sont pas utilisés dans le système devraient être supprimés car cela peut sinon provoquer des conglits avec MSN ou les numéros d'abonnés de téléphonie Internet. Les numéros de sélection directe à l'arrivée qui sont mis à disposition par un fournisseur de service de téléphonie sur Internet (ITSP, Internet Telephony Service Provider) doivent être affectés aux abonnés lors de la configuration de l'ITSP (voir Configuration d'un ITSP).

Important : La modification d'un numéro de téléphone de l'abonné réinitialise Smart VM (Voicemail) éventuellement paramétrée pour l'abonné. Tous les messages vocaux personnels, messages d'accueil et annonces sont perdus et le mot de passe est réinitialisé.

Paramètres par défaut

Les paramètres par défaut devraient être contrôlés, et adaptés si nécessaire, pour chaque abonné.

- **Numéro de téléphone, Nom, Numéro SDA**

  Par défaut, il est affecté un numéro de téléphone à chaque abonné (par ex. 101). L'abonné peut être joint en interne sous ce numéro. Avec les téléphones système, ce numéro est affiché à l'écran ainsi qu'à l'écran du poste du correspondant. Si, pour un abonné appelé en externe, un autre numéro que le véritable du numéro doit être affiché, il est possible de définir le numéro affiché.

  A chaque abonné il peut être affecté en plus un numéro SDA. Le numéro SDA permet de joindre directement l'abonné depuis l'extérieur. L'abonné peut par exemple être joint en interne à l'aide du numéro 101 et depuis l'extérieur à l'aide du numéro SDA `3654321` (MSN dans un raccordement multiposte) ou `à l'aide du <n° installation>-101` (pour un raccordement système). Lors de la première installation, il est possible, lors du raccordement de l'installation, de déterminer s'il faut utiliser comme n° SDA le numéro interne. Le numéro SDA peut aussi être différent du numéro de téléphone. Lorsque l'on utilise la téléphonie Internet, il est possible de définir également un numéro SDA permettant de joindre l'abonné à l'aide de la téléphonie Internet. Ce numéro de téléphone est fourni par le fournisseur de services téléphoniques sur Internet.

  A chaque abonné il peut être affecté un nom. Ce nom s'affiche chez le correspondant sur l'afficheur (uniquement avec les téléphones système).

  S'il existe un plan de numérotation, il convient d'adapter les numéros de téléphone, les numéros SDA et les noms des abonnés à l'aide du plan de numérotation.
- **Type**

  Pour chaque abonné, il est possible de sélectionner le type d'abonné. Un abonné IP peut par ex. être de type **Client système** ou **Client SIP**, un abonné analogiques peut être un téléphone analogique ou un fax analogique et un abonné RNIS peut être un téléphone RNIS ou un fax RNIS.
- **Numéro fax, numéro SDA fax**

  Si une boîte Fax doit être paramétrée pour l'abonné (utilisable par ex. avec les clients UC myPortal for Desktop ou myPortal for Outlook), attribuez un numéro d'appel fax (pour la réception des messages fax internes) et un numéro SDA fax (pour la réception de messages fax externes).
- **Discriminations**

  Il peut être attribué à un abonné l'une des 15 classes de services. Cela détermine par ex. si l'abonné est en droit de recevoir et de mener des communications externe ou encore les numéros d'appel que l'abonné est autorisé à composer et ceux qu'il n'est pas autorisé à composer (voir Discriminations (contrôle de la numérotation)).
- **Groupes d'interception d'appel**

  Chaque abonné peut être affecté à un groupe d'interception.

- **Langue, signalisation d'appel**

  Il est possible de paramétrer la langue des systèmes téléphoniques raccordés.

  Il est possible de sélectionner le timbre de la sonnerie d'un appel externe et interne.
- **Boîte vocale (uniquement avec UC Smart)**

  Dans la solution de communications unifiées UC Smart, on peut créer une boîte vocale pour chaque abonné et faire un choix parmi différentes données d'annonce. Pour des informations plus détaillées sur la boîte vocale, voir Boîte vocale (SmartVM)

  Dans la solution de communications unifiées UC Suite, il est affecté automatiquement une boîte vocale à chaque abonné. Dans ce cas, il manque donc les paramètres de la boîte vocale.
- **Drapeaux poste**

  Les drapeaux abonnés de chaque abonné peuvent être modifiés. Pour la description des drapeaux abonnés voir >Abonné>Abonné>Paramètres d'abonné.

Paramètres étendus

Le mode Expert vous permet de configurer tous les paramètres de tous les types d'abonnés. Les paramètres étendus peuvent être conservés tels qu'ils sont pour une exploitation standard ; ils ne doivent être adaptés que si cela est nécessaire. Pour plus d'informations sur les paramètres étendus, voir Abonnés.

Concepts associés

Discriminations (contrôle de la numérotation) à la page 706
Texte en plusieurs langues à la page 1173

10.13.1 Comment configurer les stations IP

Vous pouvez utiliser l'assistant **Téléphones IP** pour configurer les postes IP (téléphones LAN et téléphones WLAN).

Conditions préalables

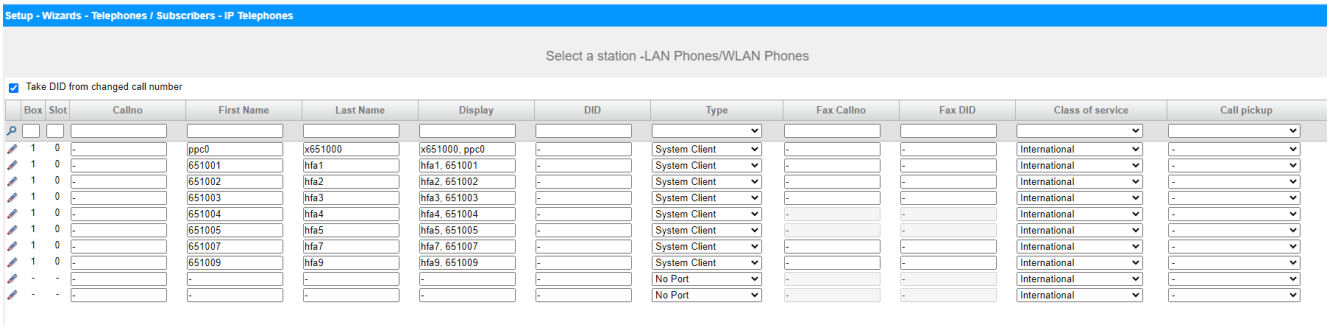
Un réseau local sans fil fonctionnel est nécessaire au fonctionnement des téléphones WLAN.

Vous êtes connecté au WBM avec le profil **Avancé** .

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration** .
2) Dans l'arborescence de navigation, cliquez sur **Wizards** > **Telephones / Subscribers** .

3) Cliquez sur **Modifier** pour démarrer l'assistant **Téléphones IP** . Une liste de toutes les stations IP apparaît.



4) Si vous souhaitez que le numéro d'appel interne soit automatiquement attribué à la station comme numéro d'appel direct entrant, activez le bouton radio **« Prendre le numéro DID à partir du numéro d'appel modifié »** .

5) Si vous souhaitez un numéro d'appel direct différent pour la station par rapport au numéro d'appel, saisissez un numéro DID pour la station sous **DID** dans la ligne de la station souhaitée :

- Uniquement pour une connexion point à point :

  Cliquez dans le champ souhaité et saisissez le numéro DID à l'aide du clavier. Le numéro DID peut également être identique au numéro de poste interne.
- Uniquement pour une connexion point à multipoint :

  Sélectionnez un MSN dans le champ souhaité via la liste déroulante. La station peut être atteinte en interne via le numéro de station interne 101, par exemple, et en externe via le MSN 654321.
- Pour les connexions point à point et point à multipoint :

  Sélectionnez l'entrée **xxx - modifiable** (xxx est le numéro de poste interne) via la liste déroulante dans le champ souhaité et saisissez le numéro DID à l'aide du clavier ou sélectionnez un MSN dans la liste déroulante.

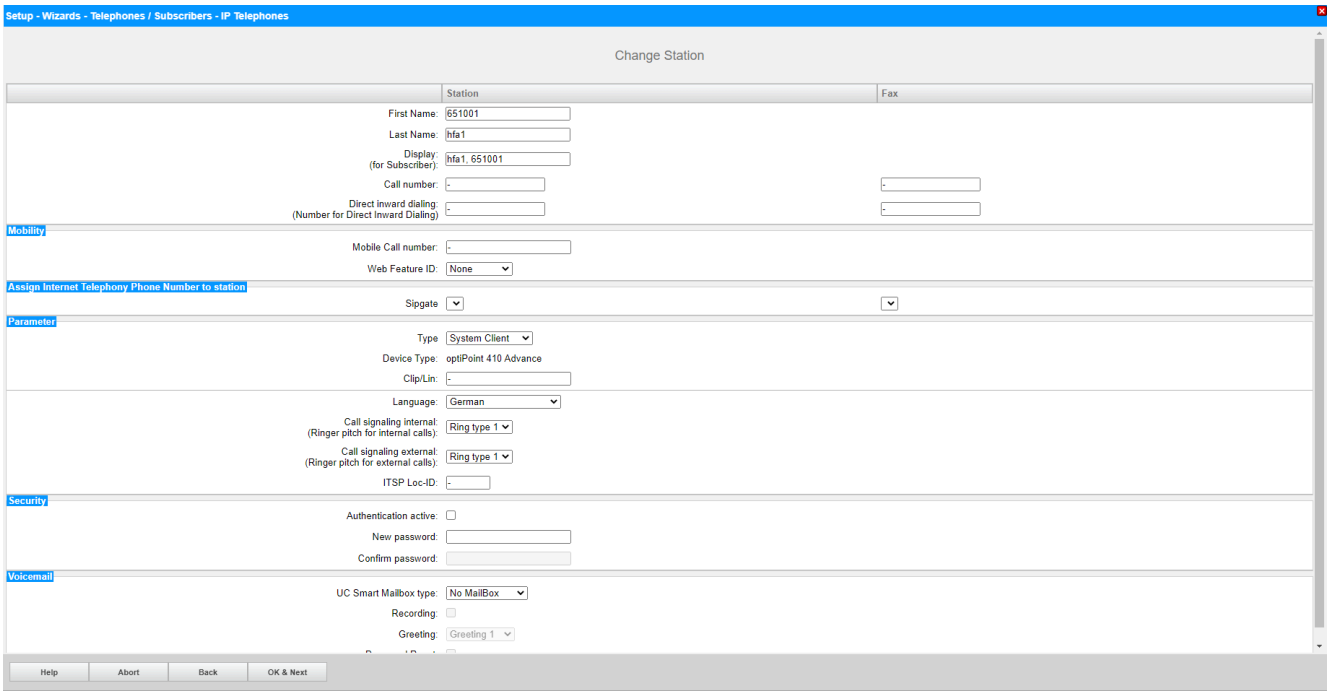
6) Si vous souhaitez qu'un numéro de téléphone de téléphonie Internet soit attribué au poste comme numéro d'appel direct entrant, laissez l'option **« Prendre le numéro DID à partir du numéro d'appel modifié »** décochée et sélectionnez plutôt le fournisseur de services de téléphonie Internet dans la liste située à côté de cette option. Sélectionnez ensuite le numéro de téléphone de téléphonie Internet dans la liste déroulante **DID** de la ligne du poste souhaité.

7) Saisissez le numéro de poste interne de l'abonné sous **« Numéro d'appel »** dans la ligne appropriée de l'abonné souhaité. Vous pouvez utiliser le numéro de téléphone prédéfini ou attribuer un autre numéro gratuit.

8) Dans la ligne de la station souhaitée, sous **Nom** , entrez un nom au format `Nom de famille, Prénom` ou `Prénom Nom de famille`.

9) Sélectionnez le type de poste IP (par exemple, **Client système** ou **Utilisateur DeskShare**) dans la liste déroulante **Type** de la ligne du poste souhaité).

10) Si vous souhaitez configurer une boîte de fax pour l'abonné (qui peut être utilisée avec les clients UC **myPortal pour ordinateur** ou **myPortal pour Outlook** , par exemple), procédez comme suit :
   a) Sur la ligne correspondant au poste souhaité, dans le champ **« N° de fax »** , saisissez le numéro de fax interne souhaité auquel l'utilisateur pourra recevoir des messages fax internes.
   b) Si vous souhaitez configurer un numéro DID pour le décodeur fax, saisissez le numéro de fax externe souhaité, sous lequel l'abonné pourra recevoir des fax externes, dans le champ **« Numéro DID du fax »** de la ligne correspondant à l'abonné.
11) Choisissez le groupe de classe de service souhaité dans la ligne de l'abonné souhaité à partir de la liste déroulante **Classe de service** .
12) Pour ajouter l'abonné à un groupe de prise d'appel, sélectionnez un groupe de prise d'appel dans la liste déroulante **Groupe de prise d'appel** de la ligne de l'abonné souhaité.
13) Effectuez d'autres réglages si nécessaire :
   a) Cliquez sur l'icône **en** forme de crayon dans la ligne correspondant à la station souhaitée.



   b) Attribuez un **numéro d'appel mobile** et sélectionnez l' **identifiant de la fonctionnalité Web** dans la liste déroulante. Zone **de mobilité** .
   c) Dans le champ **Clip/Lin** , saisissez un numéro de téléphone (numéro DID ou MSN) qui s'affichera sur le poste du correspondant appelé au lieu de votre propre numéro de téléphone dans le cas d'un appel externe.

Remarque : Cette fonctionnalité doit être déployée par l'opérateur réseau.

Remarque : Au moins un numéro DID doit être configuré. Sinon, le système ne tient pas compte du

numéro CLIP de l'appelant et le numéro d'appel interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

d) Sélectionnez la langue des commandes du menu du téléphone dans la liste déroulante **Langue** .
e) Dans la liste déroulante **Signalisation d'appel interne** , sélectionnez et attribuez l'un des huit signaux d'appel acoustiques possibles pour les appels internes. La station enverra alors la sonnerie modifiée aux autres stations internes, permettant ainsi à ses appels d'être distingués de ceux des autres stations internes (par défaut : type de sonnerie 1).
f) Dans la liste déroulante **Signalisation d'appel externe** , sélectionnez et attribuez l'un des trois signaux d'appel acoustiques possibles pour les appels externes (par défaut : type de sonnerie 1).
g) Dans le champ **Urgence SIP** , saisissez l'emplacement configuré de l'urgence SIP.
h) Uniquement avec UC Smart : sélectionnez dans la liste déroulante **Type de boîte aux lettres UC Smart** si l'abonné doit recevoir une boîte vocale par défaut ou une boîte vocale de standard automatique.
i) Uniquement avec UC Smart et la messagerie vocale par défaut : si un appelant peut laisser un message dans la boîte vocale, cochez la case **Enregistrement** .
j) Uniquement avec UC Smart : sélectionnez un message d'accueil dans la liste déroulante **« Message d'accueil »** .
k) Uniquement avec UC Smart : si vous souhaitez réinitialiser le mot de passe de votre messagerie vocale, cochez la case « **Réinitialisation du mot de passe »** .

Remarque : La case à cocher **« Réinitialisation du mot de passe »** doit être décochée lors de la configuration d'une nouvelle messagerie vocale. Il sert à réinitialiser le mot de passe de la messagerie vocale. Lors de la création d'une nouvelle boîte vocale, l'abonné doit de toute façon modifier le mot de passe initial lors de son premier accès à sa messagerie vocale.

l) Si la station est connectée à Internet, l'authentification DOIT être activée et vous DEVEZ saisir des mots de passe forts pour toutes les stations IP. Vérifiez la liste des indicateurs **d'authentification actifs** et complétez le formulaire. Champs **« Nouveau mot de passe »** et **« Confirmer le mot de passe »** .
m) Cliquez sur **OK et Suivant** .
n) Modifiez les drapeaux de la station selon les besoins. Pour une description des drapeaux de station, voir Station > Station > Paramètres de la station .
o) Cliquez sur **OK et Suivant** .

14) Si vous souhaitez configurer une autre station, répétez les étapes 5 à 13 .
15) Cliquez sur **OK et Suivant** . Une liste de toutes les stations IP configurées s'affiche. Si nécessaire, vous pouvez imprimer la liste des stations IP avec **Print** .
16) Cliquez sur **OK et Suivant,** puis sur **Terminer** .

10.13.2 Comment configurer les abonnés SIP

L'assistant **Téléphones IP** vous permet de configurer les abonnés SIP (téléphones LAN et téléphones WLAN).

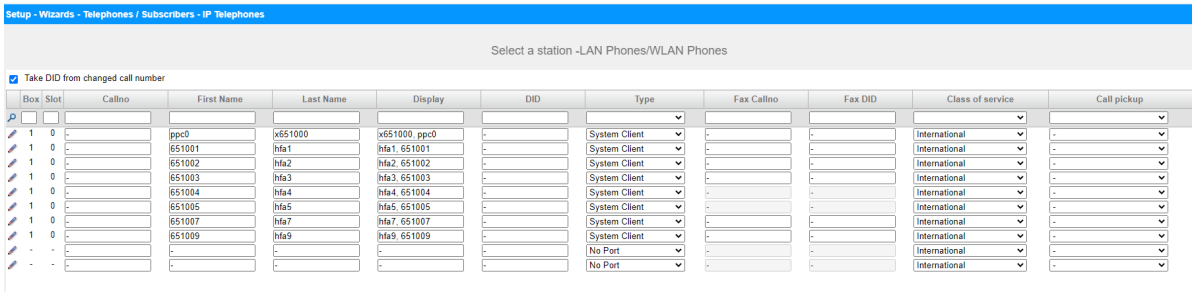
Conditions préalables

Pour que les téléphones WLAN fonctionnent, vous avez besoin d'un réseau LAN sans fil fonctionnel.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphones/ Abonnés**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Terminaux IP**. Le système affiche une liste de tous les abonnés IP. Cette liste contient également tous les abonnés SIP.



4) Si l'abonné doit recevoir automatiquement le numéro interne comme numéro SDA, activez le champ d'option **Prendre le SDA du numéro d'appel entré**.
5) Si le numéro SDA de l'abonné doit être différent de son numéro d'appel, saisissez un numéro SDA dans le champ **SDA** de la ligne de l'abonné concerné :
   - Uniquement pour le raccordement système :

     Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
   - uniquement pour un raccordement multiposte :

     À partir de la liste déroulante, sélectionnez un numéro MSN. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
   - pour le raccordement système et un raccordement multiposte :

     Dans la liste déroulante du champ souhaité, sélectionnez l'entrée **xxx - modifiable** (xxx correspondant au numéro interne) et saisissez le numéro SDA à l'aide du clavier ou sélectionnez un MSN (Multiple Subscriber Number, numéro de téléphone multiple).
6) Si l'abonné doit bénéficier d'un numéro d'abonné de téléphonie Internet en tant que numéro SDA, laissez désactivé le champ d'option **Prendre le SDA du numéro d'appel entré** , sélectionnez dans la liste figurant à côté de ce champ d'option le fournisseur de services de téléphonie sur Internet

et sélectionnez le numéro d'abonné de téléphonie Internet dans la ligne de l'abonné souhaité, à partir de la liste déroulante **SDA**.

7) Sur la ligne de l’abonné souhaité, saisissez le numéro de téléphone interne de l’abonné dans **Numéro de téléphone**. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

8) Dans le champ **Nom** de la ligne de l’abonné souhaité, saisissez un nom au format `Nom de famille, Prénom` ou `Prénom Nom de famille`.

9) Dans la ligne de l'abonné souhaité, sélectionnez dans la liste déroulante **Type** le type **Client SIP**.

10) Si vous souhaitez configurer une boîte Fax pour l’abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme suit :

a) Dans la ligne de l’abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l’utilisateur pourra recevoir des messages Fax internes.

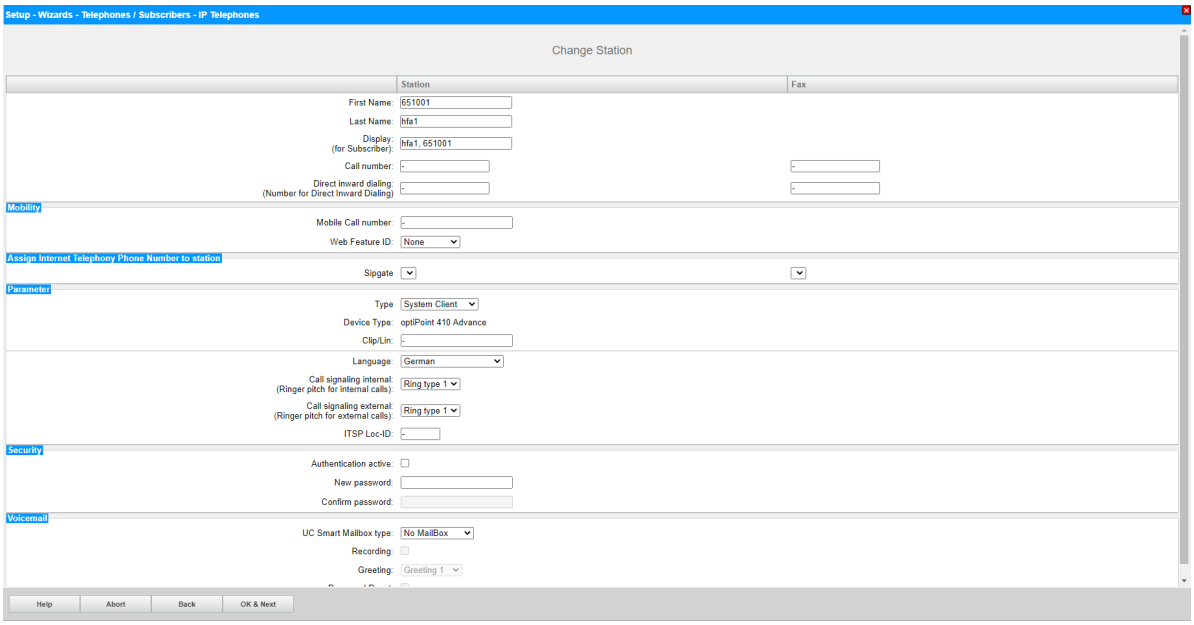
b) Si un numéro SDA doit être configuré pour la boîte Fax, entrez dans la ligne de l’abonné souhaité, champ **SDA Fax**, le numéro de fax externe souhaité sous lequel l’abonné pourra recevoir des messages Fax externes.

11) Dans la liste déroulante **Classe de service** de la ligne de l’abonné concerné, sélectionnez le groupe de classe de service souhaité.

12) Pour intégrer l’abonné à un groupe d’interception, sélectionnez un groupe dans la liste déroulante **Interception** de la ligne de l’abonné souhaité.

13) Configurez les données pour l'enregistrement SIP

a) Sur la ligne de l’abonné souhaité, cliquez sur l’icône **Modifier**.



b) Dans la zone **Sécurité**, entrez le mot de passe pour l'authentification de l'abonné SIP dans les champs **Mot de passe** et **Valider mot de passe**.

c) Dans le champ **Identifiant utilisateur SIP/Nom d'utilisateur**, attribuez un nom d'utilisateur de votre choix pour l'authentification de la station SIP, par ex. SIP-120.

d) Dans **Realm**, attribuez un nom de votre choix à la zone correspondante, par ex. OSBIZ-SIP. Cette valeur doit être la même pour tous les abonnés SIP.

Remarque : Les valeurs définies ici pour le mot de passe, l’identifiant utilisateur SIP et Realm doivent aussi être entrées sur le téléphone SIP.

---

14) Si nécessaire, définissez d'autres paramètres :

a) Si ce téléphone SIP doit être utilisé en même temps qu'un téléphone mobile dual mode, saisissez dans la zone **Mobilité**, **Numéro de mobile** l'indicatif réseau suivi du numéro du téléphone mobile (par ex. `0016012345678`). Sélectionnez en plus dans la liste déroulante **Web Feature ID** ce client SIP. (Voir Téléphonie dual mode).

b) Attribuer chaque fois un numéro SDA pour la téléphonie Internet vers l’abonné et, si on le souhaite, vers la boîte Fax, dans la zone **Sélection directe à l'arrivée pour téléphonie Internet**. Pour cela, sélectionner le numéro SDA dans les listes déroulantes des ITSP souhaités. Pour chaque ITSP activé, il est présenté une liste déroulante pour le abonné et une liste déroulante pour la boîte Fax.

Remarque : Le champ **SDA pour la téléphonie Internet** n’est pas visible lorsque la téléphonie Internet n’est pas configurée ou lorsqu’aucun fournisseur de services de téléphonie sur Internet n’est activé.

---

c) Dans le champ **Clip/Lin**, saisissez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant, et le numéro interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

---

d) Sélectionnez dans la liste déroulante **Langue** la langue des menus du téléphone.

e) Dans la liste déroulante **Signalisation des appels internes**, affectez à l'abonné l'une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres abonnés internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

f) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

g) Uniquement avec UC Smart : Sélectionnez dans la liste déroulante **Type de boîte de messagerie UC Smart** si l'abonné doit recevoir une boîte de messagerie standard ou une boîte de messagerie de diffusion (AutoAttendant).

h) Uniquement avec UC Smart et la boîte de messagerie par défaut : Si un appelant est autorisé à laisser un message sur la boîte vocale, cochez la case **Enregistrement**.

i) Uniquement avec UC Smart : Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.

j) Uniquement avec UC Smart : Si le mot de passe de la boîte vocale doit être rétabli, cochez la case **Réinitialisation mot de passe**.

Remarque : La case à cocher **Réinitialisation mot de passe** ne doit pas être sélectionnée lors de la reconfiguration d'une boîte vocale. Cela provoque la réinitialisation du mot de passe de la boîte vocale. Lors d'une nouvelle configuration, l'abonné doit de toute manière, lors du premier accès à sa boîte vocale, modifier le mot de passe initial.

---

k) Cliquez sur **OK & Suivant**.

l) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonné, voir Abonnés > Abonnés > Paramètres d'abonné.

m) Cliquez sur **OK & Suivant**.

15) Si vous souhaitez paramétrer un autre abonné, répétez les étapes 5 à 14.

16) Cliquez sur **OK & Suivant**. Le système affiche une liste de tous les abonnés IP paramétrés. Si nécessaire, vous pouvez imprimer la liste des abonnés IP à l'aide de **Imprimer**.

17) Cliquez sur **OK & Suivant**, puis sur **Quitter**.

10.13.3 Comment configurer les stations UP0

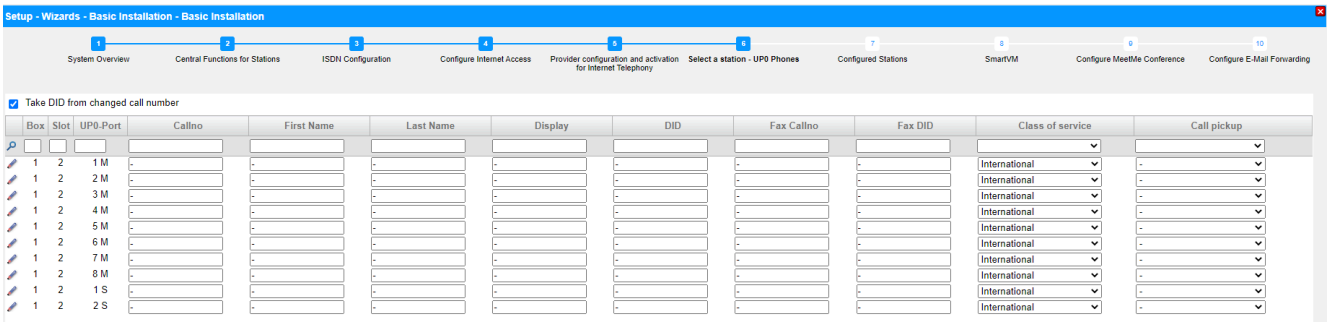
Vous pouvez utiliser l'assistant **Périphériques UP0** pour configurer les stations UP0.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téphones / Abonnés**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Périphériques UP0**. Une liste de toutes les stations UP0 s'affiche.



4) Si vous souhaitez que le numéro d'appel interne soit automatiquement attribué à la station en tant que numéro d'appel direct, activez le bouton radio **Prendre le SDA du numéro d'appel modifié**.
5) Si vous souhaitez un numéro de sélection directe à l'arrivée différent du numéro d'appel pour l'abonné, entrez un numéro SDA pour l'abonné sous **SDA** dans la ligne de l'abonné souhaité :
   - Uniquement pour le raccordement système :

     Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
   - uniquement pour un raccordement multiposte :

     Sélectionnez un MSN dans le champ souhaité à l'aide de la liste déroulante. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
   - pour le raccordement système et un raccordement multiposte :

     Sélectionnez dans le champ souhaité par la liste déroulante l'entrée **xxx - modifiable** (xxx correspond au numéro interne) et entrez le numéro SDA à l'aide du clavier ou sélectionnez un MSN dans la liste déroulante.
6) Si vous souhaitez qu'un numéro de téléphone de téléphonie Internet soit attribué à la station en tant que numéro de sélection directe à l'arrivée, ne sélectionnez pas la case d'option **Prendre la SDA à partir du numéro d'appel modifié** et sélectionnez le fournisseur de services de téléphonie Internet dans la liste située à côté du bouton radio. Sélectionnez ensuite le numéro de téléphone Internet dans la liste déroulante **SDA** correspondant au poste souhaité.

7) À la ligne de l'abonné souhaité, entrez dans **Numéro de téléphone** le numéro de téléphone interne de l'abonné. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

8) Entrez dans la ligne de l'abonné souhaité sous **Nom** un nom, sous la forme `Nom de famille, Prénom` ou `Prénom Nom de famille`.

9) Si une boîte Fax doit être paramétrée pour l'abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme indiqué ci-après :

   a) Dans la ligne de l'abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l'utilisateur pourra recevoir des messages Fax internes.

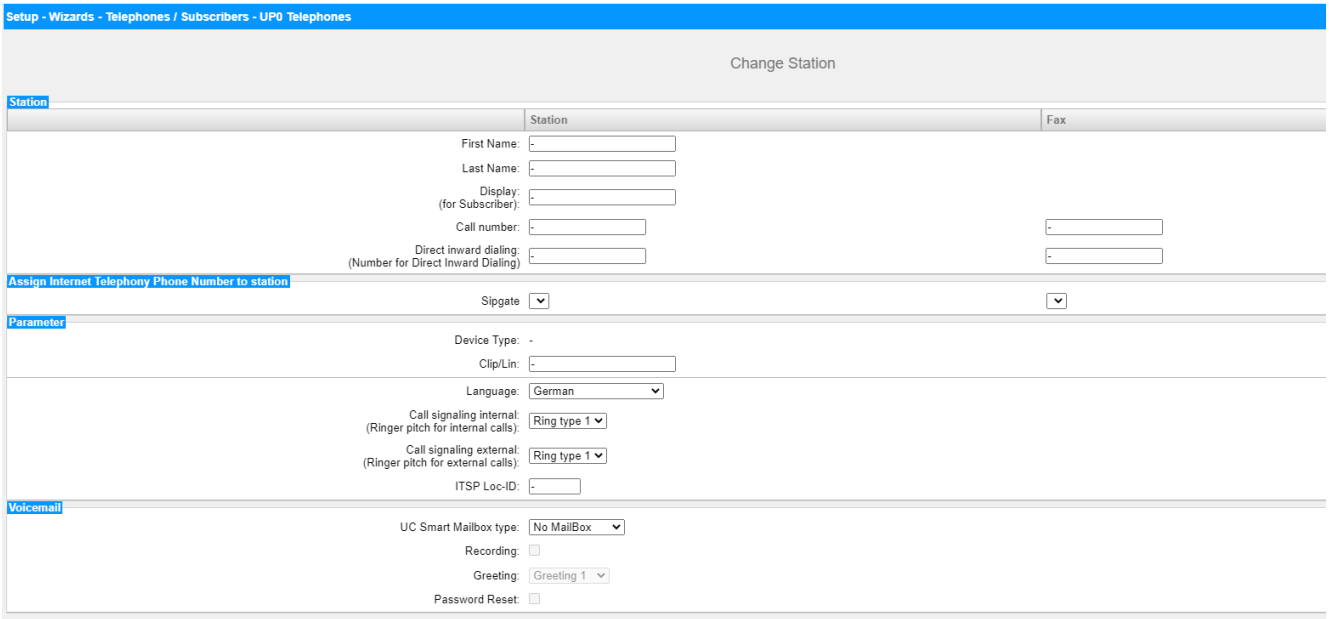
   b) Si vous souhaitez configurer un numéro SDA pour la boîte de fax, entrez le numéro de fax externe souhaité sous lequel l'abonné peut recevoir des messages fax externes dans le champ **Fax SDA** de la ligne de l'abonné souhaité.

10) À la ligne de l'abonné souhaité, sélectionnez dans la liste déroulante **Classe de service** le groupe de classe de service souhaité.

11) Pour intégrer l'abonné dans un groupe d'interception, sélectionnez un groupe d'interception dans la ligne de l'abonné souhaité de la liste déroulante **Groupe d'interception**.

12) Effectuez d'autres réglages si nécessaire :

   a) Dans la ligne de l'abonné souhaité, cliquez sur **Modifier**.



   b) Sélectionnez un numéro SDA dans une liste déroulante de la zone **SDA pour la téléphonie Internet**. Pour chaque ITSP actif, une liste déroulante s'affiche.

Remarque : Le champ **SDA pour la téléphonie Internet** n'est pas visible lorsque la téléphonie Internet

n’est pas paramétrée ou lorsque aucun fournisseur de services de téléphonie sur Internet n’est activé.

c) Dans **Clip/Lin**, entrez un numéro de téléphone (numéro SDA ou MSN) qui, lors d’un appel externe, sera affiché sur l’écran de l’appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l’opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l’appelant et le numéro interne est formaté et envoyé comme numéro de l’appelant pour l’appel externe.

d) Sélectionnez dans la liste déroulante **Langue** la langue des menus du téléphone.

e) Depuis la liste déroulante **Signalisation des appels internes**, affectez à l’abonné une des huit signalisations d’appel acoustiques possibles pour les appels internes (au total). Ainsi, l’abonné adresse aux autres abonnés internes une tonalité d’appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

f) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l’abonné une des huit signalisations d’appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

g) Uniquement avec UC Smart : Sélectionnez si l'abonné doit recevoir une boîte aux lettres par défaut ou une boîte aux lettres d'opérateur (AutoAttendant) dans la liste déroulante **Type de boîte aux lettres UC Smart**.

h) Uniquement avec UC Smart et boîte aux lettres par défaut : Si un appelant peut laisser un message dans la boîte vocale, cochez la case **Enregistrement**.

i) Uniquement avec UC Smart : Sélectionnez un message d'accueil dans la liste déroulante **Message d'accueil**.

j) Uniquement avec UC Smart : Si le mot de passe de la boîte vocale doit être réinitialisé, cochez la case **Réinitialisation du mot de passe**.

Remarque : La case **Réinitialisation du mot de passe** doit être décochée lors de la configuration d'une nouvelle boîte vocale. Elle sert à réinitialiser le mot de passe de la boîte vocale. Lorsqu'une nouvelle boîte vocale est créée, l'abonné doit de toute façon modifier le mot de passe initial lorsqu'il accède à sa boîte vocale pour la première fois.

k) Cliquez sur **OK & Suivant**.

l) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs de station, voir Station > Station > Paramètres de station.

m) Cliquez sur **OK & Suivant**.

13) Si vous souhaitez configurer une autre station, répétez les étapes 5 à 12.

14) Cliquez sur **OK & Suivant**. Une liste de toutes les stations UP0 configurées s'affiche. Si nécessaire, vous pouvez imprimer la liste des stations UP0 à l'aide de l'option **Imprimer**.
15) Cliquez sur **OK & Suivant**, puis sur **Terminer**.

10.13.4 Comment configurer les abonnés DECT

Vous pouvez utiliser l'assistant **Périphériques DECT** pour configurer les stations DECT (téléphones DECT).

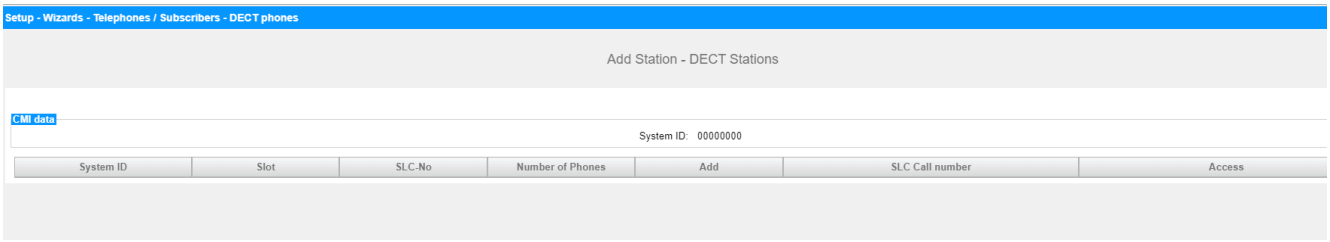
Conditions préalables

Une station de base est connectée à une interface UP0 ou à une carte SLC installée.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Tépéhones / Abonnés**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Téléphones DECT**. Une liste de toutes les stations DECT s'affiche.



4) Si vous souhaitez que le numéro d'appel interne soit automatiquement attribué à la station en tant que numéro d'appel direct, activez le bouton radio **Prendre le SDA du numéro d'appel modifié**.
5) Si vous souhaitez un numéro de sélection directe à l'arrivée différent du numéro d'appel pour l'abonné, entrez un numéro SDA pour l'abonné sous **SDA** dans la ligne de l'abonné souhaité :
   - Uniquement pour le raccordement système :

     Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
   - uniquement pour un raccordement multiposte :

     Sélectionnez un MSN dans le champ souhaité à l'aide de la liste déroulante. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
   - pour le raccordement système et un raccordement multiposte :

     Sélectionnez dans le champ souhaité par la liste déroulante l'entrée **xxx - modifiable** (xxx correspond au numéro interne) et entrez le numéro SDA à l'aide du clavier ou sélectionnez un MSN dans la liste déroulante.
6) Si vous souhaitez qu'un numéro de téléphone de téléphonie Internet soit attribué à la station en tant que numéro de sélection directe à l'arrivée, ne

sélectionnez pas la case d'option **Prendre la SDA à partir du numéro d'appel modifié** et sélectionnez le fournisseur de services de téléphonie Internet dans la liste située à côté du bouton radio. Sélectionnez ensuite le numéro de téléphone Internet dans la liste déroulante **SDA** correspondant au poste souhaité.

7) À la ligne de l'abonné souhaité, entrez dans **Numéro de téléphone** le numéro de téléphone interne de l'abonné. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

8) Entrez dans la ligne de l'abonné souhaité sous **Nom** un nom, sous la forme `Nom de famille, Prénom` ou `Prénom Nom de famille`.

9) Si une boîte Fax doit être paramétrée pour l'abonné (utilisable par ex. avec les clients UC **myPortal for Desktop** ou **myPortal for Outlook**), procédez comme indiqué ci-après :

a) Dans la ligne de l'abonné souhaité, dans le champ **Numéro Fax**, indiquez le numéro de téléphone Fax interne souhaité sous lequel l'utilisateur pourra recevoir des messages Fax internes.

b) Si vous souhaitez configurer un numéro SDA pour la boîte de fax, entrez le numéro de fax externe souhaité sous lequel l'abonné peut recevoir des messages fax externes dans le champ **Fax SDA** de la ligne de l'abonné souhaité.

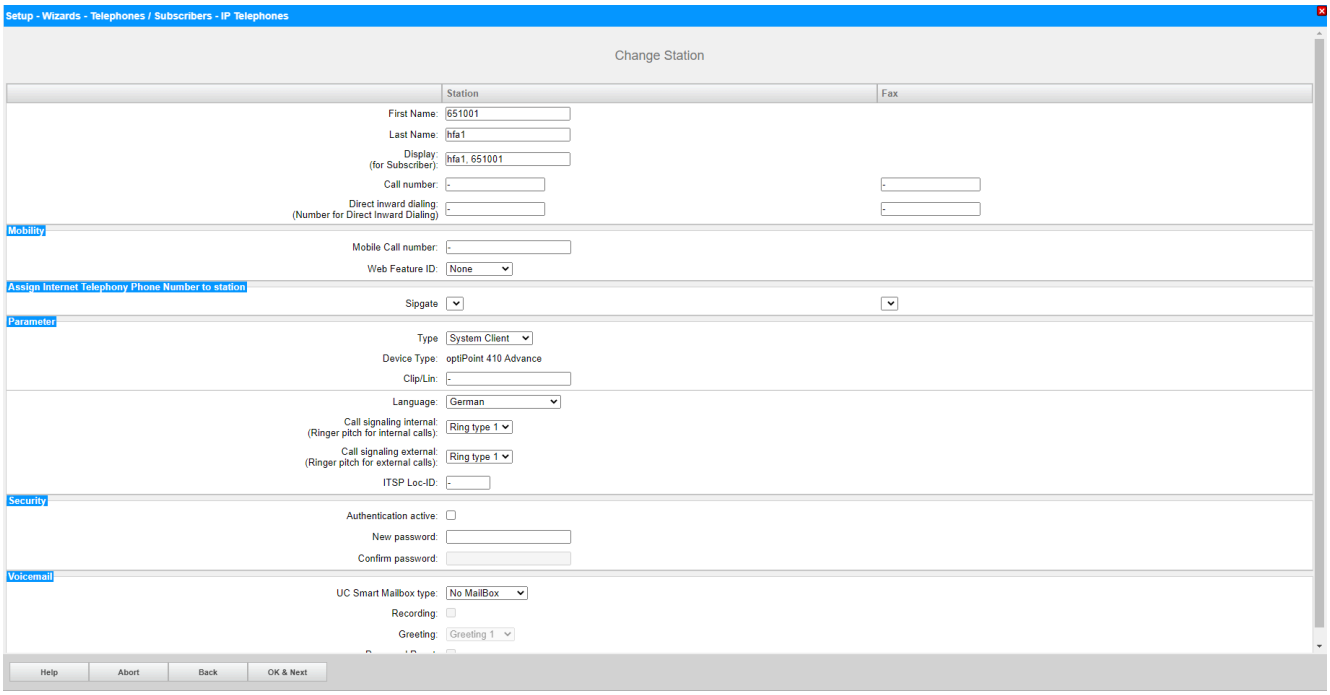
10) À la ligne de l'abonné souhaité, sélectionnez dans la liste déroulante **Classe de service** le groupe de classe de service souhaité.

11) Pour intégrer l'abonné dans un groupe d'interception, sélectionnez un groupe d'interception dans la ligne de l'abonné souhaité de la liste déroulante **Groupe d'interception**.

12) Si vous voulez modifier le code téléphone DECT (PIN), entrez le nouveau code dans la ligne de l'abonné souhaité, dans **Code mobile**. Les abonnés DECT doit s'inscrire de nouveau sur l'abonne de base en utilisant ce code.

13) Effectuez d'autres réglages si nécessaire :

a) Dans la ligne de l'abonné souhaité, cliquez sur **Modifier**.



b) Sélectionnez un numéro SDA dans une liste déroulante de la zone **SDA pour la téléphonie Internet**. Pour chaque ITSP actif, une liste déroulante s'affiche.

Remarque : Le champ **SDA pour la téléphonie Internet** n'est pas visible lorsque la téléphonie Internet n'est pas paramétrée ou lorsque aucun fournisseur de services de téléphonie sur Internet n'est activé.

---

c) Dans **Clip/Lin**, entrez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant et le numéro interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

---

d) Sélectionnez dans la liste déroulante **Langue** la langue des menus du téléphone.

e) Depuis la liste déroulante **Signalisation des appels internes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres

abonnés internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

f) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

g) Uniquement avec UC Smart : Sélectionnez si l'abonné doit recevoir une boîte aux lettres par défaut ou une boîte aux lettres d'opérateur (AutoAttendant) dans la liste déroulante **Type de boîte aux lettres UC Smart**.

h) Uniquement avec UC Smart et boîte aux lettres par défaut : Si un appelant peut laisser un message dans la boîte vocale, cochez la case **Enregistrement**.

i) Uniquement avec UC Smart : Sélectionnez un message d'accueil dans la liste déroulante **Message d'accueil**.

j) Uniquement avec UC Smart : Si le mot de passe de la boîte vocale doit être réinitialisé, cochez la case **Réinitialisation du mot de passe**.

Remarque : La case **Réinitialisation du mot de passe** doit être décochée lors de la configuration d'une nouvelle boîte vocale. Elle sert à réinitialiser le mot de passe de la boîte vocale. Lorsqu'une nouvelle boîte vocale est créée, l'abonné doit de toute façon modifier le mot de passe initial lorsqu'il accède à sa boîte vocale pour la première fois.

---

k) Cliquez sur **OK & Suivant**.

l) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs de station, voir Station > Station > Paramètres de station.

m) Cliquez sur **OK & Suivant**.

14) Si vous souhaitez configurer une autre station, répétez les étapes 5 à 13.

15) Cliquez sur **OK & Suivant**. Une liste de toutes les stations DECT configurées s'affiche. Si nécessaire, vous pouvez imprimer la liste des stations DECT à l'aide de l'option **Imprimer**.

16) Cliquez sur **OK & Suivant**, puis sur **Terminer**.

Tâches associées

Comment configurer pour la première fois les abonnés DECT à la page 907

10.13.5 Comment configurer les stations SIP-DECT Mitel via le provisioning

Vous pouvez utiliser l'assistant **SIP-DECT Mitel** pour configurer les équipements SIP-DECT et vous connecter à l'Open Mobility Manager (OMM).

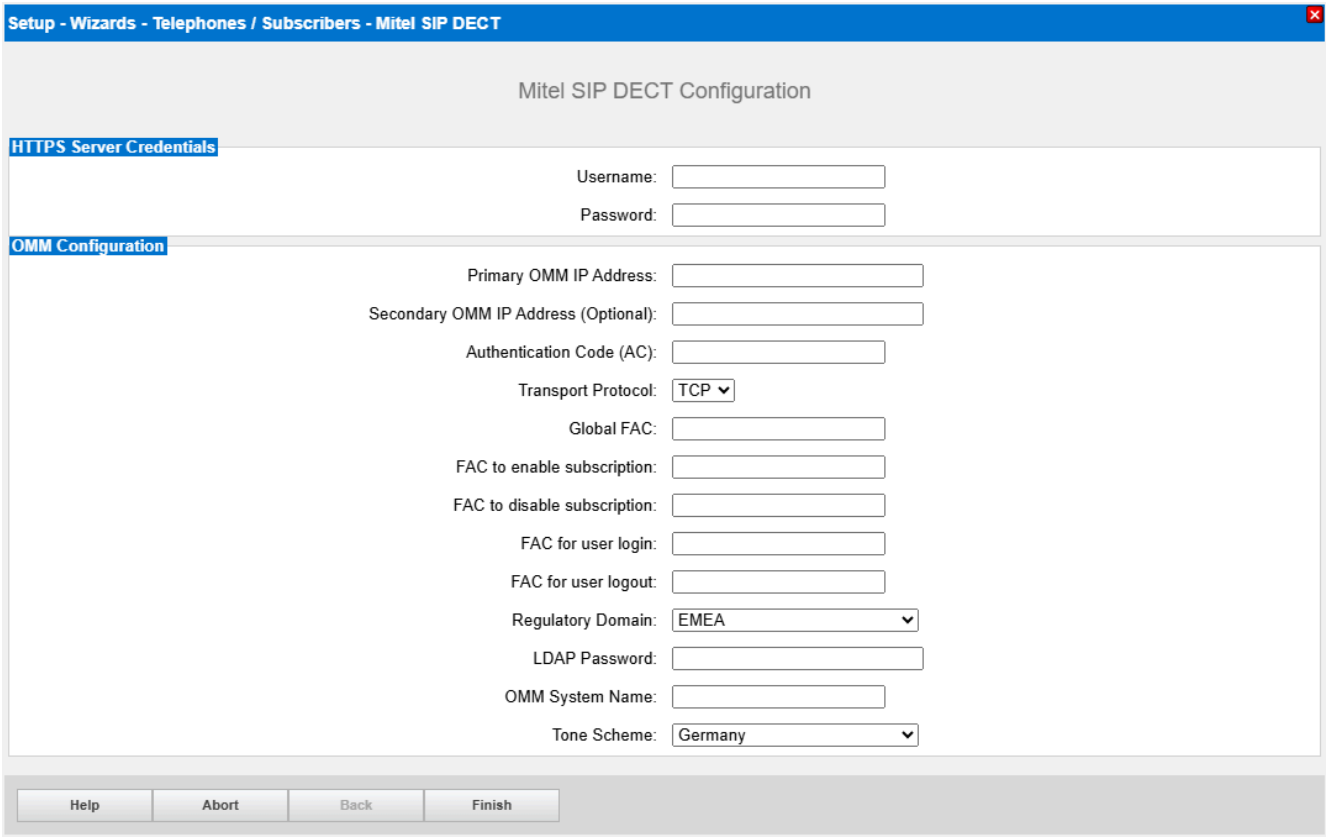
Conditions préalables

L'adresse MAC du terminal RFP SIP-DECT est connue.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert > Interfaces réseau > DHCP**.

2) Cliquer pour activer le **serveur DHCP**.
3) Dans la barre de navigation, cliquez sur **Serveur DHCP > Adresses IP statiques**.
4) Dans la fenêtre **Adresses IP statiques**, cliquez sur l'onglet « **Ajouter une adresse IP statique** ».
5) Saisissez les informations requises comme décrit dans Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Adresses IP statiques.
6) Cliquez sur **Appliquer**.
7) Dans la barre de navigation, cliquez sur **Configuration**.
8) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphones/ Abonnés**.
9) Cliquez sur **Modifier** pour démarrer l'**assistant Mitel SIP DECT**.



10) Sous **HTTPS Server Credentials** (Informations d'identification du serveur HTTPS), fournissez les informations d'identification permettant d'accéder au serveur.
    a) Définissez le **nom d'utilisateur** et le **mot de passe**.
11) Sous **Configuration OMM** :
12) Indiquez **l'adresse IP de l'OMM primaire** ainsi que **l'adresse IP de l'OMM secondaire** (facultative).
13) Définissez le **code d'authentification (CA)**
14) Dans **Protocole de transport**, choisissez l'une des valeurs suivantes dans le menu déroulant :
    - TCP
    - UDP
    - TLS

15) Définissez les différents codes d'accès aux fonctionnalités (FAC) dans les champs suivants :
    a) **Global FAC**
    b) **FAC pour activer l'abonnement.**
    c) **FAC pour la connexion de l'utilisateur**
    d) **FAC pour la déconnexion de l'utilisateur**
16) Dans **Domaine réglementaire**, choisissez l'une des valeurs suivantes dans le menu déroulant :
    - EMEA
    - ÉTATS-UNIS
    - Brésil
    - Taïwan
    - Radio 1910 - 1927 MHz 250 mW
17) Indiquez le **mot de passe LDAP** pour accéder au répertoire interne des utilisateurs d'OpenScape Business.
18) Définissez le **nom du système OMM**.
19) Choisissez le **schéma de tonalité**.
20) Cliquez sur **Terminer**.
    Les fichiers de configuration nécessaires à l'application OMM sont générés.

    Remarque :

    Après une mise à jour logicielle, les champs ci-dessus seront vides, même s'ils étaient auparavant configurés. Vous devrez les saisir de nouveau manuellement dans l'interface WBM (Web Based Management) d'OpenScape Business.

21) Configurez un terminal SIP comme décrit dans la section « Comment configurer des terminaux SIP via le mode expert ».
22) Connectez l'appareil RFP Mitel SIP DECT au réseau. Attendez quelques instants que l'appareil reçoive une adresse IP du serveur DHCP.
23) Connectez-vous à l'application OMM et configurez la station de base, comme décrit dans le « *Guide de configuration des téléphones Mitel SIP DECT* ».

10.13.5.1 Comment configurer les stations SIP via le mode Expert

Vous pouvez utiliser le **mode Expert** pour configurer les stations SIP.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Expert**.

Étape par étape

1) Dans l'arborescence de navigation, cliquez sur **mode Expert** > **Serveur de téléphonie** > **Station**.
2) Dans la nouvelle fenêtre, cliquez pour développer **Station** puis sélectionnez **Client IP**. Une liste de toutes les stations IP/SIP s'affiche.
3) Dans la colonne **Type**, sélectionnez **Client SIP**.

4) Cliquez sur **Appliquer**.
5) Cliquez sur la flèche bleue à côté du numéro d'appel de la station IP, sous la colonne **Numéro d'appel**.
6) Dans la fenêtre **Modifier les paramètres de la station**, sélectionnez **Périphérique Mitel SIP DECT** dans le menu déroulant sous **Provisionnement du périphérique**.
   L'option **Configuration Mitel SIP DECT** s'affiche.
7) Sous l'option **Configuration Mitel SIP DECT** définissez les paramètres suivants :
   a) Entrez le code **PIN** du périphérique.
   b) Dans **Verrouillage des touches activé**, activez (Oui) ou désactivez (Non) le verrouillage des touches de l'appareil.
   c) Dans **Code PIN de verrouillage des touches**, entrez le code PIN pour le verrouillage des touches.
   d) Dans **Durée du verrouillage des touches**, entrez la durée pendant laquelle le code PIN de verrouillage des touches doit rester actif.
   e) Dans **Afficher le répertoire personnel**, choisissez si le répertoire personnel est visible (Oui) ou non (Non).
8) Cliquez sur **Appliquer**.
9) Accédez à l'onglet **Modifier les données du client du poste de travail**.
10) Sous **Paramètres**, configurez les valeurs comme décrit dans Paramètres de la station.
11) Cliquez sur **Appliquer**.

10.13.6 Comment configurer les abonnés RNIS

L'Assistant **Terminaux RNIS** vous permet de configurer les abonnés RNIS (par ex. téléphones RNIS ou fax RNIS).

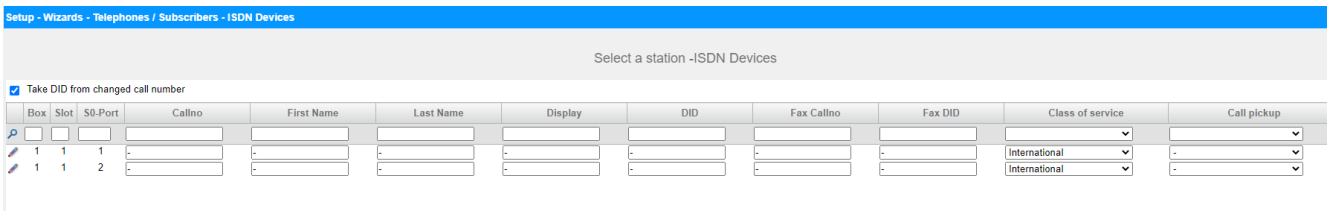
Conditions préalables

Au moins une interface es S_0 est disponibles. Si l'un des ports S_0 d'une plate-forme matérielle est utilisé, il doit être paramétré en tant que raccordement S_0 interne.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphones/ Abonnés**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Terminaux RNIS**. Le système affiche une liste de tous les abonnés RNIS.



4) Lorsque le numéro SDA de l'abonné doit être automatiquement adapté à son numéro, activez le champ d'option **Prendre le SDA du numéro d'appel modifié**.

5) Si le numéro SDA de l’abonné doit être différent de son numéro d’appel, saisissez un numéro SDA dans le champ **SDA** de la ligne de l’abonné concerné :

- Uniquement pour le raccordement système :

  Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
- uniquement pour un raccordement multiposte :

  À partir de la liste déroulante, sélectionnez un numéro MSN. L’abonné pourra ainsi être appelé en interne à l’aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
- pour le raccordement système et un raccordement multiposte :

  Dans la liste déroulante du champ souhaité, sélectionnez l’entrée **xxx - modifiable** (xxx correspondant au numéro interne) et saisissez le numéro SDA à l’aide du clavier ou sélectionnez un MSN (Multiple Subscriber Number, numéro de téléphone multiple).

6) Sur la ligne de l’abonné souhaité, saisissez le numéro de téléphone interne de l’abonné dans **Numéro de téléphone**. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

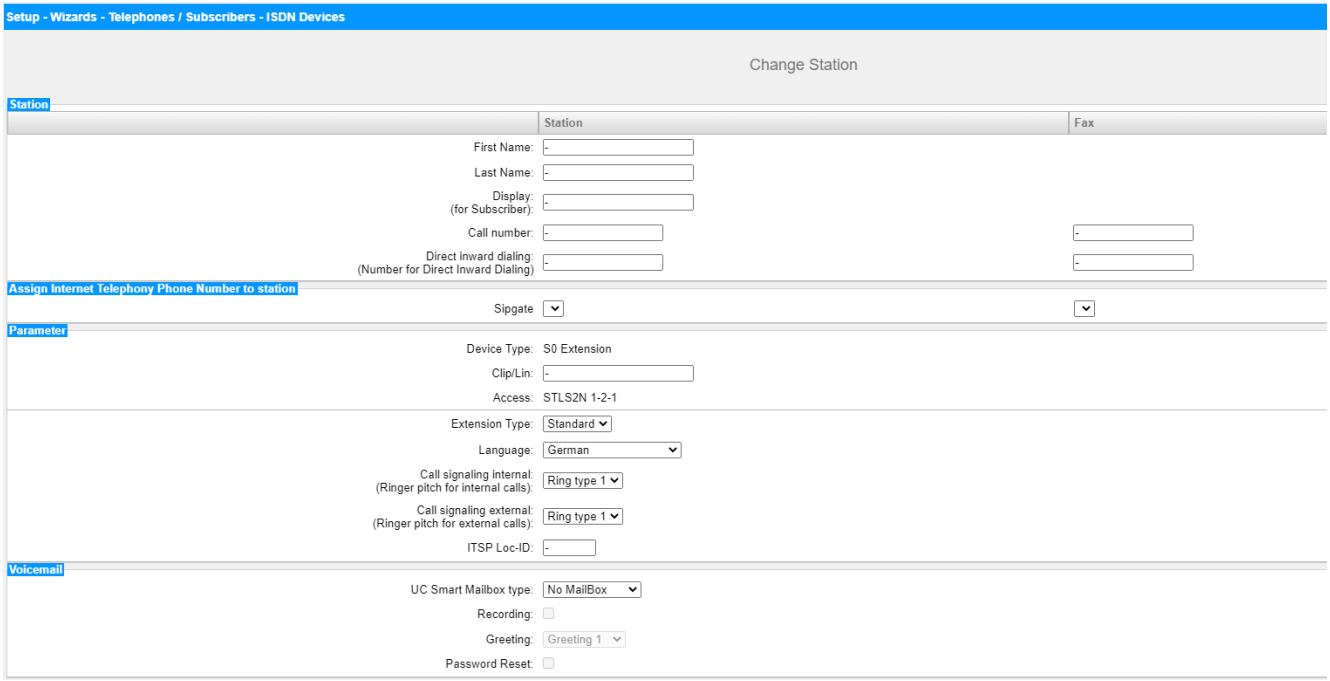
7) Dans le champ **Nom** de la ligne de l’abonné souhaité, saisissez un nom au format `Nom de famille, Prénom` ou `Prénom Nom de famille`.

8) A la ligne de l'abonné souhaité, sélectionnez dans la liste déroulante **Classe de discrimination** l'un des groupes de discrimination (catégorie d'accès) souhaités.

9) Pour intégrer l’abonné à un groupe d’interception, sélectionnez un groupe dans la liste déroulante **Interception** de la ligne de l’abonné souhaité.

10) Si nécessaire, définissez d'autres paramètres :

a) Sur la ligne de l'abonné souhaité, cliquez sur l'icône **Modifier**.



b) Sélectionnez un numéro SDA dans une liste déroulante de la zone **SDA pour la téléphonie Internet**. Pour chaque ITSP actif, une liste déroulante s'affiche.

Remarque : Le champ **SDA pour la téléphonie Internet** n'est pas visible lorsque la téléphonie Internet n'est pas configurée ou lorsqu'aucun fournisseur de services de téléphonie sur Internet n'est activé.

---

c) Dans le champ **Clip/Lin**, saisissez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant, et le numéro interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

---

d) Dans la liste déroulante **Type d'abonné**, sélectionnez le type de terminal RNIS (`par défaut` ou `Fax`).

e) Ne modifiez pas la sélection par défaut de la liste déroulante **Langue**. Pour les terminaux RNIS, ce paramétrage est sans importance.

f) Dans la liste déroulante **Signalisation des appels internes**, affectez à l'abonné l'une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres

abonnés internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

g) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

h) Uniquement avec UC Smart : Sélectionnez dans la liste déroulante **Type de boîte de messagerie UC Smart** si l'abonné doit recevoir une boîte de messagerie standard ou une boîte de messagerie de diffusion (AutoAttendant).

i) Uniquement avec UC Smart et la boîte de messagerie par défaut : Si un appelant est autorisé à laisser un message sur la boîte vocale, cochez la case **Enregistrement**.

j) Uniquement avec UC Smart : Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.

k) Uniquement avec UC Smart : Si le mot de passe de la boîte vocale doit être rétabli, cochez la case **Réinitialisation mot de passe**.

Remarque : La case à cocher **Réinitialisation mot de passe** ne doit pas être sélectionnée lors de la reconfiguration d'une boîte vocale. Cela provoque la réinitialisation du mot de passe de la boîte vocale. Lors d'une nouvelle configuration, l'abonné doit de toute manière, lors du premier accès à sa boîte vocale, modifier le mot de passe initial.

---

l) Cliquez sur **OK & Suivant**.

m) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonné, voir Abonnés > Abonnés > Paramètres d'abonné.

n) Cliquez sur **OK & Suivant**.

11) Si vous souhaitez paramétrer un autre abonné, répétez les étapes 5 à 10.

12) Cliquez sur **OK & Suivant**. Le système affiche une liste de tous les abonnés RNIS paramétrés. Si nécessaire, vous pouvez imprimer la liste des abonnés RNIS à l'aide de **Imprimer**.

13) Cliquez sur **OK & Suivant**, puis sur **Quitter**.

10.13.7 Comment configurer les abonnés analogiques

L'Assistant **Terminaux analogiques** vous permet de paramétrer les abonnés analogiques raccordés au (par ex. un téléphone analogique ou un fax analogique).

Conditions préalables

Au moins une interface analogique libre est disponible.

MFV est activée sur les appareils analogiques.

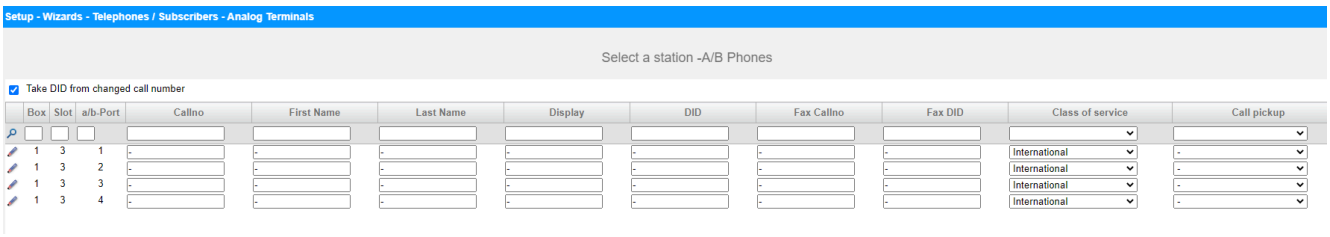
Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphones/ Abonnés**.

3) Cliquez sur **Modifier** pour démarrer l'Assistant **Terminaux analogiques**. Le système affiche une liste de tous les abonnés analogiques.



4) Lorsque le numéro SDA de l'abonné doit être automatiquement adapté à son numéro, activez le champ d'option **Prendre le SDA du numéro d'appel modifié**.

5) Si le numéro SDA de l'abonné doit être différent de son numéro d'appel, saisissez un numéro SDA dans le champ **SDA** de la ligne de l'abonné concerné :

   - Uniquement pour le raccordement système :

     Cliquez sur le champ souhaité et entrez le numéro SDA par le clavier. Le numéro SDA peut être identique au numéro interne.
   - uniquement pour un raccordement multiposte :

     À partir de la liste déroulante, sélectionnez un numéro MSN. L'abonné pourra ainsi être appelé en interne à l'aide du numéro interne 101 et en externe depuis le numéro MSN 654321.
   - pour le raccordement système et un raccordement multiposte :

     Dans la liste déroulante du champ souhaité, sélectionnez l'entrée **xxx - modifiable** (xxx correspondant au numéro interne) et saisissez le numéro SDA à l'aide du clavier ou sélectionnez un MSN (Multiple Subscriber Number, numéro de téléphone multiple).

6) Sur la ligne de l'abonné souhaité, saisissez le numéro de téléphone interne de l'abonné dans **Numéro de téléphone**. Vous pouvez utiliser le numéro prédéfini ou un autre, non encore affecté.

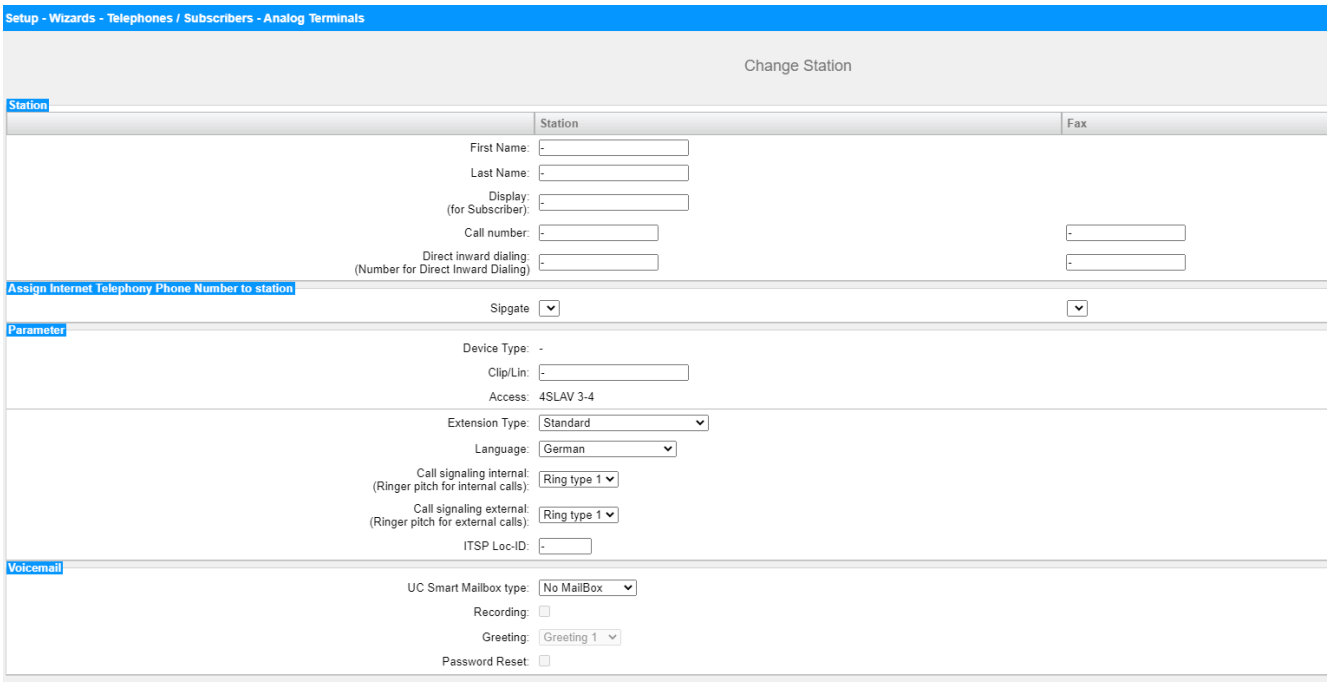
7) Dans le champ **Nom** de la ligne de l'abonné souhaité, saisissez un nom au format `Nom de famille, Prénom` ou `Prénom Nom de famille`.

8) A la ligne de l'abonné souhaité, sélectionnez dans la liste déroulante **Classe de discrimination** l'un des groupes de discrimination (catégorie d'accès) souhaités.

9) Pour intégrer l'abonné à un groupe d'interception, sélectionnez un groupe dans la liste déroulante **Interception** de la ligne de l'abonné souhaité.

10) Si nécessaire, définissez d'autres paramètres : pour un modem analogique, il faut sélectionner ici le type de terminal **Modem** :

a) Sur la ligne de l'abonné souhaité, cliquez sur l'icône **Modifier**.



b) Sélectionnez un numéro SDA dans une liste déroulante de la zone **SDA pour la téléphonie Internet**. Pour chaque ITSP actif, une liste déroulante s'affiche.

Remarque : Le champ **SDA pour la téléphonie Internet** n'est pas visible lorsque la téléphonie Internet n'est pas configurée ou lorsqu'aucun fournisseur de services de téléphonie sur Internet n'est activé.

---

c) Dans le champ **Clip/Lin**, saisissez un numéro de téléphone (numéro SDA ou MSN) qui, lors d'un appel externe, sera affiché sur l'écran de l'appelé à la place du vrai numéro.

Remarque : Cette fonctionnalité doit être validée par l'opérateur.

Remarque : Au moins un numéro SDA doit être configuré. Dans le cas contraire, le système ne tient pas compte du numéro CLIP de l'appelant, et le numéro

interne est formaté et envoyé comme numéro de l'appelant pour l'appel externe.

d) Sélectionnez dans la liste déroulante **Type de terminal** le type de terminal analogique (par ex. **fax**).

   Si un modem analogique doit être paramétré, il faut sélectionner ici le type de terminal **Modem**.

e) Ne modifiez pas la sélection par défaut de la liste déroulante **Langue**. Pour les terminaux analogiques, ce paramétrage est sans importance.

f) Dans la liste déroulante **Signalisation des appels internes**, affectez à l'abonné l'une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total). Ainsi, l'abonné adresse aux autres abonnés internes une tonalité d'appel modifiée ce qui permet de le distinguer des autres abonnés (par défaut : Type de sonnerie 1).

g) Depuis la liste déroulante **Signalisation des appels externes**, affectez à l'abonné une des huit signalisations d'appel acoustiques possibles pour les appels internes (au total) (par défaut : Type de sonnerie 1).

h) Uniquement avec UC Smart : Sélectionnez dans la liste déroulante **Type de boîte de messagerie UC Smart** si l'abonné doit recevoir une boîte de messagerie standard ou une boîte de messagerie de diffusion (AutoAttendant).

i) Uniquement avec UC Smart et la boîte de messagerie par défaut : Si un appelant est autorisé à laisser un message sur la boîte vocale, cochez la case **Enregistrement**.

j) Uniquement avec UC Smart : Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.

k) Uniquement avec UC Smart : Si le mot de passe de la boîte vocale doit être rétabli, cochez la case **Réinitialisation mot de passe**.

   Remarque : La case à cocher **Réinitialisation mot de passe** ne doit pas être sélectionnée lors de la reconfiguration d'une boîte vocale. Cela provoque la réinitialisation du mot de passe de la boîte vocale. Lors d'une nouvelle configuration, l'abonné doit de toute manière, lors du premier accès à sa boîte vocale, modifier le mot de passe initial.

l) Cliquez sur **OK & Suivant**.

m) Modifier les indicateurs abonné si nécessaire. Pour une description des indicateurs abonnés, voir Abonnés > Abonnés > Paramètres d'abonné.

n) Cliquez sur **OK & Suivant**.

11) Si vous souhaitez paramétrer un autre abonné, répétez les étapes 5 à 10.

12) Cliquez sur **OK & Suivant**. Le système affiche une liste de tous les abonnés analogiques paramétrés. Si nécessaire, vous pouvez imprimer la liste des abonnés analogiques à l'aide de **Imprimer**.

13) Cliquez sur **OK & Suivant**, puis sur **Quitter**.

10.13.8 Comment modifier les noms des abonnés

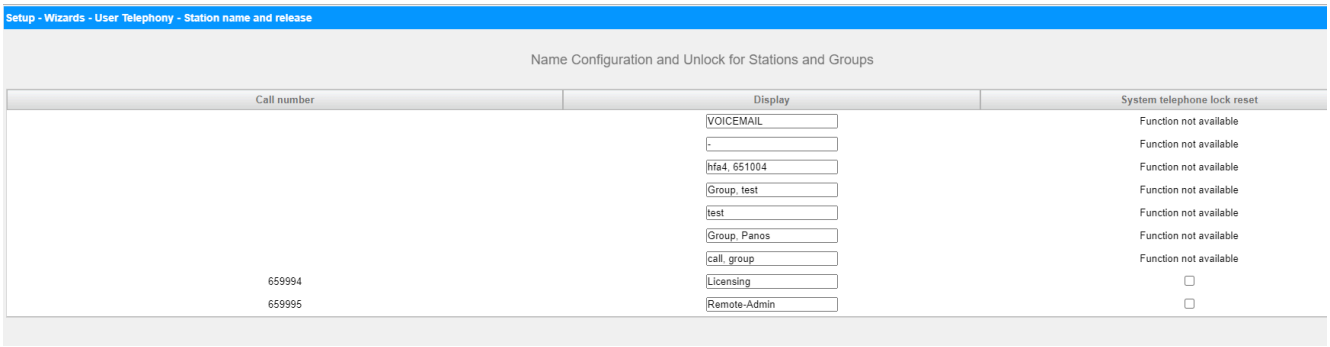
Avec l'assistant **Nom et version d'abonné** vous pouvez modifier le nom des abonnés.

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Nom et version d'abonné**.



4) Cliquez dans la colonne **Afficher** sur le champ de l'abonné souhaité et modifiez le nom de l'abonné sous la forme `Nom de famille, Prénom` ou `Prénom Nom de famille`.
5) Si vous souhaitez modifier les noms d'autres abonnés, répétez le point 4.
6) Cliquez sur **OK&Suivant** puis sur **Quitter**.

10.14 Configuration des profils d'abonné

Dans les profils d'abonné sont enregistrées les valeurs et caractéristiques des abonnés IP.

A l'aide de l'assistant **Profils**, un administrateur de profil **Advanced** peut réaliser les configurations suivantes.

- Créer un nouveau profil
- Afficher les profils et leurs membres
- Ajouter des membres à un profil
- Effacer les membres d'un profil
- Exporter ou importer un profil

A l'aide du mode Expert, un administrateur de profil **Expert** peut réaliser en plus les configurations suivantes.

- Modifier les valeurs et paramètres d'un profil existant
- Exporter ou importer tous les profils

Les profils d'abonné déjà créés ne peuvent pas être effacés, mais ils peuvent être écrasés.

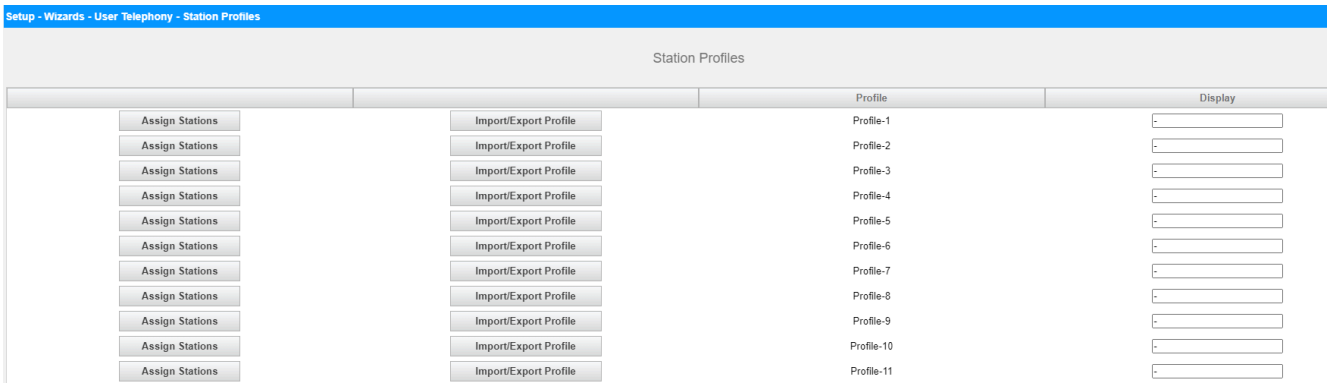
10.14.1 Comment créer un nouveau profil d'abonné

Conditions préalables

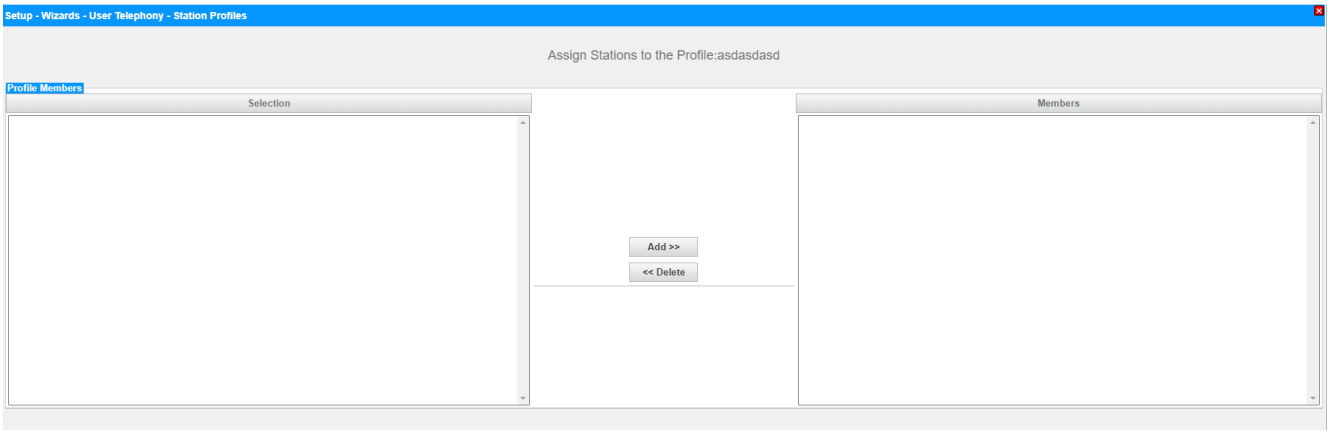
Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Pour démarrer l'assistant **Profils d'abonnés**, cliquez sur **Modifier**. Tous les Profils d'abonnés disponibles vous sont présentés.



4) Dans la colonne **Afficher** de la ligne du profil d'abonné souhaité, saisissez un nom de votre choix pour le profil (16 caractères max.).
5) Sur la ligne du profil d'abonné souhaité, cliquez sur **Affecter les abonnés**.



6) Dans le tableau **Profils membres**, sélectionnez les membres souhaités (sélection multiple possible) et cliquez sur **Ajouter**. Ces abonnés sont affectés au profil d'abonné et et ne peuvent plus être affectés à un autre profil d'abonné.
7) Cliquez sur **OK**.
8) Cliquez sur **OK & Suivant**. Tous les profils d'abonné existants et leurs membres sont affichés.
9) Cliquez sur **OK & Suivant**, puis sur **Quitter**.

10.14.2 Comment afficher les profils d'abonné et leurs membres

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Profils abonnés**. Tous les Profils d'abonnés disponibles vous sont présentés.
4) Cliquez sur **OK&Suivant**. Tous les profils d'abonné existants et leurs membres sont affichés.

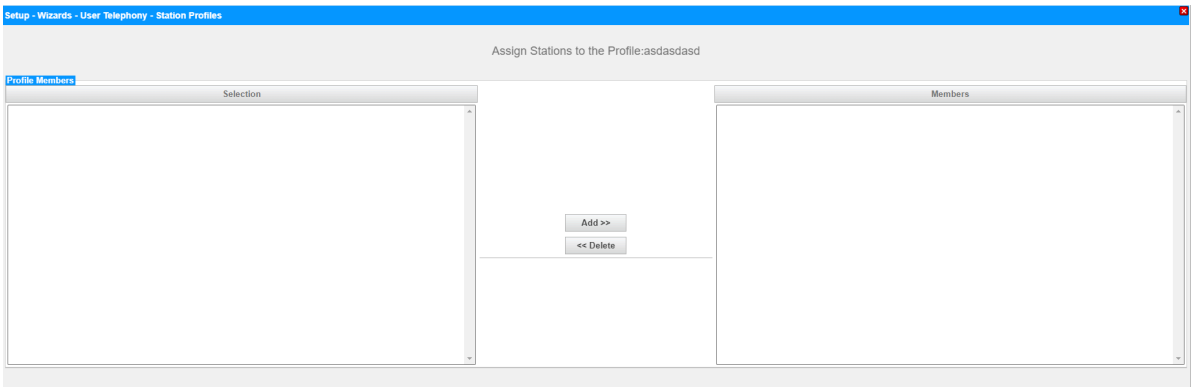
10.14.3 Comment ajouter des membres à un profil d'abonné

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Profils abonnés**. Tous les profils d'abonné existants et leurs membres sont affichés.
4) Dans la ligne du profil d'abonné souhaité, cliquez sur **Affecter les abonnés**.



5) Sélectionnez dans le Liste **Membres du profil** les membres souhaités (sélection multiple possible) et cliquez sur **Ajouter**. Ces abonnés sont affectés au profil d'abonné et et ne peuvent plus être affectés à un autre profil d'abonné.
6) Cliquez sur **OK**.
7) Cliquez sur **OK&Suivant**. Tous les profils d'abonné existants et leurs membres sont affichés.
8) Cliquez sur **OK&Suivant** puis sur **Terminer**.

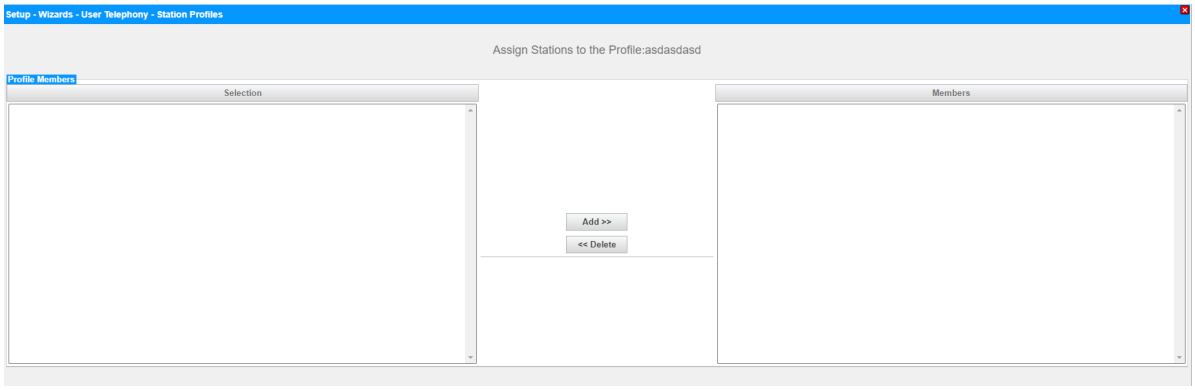
10.14.4 Comment effacer les membres d'un profil d'abonné

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Profils abonnés**. Tous les profils d'abonné existants et leurs membres sont affichés.
4) Dans la ligne du profil d'abonné souhaité, cliquez sur **Affecter les abonnés**.



5) Sélectionnez dans la liste **Membres** les membres souhaités (sélection multiple possible) et cliquez sur **Effacer**. Ces abonnés peuvent être affectés à un autre profil d'abonné.
6) Cliquez sur **OK**.
7) Cliquez sur **OK&Suivant**. Tous les profils d'abonné existants et leurs membres sont affichés.
8) Cliquez sur **OK&Suivant** puis sur **Terminer**.

10.14.5 Comment exporter ou importer un profil d'abonné

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Profils abonnés**. Tous les profils d'abonné existants et leurs membres sont affichés.
4) Dans la ligne du profil d'abonné souhaité, cliquez sur **Importer/exporter un profil**.

5) Si vous voulez exporter le profil d'abonné dans un fichier, cliquez sur **Téléchargement** et enregistrez le fichier dans un répertoire de votre choix.
6) Pour importer un profil d'abonné à partir d'un fichier, cliquez sur **Parcourir**, allez à l'endroit où le fichier a été enregistré et chargez le fichier dans le système de communication.
7) Cliquez sur **OK**.
8) Cliquez sur **OK&Suivant**. Tous les profils d'abonné existants et leurs membres sont affichés.
9) Cliquez sur **OK&Suivant** puis sur **Terminer**.

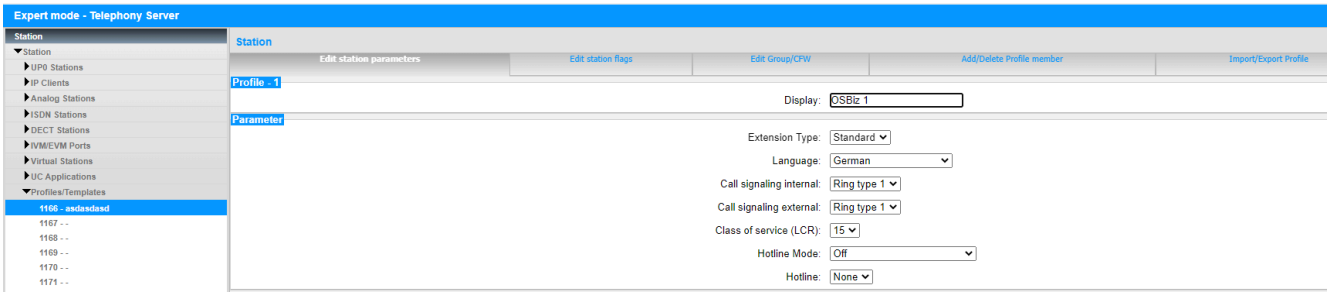
10.14.6 Comment modifier les valeurs et paramètres d'un profil

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

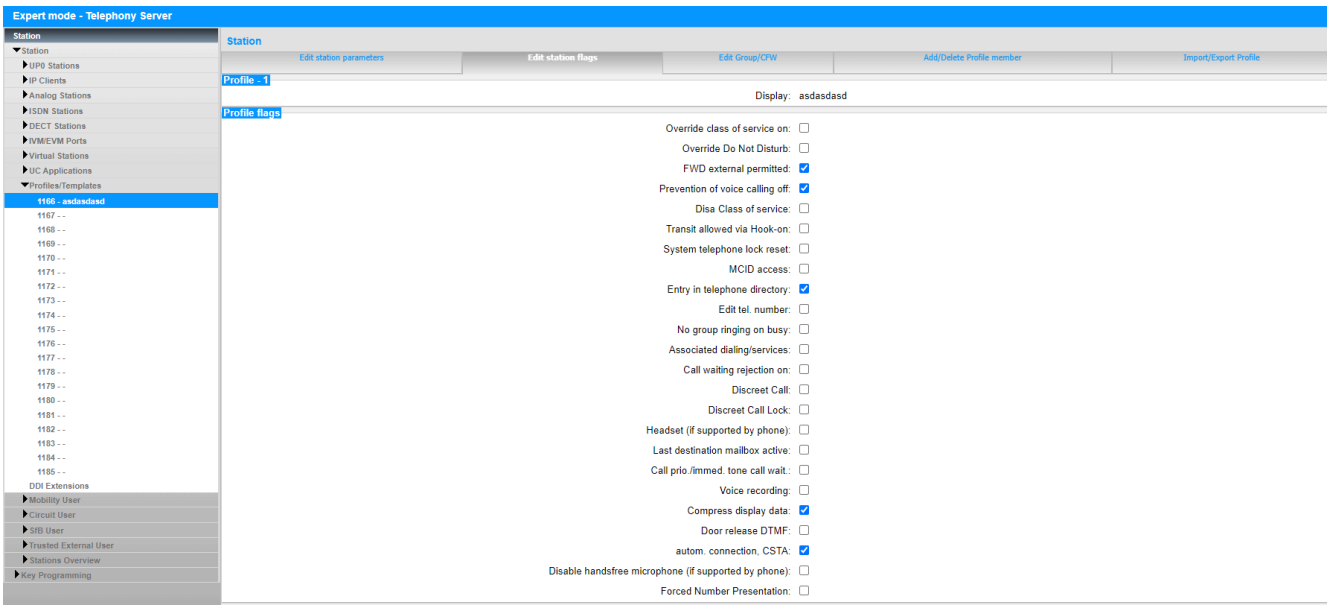
Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés** > **Profils/Modèles**.
4) Dans l'arborescence du menu, cliquez sur un numéro de profil d'abonné.

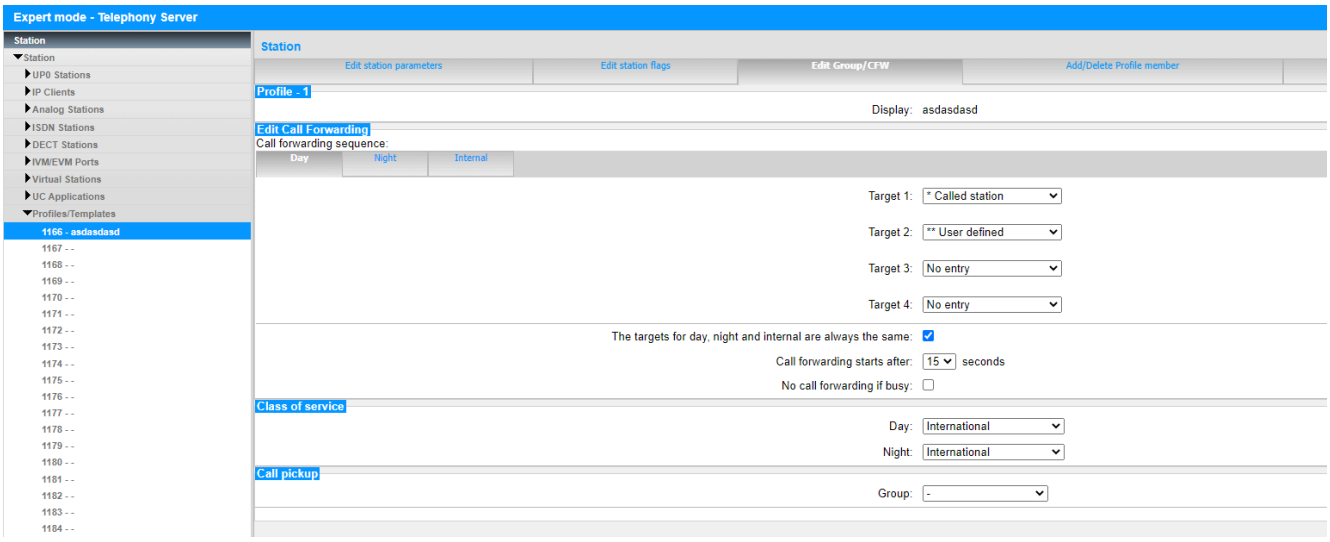


5) Dans le champ **Nom** de l'onglet **Paramètres de l'abonné**, modifiez si nécessaire le nom du profil d'abonné (16 caractères max.), puis cliquez sur **Appliquer**.

6) Dans l'onglet **Paramètres d'abonné** du profil d'abonné, modifiez si nécessaire les paramètres d'abonné souhaités, puis cliquez sur **Appliquer**.



7) Dans l'onglet **Drapeaux poste** du profil d'abonné, modifiez si nécessaire les drapeaux souhaités, puis cliquez sur **Appliquer**.



8) Dans l'onglet **Modifier les groupes de renvoi** du profil d'abonné, modifiez si nécessaire les renvois d'appels souhaités, puis cliquez sur **Appliquer**.

9) Cliquez sur **Appliquer**.

10.14.7 Comment exporter ou importer tous les profils d'abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés** > **Profils/Modèles**.
4) Cliquez sur le registre **Importer/Exporter tous les profils**.
5) Si vous voulez exporter tous les profils d'abonné dans un fichier, cliquez sur **Téléchargement** et enregistrez le fichier dans un répertoire de votre choix.
6) Pour importer tous les profils d'abonné à partir d'un fichier, cliquez sur **Parcourir**, allez à l'endroit où le fichier a été enregistré et chargez le fichier dans le système de communication.

10.15 Configuration des données d'authentification sur le téléphone SIP

Les données d'authentification d'un abonné SIP sur le système de communication doivent de plus être entrées directement sur le téléphone SIP. Pour cela, il faut utiliser les données qui sont inscrites pour chaque abonné SIP dans la WBM.

Les données suivantes doivent être reprises de la WBM et inscrites dans le téléphone SIP (séparément pour chaque téléphone SIP) :

- Mot de passe

  Mot de passe pour l'authentification.
- SIP ID utilisateur / Nom utilisateur

  Nom utilisateur pour l'authentification.
- Realm

  Zone ou Domaine pour l'authentification.

La configuration peut être réalisée par le WBM du téléphone SIP ou bien directement sur l'écran du téléphone SIP.

10.15.1 Comment configurer les données d'authentification avec la WBM du téléphone SIP

Conditions préalables

Le téléphone SIP est intégré au LAN.

PC Admin a accès au WBM du téléphone SIP.

Vous connaissez l'adresse IP du téléphone SIP.

La configuration est décrite à l'exemple de OpenStage 60 SIP.

Étape par étape

1) Sur le PC Admin, démarrez le navigateur Web et sélectionnez la page d'accueil du WBM du téléphone SIP, à l'adresse ci-après :

   `https://<adresse IP du téléphone SIP>`

   Remarque : S'il est impossible de démarrer la WBM, contrôlez la liaison LAN et répétez l'appel. S'il est toujours impossible de démarrer, vérifiez si l'adresse IP n'est pas bloquée par votre pare-feu. Vous trouverez des

informations plus précises dans la documentation de votre pare-feu.

2) Lorsque le navigateur web signale un problème avec un certificat de sécurité, installez le certificat (à l'exemple d'Internet Explorer V10).

a) Fermez le navigateur web.

b) Ouvrez le navigateur web avec droits d'administrateur : pour cela, cliquez avec le bouton droit de la souris sur l'icône du Navigateur web et sélectionnez dans le menu contextuel l'entrée **Exécuter en tant qu'administrateur**.

c) Autorisez la gestion des comptes utilisateur.

d) Sélectionnez la page d'accueil du WBM du téléphone SIP, à l'adresse ci-après :

```
https://<adresse IP du téléphone SIP>
```

e) Cliquez sur **Poursuivre le chargement de ce site Web**.

f) Cliquez sur le message **Erreur de certificat** dans la barre de navigation du navigateur Web.

g) Cliquez sur **Afficher les certificats**.

h) Cliquez sur **Installer le certificat** (visible uniquement avec des droits d'administrateur).

i) Sélectionnez l'option **Ordinateur local** et confirmez avec **Suivant**.

j) Sélectionnez l'option **Enregistrer tous les certificats dans la mémoire suivante**, cliquez sur **Parcourir** et indiquez des **entités de certification d'origine (Root CA) dignes de confiance**.

k) Confirmez avec **OK** et ensuite avec **Suivant** et **Terminer**.

l) Confirmez l'importation de certificat avec **OK** et fermez la fenêtre de certificat avec **OK**.

m) Fermez le navigateur web.

n) Démarrer de nouveau le navigateur Web (sans droits d'administrateur) et sélectionnez la page d'accueil du WBM du téléphone SIP, à l'adresse ci-après :

```
https://<adresse IP du téléphone SIP>
```

3) Lors de la première connexion, il est demandé d'entrer un mot de passe.

a) Dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**, entrez un nouveau mot de passe afin de protéger le système contre les utilisations malveillantes. Tenir compte des majuscules/minuscules et de l'état de la touche **Num**. Le mot de passe est masqué, le système affiche uniquement des étoiles (*).

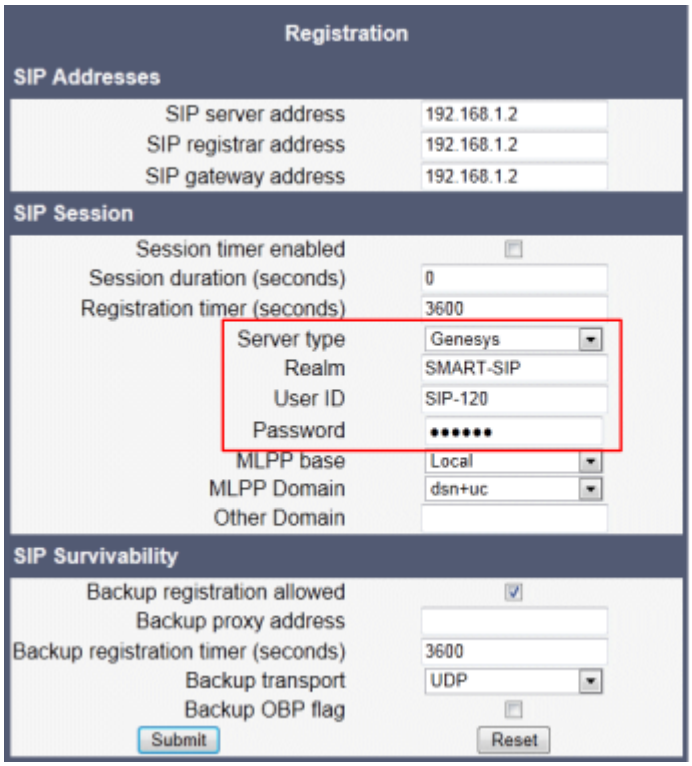
Remarque : Le mot de passe doit comprendre au moins 6 caractères et un chiffre. Mémorisez votre nouveau mot de passe.

4) Cliquez sur **OK**.

5) Cliquez sur l'onglet **Pages administrateur (Admin)**.

6) Entrez le mot de passe Administrateur (par défaut : 123456) et cliquez sur **Connexion**.

7) Allez à **System** > **Registration**.



8) Dans la zone **SIP Session**, liste déroulante **Server type**, sélectionnez l'entrée **Genesys**.

9) Dans le champ **Realm**, faire figurer l'entrée Realm que vous avez attribuée lors de la configuration de l'abonné SIP, dans la WBM du système de communication (par ex. `SMART-SIP`).

10) Dans le champ **User ID**, entrez l'ID utilisateur que vous avez défini dans la WBM du système de communication, lors de la configuration de l'abonnés SIP (par ex. `SIP-120`).

11) Dans le champ **Password**, entrez le mot de passe que vous avez indiqué dans la WBM du système de communication, lors de la configuration de l'abonné SIP.

12) Cliquez sur **Submit**. Les modifications sont enregistrées.

13) Déconnectez-vous du WBM à l'aide du bouton **Fermer la session**.

10.15.2 Comment configurer les données d'authentification sur l'écran du téléphone SIP

Conditions préalables

Vous connaissez les données d'authentification (ID utilisateur, mot de passe et Realm).

La configuration est décrite à l'exemple de OpenStage 80 SIP.

Étape par étape

1) Pour accéder au mode Administration du téléphone système appuyez sur la touche du téléphone correspondant au menu Paramètres / Applications.

2) Dans l'onglet `Paramètres` à `Admin` et confirmez avec la touche OK.
3) Entrez le mot de passe Administrateur (par défaut : `123456` et confirmez avec la touche OK.
4) Recherchez `System` (système) et confirmez avec la touche OK.
5) Recherchez `Registration` et confirmez avec la touche OK.
6) Recherchez `SIP session` (session SIP) et confirmez avec la touche OK.
7) Recherchez `Server type` (type de serveur) et confirmez avec la touche OK.
8) Recherchez `Genesys` (numéro du terminal) et confirmez avec la touche OK.
9) Recherchez `Realm`et confirmez avec la touche OK.
10) Entrez la valeur Realm que vous avez défini dans la WBM du système de communication, lors de la configuration des abonnés SIP (par ex. `SMART-SIP`). Confirmez avec l'icône OK.
11) Recherchez `User ID` (ID utilisateur) et confirmez avec la touche OK.
12) Entrez l'ID utilisateur que vous avez défini dans la WBM du système de communication, lors de la configuration des abonnés SIP (par ex. `SIP-120`). Confirmez avec l'icône OK.
13) Recherchez `Mot de passe` et confirmez avec la touche OK.
14) Entrez le mot de passe que vous avez indiqué dans la WBM du système de communication, lors de la configuration des abonnés SIP. Confirmez avec l'icône OK.
15) Confirmer la question de la sauvegarde des modifications en sélectionnant `Save` (enregistrer) et en confirmant avec la touche OK.
16) A l'aide de la touche Précédent, revenir au menu `Admin`.
17) Si, en raison des modifications, le téléphone système doit effectuer un redémarrage, il apparaît dans le menu `Admin` l'option de menu `Redémarrage`. Confirmez `Redémarrage` avec le touche OK puis `Oui` ainsi que la touche OK. Le téléphone système effectue un redémarrage et se connecte au système de communication.

10.16 Exporter les données d'abonné

Les données abonnés importantes peuvent être exportées dans un fichier XML.

En plus des données abonnés comme les noms et numéros d'appel des abonnés, les adresse e-mail et le type de téléphone, le fichier XML peut comporter d'autres données, par ex. les numéros des appels de groupe et les affectations de licence.

Vous pouvez traiter le fichier XML avec un tableur comme Microsoft Office Excel.

Vous trouverez un modèle avec des exemples de données et une description dans le fichier `csv-templates.zip` dans **Centre de service** > **Documents** > **Modèles CSV**.

10.16.1 Comment exporter les données d'abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Configuration**.
3) Dans l'arborescence du menu, cliquez sur **Configuration** > **Configuration du port**.
4) Cliquez sur le registre **Exporter la configuration**.
5) Cliquez sur le bouton **Téléchargement**.
6) Confirmez cette demande avec **OK**.
7) Cliquez sur **Sauvegarder** et sélectionnez l'emplacement de stockage du fichier XML.
8) Pour finir, cliquez sur **Enregistrer**.

11 UC Smart

UC Smart est intégré à tous les modèles commerciaux d'OpenScape et offre des fonctionnalités de communication unifiées telles que le statut de présence et les messages vocaux ainsi que la conférence, par exemple.

Clients pour UC Smart

Les fonctionnalités UC Smart peuvent être utilisées avec les clients suivants :

- myPortal au travail
- Lanceur d'applications
- Clients WSI tiers

Les limites de capacité (pour l'extension) dépendent du modèle OpenScape Business utilisé et des variantes OpenScape Business UC Booster éventuellement installées.

Aspects spécifiques de UC Smart avec OpenScape Business S

En raison de l'architecture du système, les restrictions suivantes s'appliquent à OpenScape Business S :

- Le nombre de messages vocaux n'est pas affiché sur l'écran du téléphone (MWI).
- La détection de fax, d'occupation ou d'inactivité n'est pas prise en charge pour la messagerie vocale (SmartVM). Les appels fax entrants ne peuvent pas être redirigés vers un périphérique fax par défaut après avoir été pris en charge par le SmartVM. Le SmartVM enregistre pendant 2 minutes.
- Lorsque le standard automatique de l'entreprise bascule les appels vers des abonnés occupés, l'appelant reçoit une tonalité d'occupation. Il n'est pas possible de laisser un message vocal.
- Si, lors de la consultation d'un message vocal, vous souhaitez être redirigé vers le numéro de téléphone enregistré dans le SmartVM (numéro de l'appelant), ce numéro doit être identique au numéro de téléphone de l'utilisateur configuré pour le SmartVM.
- Pour les connexions à la messagerie vocale (SmartVM), aucune licence de jonction n'est requise.
- Les canaux MEB sont occupés pour des annonces simultanées.
- Soixante canaux MEB sont disponibles pour les connexions vocales à la boîte vocale (SmartVM) ou au standard automatique.

Remarque : Après toute modification de la configuration des stations, des groupes, de la mobilité ou d'autres paramètres système tels que les codes d'accès aux lignes, les données UC pour UC Smart ou UC Suite doivent être synchronisées. La synchronisation a lieu cinq minutes après la dernière modification de la configuration. Si une modification de configuration ultérieure survient avant l'expiration du délai de 5 minutes, le minuteur est redémarré. Les données UC peuvent être obsolètes jusqu'au démarrage de la synchronisation.

Concepts associés

Fonctionnalités des communications unifiées (Présentation) à la page 64

11.1 Configuration de base pour UC Smart

Les paramètres de base pour UC Smart peuvent être adaptés.

UC Smart peut être activé ou désactivé. Si UC Smart est utilisé, UC Suite doit être désactivé.

Paramètres du mot de passe

L'administrateur doit définir pour tous les utilisateurs d'UC Smart un mot de passe initial et le communiquer à tous les utilisateurs. Le mot de passe d'origine peut être le même pour tous les utilisateurs ou il peut être différent pour chaque utilisateur. Le mot de passe initial doit être modifié par l'utilisateur lors de sa première connexion à un client UC Smart. Sans l'attribution d'un mot de passe initial, l'utilisateur ne peut pas se connecter à un client UC Smart.

Le nouveau mot de passe attribué par l'utilisateur devrait répondre aux directives strictes concernant le mot de passe.

Paramètres étendus pour Conférences gérées par l'application (facultatif)

Durant l'installation de base, l'administrateur doit, dans la WBM, paramétrer le **numéro fonctionnel pour conférence MeeetMe** (numéro de sélection MeetMe) et au moins un **numéro fonctionnel pour conférence** (salle de conférence).

Avec les systèmes OpenScape Business X, il faut affecter au numéro de sélection MeetMe une table d'acheminement dans laquelle la première entrée est vide et la seconde entrée correspond au numéro d'appel de la boîte vocale (SmartVM).

Avec les systèmes OpenScape Business S, il faut affecter au numéro de sélection MeetMe une table d'acheminement dans laquelle la première entrée correspond au numéro d'appel de la boîte vocale (faisceau Application Suite).

Enfin il faut affecter au numéro de sélection MeetMe une boîte de messagerie standard.

Vous trouverez ici la description de la configuration : Comment configurer les conférences gérées par une application,

Affectation de licence

L'administrateur doit attribuer à chaque utilisateur UC Smart une licence UC User.

En option, il est possible d'attribuer des licences supplémentaires pour :

- Messagerie vocale (utilisable aussi sans UC Smart)
- Conférence
- Application Launcher

11.1.1 Comment activer UC Smart

Conditions préalables

Vous êtes connecté au WBM avec le profil **Expert** .

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert** .
2) Dans l’arborescence de navigation, cliquez sur **Applications** > **Sélection de l’application**.
3) Cliquez sur **Package avec UC Smart**,
4) Cliquez sur **Appliquer** .

Étapes suivantes

Comment configurer UC Smart

11.1.2 Comment configurer UC Smart

Conditions préalables

Vous êtes connecté au WBM avec le profil **Avancé** .

Le **pack avec UC Smart** a été activé dans **la sélection d'applications** en mode expert.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration** .
2) Dans l’arborescence de navigation, cliquez sur **Assistants** > **UC Smart**.
3) Cliquez sur **Modifier** pour démarrer l'assistant **UC Smart** .
4) Dans l’arborescence du menu, cliquez sur **Administration** > **Paramètres de base**.
5) Sous **Activer / Désactiver UC Smart**, cochez la case **Actif**.
6) Attribuer le mot de passe initial sous la **politique de mot de passe** :
   a) Accédez au **Mot de passe UC Smart initial à l'échelle du système**, puis cliquez sur **Configurer**.
   b) Entrez le mot de passe initial pour tous les utilisateurs UC Smart dans le champ **Mot de passe initial UC Smart à l'échelle du système**.
   c) Cliquez sur **Appliquer** .
7) Spécifiez les politiques de mot de passe sous **Politique de mot de passe** :

   Remarque : Pour plus d'informations sur les politiques de mot de passe, cliquez sur l'icône **i**.

   - Si vous souhaitez appliquer une politique de mot de passe stricte pour les mots de passe utilisateur (recommandé), cochez la case **Forcer l'utilisateur à choisir un mot de passe sécurisé**.
   - Si vous ne souhaitez pas appliquer une politique de mot de passe stricte pour les mots de passe utilisateur (non recommandé), désactivez la case à cocher **Forcer l'utilisateur à choisir un mot de passe sécurisé**.
8) Spécifiez l'accès au système sous **Règles d'accès** :
   - Si vous souhaitez activer l'accès crypté des clients UC Smart au système, cochez la case **HTTPS**.
   - Si vous souhaitez activer l'accès non chiffré des clients UC Smart au système, cochez la case **HTTP**.

9) Cochez la case **Enregistrer les données de connexion pour les appareils** si les informations d'identification de connexion doivent être stockées dans le téléphone.
10) Cliquez sur **Appliquer** .

11.1.3 Comment configurer les conférences gérées par une application

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

En mode expert, dans **Sélection de l'application**, le **paquet avec UC Smart** est activé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez sur **Modifier** pour lancer l'Assistant **Installation de base**.
3) Sautez la fenêtre **Vue d'ensemble** avec **OK & Suite**. La fenêtre **Fonctions centrales pour les abonnés** s'affiche.
4) Cochez le champ **Modifier les numéros d'appel et les numéros fonctionnels préconfigurés**.
5) Cliquez sur **Exécuter la fonction**. La fenêtre **Modifier les numéros d'appel préconfigurés** s'affiche.
6) Si nécessaire, adaptez le **numéro fonctionnel pour conférence MeeetMe** à vos nécessités.
7) Attribuez au moins un **numéro fonctionnel pour conférence** pour la salle de conférence.
8) Pour finir, cliquez sur **OK**. Vous revenez à la fenêtre **Fonctions centrales pour les abonnés**.
9) Cliquez sur **OK&Suite**.
10) Quittez l'assistant en sautant toutes les fenêtres suivantes avec **OK&Suite**.
11) Cliquez dans la barre de navigation sur **Mode Expert**.
12) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
13) Dans l'arborescence du menu, cliquez sur **Appels entrants** > **Renvois temporisés**.
14) Cliquez sur l'onglet **Table d'acheminement - Définition**.
15) Pour OpenScape Business X, définissez la table d'acheminement pour numéro de sélection MeetMe de la manière suivante.
    a) Dans la **Table d'acheminement**, sélectionnez une table d'acheminement libre, par ex. `500`.
    b) Sélectionnez comme première destination **Pas d'entrée** et comme deuxième destination le numéro d'appel de la boîte vocale (par ex. `351 VOICEMAIL Groupe`).

16) Pour OpenScape Business S, vous devez définir la table d'acheminement pour le numéro de sélection MeetMe comme indiqué ci-après.
    a) Dans la **Table d'acheminement**, sélectionnez une table d'acheminement libre, par ex. `500`.
    b) Sélectionner Destination externe comme première destination (route : Suite Application) et entrer le numéro d'appel de la boîte vocale dans le champ "Destination externe".
17) Cliquez sur **Appliquer** puis sur **OK**.
18) Fermez la fenêtre.
19) Cliquez dans la barre de navigation sur **Mode Expert**.
20) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Connexion**.
21) Dans l'arborescence du menu, cliquez sur **Connexions** > **SmartVM**.
22) Cliquez sur l'onglet **Modifier boîtes de messageries SmartVM**.
23) Dans la colonne **N° boîte vocale** , indiquez dans un champ libre le numéro de sélection MeetMe auquel la boîte vocale doit être ajoutée.
24) Cliquez sur **Appliquer** puis sur **OK**.

11.1.4 Comment déterminer les adresses IP des composants du système

Conditions préalables

Vous êtes connecté au WBM avec le profil **Expert** .

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert** .
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **Sélection de l'application**.

   Sous **Sélection de l'application**, les adresses IP de différentes composantes du système sont indiquées, par ex. celles de **UC Smart**, d'**Application Launcher**, de **CSTA-Connector**, d'**Open Directory Service** et d'**UC Suite**.

Concepts associés

Configuration de base pour UC Suite à la page 488

11.1.5 Comment déterminer l'état de UC Smart

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

En mode expert, dans **Sélection de l'application**, le **paquet avec UC Smart** est activé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence du menu, cliquez sur **Assistants** > **UC Smart**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **UC Smart**.

4) Dans l'arborescence du menu, cliquez sur **Administration** > **Etat**.

   Dans **Serveur d'application** il est présenté les informations d'état pour UC Smart, par ex. **Etat**, **Version**, **Installation téléphonique**, **Base de données**, **EVM**, **Points de surveillance manquants**, **Utilisateurs actifs**, **Connexions actives**, **Connexions HTTPS actives**, **Utilisateur Mobility Entry**, **Utilisateur sans terminal** et **Utilisateurs verrouillés**.

11.2 Clients intelligents UC

Les clients UC Smart offrent aux abonnés des interfaces utilisateur conviviales pour les communications unifiées.

Le système propose les clients UC Smart suivants pour les appareils suivants :

Type de client	Client	Appareil
Client de communications	myPortal au travail	PC
Client mobile	Mitel WX (voir Mobilité à la page 888)	Smartphone, tablette PC
Client de communication	Téléphone de bureau OpenScape CP 400/600/600E/700/700X/710 HFA (logiciel client intégré au téléphone)	Téléphone de bureau OpenScape CP 400/600/600E/700/700X/710 HFA

11.2.1 myPortal @work

myPortal @work est une application Unified Communications (Microsoft Windows et Mac OS X), qui combine toutes les fonctions et tous les services nécessaires, comme la composition pratique depuis les répertoires téléphoniques, les favoris, les conversations et les informations sur l'état Présence des collègues, en une solution unique pour accélérer la communication quotidienne, améliorer le travail d'équipe et entrer rapidement en contact avec les collègues, les clients et les partenaires.

myPortal @work peut être utilisé en mode UC Smart ou UC Suite. Les fonctionnalités offertes dans l'interface utilisateur dépendent du mode. Vous ne pouvez pas modifier le mode de fonctionnement, qui dépend de l'administrateur système. En cas de doute sur le mode de fonctionnement actuel du client myPortal @work, demandez de plus amples détails à votre administrateur système.

myPortal @work offre un client de téléphonie voix sur IP (VoIP) intégré. Si l'option VoIP est activée, les fonctionnalités du client myPortal @work associées aux appels vocaux utilisent la fonctionnalité VoIP.

Remarque : Pour utiliser la fonctionnalité Voix sur IP (VoIP), l'utilisateur doit être configuré en tant que client système.

Pour utiliser la fonctionnalité Voix sur IP (VoIP) à distance avec Device@Home, consultez 1 Configuration de System Device@Home

La fonctionnalité VoIP prend en charge un jeu de fonctionnalités en plus des fonctionnalités UC :

- Faire un appel
- Répondre à un appel
- Mettre fin à un appel
- Consultation
- Transférer après avoir répondu
- Transfert aveugle
- Transférer
- Transférer vers la messagerie vocale
- Rappel automatique (l'affichage d'une notification de rappel n'est pas encore pris en charge)
- Va-et-vient
- Silencieux/Réactiver le son (uniquement pour la fonctionnalité VoIP)
- Conférence de système
- Rejet des appels en instance
- En attente
- Ne pas déranger (DND)
- DTMF
- Interception d'appel

Remarque : Étant donné que le client myPortal @work ne prend pas en charge la capacité d'envoyer des tonalités DTMF à un autre abonné, l'envoi d'une tonalité DTMF via la commande CSTA "generateDigits" n'est pas non plus pris en charge et une telle demande sera refusée et rejetée par le système.

Travailler en équipe :

Le client VoIP de myPortal @work peut également être utilisé :

- En groupe (p. ex. linéaire, appel en instance)
- MULAP en tant que membre MULAP

Le cryptage de la signalisation et de la charge utile (SPE) est également pris en charge pour le système de communication. Le client VoIP utilise une pile de sécurité WebRTC moderne et bénéficie par conséquent de transferts de données sécurisés via DTLS.

Remarque : La configuration ITSP SDES est également prise en charge.

Des codes de service peuvent être initiés depuis la barre de recherche, mais ils ne sont pas pris en charge en cas de problème. Aucun retour n'est fourni sur la réussite ou l'échec des codes de service et il est par conséquent fortement conseillé d'utiliser les options de l'interface utilisateur de myPortal @work pour contrôler les différentes fonctionnalités.

myPortal @work en mode UC Suite peut être utilisé non seulement de manière autonome, mais aussi en combinaison avec les clients myPortal for Desktop/ Outlook, myAgent, myAttendant (CTI, Favoris et Conversations). Les licences utilisateur UC peuvent également être utilisées avec myPortal @work.

La description suivante fait essentiellement référence à myPortal @work en mode UC Smart. Les différences du mode UC Suite sont précisées dans le guide de l'utilisateur de myPortal @work.

myPortal @work prend généralement en charge les fonctionnalités suivantes :

- État de présence
- Renvoi d'appel en fonction de l'état
- Répertoires avec recherche par nom
- Favoris
- Conversations : jusqu'à 25 conversations sont affichées dans le client et chaque conversation peut contenir jusqu'à 50 entrées
- Conférences
- Touches de raccourci de numérotation / de recherche / hyperliens téléphoniques
- Fonctions d'appel via :
  1) Le téléphone associé
  2) Le client de téléphonie voix sur IP intégré
- Les commandes de la messagerie vocale
- Zoom avant / Zoom arrière

Utilisation de myPortal @work dans un environnement Microsoft Terminal Server

myPortal @work est validé pour les fonctionnalités UC et CTI au sein d'environnements Microsoft Terminal Server avec les limites suivantes :

- Les Hyperliens téléphoniques et la fonction Cliquer pour composer ne sont pas pris en charge
- La fonction Lancer l'application au démarrage n'est pas prise en charge
- Le chargement d'une image de l'utilisateur n'est pas pris en charge
- La fonctionnalité Attache/détachement, Épingler/détacher et Réduire en barre d'état est limitée
- La fonctionnalité VoIP n'est pas prise en charge

11.2.1.1 Prérequis pour myPortal @work

Pour utiliser le client UC, le PC client doit être équipé de la configuration matérielle et logicielle appropriée. Selon la configuration, des droits d'administrateur sont nécessaires pour l'installation et les mises à jour automatiques. Les fonctionnalités disponibles dépendent des licences utilisées.

Les prérequis suivants sont nécessaires pour l'installation de myPortal @work :

- droits d'administrateur
- Programme d'installation du logiciel myPortal @work
- Adresses IP et ports du système de communication
- Nom de domaine complet (FQDN) ou adresse IP, port pour la connectivité WAN (device@home)

- Données de connexion (nom d'utilisateur et mot de passe) pour votre compte utilisateur UC dans le système de communication
- Informations du compte de messagerie vocale (facultatif)
- Numéro d'appel MULAP en cas d'attribution de plusieurs numéros (facultatif)
- Systèmes d'exploitation Windows et Apple Mac OS X

Remarque : Assurez-vous que TLS 1.2 est activé dans les options Internet (dans le panneau de configuration) et que les derniers correctifs de Microsoft sont installés ou activés manuellement.

Si les actions ci-dessus ne sont pas effectuées, l'accès HTTPS sera refusé.

Téléphones

myPortal @work peut être utilisé en combinaison avec les téléphones suivants :

Remarque : myPortal @work peut également être utilisé de manière autonome, grâce à sa fonctionnalité VoIP, sans nécessiter d'appareil physique.

- OpenStage HFA
- Téléphone de bureau OpenScape IP 35G/55G HFA
- Téléphone de bureau OpenScape IP 35G Eco HFA
- Téléphone de bureau OpenScape CP 100/200/205/400/600/600E/700/700X HFA
- Téléphone de bureau OpenScape CP 110/210/410/710 HFA
- Téléphones analogiques
- Téléphones ISDN
- OpenScape Édition Personnelle HFA

Les appareils plus anciens (tels que optiPoint 410/420/500 et Gigaset M2/SL3/S4/SL4/S5) sont pris en charge. Les appareils Optiset E ne peuvent pas être utilisés. Pour plus de détails sur les appareils testés et mis sur le marché, veuillez consulter l'avis de mise sur le marché.

Remarque : Le client intégré OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA ne nécessite aucune condition particulière, outre la configuration client standard et la licence.

La section « Favoris » du menu du téléphone contient les touches programmables gratuites et n'a aucun lien avec les favoris UC. Vous trouverez des informations détaillées sur ces touches et leur utilisation dans la documentation de l'appareil.

Remarque : Pour les téléphones analogiques et DECT, l'indication de message en attente (MWI) n'est pas prise en charge, et seule une prise en charge limitée est disponible pour l'affichage des informations sur le téléphone.

Navigateurs Web

Les navigateurs Web suivants ont été publiés pour la programmation des touches téléphoniques via le client UC :

- Microsoft Internet Explorer version 10 (ou ultérieure)
- Mozilla Firefox version 19 (ou ultérieure)
- Google Chrome

Fichiers d'installation

L'administrateur peut télécharger les fichiers d'installation depuis le **logiciel** > **Service Center** et les mettre à la disposition des utilisateurs via un lecteur réseau, par exemple.

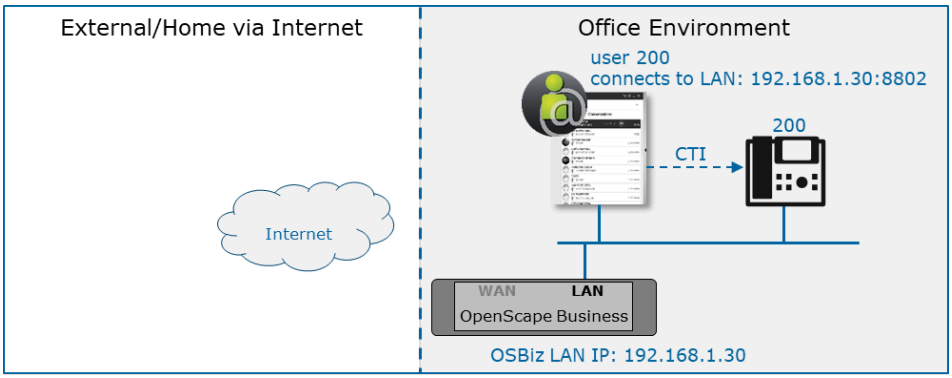
11.2.1.2 Configuration des utilisateurs myPortal @work

myPortal @work combine un client UC et un client VoIP. Ces deux fonctionnalités nécessitent les configurations/licences suivantes selon les modes UC (Smart/UC Suite) et les cas d'utilisation.

Remarque : Si un compte utilisateur myPortal @work est bloqué après plusieurs tentatives de connexion infructueuses en mode UC Suite, il n'apparaît pas dans le répertoire utilisateur de UC Suite. Vous pouvez afficher les utilisateurs bloqués de myPortal @work sous **Mode Expert > Services Web > Web Services Assistant > Gestion des utilisateurs**. Vous pouvez également débloquer ces comptes sous **Mode Expert > OpenScape Business UC Suite > Répertoire utilisateur**.

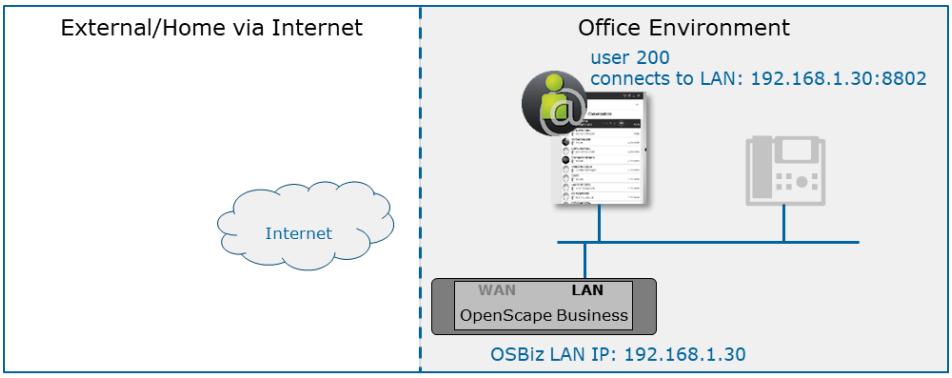
Configuration LAN locale - Client UC et CTI uniquement

myPortal @work est utilisé comme client UC et CTI pour un téléphone de bureau associé sans VoIP.



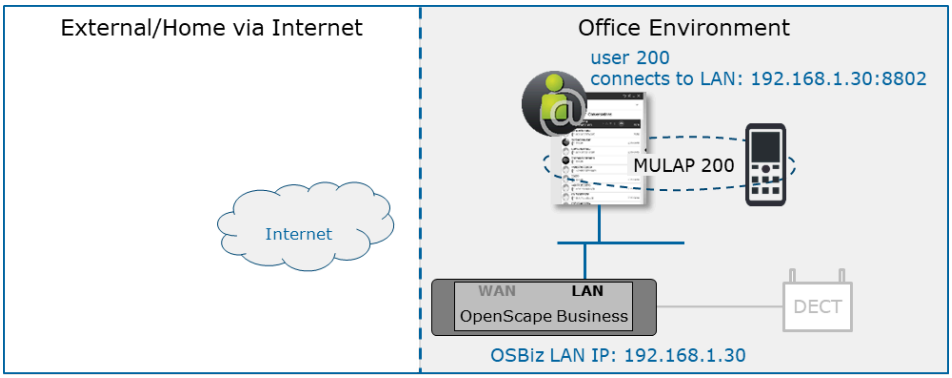
- Licences : Utilisateur UC ou Utilisateur Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez votre nom d'utilisateur/mot de passe / Adresse IP LAN : 8802

Configuration LAN locale - Client UC et VoIP



- Licences : Licence Utilisateur IP et Utilisateur UC ou Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez votre nom d'utilisateur/mot de passe / Adresse IP LAN : 8802
- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP > Activer VoIP
- Aucune connectivité STUN n'est requise au niveau du client pour les connexions internes pures. Elle est toutefois nécessaire dans certains scénarios hybrides où d'autres utilisateurs utilisent le VoIP myPortal @work via un réseau public. Pour vérifier la connectivité STUN, accédez à Paramètres > VoIP > Paramètres ICE avancés > Vérifier l'état ICE.

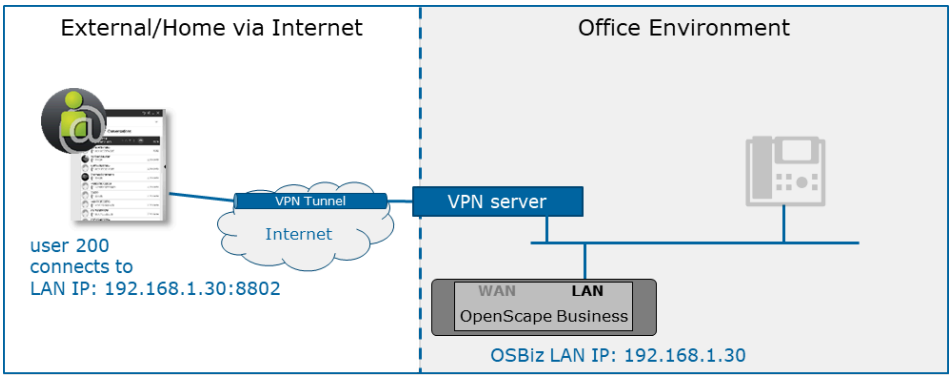
Configuration des utilisateurs MULAP (LAN local)



- Licences :
  - myPortal @work : Licence Utilisateur IP et Utilisateur UC ou Groupware
  - Autre équipement MULAP - dans cet exemple, DECT : Licence Utilisateur TDM ou Utilisateur IP (la configuration MULAP est recommandée en cas d'association avec des équipements TDM ou DECT, mais peut aussi être utilisée avec un équipement IP. Dans le cas d'un équipement IP, voir également les rubriques Utilisateur Deskshare connecté via un LAN local à la page 453 et Utilisateur Deskshare distant connecté via VPN à la page 454).
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez le nom d'utilisateur/mot de passe pour le numéro MULAP / Adresse IP LAN : 8802
- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP, choisissez l'équipement contrôlé et activez VoIP.
- Aucune connectivité STUN n'est requise au niveau du client pour les connexions internes pures. Elle est toutefois nécessaire dans certains

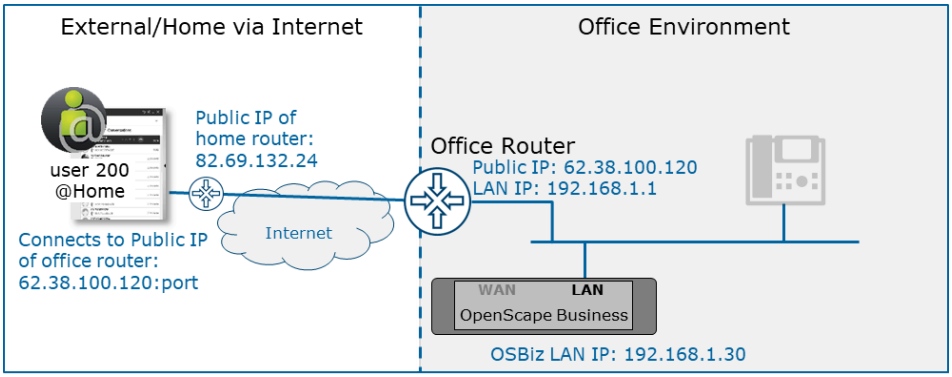
scénarios hybrides où d'autres utilisateurs utilisent le VoIP myPortal @work via un réseau public. Pour vérifier la connectivité STUN, accédez à **Paramètres > VoIP > Paramètres ICE avancés > Vérifier l'état ICE**.

Utilisateur à domicile avec une connexion VPN



- Licences : Licence Utilisateur IP et Utilisateur UC ou Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez votre nom d'utilisateur/mot de passe / Adresse IP LAN : 8802
- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP > Activer VoIP
- La connexion STUN est obligatoire. Pour vérifier la connectivité STUN, accédez à Paramètres > VoIP > Paramètres ICE avancés > Vérifier l'état ICE.

myPortal @work via un réseau public

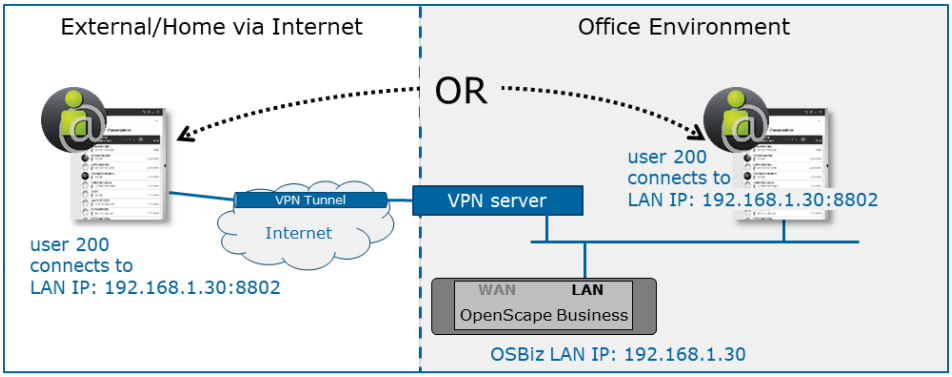


- Licences : Licence Utilisateur IP et Utilisateur UC ou Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez votre nom d'utilisateur/mot de passe / Adresse IP publique : port configuré par l'administrateur.
- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP > Activer VoIP
- Préparez l'environnement réseau comme décrit dans le chapitre Étapes de configuration pour utiliser myPortal @work via Internet à la page 456
- L'indicateur SBC n'est pas requis pour myPortal @work. Il n'est nécessaire que si vous utilisez un équipement matériel.
- N'utilisez pas l'interface WAN OSBiz pour vous connecter à Internet lorsque vous utilisez myPortal @work via l'adresse IP publique. Si c'est le cas, l'instance SBC interne détectera l'adresse IP publique de l'interface WAN

et l'utilisera pour établir la communication entre le client et OSBiz, ce qui entraînera des problèmes de charge utile. Proposition de configuration : Établissez la connexion à l'ITSP via l'interface LAN. Pour cela, vous pouvez utiliser le routeur FAI normal ou un second routeur et des itinéraires statiques.

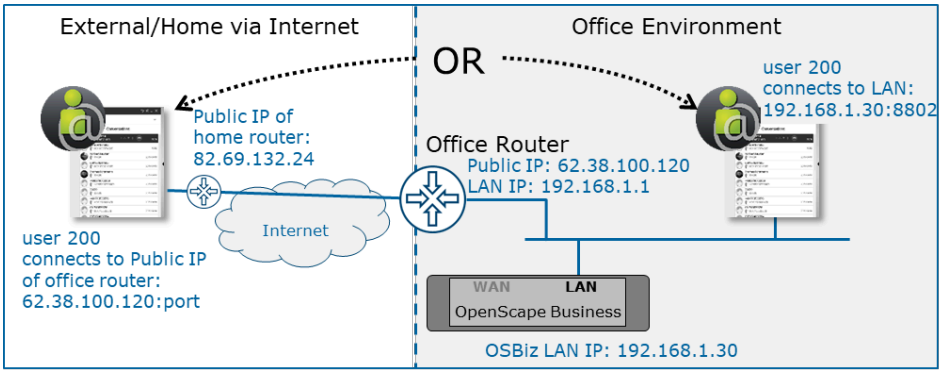
- La connectivité STUN est obligatoire. Pour vérifier la connectivité STUN, accédez à Paramètres > VoIP > Paramètres ICE avancés > Vérifier l'état ICE.

Utilisateur à domicile avec une configuration VPN et LAN local (par ex., alternance entre le bureau et le domicile)



- Licences : Licence Utilisateur IP et Utilisateur UC ou Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez votre nom d'utilisateur/mot de passe / Adresse IP LAN : 8802
- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP > Activer VoIP
- myPortal @work peut être utilisé dans les deux environnements sans modifier les paramètres.
- La connectivité STUN est obligatoire. Pour vérifier la connectivité STUN, accédez à Paramètres > VoIP > Paramètres ICE avancés > Vérifier l'état ICE.

myPortal @work avec une configuration de réseau public et LAN local (par ex., alternance entre le bureau et le domicile)



- Licences : Licence Utilisateur IP et Utilisateur UC ou Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez votre nom d'utilisateur/mot de passe / Adresse IP LAN : 8802 et Adresse IP publique : port configuré par l'administrateur. Si vous configurez les

deux adresses, il n'est pas nécessaire d'utiliser un second profil lors de l'alternance entre le bureau et le domicile.

- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP > Activer VoIP
- Préparez l'environnement réseau comme décrit dans le chapitre Étapes de configuration pour utiliser myPortal @work via Internet à la page 456
- L'indicateur SBC n'est pas requis pour myPortal @work. Il n'est nécessaire que si vous utilisez un équipement matériel.

Pour l'enregistrement VoIP

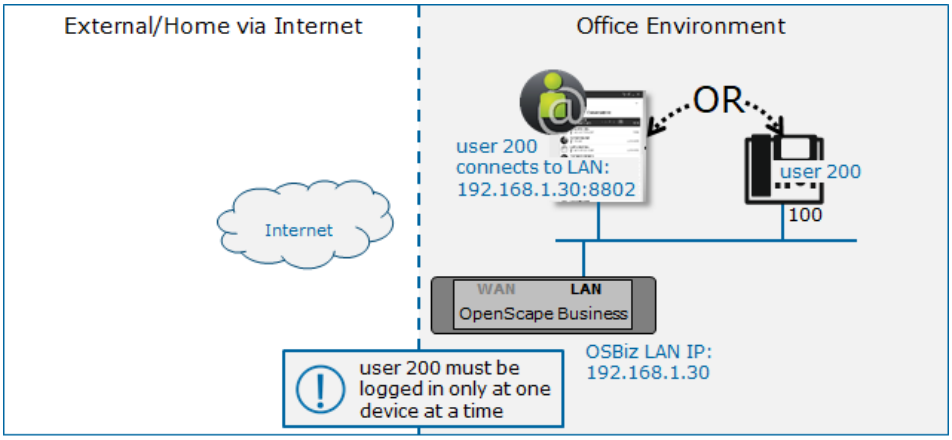
Lorsque l'utilisateur alterne entre le bureau et son domicile, il ne doit avoir qu'une seule connexion VoIP sur les deux sites.

Pour UC

Lorsque l'utilisateur souhaite se connecter en même temps dans UC à plusieurs endroits :

- Mode UC Smart Le client UC peut être connecté en même temps depuis le domicile et depuis le bureau, mais un seul client VoIP est pris en charge dans ce scénario et l'enregistrement VoIP ne doit pas être activé pour l'autre client.
- Mode UC Suite : Reportez-vous au paragraphe « Association de myPortal @work avec d'autres clients UC Suite et configuration de licence ». Seul un client myPortal @work est autorisé.

Utilisateur Deskshare connecté via un LAN local



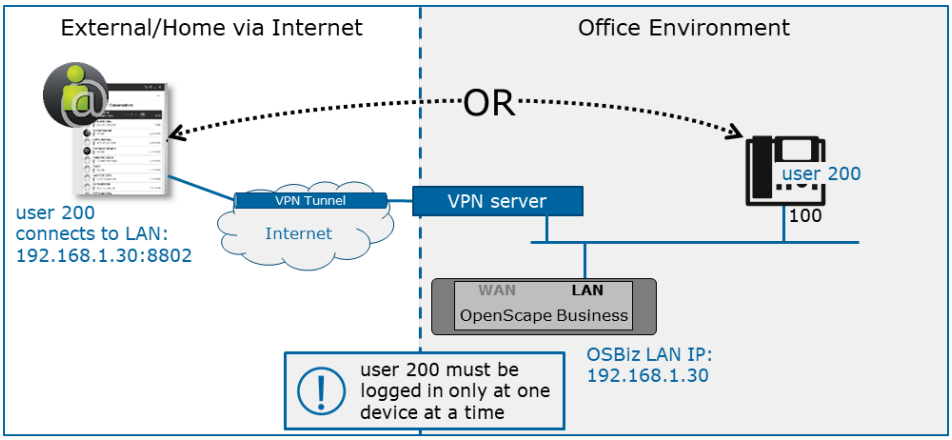
- Licences : Licence Deskshare et Utilisateur UC ou Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez le nom d'utilisateur/mot de passe pour l'extension Deskshare / Adresse IP LAN : 8802
- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP > Activer VoIP

Exemple: L'équipement utilise le numéro fictif « 100 » Connectez-vous au numéro « 100 » avec votre téléphone de bureau en mode Deskshare avec par exemple le numéro 200 en utilisant le code de service *9419.

Pour utiliser myPortal @work avec l'utilisateur 200, le téléphone de bureau est automatiquement déconnecté et reconnecté au nombre fictif 100. Lorsque vous reprenez le téléphone de bureau, assurez-vous que myPortal @work n'est pas enregistré (l'utilisateur # doit quitter l'application ou se déconnecter).

Utilisateur Deskshare distant connecté via VPN

La même configuration que celle décrite dans le chapitre Utilisateur Deskshare connecté via un LAN local à la page 453 est également prise en charge pour un utilisateur à domicile connecté via VPN.



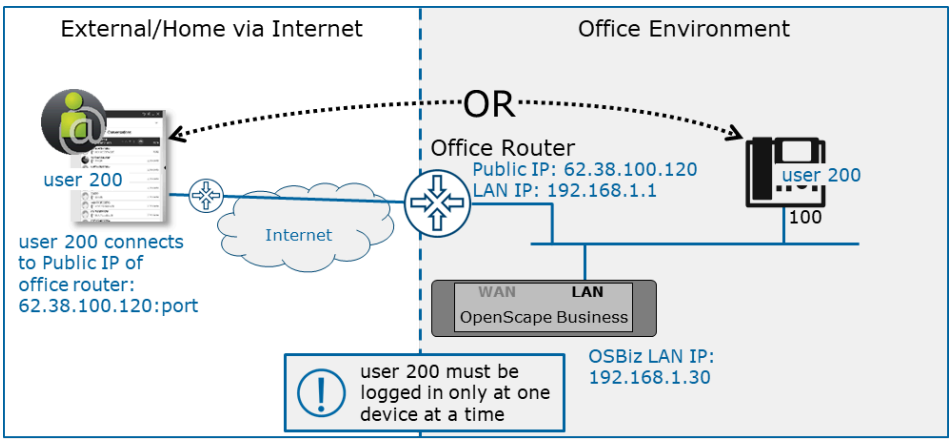
- Licences : Licence Deskshare et Utilisateur UC ou Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez le nom d'utilisateur/mot de passe pour l'extension Deskshare / Adresse IP LAN : 8802
- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP > Activer VoIP

Exemple: L'équipement utilise le numéro fictif « 100 » Connectez-vous au numéro « 100 » avec votre téléphone de bureau en mode Deskshare avec par exemple le numéro 200 en utilisant le code de service *9419.

Pour utiliser myPortal @work avec l'utilisateur 200, le téléphone de bureau est automatiquement déconnecté et reconnecté au nombre fictif 100. Lorsque vous reprenez le téléphone de bureau, assurez-vous que myPortal @work n'est pas enregistré (l'utilisateur # doit quitter l'application ou se déconnecter).

Utilisateur Deskshare distant connecté via un réseau public

La même configuration que celle décrite dans le chapitre Utilisateur Deskshare connecté via un LAN local à la page 453 est techniquement possible pour un utilisateur à domicile connecté via un réseau public. Toutefois, cette configuration n'a pas encore été entièrement testée et est donc décrite comme provisoire dans cette version du document.



- Licences : Licence Deskshare et Utilisateur UC ou Groupware
- Connexion à myPortal @work : sur l'écran de connexion, spécifiez le nom d'utilisateur/mot de passe pour l'extension Deskshare / Adresse IP LAN : 8802
- Enregistrement VoIP dans myPortal @work : Une fois connecté, accédez à Paramètres > VoIP > Activer VoIP

Exemple: L'équipement utilise le numéro fictif « 100 » Connectez-vous au numéro « 100 » avec votre téléphone de bureau en mode Deskshare avec par exemple le numéro 200 en utilisant le code de service *9419.

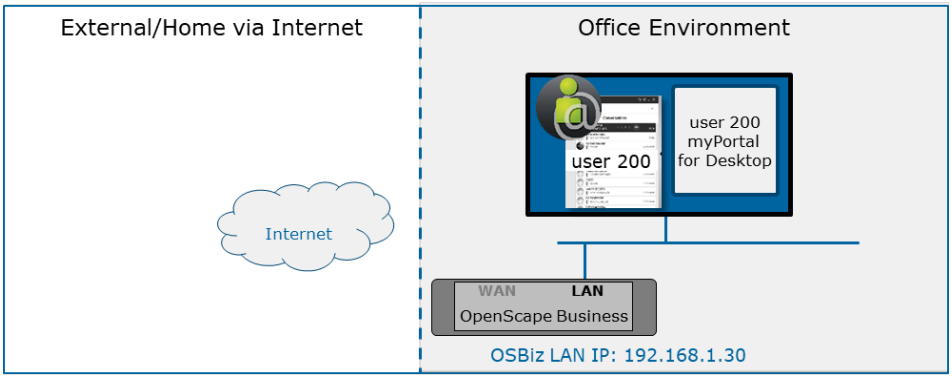
Pour utiliser myPortal @work avec l'utilisateur 200, le téléphone de bureau est automatiquement déconnecté et reconnecté au nombre fictif 100. Lorsque vous reprenez le téléphone de bureau, assurez-vous que myPortal @work n'est pas enregistré (l'utilisateur # doit quitter l'application ou se déconnecter).

Association de myPortal @work avec d'autres clients UC Suite et configuration de licence

Remarque : Les configurations décrites dans ce chapitre sont également prises en charge pour un utilisateur à domicile connecté via VPN.

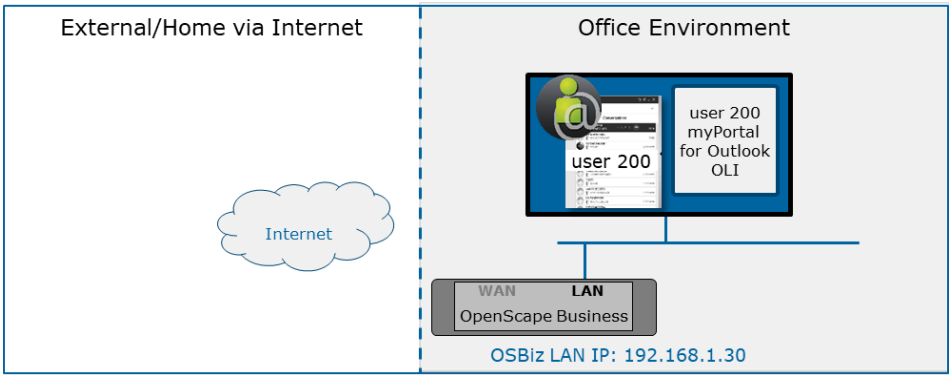
Licence Utilisateur UC

Le même utilisateur peut être connecté en parallèle avec myPortal @work et myPortal for Desktop.



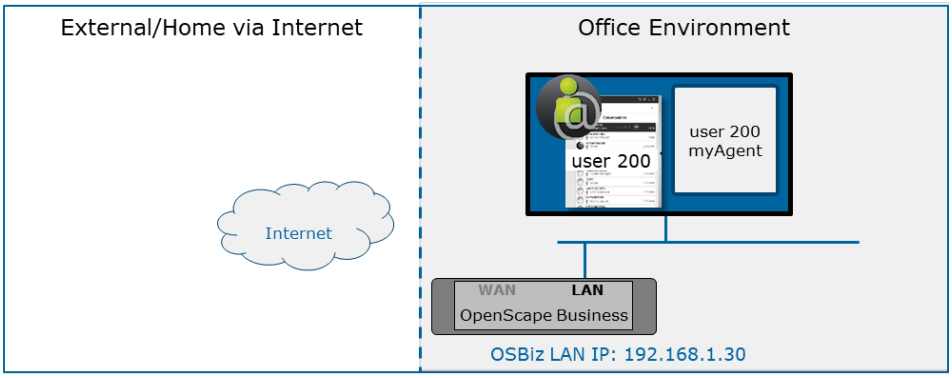
Licence Groupware

Le même utilisateur peut être connecté en parallèle avec myPortal @work et OLI.



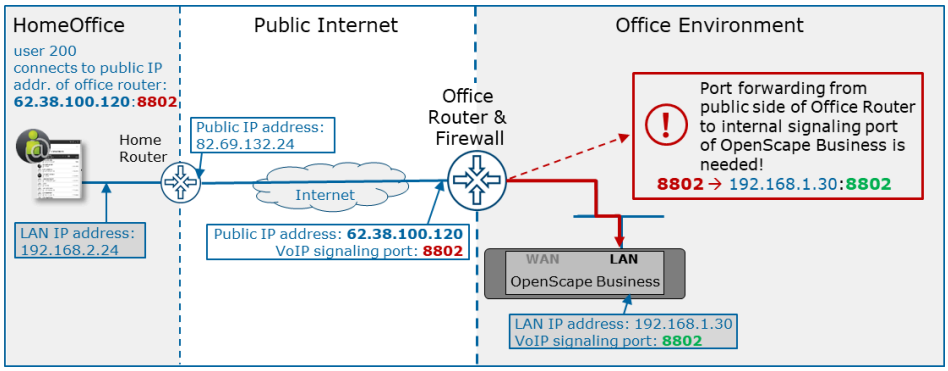
Combinaison de licences IP, Utilisateur UC et myAgent

myAgent et le client VoIP myPortal @work peuvent être utilisés en parallèle comme softphones.



11.2.1.3 Étapes de configuration pour utiliser myPortal @work via Internet

Pour utiliser myPortal @work à partir d'Internet, OpenScape Business doit également être accessible via Internet. Tous les exemples de ce chapitre reposent sur le scénario de mise en réseau de base suivant.



Description du scénario de mise en réseau

OpenScape Business se trouve au sein de l'environnement de bureau qui est connecté à Internet via le routeur de bureau. Ce routeur est accessible depuis Internet via l'adresse IP publique « 62.38.100.120 » ou via un nom DNS.

Le client myPortal @work est connecté au LAN au sein d'un réseau domestique ou externe qui est connecté à Internet via un routeur distinct. Le routeur externe est accessible depuis Internet via l'adresse IP publique « 82.69.132.24 ».

Étapes de configuration

Pour utiliser le client myPortal @work dans OpenScape Business via Internet, il est nécessaire de configurer les composants suivants de manière appropriée.

OpenScape Business au sein du bureau

Activez la prise en charge STUN sur le système si ce n'est déjà fait pour un ITSP.

Configurez l'utilisateur myPortal @work (l'indicateur SBC n'est pas nécessaire pour la VoIP).

Routeur de bureau

Comme le client myPortal @work doit se connecter à OpenScape Business depuis Internet et inversement, la configuration suivante doit être effectuée sur le routeur de bureau pour permettre cela :

- Renvoi de port HTTPS du port externe (par défaut 8802) vers le port interne 8802 du système.
  - Port externe (par défaut 8802) -> Routeur de bureau -> 192.168.1.30:8802

Pour en savoir plus, voir également le chapitre Paramètres des ports et du pare-feu à la page 457

myPortal @work/routeur externe

Le client myPortal @work doit se connecter à l'adresse IP publique ou au DNS du routeur Internet de bureau sur le port externe (par défaut 8802). En raison du renvoi de port configuré précédemment, la liaison est établie avec l'instance OpenScape Business du réseau de bureau.

Dans la plupart des cas, aucun autre paramètre ne doit être configuré sur le routeur externe, mais en cas de problème, reportez-vous au chapitre Paramètres des ports et du pare-feu à la page 457.

11.2.1.4 Autres conseils de configuration & Paramètres

Paramètres du serveur STUN

Pour plus d'informations sur la configuration du serveur STUN, reportez-vous au chapitre « Configuration STUN » du guide « Configuration du système device@home » et au guide de l'utilisateur OpenScape Business V3, myPortal @work, section « Comment ajouter un serveur STUN ».

Casque

Chaque équipement sonore/microphone détecté dans le système d'exploitation peut être utilisé.

Intégration de casque Jabra/Plantronics

En cas de problème lors de l'intégration d'un casque Jabra, exécutez l'application avec des droits d'administrateur.

Pour pouvoir utiliser l'intégration de casque Jabra, l'équipement Jabra doit être configuré comme équipement microphone principal dans myPortal @work.

Pour l'intégration de casque Plantronics, le hub Plantronics doit être installé.

Paramètres des ports et du pare-feu

Généralement, les ports suivants doivent être configurés pour la signalisation myPortal @work :

- Fonctionnalités UC & signalisation WebRTC / VoIP : 8802
- Port de serveur STUN par défaut : 3478. Si un serveur STUN personnalisé est configuré, un port différent peut être requis.

La configuration des ports pour la charge utile WebRTC/VoIP dépend du type de pare-feu utilisé dans l'environnement client. Pour pouvoir exécuter

myPortal @work dans un environnement réseau client, il est essentiel de connaître le type de pare-feu utilisé, à savoir avec état ou sans état, et de configurer les paramètres du pare-feu avec l'administrateur IT compétent.

Pour mieux comprendre les différences entre les deux types de pare-feu, veuillez lire ce qui suit :

- Les pare-feu sans état sont conçus pour protéger les réseaux à l'aide d'informations statiques comme la source et la destination.
- Un pare-feu avec état surveille l'état complet des connexions réseau actives. Cela signifie que les pare-feu avec état analysent en permanence le contexte intégral des paquets de données et du trafic.

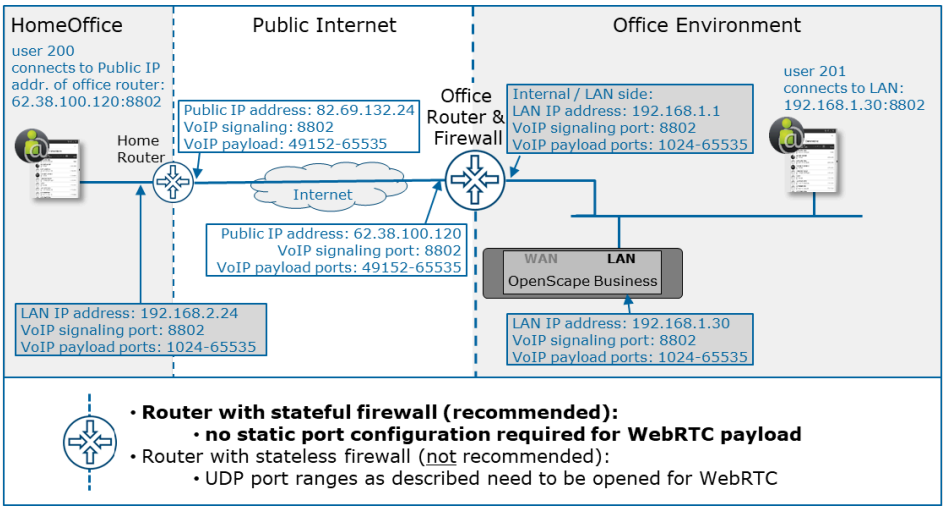
Pour plus d'informations sur ces types de pare-feu, consultez les ressources disponibles sur Internet ou toute autre documentation technique pertinente.

On suppose qu'un dispositif de pare-feu/NAT avec état va être utilisé pour mieux protéger les réseaux privés des clients, ce qui signifie que ce dispositif doit autoriser les connexions internes sortantes vers leur destination.

Le pare-feu/l'équipement NAT bloquera tous les paquets entrants, sauf s'ils appartiennent à une session déjà établie comme sortante (sur un port éphémère ou dynamique).

En ce qui concerne l'utilisation des ports, aucun paramètre ne doit être configuré dans le pare-feu/l'équipement NAT, car tout est géré et négocié automatiquement dans le cadre d'un pare-feu avec état.

L'utilisation d'un pare-feu avec état est la procédure recommandée et la plus sécurisée pour exécuter des solutions VoIP basées sur WebRTC.



Dans le cadre d'un pare-feu sans état (qui n'est pas recommandé pour la VoIP), la plage de ports sources UDP suivante doit être ouverte pour le trafic de charge utile interne des équipements connectés au réseau client : 1024-65535.

Pour tous les trafics de charge utile acheminés via Internet, la technologie WebRTC utilise des ports de la plage UDP 49152-65535. Pour en savoir plus, reportez-vous à la documentation technique correspondante.

Chaque équipement réseau se trouvant sur le chemin reliant les terminaux de charge utile concernés doit être configuré en conséquence (par ex., routeur, pare-feu, NAT, proxy, etc.).

En raison de la vaste plage de ports qui doit être ouverte, il n'est pas recommandé d'utiliser un pare-feu sans état pour la VoIP.

Tableau 4 :

	Pare-feu avec état	Pare-feu sans état à ouvrir de manière statique
Port de signalisation WebRTC/VoIP	8802	8802
Charge utile WebRTC/ VoIP Plage de ports UDP au sein du LAN local, c'est-à-dire au sein de l'environnement client	dynamique[2]	1024-65535
Charge utile WebRTC/ VoIP Plage de ports UDP utilisée sur l'Internet public	dynamique[2]	49152-65535

Restrictions relatives à la VoIP

- Dans les scénarios avec plusieurs appels (transfert, conférence, avertissement, etc.), nous recommandons de désactiver l'intégration de casque en cas d'erreur. En désactivant l'indicateur d'intégration de casque dans myPortal @work, vous désactiverez uniquement les commandes d'appel du casque. Celui-ci pourra toujours être utilisé comme équipement audio.
- La fonctionnalité de connexion gratuite de myAgent (où l'agent peut sélectionner le téléphone à utiliser dans un menu déroulant lors de la connexion), c'est-à-dire la sélection libre d'un équipement par un agent, n'est pas compatible avec myPortal @work.
- La configuration NAT symétrique n'est pas prise en charge.
- Les pare-feu stricts ne sont pas pris en charge.

11.2.1.5 Guide de dépannage

Connexion expirée

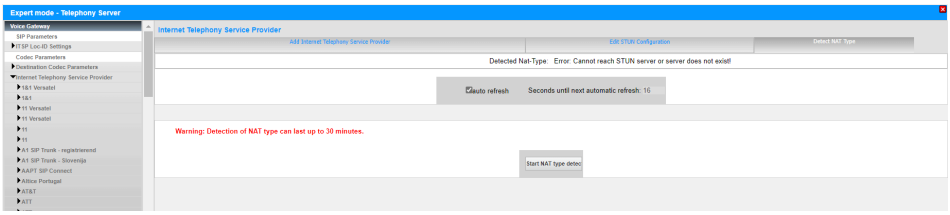
- En tant qu'utilisateur à domicile avec une connexion VPN, assurez-vous que l'utilisateur peut accéder à l'adresse LAN du système et se connecter à l'adresse LAN : port 8802. Résoudre le message d'erreur suivant : Message d'erreur « connexion expirée », action : vérifiez si l'utilisateur connecté via le VPN dispose d'une adresse IP locale du réseau VPN.
- En tant qu'utilisateur autonome, assurez-vous qu'il n'existe aucun autre appareil ni client VoIP myPortal @work enregistré avec le même numéro d'abonné. Recherchez également des connexions ouvertes sous **WBM > Mode Expert > Web Services Assistant**.

[2] Aucune action de configuration nécessaire ; les ports seront ouverts de manière dynamique à partir de la même plage de ports UDP que celle définie pour un pare-feu sans état

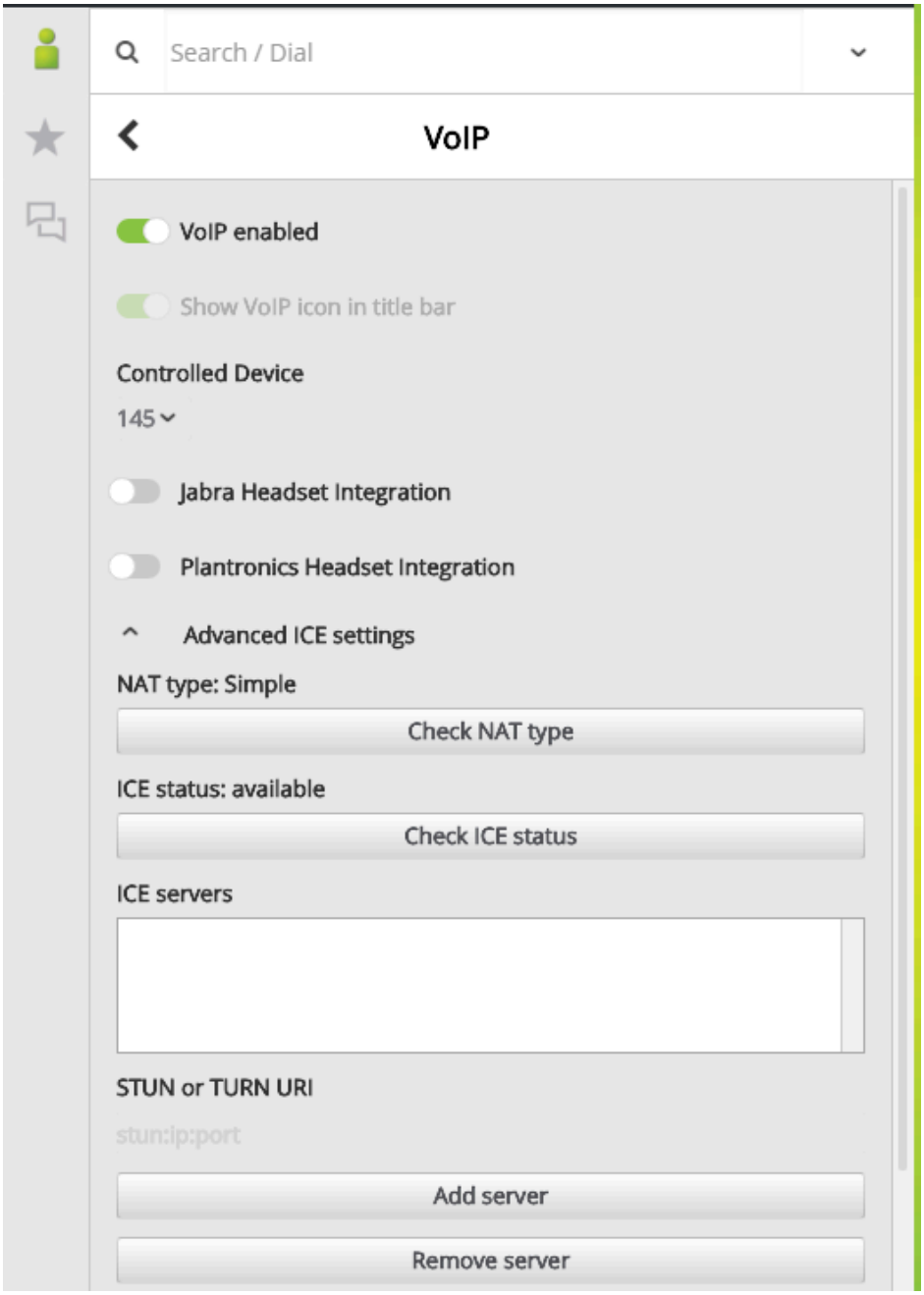
Pas de charge utile

En cas de problème permanent d'absence de charge utile :

- Vérifiez que les ports autorisés sont ouverts dans le pare-feu. Pour en savoir plus, voir le chapitre Paramètres des ports et du pare-feu à la page 457.
- Vérifiez la configuration du pare-feu NAT. La configuration NAT symétrique n'est pas prise en charge.
- Vous pouvez détecter le type NAT depuis le système sous **WBM > Mode Expert > Passerelle vocale > Détecter le type NAT**.
- Vérifiez la connectivité du serveur STUN dans le système.



- Vérifiez la connectivité ICE dans myPortal @work : **Paramètres > VoIP > Paramètres ICE avancés**. Si le type NAT et/ou l'état ICE ne sont pas indiqués ci-dessous, les paramètres de réseau/pare-feu doivent être vérifiés par votre administrateur.



Exécutez « Vérifier le type NAT » > Type NAT : Simple

Exécutez « Vérifier l'état ICE » > État ICE : disponible

- Désactivez l'intégration de casque à partir de myPortal @work et répétez la procédure.
- Sélectionnez à nouveau les équipements audio dans les paramètres VoIP.

11.2.1.6 Autres conseils

SIP ALG (Passerelle de couche d'application)

Si vous rencontrez l'un des problèmes suivants, veuillez vérifier si un SIP ALG est activé sur l'un des routeurs concernés. Il y a quelques catégories de symptômes qui font que le SIP ALG peut affecter les connexions VoIP. Ce n'est pas toujours évident, d'autant plus que ces problèmes se produisent souvent silencieusement, à l'insu des utilisateurs.

- Audio unidirectionnel (une seule personne peut entendre l'autre)
- Le client ne sonne pas lorsqu'il est appelé
- Les appels sont interrompus après avoir été connectés
- Les appels aboutissent directement à la messagerie vocale sans raison connue

11.3 Utilisateurs de UC Smart

Les utilisateurs de UC Smart sont des abonnés qui utilisent UC Clients de UC Smart.

Les paramètres suivants pour UC Smart Clients sont disponibles dans UC Smart Assistant :

Paramètres	Explication
Paramètres	
Utilisateurs	Le paramétrage est affiché uniquement ici.
Nom	Le paramétrage est affiché uniquement ici.
Mot de passe	Mot de passe pour UC Smart Clients et UC Smart Assistant.
Langue	Langue de l'interface utilisateur.
L'utilisateur doit attribuer un nouveau mot de passe	Le paramétrage est affiché uniquement ici.
Accès UC Smart Assistant	Autorisation pour l'utilisateur d'utiliser UC Smart Assistant dans le navigateur afin de réaliser des tâches de configuration.
Configuré comme abonné Mobility	Le paramétrage est affiché uniquement ici.
Licence de messagerie vocale	Le paramétrage est affiché uniquement ici.
Services associés	Le paramétrage est affiché uniquement ici.
Détails du profil	
Numéro de téléphone mobile	Numéro de téléphone mobile de l'abonné au format canonique (par ex. `+49 173 1234567`).
Numéro privé / externe	Numéro de téléphone supplémentaire de l'abonné au format canonique (par ex. `+49 89 987654321`).
Adresse e-mail	Adresse e-mail de l'abonné.

Paramètres	Explication
Messagerie vocale à e-mail	Activation/Désactivation de la notification par e-mail lors de la réception d'un nouveau message vocal.
Visibilité de l'état Présence	Configuration pour déterminer si l'état Présence doit-il être visible pour les abonnés internes et externes ou être uniquement visible pour les abonnés ou ne jamais être visible.
Informations sur la licence	
Affichage des licences attribuées à l'utilisateur	

11.3.1 Comment configurer un utilisateur de UC Smart

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

En mode expert, dans **Sélection de l'application**, le **paquet avec UC Smart** est activé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence du menu, cliquez sur **Assistants** > **UC Smart**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **UC Smart**.
4) Dans l'arborescence du menu, cliquez sur **Administration** > **Configuration de base**.
5) Dans la liste **Utilisateurs**, sélectionnez l'utilisateur souhaité.
6) Dans **Paramètres**, **Détails du profil**, modifiez les données de l'utilisateur.
7) Cliquez sur **Appliquer**.
8) Si vous souhaitez configurer un autre utilisateur, répétez les étapes 5 à 7.

11.3.2 Comment changer le mot de passe pour un utilisateur de UC Smart

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

En mode expert, dans **Sélection de l'application**, le **paquet avec UC Smart** est activé.

Remarque : Vous devez savoir que les utilisateurs de UC Smart doivent modifier par défaut leur mot de passe lorsque l'administrateur l'a modifié. Si cela n'est pas souhaité, après la modification du mot de passe, désactiver le flag "L'utilisateur doit attribuer un nouveau mot de passe".

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Smart**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **UC Smart**.
4) Dans l'arborescence du menu, cliquez sur **Administration** > **Gestion des utilisateurs**.
5) Dans la plage **Utilisateurs**, sélectionnez l'utilisateur concerné.

Remarque : Pour des raisons de sécurité, un mot de passe composé de 5 étoiles (*****) n'est pas accepté par le système.

---

6) Dans la plage **Paramètres**, sous **Mot de passe**, saisissez le nouveau mot de passe.
7) Cliquez sur **Appliquer**.
8) Si vous souhaitez réinitialiser le mot de passe d'un autre utilisateur, répétez les étapes 5 à 7.

Étapes suivantes

Informez le/les utilisateur(s) concernés du nouveau mot de passe.

11.4 Statut de présence (Présence)

Le statut de présence dans l'annuaire interne fournit des informations sur la disponibilité des abonnés internes (y compris les stations Mobility Entry). Le statut de présence contrôle également la disponibilité des abonnés internes grâce au renvoi d'appel basé sur le statut.

En tant qu'abonné, vous pouvez modifier votre statut de présence dans myPortal @work. Pour chaque changement de statut de présence (sauf pour **le statut Bureau**), vous pouvez également définir l'heure prévue de votre retour au statut **Bureau** si nécessaire.

En tant qu'abonné, vous pouvez sélectionner les statuts suivants :

- **Bureau**
- **Réunion**
- **Malade**
- **Casser**
- **Sorti**
- **Vacances**
- **Déjeuner**
- **Rentrée à la maison**
- **Ne pas déranger**

Remarque : L'administrateur système peut activer/désactiver la visibilité du statut « malade » dans l'administration système. Voir OpenScape Business UC Suite > Serveur

---

Grâce au renvoi d'appel basé sur le statut, les appels peuvent être transférés vers la messagerie vocale personnelle, par exemple. Les abonnés qui ne disposent pas de messagerie vocale personnelle peuvent transférer leurs

appels vers une messagerie vocale de groupe ou une messagerie vocale système.

11.5 Répertoires et Journal

Les répertoires et le journal organisent les contacts et appels.

11.5.1 Répertoires

Les répertoires organisent les contacts des abonnés. Les abonnés peuvent accéder aux contacts avec UC Smart Clients.

Le système fournit les répertoires suivants qui prennent en charge les fonctions suivantes et avec la priorité indiquée ci-dessous pour le numéro de recherche (le numéro de recherche ne sera pris en charge que pour un appel externe et dans le cas où CO/ITSP ne fournit pas le nom) :

Répertoire	UC Smart Clients	Téléphone système avec écran
Répertoire personnel	Contacts Outlook importés à l'aide de l'assistant personnel.	
Annuaire interne	Comprend tous les abonnés et groupes internes avec leurs éventuels numéros supplémentaires pour lesquels l'affichage est activé dans le système. Les abonnés internes avec téléphones système sont représentés avec l'état Présence. La condition pour l'affichage de l'état de présence d'un abonné est que l'abonné concerné l'autorise.	Comprend tous les abonnés et groupes internes pour lesquels l'affichage est activé dans le système.
Liste des favoris	Il contient des contacts sélectionnés par l'abonné provenant du répertoire personne et de l'annuaire interne. Les abonnés internes avec téléphones système sont représentés avec l'état Présence. La condition pour l'affichage de l'état de présence d'un abonné est que l'abonné concerné l'autorise.	
Répertoire système	Contient tous les numéros abrégés centralisés.	

Remarque : Entrez toujours les numéros de téléphone au format canonique dans les répertoires.

Remarque : Lors de l'ajout ou de la suppression d'un contact UC, il peut s'écouler plusieurs minutes**(et** jusqu'à 30 minutes)

avant que les changements ne soient appliqués à tous les clients et appareils en raison des mécanismes de mise en cache utilisés. Il est également possible de redémarrer le système pour que les modifications prennent effet **immédiatement**.

11.5.1.1 Comment configurer les répertoires des téléphones système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Vous pouvez sélectionner les répertoires disponibles sur les téléphones système avec écran.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système** > **Affichage**.
4) Dans la liste déroulante **Annuaire**, sélectionner l'une des options ci-après.
   - Si vous devez rendre disponible les contacts personnels, le répertoire interne, externe et mise en réseau ainsi que le répertoire LDAP, sélectionnez **Tout**.
   - Si vous devez rendre disponible uniquement les contacts personnels, le répertoire interne, externe et mise en réseau, sélectionnez **Interne**.
   - Si seul le répertoire LDAP doit être disponible, sélectionnez **LDAP**.
   - Si aucun répertoire ne doit être disponible, sélectionnez **Non**.

   Remarque : En sélectionnant le **répertoire téléphonique interne via le répertoire unifié**, l'utilisateur peut activer les demandes de recherche/consultation de manière à ce qu'elles soit traitées comme des demandes en direction du répertoire unifié. Lorsque l'indicateur est désactivé et en l'absence d'accès à Unified Directory, la vue de liste du menu du répertoire, établie pour le téléphone OpenScape CP 200/205, n'est pas disponible.
5) Cliquez sur **Appliquer**.

Étapes suivantes

Si vous avez sélectionné **Tous** ou **LDAP**, veillez à ce qu'un répertoire LDAP correspondant (par ex. Open Directory Service) soit disponible pur les téléphones système.

11.5.2 Répertoire interne

Le répertoire interne contient les détails de contact des abonnés internes et des groupes MULAP du système de communication. Les clients UC Suite ont accès au répertoire interne.

En tant qu'administrateur, vous avez un accès non limité à toutes les données du répertoire interne. En tant qu'abonnés, vous pouvez numéroter à partir du répertoire interne.

L'affichage des abonnés et groupes interne dans le répertoire interne dépend du paramètre d'abonné **Entrée dans l'annuaire** (réglable dans la WBM via les assistants abonné).

Dans une interconnexion de réseaux, le répertoire interne est valable sur l'ensemble des noeuds.

Concepts associés

Appel de groupe à la page 633

11.5.2.1 Comment activer ou désactiver l'affichage d'un abonné dans le répertoire interne

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence menu, naviguez sous **Abonnés** > **Abonné** > **…** pour accéder à l'abonné souhaité (Index - Numéro - Nom).
4) Cliquez sur l'onglet **Modifier les flags abonné**.
5) Sélectionnez une des possibilités suivantes :
   - Pour afficher le nom de l'abonné dans le répertoire interne, cochez la case **Entrée dans l'annuaire**.
   - Pour ne pas afficher le nom de l'abonné dans le répertoire interne, décochez la case **Entrée dans l'annuaire**.
6) Cliquez sur **Appliquer** puis sur **OK**.

11.5.3 Liste des favoris

La liste des favoris contient les contacts sélectionnés par l'abonné en provenant du répertoire personnel et interne. Les UC Smart Clients ont accès à la liste des favoris.

Un utilisateur UC Smart peut appeler directement un contact à partir de la liste des favoris. Si un abonné interne reçoit un appel, l'état d'appel de l'abonné est affiché. L'utilisateur UC Smart peut reprendre cet appel. En plus, l'état Présence est affiché pour les abonnés internes.

11.5.4 Répertoire système

Le répertoire système contient tous les numéros abrégés centralisés pour lesquels un nom a été attribué. Les UC Smart Clients ont accès au répertoire système.

L'administrateur peut désactiver individuellement l'affichage pour chaque abonné ou chaque numéro abrégé avec nom.

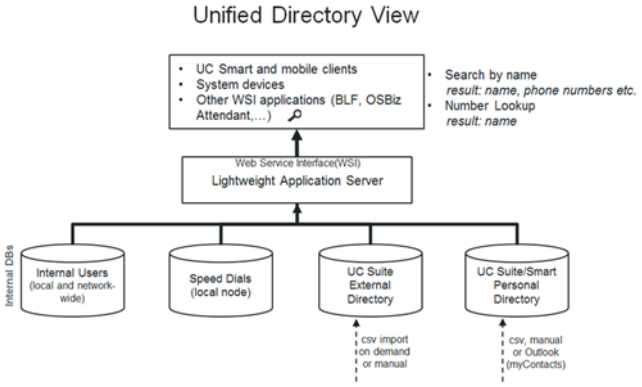
11.5.5 Annuaire unifié

OpenScape Business fournit différentes sources de données pour stocker et récupérer les données relatives aux utilisateurs ou aux contacts, en commençant par les données utilisateur internes dans la configuration utilisateur interne, via la liste de numérotation rapide interne, jusqu'aux différents répertoires des applications UC.

Chaque source de données au sein d'OpenScape Business est utilisée par une application cliente spécifique, soit située dans le logiciel système lui-même, dans les appareils téléphoniques, soit dans une application cliente de communications unifiées. En fonction des sources de données et des clients utilisés, les données récupérées et leur présentation diffèrent.

Le service « Unified Directory » d'OpenScape Business comprend les sources de données OpenScape Business existantes pour les fonctions communes de recherche et de résolution de noms. Il fournit les mêmes résultats de recherche ou informations de résolution de noms à tous les périphériques du système et aux clients OpenScape Business.

Le service d'annuaire unifié peut être accessible soit via l'interface de service Web (WSI) depuis des clients situés à l'extérieur, soit en interne via les mécanismes de traitement des appels (par exemple depuis les téléphones OpenStage).



Unified Directory utilise les bases de données et répertoires internes suivants d'OpenScape Business :

- Annuaire utilisateur interne (à l'échelle du réseau)
- Listes de numérotation rapide
- Répertoire personnel intelligent UC (facultatif)
- Répertoire externe UC Suite (facultatif)

Le service Unified Directory est disponible dans tous les systèmes OpenScape Business à partir de la version V2R2. Il ne nécessite aucun prérequis matériel, logiciel ou de licence spécifique.

Pour obtenir les meilleurs résultats lors de l'utilisation de l'annuaire unifié, certaines règles concernant le format des numéros de téléphone et l'orthographe des noms doivent être respectées.

11.5.5.1 Caractéristiques

Appareils/clients pris en charge

Le service d'annuaire unifié fournit :

- Recherche dans plusieurs sources de données internes d'OpenScape Business
- Offre unifiée des résultats de recherche à tous les clients pris en charge
- Recherche de numéros de téléphone / Résolution de noms dans plusieurs sources de données internes
- Offre unifiée de résultats de résolution de noms pour tous les clients pris en charge
- Accès aux données externes via l'interface WebServices (WSI)

Ces fonctionnalités sont disponibles pour les systèmes à nœud unique, comme décrit ci-après. Au sein des réseaux OpenScape Business, la disponibilité des fonctionnalités dépend principalement du type de connexion des liaisons, des appareils et des clients au sein du réseau.

Unified Directory prend en charge les clients/périphériques système Unify suivants via les interfaces indiquées :

Appareil/Client	Interface/Protocole utilisé	Remarques
Téléphones OpenStage	Traitement des appels / Protocole CorNet	WSI/HTTP(S) est optionnel sur OpenStage 60/80 pour les images de l'appelant
Téléphone de bureau OpenScape IP	Traitement des appels / Protocole CorNet	WSI/HTTP(S) est optionnel sur le DeskPhone IP 55 pour les images de l'appelant
Dispositifs sans fil (CMI)	Protocole de traitement des appels / CMI	
CP 100/110/200/205/210/405	Traitement des appels / Protocole CorNet	
Téléphone de bureau CP400/ 600/600E/ 700/700X/710	WSI / HTTP(S)	
myPortal au travail	WSI / HTTP(S)	

Remarque : Les clients UC Suite myPortal, myAttendant et myAgent utilisent leurs propres mécanismes pour la recherche dans l'annuaire et la résolution des noms.

Fonction de recherche

La recherche dans l'annuaire unifié est toujours effectuée à l'aide de l'interface utilisateur spécifique du périphérique/client. Les critères de recherche et le jeu de caractères utilisé peuvent être restreints, en fonction des clients utilisés.

Une fois les critères de recherche saisis, la recherche est effectuée dans les répertoires suivants.

- Annuaire utilisateur interne (à l'échelle du réseau)
- Listes de numérotation rapide
- Répertoire personnel intelligent UC (facultatif)
- Répertoire externe UC Suite (facultatif)

Tous les résultats de recherche figurant dans les répertoires ci-dessus sont affichés avec leur origine. Les correspondances contiennent soit l'ensemble complet des données de contact, soit seulement une partie de celles-ci. La profondeur des informations fournies dans les résultats dépend de la source des données.

Remarque : La recherche par nom de groupe dans myportal@work n'est pas prise en charge en mode UC Suite. Seules les recherches des utilisateurs sous licence (licence de base) et des groupes MULAP sous licence (entrées UC) sont prises en charge.

Les matchs sont affichés sur les appareils ou les clients en fonction des capacités d'affichage.

	Annuaire des utilisateurs internes	**Numéros abrégés**	**Annuaire personnel intelligent UC**	**Répertoire externe UC Suite**	**Contacts Outlook personnels (via Mes Contacts)**
Nom de famille	X	---	X	X	X
Prénom	X	---	X	X	X
Nom court/ d'affichage	X	X	---	---	---
Numéro de téléphone du bureau	---	---	X	X	X
Accueil/Ext. Numéro de téléphone	---	---	X	---	X
Numéro de téléphone portable	---	---	X	X	X
Adresse e-mail	---	---	X	X	X
Nom de l'entreprise	---	---	X	X	X
Ville	---	---	---	---	---
Photo de contact	---	---	X	---	X
Aperçu de l'image de contact	---	---	X	---	X

Recherche de numéro de téléphone

La recherche de numéro de téléphone dans l'annuaire unifié résout le problème de l'appelant transféré (CLI) par une recherche de numéro dans toutes les sources de données internes prises en charge. La recherche est effectuée dans les champs de numéro de téléphone suivants :

- Numéro de bureau
- Numéro de portable
- Numéro de téléphone fixe

La recherche de numéro de téléphone est déclenchée en cas d'appels entrants ou sortants en général, tandis que les fonctions spécifiques de routage et de transfert sont prises en compte en outre.

Une priorisation fixe des sources de données utilisées pour la recherche de numéros de téléphone est mise en œuvre afin d'obtenir le résultat le plus rapidement possible. Le résultat contient soit uniquement le nom de famille, le prénom, le nom d'affichage ou, le cas échéant, l'ensemble des données de contact associées.

Tableau 5 : Sources de données prises en charge et priorisation

Priorité	Sources de données	Remarque
1	Nom du CO/ITSP (tel qu'envoyé par le fournisseur)	La condition préalable est d'activer l'indicateur « Nom dans CO ».
2	Liste de numérotation rapide	
3	Contacts personnels	
4	Détails de l'utilisateur UC	

Les données récupérées sont présentées sur l'appareil de l'utilisateur et/ou dans le client UC. La profondeur des informations dépend des capacités d'affichage.

- **Appels entrants**

  Scénario pris en charge pour les systèmes à nœud unique :

  – Appel de base
  – Appel de groupe/Appel MULAP
  – Groupe de sonnerie
  – Transfert d'appel en une seule étape (SSCT)
  – Transfert avec présence/supervision/consultation
  – Renvoi d'appel inconditionnel (CFU)
  – Renvoi d'appel sans réponse (CFNR)
  – Renvoi d'appel occupé (CFB)
  – transfert aveugle
  – Prise d'appel

  Remarque : La prise d'appel est différente du groupe de prise d'appel. Dans le groupe de prise d'appel, lorsqu'un

numéro externe est enregistré dans l'annuaire unifié, le nom de l'appelant n'est pas affiché pour les membres du groupe.

Le scénario pris en charge pour les scénarios multi-nœuds (réseau) est un appel de passerelle.

- **Appel sortant**

  En cas d'appel sortant, la recherche du numéro de téléphone du correspondant appelé n'a lieu qu'une seule fois.

  Le scénario pris en charge pour les systèmes à nœud unique est un appel de base vers un numéro externe.

L'affichage des résultats de la recherche de numéro de téléphone dépend des capacités d'affichage des téléphones.

11.5.5.2 Règles et Conventions

Certaines conventions relatives aux formats des numéros et des noms dans les sources de données doivent être respectées pour pouvoir obtenir des résultats optimaux à l'aide du service Répertoire unifié.

Formats des numéros pris en charge

Tous les numéros de téléphone externes dans les sources de données doivent être saisis au format canonique, incluant l'indicatif pays et local, par ex. +4989700712345

La liste de numérotation abrégée prend en charge uniquement le format sélectionnable du système, par ex. 0089700712345 ou 0004989700712345

Lorsque les numéros abrégés sont configurés de façon à être accessibles via LDAP, vous devez activer l'option de conversion de nombre pour afficher le nom du contact, lorsque le numéro est au format canonique. Pour plus d'informations sur l'activation de la conversion de nombre, voir Comment ajouter une source de données externe pour Open Directory Service à la page 1120.

Formats des noms pris en charge

Les conventions suivantes relatives aux formats des noms et aux jeux de caractères doivent être respectées :

- **Format du nom pour la numérotation abrégée**

  La recherche de nom à l'intérieur de la liste de numérotation abrégée est prise en charge uniquement avec les règles de configuration spécifiques. Le prénom et le nom de famille doivent être saisis dans le champ de nom existant à l'aide du modèle suivant :

  <Nom de famille>, <Prénom> (séparés par des virgules)

- **Utilisateurs internes en cas de migrations**

  La migration vers V2R1 et versions ultérieures avec des utilisateurs internes ne suivant pas ces règles de configuration ne sera pas prise en charge de la manière prévue. En d'autres termes, l'administrateur doit convertir les noms internes selon le modèle suivant, et ce, avant la migration :

  <Nom de famille>, <Prénom> (séparés par des virgules)

Disponibilité des changements de répertoire

Après la création, mise à jour ou suppression de contacts dans les différentes sources de données, la répercussion de toutes les modifications dans les résultats de recherche de numéro de téléphone peut prendre dix minutes.

11.5.5.3 Chapitre 11.5.5.3 Limites fonctionnelles

Les limites fonctionnelles suivantes existent pour les répertoires unifiés (Unified Directories) :

Recherche de nom

- Support du nom de groupe

  Les noms de groupe (pas les noms MULAP) ne peuvent pas être recherchés dans tous les types de configurations.
- Support de caractères spéciaux

  Sur la plupart des équipements téléphoniques, l'utilisateur peut uniquement rechercher les caractères standard « a-z ». Les caractères spéciaux (diacritiques) comme les caractères allemandes Ää,Öö,Üü, ß ne sont pas accessibles via l'interface utilisateur de l'équipement téléphonique.

  Par conséquent, un résultat de recherche de caractères simples inclut aussi les caractères spéciaux. La recherche de l’un des caractères suivants : « acdegilnorstuyz », trouve aussi les caractères spéciaux correspondants : « àáâãåäăąçćčďđèéêêëêìıîíľłñńòòôõöøåêhťùúúÿ »

  dans les résultats de recherche.

  Remarque : La recherche dans l'annuaire avec le caractère générique au début de la chaîne de recherche, par exemple <*jo*> ne fonctionne que pour les utilisateurs internes.
- Support du format du nom pour la numérotation abrégée

  La recherche de nom à l'intérieur de la liste de numérotation abrégée est prise en charge uniquement avec les règles de configuration spécifiques. Le prénom et le nom de famille doivent être entrés dans le champ de nom existant à l'aide de l'un des modèles suivants

  – <Nom de famille>, <Prénom> (séparées par des virgules)
  – <Prénom> <Nom de famille> (séparateur d'espace dans ce cas)

Présentation du nom

Les contacts personnels dans UC Smart et à partir d'un répertoire hors ligne externe dont la longueur du prénom plus la longueur du nom de famille sont supérieures à 24 caractères, sont tronqués à 24 caractères pour correspondre à la longueur d'affichage de l'équipement.

Recherche de numéro de téléphone

La fonctionnalité de recherche du numéro de téléphone (retrouver le nom du contact à partir du numéro de l'appelant) n'est pas prise en charge dans Unified Directory pour les équipements SIP et S0.

11.5.5.4 Annuaire unifié dans les systèmes en réseau

Le service d'annuaire unifié est actif sur chaque nœud d'un réseau d'entreprise OpenScape et utilise les sources de données de son propre système. Les appareils téléphoniques et les clients utilisent toujours le service d'annuaire unifié au sein de leur propre nœud.

La disponibilité des contacts à l'échelle du réseau dépend donc du type de contenu de la source de données.

Tableau 6 : Source de données locale et à l'échelle du réseau

Source de données	Données locales	Données à l'échelle du réseau
Annuaire des utilisateurs internes	X	X
listes de numérotation rapide	X	---
Annuaire personnel intelligent UC	X	---

Remarque : L'annuaire unifié n'est pas entièrement pris en charge dans les environnements mixtes UC Suite/UC Smart.

Recherche de numéro de téléphone

Dans les scénarios de mise en réseau, la fonctionnalité de recherche de numéro de téléphone n'est pas utilisée. Dans de tels scénarios, le nom est transporté via les mécanismes de réseau normaux entre les nœuds du réseau.

Pour les utilisateurs internes, le nom d'affichage configuré est utilisé, la recherche n'est donc pas nécessaire.

11.5.6 Journal

Le journal est la liste de tous les appels entrants et sortants d'un abonné. A partir du journal, l'abonné peut rappeler les contacts de manière aisée et rapide ou répondre aux appels manqués.

Pour l'utilisateur UC Smart, il est affiché au maximum les 100 derniers appels.

Dossiers pour les types d'appel

Les appels sont répartis dans les groupes suivants :

- **Ouverts**
- **Manqués**
- **Acceptés**
- **Tous les appels**

Détails de l'appel

Chaque appel est affiché avec Date et Heure et, si disponible, avec le numéro. Si, en plus du numéro d'appel, le répertoire contient d'autres informations

comme **Nom de famille** et **Prénom**, elles sont également affichées. Il est en plus indiqué la **direction** de l'appel et la **durée** ainsi que, éventuellement, les renvois temporisés ou les interceptions d'appel intervenus.

11.6 Appels

Pour les appels, le format du numéro d'appel revêt une importance particulière.

11.6.1 Formats des numéros d'appel

Il existe différents formats pour la fourniture des numéros d'appel.

Format	Description	Exemple
canonique	Débute par + et contient toujours le code du pays, l'indicatif local et le reste complet du numéro d'appel. Les caractères vides et les caractères spéciaux + ( ) / - : ; sont admissibles.	+49 (89) 7007-98765
composable	De la manière dont vous composeriez le numéro d'appel au téléphone système au bureau, toujours avec indicatif réseau.	• 321 (interne) • 0700798765 (propre réseau local) • 0089700798765 (réseau local tiers) • 0004989700798765 (étranger)

Conseil : Lorsque cela est possible, utilisez toujours les numéros d'appel au format canonique. Ainsi, le numéro d'appel est toujours complet et univoque dans toutes les situations et il est cohérent pour la mise en réseau et pour les utilisateurs mobiles.

Lors de la sélection manuelle (format au choix) d'un numéro externe, il faut toujours indiquer l'indicatif réseau.

Lors de la sélection d'un numéro de téléphone externe au format sélectionnable, à partir d'un répertoire (ainsi que, pour certains clients UC, lors de la sélection au niveau du bureau ou au niveau du presse-papiers, le système de communication ajoute automatiquement l'indicatif réseau (faisceau 1).

Remarque : Lors d'un appel à l'intérieur des Etats-Unis via CSTA en direction d'un numéro au format canonique, le numéro est converti au format sélectionnable.

11.7 Conférences

Lors d'une conférence, plusieurs participants (y compris des intervenants extérieurs) peuvent communiquer entre eux simultanément. La fonction de gestion des conférences vous permet d'organiser rapidement et facilement des conférences et également de les programmer à l'avance.

Conférences contrôlées par téléphone et par application

En tant qu'abonné, vous pouvez organiser des conférences à la fois par téléphone et via les applications UC Smart.

Vous pouvez lancer une conférence téléphonique de différentes manières, puis la contrôler par téléphone :

- Appelez le participant souhaité à la conférence et mettez-le en relation avec celle-ci.
- Transformer un appel de consultation en conférence
- Transformez le deuxième appel en conférence.

Vous pouvez lancer, contrôler et gérer des conférences pilotées par application via la Gestion des conférences. Une licence de conférence est requise pour utiliser la gestion des conférences.

Différences entre les types de conférences :

	Conférence contrôlée par téléphone	**Conférence contrôlée par application**
Orientation de la configuration de la connexion du point de vue du système	• Sortie	• Appel entrant (connexion par le participant)
Authentification des participants à la conférence	-	• Code PIN personnel (identifiant de conférence) • Code PIN invité (facultatif)
Invitation prédéfinie aux participants à la conférence	-	• Nom de la conférence • Numéro d'appel (MeetMe) • Code PIN personnel (identifiant de conférence) • Code PIN invité (facultatif)
Nombre maximal de participants par conférence	8	16

Conférence programmée

Les conférences programmées sont créées en tant que conférences permanentes. La conférence peut être utilisée à tout moment et selon les besoins, sans planification supplémentaire. Les conférences programmées n'occupent aucun canal de conférence tant qu'aucun participant ne s'est connecté à la conférence. L'ordre dans lequel les participants composent le numéro détermine l'attribution des canaux de conférence.

Les administrateurs peuvent modifier le numéro d'appel spécifié (MeetMe) pour les conférences via le WBM lors de la configuration initiale. Le numéro à composer pour se connecter à la conférence est affiché aux participants. Ils

doivent ensuite s'authentifier avec leur code PIN personnel ou avec le code PIN général des invités si celui-ci est autorisé.

Modérateurs

L'initiateur d'une conférence en est automatiquement le modérateur et peut :

- Créer, modifier et supprimer des conférences planifiées.
- Ajouter et supprimer des participants à la conférence.

  Les participants exclus ne restent pas à la conférence.
- Déconnecter les participants à la conférence.

  Les participants déconnectés peuvent se reconnecter à la conférence.
- Spécifiez un autre participant interne sur le même nœud que le modérateur.
- Quittez la conférence sans la terminer immédiatement.

  Si le dernier modérateur quitte la conférence, celle-ci prend fin au bout de 5 minutes.
- Mettre fin aux conférences en cours.
- Envoyer des invitations prédéfinies à tous les participants à la conférence ou à des participants individuels.

Tous les participants internes à un nœud peuvent être modérateurs. Toutefois, une licence de conférence est requise.

Les participants à la conférence dont les coordonnées ont été saisies manuellement sont considérés comme des participants externes et ne peuvent pas être désignés comme modérateurs.

Participants à la conférence

Les participants à la conférence peuvent la quitter et s'y reconnecter. De plus, ils peuvent participer à une session de collaboration en ligne qui a déjà commencé. Tant qu'une conférence ne compte qu'un seul participant, celui-ci entend de la musique d'attente. Le nombre maximal de participants externes à la conférence est limité, entre autres, par le nombre de coffres disponibles.

Suppression automatique sans modérateur

Si le dernier modérateur quitte la conférence, les autres participants sont avertis par SMS que la conférence prendra fin dans environ 5 minutes.

Notification des participants à la conférence

Le modérateur peut envoyer une invitation par courriel à tous les participants à la conférence ou à certains d'entre eux. Cela nécessite qu'un logiciel de messagerie soit installé sur l'ordinateur client. Les adresses électroniques connues sont automatiquement ajoutées à la liste de diffusion. Dans l'invitation adressée à tous les participants à la conférence, seul le code PIN général (si autorisé) est inclus ; pour les invitations individuelles, le code PIN personnel est également envoyé.

Il est également possible de copier un texte d'invitation prédéfini dans le presse-papiers pour l'utiliser ultérieurement dans d'autres programmes (par exemple, un programme de chat).

11.8 Messagerie instantanée

La messagerie instantanée est un moyen de communiqué directement (chat)

11.8.1 Messagerie instantanée

Les Messages instantanés vous permettent de chatter avec les autres utilisateurs UC Smart.

Les messages instantanés envoyés et reçus sont affichés sous forme de dialogue chez les partenaires de communication. Lors de la sélection du destinataire, le client indique si le partenaire de communication est momentanément en ligne ou non. Lorsque le correspondant est hors ligne, il n'est pas possible de lui envoyer de message instantané. La page d'aperçu des messages instantanés indique les derniers flux (stream). Le système enregistre un nombre limité de messages instantanés. Il est affiché au maximum les 100 derniers messages instantanés d'un utilisateur.

11.9 Boîte vocale (SmartVM)

La messagerie vocale (également appelée SmartVM) diffuse un message d'accueil aux appelants et leur offre la possibilité d'enregistrer un message ou d'être redirigés vers un autre numéro. Les abonnés internes peuvent accéder à la messagerie vocale via un téléphone et avec le client UC Smart. Les abonnés qui souhaitent utiliser une messagerie vocale doivent se munir d'une licence de messagerie vocale.

Types de boîtes vocales

Il existe les différents types de boîtes vocales suivants :

- Boîte vocale standard :

  La messagerie vocale standard est la messagerie vocale personnelle d'un abonné. Il accepte l'appel, accueille l'appelant par une annonce personnalisée ou standard et lui offre la possibilité de laisser un message. La messagerie vocale standard peut être configurée par l'abonné (en enregistrant un message d'accueil personnalisé, par exemple) via le téléphone ou via le client UC Smart.
- Boîte vocale de groupe :

  La messagerie vocale de groupe possède les mêmes fonctionnalités que la messagerie vocale standard, à la différence qu'elle n'est pas attribuée à un seul utilisateur, mais à un groupe d'utilisateurs. L'enregistrement de messages pour une messagerie vocale de groupe n'est possible que si au moins un membre du groupe possède une licence de messagerie vocale. Les informations de la messagerie vocale sont affichées à tous les membres du groupe disposant d'une licence de messagerie vocale. La lecture des messages est possible via le menu téléphonique de la messagerie vocale personnelle des membres du groupe.

- Boîtes vocales de standard (standard automatique / standard automatique d'entreprise) :

  La messagerie vocale de l'opérateur offre aux appelants un message d'accueil avec ou sans options de routage ultérieures. Le standard automatique d'entreprise est une forme particulière de messagerie vocale automatique. Ici, l'appelant peut être transféré automatiquement (vers le standard, par exemple) ou sélectivement vers un autre poste (par exemple, vers le service ou la hotline) en composant un numéro d'appel interne ou un numéro de numérotation rapide (chiffres 0-9). Ces options de numérotation doivent bien entendu être expliquées par une annonce correspondante. Il est également possible de configurer une destination d'interception vers laquelle l'appelant sera redirigé s'il ne saisit pas de chiffre ou s'il saisit un chiffre invalide (c'est-à-dire non attribué). L'administrateur peut configurer jusqu'à 100 boîtes vocales d'opérateur.
- Messagerie vocale d'annonce :

  La fonction d'annonce est configurée en attribuant un index d'annonce à un port d'annonce et en configurant une messagerie vocale avec le numéro d'appel du port d'annonce. Le message d'accueil de la boîte aux lettres sert d'annonce. Selon le type d'annonce, la lecture peut avoir lieu une seule fois (message sortant) ou de manière cyclique (musique). Le menu téléphonique d'une messagerie vocale d'annonce ne peut être utilisé que depuis un autre téléphone, puisqu'aucun téléphone n'y est associé. Par conséquent, un code PIN différent doit être utilisé pour la messagerie vocale d'annonce que pour la messagerie vocale du téléphone utilisé.
- Boîte vocale du système :

  La boîte vocale associée au numéro d'appel du groupe de recherche du SmartVM est utilisée comme boîte vocale système. La messagerie vocale du système doit être une messagerie vocale standard (et non un standard automatique) avec l'enregistrement vocal activé. Les informations de la boîte vocale sont affichées au propriétaire de la boîte vocale portant l'index 1 et peuvent également être consultées à partir de là. Cette première boîte vocale ne doit pas être une boîte vocale de groupe, de standard ou d'annonce. Si la messagerie vocale système ne doit pas être utilisée, aucune messagerie vocale ne doit être configurée avec le numéro d'appel du groupe de recherche SmartVM.

Fonctionnalités de la boîte vocale

- Vérification et contrôle par téléphone

  (Depuis l'extérieur : votre propre numéro de téléphone est requis)
- Sélection manuelle ou automatique des différents messages d'accueil
- Menu téléphonique (interface utilisateur téléphonique, TUI) avec une structure de menu commutable à l'échelle du système :
  - Menu téléphone, UC Smart : **SmartVM** (similaire à EVM)
  - Menu téléphone, UC Suite : **OSO** (similaire à UC Suite)
- Chaque système peut configurer jusqu'à 320 boîtes vocales.
- Capacité d'enregistrement vocal jusqu'à 32 heures par système
- Jusqu'à 100 messages enregistrés par boîte vocale
- Jusqu'à 2 minutes d'enregistrement par boîte vocale.
- Jusqu'à 10 opérations de commutation et de réponse d'appel simultanées sont possibles.
- Annonce/musique avant de répondre

- Lecture des annonces individuelles
- Transfert automatique des appels de fax vers une destination de fax préconfigurée grâce à la reconnaissance automatique de la tonalité.

Remarque : Vous trouverez des informations détaillées sur le menu du téléphone dans les deux guides de référence rapide, UC Smart Telephone User Interface (TUI) et UC Suite Telephone User Interface (TUI).

Paramètres du numéro de code

Avant la première utilisation de la boîte vocale, chaque abonné doit modifier le code prédéfini (par défaut : `123456`).

Le code numérique est composé d'une séquence de six chiffres. Les chiffres répétés (par exemple, `333333`) et les séquences de chiffres en ordre croissant ou décroissant (par exemple, `987654`) ne sont pas autorisés. Après six saisies d'un code invalide, l'accès à la messagerie vocale correspondante est verrouillé jusqu'à ce que le mot de passe soit réinitialisé par l'administrateur. Après deux saisies incorrectes du mot de passe via le menu du téléphone, la connexion est interrompue.

Ports

La boîte de messagerie vocale utilise les ports S_0 500 à 509, auxquels sont attribués les numéros d'appel 739 à 748, respectivement. Les ports 504 et 505 sont attribués par défaut au standard automatique de l'entreprise (numéro d'appel 352), et les 8 ports restants sont attribués à la boîte vocale du groupe de recherche (numéro d'appel 351). Le numéro d'appel 351 est le numéro d'appel général de la messagerie vocale par lequel le menu téléphonique est accessible.

Restriction de péage

Pour des raisons de sécurité, les ports de la messagerie vocale n'ont par défaut qu'un accès réseau sortant restreint. Les fonctionnalités suivantes nécessitent l'attribution d'un groupe COS avec accès direct au trunk :

- Appeler l'expéditeur d'un message vocal
- Les utilisateurs mobiles peuvent écouter les messages vocaux via rappel.
- Les messages sont transférés vers une destination externe via le standard automatique de l'entreprise.

Salutations / Annonces

Les messages d'accueil personnalisés peuvent être enregistrés depuis un téléphone ou chargés dans le système via le WBM. Pour configurer un message d'accueil personnalisé par téléphone, composez le numéro de la messagerie vocale, puis suivez les instructions vocales pour enregistrer un nouveau message.

Les messages d'accueil peuvent toutefois également être chargés séparément dans le système pour chaque boîte vocale, puis enregistrés ou supprimés en mode Expert.

Remarque : Pour la lecture des messages vocaux via des numéros de téléphone externes, la classe de service des ports

Smart VM doit être ajustée. Il est recommandé d'utiliser une « liste blanche » pour ces numéros très connus.

11.9.1 Configuration de la boîte vocale (SmartVM)

La configuration de la boîte vocale (SmartVM) comprend la configuration des boîtes de messagerie standard/boîtes de messagerie de groupe ainsi que des boîtes de messagerie de diffusion.

Les paramètres généraux de la boîte vocale (SmartVM) sont réalisés à l'aide de l'assistant **SmartVM** comme l'adaptation du numéro de la boîte vocale à un plan de numérotation à 4 positions.

Les réglages spéciaux de la boîte vocale (SmartVM) et la configuration des boîtes de messagerie standard/boîtes de messagerie de groupe et boîtes de messagerie de diffusion sont réalisés à l'aide du mode Expert.

Remarque : La modification d'un numéro de téléphone réinitialise la boîte vocale de l'abonné concerné. Tous les messages vocaux personnels, messages d'accueil et annonces sont perdus et le mot de passe est réinitialisé.

Vous pouvez aussi charger, enregistrer et effacer des messages d'accueil dans SmartVM et sauvegarder et rétablir des messages d'accueil et messages de certaines boîtes vocales ou de toutes les boîtes vocales. Vous pouvez également interroger les langues chargées pour le guidage de l'utilisateur et consulter les 10 boîtes vocales où se trouvent le plus grand nombre de messages ainsi que l'emplacement de sauvegarde des messages et messages d'accueil.

La configuration des boîtes de messagerie de diffusion est expliquée au chapitre Attendants - standards automatiques (AutoAttendant) - standard automatique d'entreprise (UC Smart).

Affectation de la boîte vocale aux abonnés

Si la messagerie vocale (SmartVM) est configurée, il est possible d'affecter leurs boîtes vocale standard aux abonnés. Cela est possible à l'aide de

- un renvoi temporisé pour l'abonné à l'aide d'une table d'acheminement (configuré par l'administrateur). Dans ce cas, l'appel est renvoyé aux destinations d'appel sélectionnées, l'une après l'autre (par ex. tout d'abord à l'abonné puis, après un délai configurable, à la boîte vocale).
- un renvoi d'appel sur le téléphone de l'abonné (peut être effectué par l'abonné lui-même). Dans ce cas, l'appel est immédiatement dirigé vers la boîte vocale.

  Si l'abonné fait partie d'un groupement de recherche et si le groupement de recherche est appelé, l'appel n'est pas renvoyé vers la boîte vocale du groupement de recherche.

11.9.1.1 Comment désactiver ou activer la boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

UC Smart est activé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Connexions**.
3) Dans l'arborescence du menu, cliquez sur **Connexions** > **SmartVM**.
4) Cliquez sur l'onglet **Modifier les paramètres SmartVM**.
5) Si vous souhaitez désactiver la boîte vocale, cochez la case **Désactiver EVM**.
6) Si vous souhaitez activer la boîte vocale, décochez la case **Désactiver EVM**.
7) Cliquez sur **Appliquer** puis sur **OK**.

11.9.1.2 Comment configurer la boîte vocale (SmartVM)

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **SmartVM**.
4) Cochez la case **Activer SmartVM**.
5) Si nécessaire, modifiez les paramètres généraux de la boîte de messagerie système dans la colonne **Boîte vocale** :
   a) Si nécessaire modifiez dans le champ **Numéro de téléphone** le numéro de téléphone de la boîte vocale (par défaut `351`) afin par ex. de l'adapter à un plan de numérotation à 4 positions.
   b) Si nécessaire modifiez dans le champ **SDA** le numéro SDA de la boîte vocale (par défaut: `351`) afin par ex. de l'adapter à un plan de numérotation à 4 positions.
   c) Si nécessaire, modifiez dans le champ **Nom** le nom de la boîte vocale (par défaut `MESSAGERIE VOCALE`).
6) Si nécessaire, modifiez les paramètres généraux de la boîte de messagerie de diffusion dans la colonne **AutoAttendant** :
   a) Si nécessaire modifiez dans le champ **Numéro de téléphone** le numéro de téléphone de la boîte vocale (par défaut `352`) afin par ex. de l'adapter à un plan de numérotation à 4 positions.
   b) Si nécessaire modifiez dans le champ **SDA** le numéro SDA de la boîte vocale (par défaut: `352`) afin par ex. de l'adapter à un plan de numérotation à 4 positions.
   c) Si nécessaire, modifiez dans le champ **Nom** le nom de la boîte vocale (par défaut `Standard automatique`).

7) Cliquez sur **OK&Suivant**.
8) Si nécessaire, dans la ligne du port souhaité, dans le champ **N° de téléphone**, modifiez le numéro de téléphone du port (par défaut : `739-748`) afin par ex. de l'adapter à un plan de numérotation à 4 positions.
9) Si nécessaire, dans la ligne du port souhaité, dans le champ **Nom**, modifiez le nom du port (par défaut : `SmartVM 1-10`).
10) Si nécessaire, dans la ligne du port souhaité, dans la liste déroulante **Type**, modifiez le type de port :
    - **Phone Mail (Numéro 5 chiffres)**: le port est affecté aux boîtes de messagerie standard et aux boîtes de messagerie de type standard automatique. Les ports de ce types sont automatiquement intégrés dans le groupement 351.
    - **Par défaut** : le port est affecté aux boîtes de messagerie de diffusion de type standard automatique d'entreprise et aux boîtes de messagerie d'annonces. Les ports de ce types sont automatiquement intégrés dans le groupement 352.
11) Si nécessaire, dans la ligne du port souhaité, dans la liste déroulante **Mode**, modifiez le mode du port :
    - **Annonce** : un message d'accueil/une annonce est diffusé une seule fois.
    - **Musique d'attente** : message d'accueil/annonce/musique sont diffusés dans une boucle sans fin.
    - **Company AutoAttendant** : après la diffusion d'un message d'accueil/annonce il est possible d'effectuer un renvoi.
12) Cliquez sur **OK&Suivant**.
13) Dans la liste déroulante **Sélection de la boîte de messagerie**, indiquez la boîte de messagerie souhaitée. Il s'affiche ensuite les champs servant à configurer les messages d'accueil.
14) Si vous voulez utiliser vos propres messages d'accueil pour la boîte de messagerie sélectionnée, cliquez sur **Parcourir**, naviguez vers l'endroit de stockage des fichiers (format : wave, PCM, 16 bits, 8kHz, mono) et cliquez sur **Charger**. Les messages d'accueil sélectionnés sont chargés dans le système.

    Remarque : Vous pouvez sauvegarder et effacer les messages d'accueil déjà chargés.

15) Si vous souhaitez paramétrer des messages d'accueil pour d'autres boîtes de messagerie, répétez les étapes 13 à 14.
16) Cliquez sur **OK&Suivant**.
17) Ne modifiez les paramètres généraux que si cela est nécessaire. Pour une description des paramètres généraux, voir Connexions>SmartVM .
18) Cliquez sur **OK & Suivant** puis sur **Quitter**.

11.9.1.3 Comment ajouter une boîte de messagerie standard pour un abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Il est affecté une licence Messagerie vocale à l'abonné correspondant.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Connexions**.
3) Dans l'arborescence du menu, cliquez sur **Connexions** > **SmartVM**.
4) Cliquez sur l'onglet **Modifier boîtes de messageries SmartVM**.
5) Dans le champ **N° boîte de messagerie**, entrez le numéro de téléphone de l'abonné pour lequel la boîte de messagerie doit être ajoutée.
6) Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.
7) Si un appelant est autorisé à laisser un message sur la boîte vocale, cochez la case **Enregistrement**.
8) Assurez-vous que la case **AutoAttendant** est bien décochée.
9) La case à cocher **Réinitialisation mot de passe** ne doit pas être sélectionnée lors de la reconfiguration d'une boîte vocale. Cela provoque la réinitialisation du mot de masse de la boîte vocale. Lors d'une nouvelle configuration, l'abonné doit de toute manière, lors du premier accès à sa boîte vocale, modifier le mot de passe initial.
10) Cliquez sur **Appliquer** puis sur **OK**.

11.9.1.4 Comment modifier le groupe de discrimination pour un port de boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

UC Smart est activé.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dns l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Classes de service**.
3) Cliquez dans l'arborescence sur**Classes de service** > **Station** > **EVM**, puis sur le port de la boîte vocale souhaitée.
4) Sélectionnez les groupes COS souhaités pour le service de jour et de nuit dans l'onglet **Modifier le groupe COS** à partir des listes déroulantes **Groupe de classe de service jour** et **Groupe de classe de service nuit**, respectivement.
5) Cliquez sur **Appliquer**, puis sur **OK**.

Remarque : Les textes des ports EVM sont générés conformément à l'assistant **Configuration de base** > **Indicatif de pays du système**.

11.9.1.5 Comment modifier la structure du menu téléphone ou de la boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

UC Smart est activé.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Connexions**.
3) Dans l'arborescence du menu, cliquez sur **Connexions** > **SmartVM**.
4) Cliquez sur l'onglet **Modifier les paramètres SmartVM**.
5) Si vous souhaitez que la structure du menu téléphonique soit similaire à celle d'OpenScape Office, sélectionnez l'entrée **OSO** dans la liste déroulante **Interface utilisateur téléphonique**.
6) Cliquez sur **Appliquer**, puis sur **OK**.

11.9.1.6 Comment charger, sauvegarder et effacer des messages d'accueils

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

UC Smart est activé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Configuration**.
3) Dans l'arborescence du menu, cliquez sur **Configuration** > **Configuration SmartVM** > **Opérations fichier**.
4) Cliquez sur l'onglet **Données d'annonce**.
5) Sélectionnez dans la liste déroulante **Sélection de la boîte de messagerie** la boîte vocale souhaitée.
6) Si vous souhaitez charger dans SmartVM un message d'accueil sauvegardé antérieurement ou un fichier Wave, cliquez pour le message d'accueil souhaité sur **Parcourir** et naviguez vers l'emplacement de stockage du message d'accueil. Pour finir, cliquez sur **Charger**.

   Remarque : Le fichier Wave à charger doit avoir le format suivant : PCM, 16 bits, 8 kHz, mono. Le fichier son est converti lors du chargement. Cela peut prendre plusieurs minutes suivant la taille du fichier Wave.

7) Si vous souhaitez sauvegarder un message d'accueil existant, cliquez pour le message d'accueil existant sur **Sauvegarder** et enregistrez le fichier vma à un endroit de votre choix.
8) Si vous voulez effacer un message d'accueil existant, cliquez pour le message d'accueil souhaité sur **Effacer** et confirmez avec **OK**.

11.9.1.7 Comment sauvegarder et rétablir les messages d'accueil et les messages

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

UC Smart est activé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Configuration**.
3) Dans l'arborescence du menu, cliquez sur **Configuration** > **Configuration SmartVM** > **Opérations fichier**.
4) Si vous voulez sauvegarder les messages d'accueil et les messages :
   a) Cliquez sur l'onglet **Sauvegarde**.
   b) Cochez la case **Messages**, si, en plus des messages d'accueil, les messages doivent être enregistrés.
   c) Transférez les boîtes vocales à sauvegarder de la liste **Boîtes de messagerie disponibles** à la liste **Boîtes de messagerie à sauvegarder**.
   d) Cliquez sur **Appliquer**. Les messages d'accueil (et les messages si le flag **Messages** a été activé) des boîtes vocales à sauvegarder sont enregistrés dans un fichier de sauvegarde (*.tar). Sauvegardez le fichier dans un répertoire de votre choix.
5) Si vous voulez rétablir les messages d'accueil et les messages :
   a) Cliquez sur l'onglet **Restaurer**.
   b) Cliquez sur **Parcourir**, allez à l'endroit où votre fichier de sauvegarde (*.tar) est sauvegardé et cliquez sur **Ouvrir**.
   c) Cliquez sur **Charger** et ensuite sur **OK**. Les boîtes vocales comprises dans le fichier de sauvegarde sont indiquées.
   d) Transférez les boîtes vocales à rétablir de la liste **Boîtes de messagerie disponibles** à la liste **Boîtes de messagerie pour restauration**.
   e) Cochez la case **Messages**, si, en plus des messages d'accueil des boîtes vocales sélectionnées, les messages doivent être rétablis.
   f) Si la case **Entrée en tiers** est décochée, seuls sont remplacés les messages d'accueil des boîtes vocales qui figurent dans les données de sauvegarde. Si, en plus, la case **Messages** est cochée, il est également ajouté les messages contenus dans les données de sauvegarde. Les messages déjà existants sont conservés.
   g) Si la case **Entrée en tiers** est cochée, avant le rétablissement tous les messages d'accueil et tous les messages des boîtes vocale sélectionnées sont effacés dans SmartVM. Si des boîtes vocales qui ne figurent pas dans les données de sauvegarde sont sélectionnées, elle sont également effacées. Les messages d'accueil figurant dans les données de sécurité sont transférés. Si en plus la case **Messages** est activée, les messages contenus dans les données de restauration sont également transférés.
   h) Cliquez sur **Charger** et ensuite sur **OK**. Les messages d'accueil et messages des boîtes vocales sélectionnées sont rétablis.

11.9.2 Service de notification pour les nouveaux messages

Le système peut informer un utilisateur de UC Smart d'un nouveau message vocal, sur demande, par e-mail.

Condition pour le service de notification

- L'envoi d'e-mails (renvoi e-mail) doit être configuré dans le système par l'administrateur du système.

- L'adresse e-mail de l'utilisateur doit être connue du système. L'administrateur peut importer toutes les adresses e-mail dans WBM lors de la première installation, sous la forme d'un fichier XML ou bien, dans UC Smart Assistant, inscrire pour chaque utilisateur une adresse e-mail (voir Comment configurer un utilisateur de UC Smart). Ou bien, l'utilisateur peut lui-même indiquer son adresse e-mail dans son UC Smart Client.
- Il a été attribué à l'utilisateur une licence Boîte vocale.
- La fonctionnalité **Messagerie vocale à e-mail** est activée. L'administrateur peut activer la fonctionnalité dans UC Smart Assistant pour chaque utilisateur (Comment activer ou désactiver la notification par e-mail). Ou bien, l'utilisateur peut lui-même activer la fonctionnalité dans son UC Smart Client.

L'utilisateur de UC Smart reçoit un e-mail avec le message vocal associé sous forme de fichier WAV (16 bits, mono), la date et heure de la réception, la durée du message vocal et, si disponible, le numéro de téléphone ainsi que le nom de l'expéditeur.

11.9.2.1 Comment activer ou désactiver la notification par e-mail

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

En mode expert, dans **Sélection de l'application**, le **paquet avec UC Smart** est activé.

L'adresse e-mail de l'utilisateur est inscrite dans les détails de son profil.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence du menu, cliquez sur **Assistants** > **UC Smart**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **UC Smart**.
4) Dans l'arborescence du menu, cliquez sur **Administration** > **Configuration de base**.
5) Dans la liste **Utilisateurs**, sélectionnez l'utilisateur souhaité.
6) Sélectionnez une des possibilités suivantes :
   a) Si vous voulez activer le service de notification pour les nouveaux messages, dans la zone **Détails du profil**, cochez la case **Messagerie vocale à e-mail**.
   b) Si vous voulez désactiver le service de notification pour les nouveaux messages, dans la zone **Détails du profil**, décochez la case **Messagerie vocale à e-mail**.
7) Cliquez sur **Appliquer**.
8) Si vous souhaitez configurer un autre utilisateur, répétez les étapes 5 à 7.

12 Suite UC

La suite UC offre des fonctionnalités de communications unifiées telles que l'état de présence et CallMe, la conférence, ainsi que la messagerie vocale, la fonction fax et les fonctions de la console d'opérateur.

Remarque : Après toute modification de la configuration des stations, des groupes, de la mobilité ou d'autres paramètres système tels que les codes d'accès aux lignes, les données UC pour UC Smart ou UC Suite doivent être synchronisées. La synchronisation a lieu cinq minutes après la dernière modification de la configuration. Si une modification de configuration ultérieure survient avant l'expiration du délai de 5 minutes, le minuteur est redémarré. Les données UC peuvent être obsolètes jusqu'au démarrage de la synchronisation.

12.1 Configuration de base pour UC Suite

Les paramètres de base de UC Suite peuvent être adaptés.

UC Suite peut être activé ou désactivé. Si UC Suite est utilisé, UC Smart doit être désactivé.

En outre, tous les appels UC lancés par le système (par ex. à l'aide du service Appelle-moi - CallMe) peuvent être contrôlés avant la numérotation afin de savoir si l'utilisateur UC qui effectue la demande dispose de l'autorisation pour effectuer cet appel. Si l'utilisateur UC ne dispose pas de l'autorisation, l'appel n'est pas effectué.

Remarque : Si des applications CSTA sont utilisées, la valeur de ce paramètre pour toutes les lignes actives doit être définie.

Tâches associées

Comment déterminer les adresses IP des composants du système à la page 444

12.1.1 Comment activer UC Suite

Conditions préalables

Vous êtes connecté au WBM avec le profil **Expert** .

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert** .
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **Services Web**.
3) Dans l'arborescence du menu, cliquez sur **Sélection de l'application** > **Sélection de l'application**.
4) Cliquez sur **Package avec UC Suite**.
5) Cliquez sur **Appliquer** .

12.1.2 Comment limiter la classe de discrimination des appels UC lancés côté système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Configur. de base** > **Système** > **Flags système**.
4) Si, avant la numérotation d'appels UC qui sont lancés par le système, il faut contrôler si l'utilisateur de la UC Suite effectuant la demande dispose de l'autorisation relative à cet appel, dans la zone **Restriction pour les appels UC** cochez la case **Restriction pour les appels UC**.
5) Si, avant la numérotation d'appels UC qui sont lancés par le système, il faut pas contrôler si l'utilisateur de la UC Suite effectuant la demande dispose de l'autorisation relative à cet appel, dans la zone **Restriction pour les appels UC** décochez la case **Restriction pour les appels UC**.
6) Cliquez sur **Appliquer**.

12.2 Clients UC Suite

Les clients UC Suite offrent aux abonnés des interfaces utilisateur conviviales pour des fonctions de communications unifiées complètes.

Le système propose les clients UC Suite suivants pour les appareils suivants :

Type de client	Client	Appareil
Client de communication	myPortal pour ordinateur	PC
	myPortail pour Outlook	
	myPortal au travail	
	Imprimante fax	
	mon assistant	
Client mobile	Mitel WX (voir Mobilité)	Smartphone, tablette PC
Client du centre de contact	monAgent (voir Centre de contacts multimédia)	PC
	mes rapports (voir Centre de contacts multimédia)	

Les abonnés ayant configuré une adresse e-mail reçoivent un e-mail de bienvenue contenant les instructions de démarrage.

Paramètres personnalisés

Les paramètres personnalisés (c'est-à-dire spécifiques à l'abonné) de myPortal pour ordinateur de bureau sont stockés dans des fichiers ini sur le PC. Un fichier ini distinct est créé pour chaque utilisateur. Les paramètres personnalisés de myPortal pour Outlook, de myAttendant et de l'imprimante fax sont stockés dans le registre du PC. Cela permet à différents utilisateurs d'utiliser les applications myPortal for Desktop, myPortal for Outlook, my Attendant et Fax Printer sur un seul PC (partage de bureau) ainsi que le déploiement dans les environnements Windows Terminal Server et Citrix Server. Cela permet à différents utilisateurs d'accéder aux applications depuis leurs PC sans installation locale.

12.2.1 myPortal for Desktop

myPortal for Desktop est un client pour Unified Communications sur votre PC. En dehors des aides confortables à la numérotation avec répertoires et favoris, des informations sur la présence des autres abonnés, l'abonné a aussi accès aux messages vocaux et fax, par ex.

myPortal for Desktop offre les fonctionnalités suivantes :

- Répertoires
- Liste des favoris
- Journal
- Numérotation via le bureau
- Fenêtres contextuelles
- État de présence
- Service CallMe avec ONS (One Number Service)
- Renvoi d’appel en fonction de l’état
- Standard automatique personnel
- Gestion des conférences
- Enregistrement des conférences
- Enregistrement des appels
- Messagerie instantanée
- Messages vocaux et fax

12.2.2 myPortal @work

myPortal @work est une application de communications unifiées, qui combine toutes les fonctions et tous les services nécessaires, comme la composition pratique depuis les répertoires téléphoniques, les favoris, les conversations et les informations sur l’état Présence des collègues, en une solution unique pour accélérer la communication quotidienne, améliorer le travail d’équipe et entrer rapidement en contact avec les collègues, les clients et les partenaires.

Remarque : Lorsque le client VoIP myportal@work est utilisé en combinaison avec d'autres clients UC Suite, il est recommandé d'utiliser la fonction double appel de

myportal@work plutôt que la fonction double appel commune des clients UC Suite.

myPortal @work peut être utilisé avec les solutions UC Smart et UC Suite. Pour des informations supplémentaires, voir myPortal @work.

12.2.3 myPortal for Outlook

myPortal for Outlook est le client pour les Unified Communications dans Microsoft Outlook (Plug-In) de manière analogique à myPortal for Desktop.

En plus des fonctions de myPortal for Desktop, myPortal for Outlook offre les fonctionnalités supplémentaires suivantes :

- Appeler un contact Outlook
- Comment enregistrer l'expéditeur d'un message vocal comme un contact d'Outlook
- Comment envoyer le message vocal sous forme d’e-mail
- Comment envoyer un message Fax sous forme d'e-mail

12.2.4 Fax Printer (imprimante Fax)

Fax Printer est une application Windows pour l'envoi de messages fax à partir d'autres applications Windows comme Microsoft Word avec pages de garde individualisées.

Fax Printer (imprimante Fax) comprend les composantes suivantes :

- Fax Printer Cover Editor
- Fax Printer Driver - avec les fonctionnalités suivantes :
  - Envoi de fax à des destinataires individuels
  - Répertoires
  - Utilisation des pages de garde centralisées
  - Utilisation de lignes d'en-tête prédéfinies
  - Fax en série
  - Gestion via l'interface utilisateur
  - Gestion à l'aide de la ligne de commande

12.2.5 myAttendant

myAttendant est une application de communications unifiées (Unified Communications) pour fonctions de commutation. En plus des fonctions de commutation conviviales, des aides à la numérotation grâce aux répertoires et aux informations sur l'état Présence des abonnés, il est par ex. également possible d'accéder aux messages Voix et Fax. Messagerie instantanée soutient la communication avec les abonnés internes.

myAttendant offre les fonctionnalités suivantes.

- Fonctions de commutation
- Répertoires

- Journal
- Fenêtre surgissante
- Modifier l'état Présence des utilisateurs
- Enregistrement des appels
- Centre de messagerie
- Boutons utilisateur
- Administration des messages Voix et Fax
- Messagerie instantanée
- Fonctions équipe
- Gestion des conférences

12.2.6 Prérequis pour les clients PC UC Suite

Pour utiliser les clients PC UC Suite, le PC client doit être équipé de la configuration matérielle et logicielle appropriée. Selon la configuration, des droits d'administrateur sont requis pour l'installation et les mises à jour automatiques. Les fonctionnalités disponibles dépendent des licences utilisées.

Remarque : Vous devez impérativement tenir compte des remarques figurant dans le fichier `ReadMe Premier` se trouvant dans répertoire de stockage des fichiers d'installation.

Téléphones

Les clients UC peuvent être utilisés en combinaison avec les téléphones suivants :

- OpenStage HFA et SIP
- Téléphone de bureau OpenScape IP 35G/55G HFA et SIP
- Téléphone de bureau OpenScape IP 35G Eco HFA et SIP
- Téléphone de bureau OpenScape CP 100/200/205/400/600/600E/700/700X HFA et SIP
- Téléphone de bureau OpenScape CP 110/210/410/710 HFA et SIP
- Téléphones SIP compatibles avec 3PCC
- Téléphones analogiques
- Téléphones ISDN
- OpenScape Édition Personnelle HFA et SIP
- optiPoint WL3 professionnel SIP

Les appareils plus anciens (tels que optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 et optiPoint WL2 SIP) sont pris en charge. Les appareils Optiset E ne peuvent pas être utilisés. Pour plus de détails sur les appareils testés et mis sur le marché, veuillez consulter l'avis de mise sur le marché.

Remarque : Le client intégré OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA ne nécessite aucune condition particulière, outre la configuration client standard et la licence.

La section « Favoris » du menu du téléphone contient les touches programmables gratuites et n'a aucun lien avec les

favoris UC. Vous trouverez des informations détaillées sur ces touches et leur utilisation dans la documentation de l'appareil.

Remarque : Pour les téléphones analogiques et DECT, l'indication de message en attente (MWI) n'est pas prise en charge, et seule une prise en charge limitée est disponible pour l'affichage des informations sur le téléphone.

Systèmes d'exploitation

Les clients PC de la suite UC peuvent être utilisés conjointement avec les systèmes d'exploitation suivants :

- Microsoft Windows 11 (64 bits) toutes versions
- Microsoft Windows 10 (64 bits) toutes versions
- Apple macOS 13 / 14 / 15.1 à 15.4

Conseil : Le système d'exploitation utilisé requiert toujours la dernière version de toutes les mises à jour disponibles (Service Packs et correctifs).

La prise en charge des clients PC UC Suite pour Microsoft Office 2003, Microsoft Windows XP et Microsoft Windows Server 2003 prendra fin en même temps que la fin du support de ces produits par Microsoft. Le produit continuera d'être pris en charge, mais ne sera plus testé en détail.

Les droits d'administrateur local sur un PC client sont requis pour l'installation sous Windows, mais pas pour les mises à jour automatiques. Les interfaces utilisateur russe et chinoise de myPortal pour Outlook nécessitent une installation Windows correspondante en russe ou en chinois.

myPortal pour ordinateur de bureau Apple MAC est disponible avec la même interface que sous Microsoft Windows. Cependant, en raison de l'architecture du système d'exploitation macOS d'Apple, les fonctions suivantes ne sont actuellement pas prises en charge :

- Envoi de fax
- Intégration Outlook et Entourage

myPortal pour Outlook est pris en charge dans les environnements Microsoft Office 365. Microsoft Office 365 est une application cloud. Elle comprend, entre autres, un serveur Exchange pour la distribution centralisée des courriels ainsi que les produits Microsoft Office traditionnels. OpenScape Business prend en charge Microsoft Office 365.

Les fonctions suivantes peuvent être utilisées sous Microsoft Office 365 :

- Intégration du calendrier Exchange
- Transfert de courriel

Navigateurs Web

Les navigateurs Web suivants ont été publiés pour la programmation des touches téléphoniques via les clients UC :

- Microsoft Internet Explorer version 10 (ou ultérieure)
- Microsoft Edge

- Mozilla Firefox version 19 (ou ultérieure)
- Google Chrome

Logiciels supplémentaires

Logiciels supplémentaires	myPortal pour ordinateur	mon assistant	myPortail pour Outlook
Oracle Java JRE 1.8.x ou supérieur (32 bits / 64 bits) OpenJDK V8 ou supérieur (32 bits / 64 bits)	X	X	
Microsoft Outlook / Office • 2021 (32 bits / 64 bits) + Office 365 • 2019 (32 bits / 64 bits) • 2016 (32 bits / 64 bits) - Prise en charge, mais ne fait plus partie des tests système - en cas d'erreur, aucune correction logicielle ne sera fournie (fin du support par OpenScape Business)			X
Accès au serveur Microsoft Exchange (pour les contacts et les rendez-vous Outlook) Exchange 2015 / 2013 / 2010 (64 bits)	X		X
Microsoft .NET Framework >= 4.0 (à partir d'Outlook 2010)			X

Remarque : Pour utiliser l'intégration du calendrier Exchange avec Microsoft Small Business Server, l'authentification basée sur un formulaire (FBA) peut devoir être désactivée dans certaines circonstances.

Remarque concernant Java 32 bits ou 64 bits

Pour utiliser la fonction « Importer les contacts Outlook au démarrage » de myPortal pour ordinateur de bureau avec la version 64 bits de Microsoft Office 2013, l'installation de la version 64 bits de Java est requise. Si cette fonction n'est pas utilisée, la version Java 32 bits est recommandée, car ses besoins en mémoire sont nettement inférieurs. Pour cette raison, la version 32 bits d'Oracle Java ou d'OpenJDK est généralement recommandée pour toutes les autres installations également.

Remarque : L'utilisation continue de la version existante d'Oracle Java avec OpenScape Business ne nécessite aucune modification. Si un changement de version de Java est nécessaire (par exemple, une mise à niveau d'Oracle Java 7 vers Oracle Java 8 ou vers Open JDK V8), une réinstallation du client de communication est requise.

Configuration matérielle minimale requise

- Processeur 2 GHz
- RAM : 2 GO

- Réseau local 100 Mbps (réseau local 1 Gbps recommandé)
- Résolution d'écran XGA (1024 x 768), myPortal pour Outlook : résolution d'écran SVGA (800 x 600)

Remarque : Les moniteurs 4K ne sont pas pris en charge par myPortal et myAttendant.

Serveur Terminal Microsoft, serveur Citrix XenApp

Les clients PC de la suite UC peuvent être utilisés dans les environnements Microsoft Terminal Server et Citrix Server sous les conditions préalables suivantes :

Conseil : Les environnements Terminal Server et Citrix Server, y compris les services hébergés et les environnements virtuels, sont sous la responsabilité du client.

Conseil : Les environnements serveur Citrix peuvent décoder correctement certains caractères régionaux (par exemple, les trémas allemands).

Systèmes d'exploitation :

- Microsoft Windows Server 2022 64 bits
- Microsoft Windows Server 2019 64 bits
- Serveur Microsoft Windows 2016 64 bits
- Microsoft Windows Server 2025 64 bits

Applications bureautiques :

Microsoft Outlook / Office

- 2021 (32 bits / 64 bits) + Office 365
- 2019 (32 bits / 64 bits)
- 2016 (32 bits / 64 bits) - Prise en charge, mais ne fait plus partie des tests système - en cas d'erreur, aucune correction logicielle ne sera fournie (fin du support par OpenScape Business)

Configuration matérielle requise :

Le nombre de clients installables dépend des performances du serveur et de la quantité de mémoire disponible. Si le serveur est également utilisé pour d'autres applications, leurs besoins en mémoire doivent également être pris en compte.

Fichiers d'installation

Les options suivantes sont disponibles pour fournir les fichiers d'installation aux utilisateurs :

- L'administrateur télécharge les fichiers d'installation depuis le **Service Center** et les met à disposition des utilisateurs via un lecteur réseau, par exemple.
- L'administrateur télécharge également le référentiel d'installation hors ligne à partir de l'exemple.

- L'administrateur peut également télécharger le référentiel d'installation hors ligne depuis le **Centre de services** , et les clients peuvent être installés hors ligne.

12.2.7 Installation/Désinstallation silencieuse pour PC client UC Suite

L’installation/la désinstallation silencieuse est une méthode basée sur des lignes de commande permettant l’installation, la désinstallation et la modification automatiques des PC clients UC Suite, sans avoir à effectuer d’autres entrées.

Remarque : Vous devez impérativement tenir compte des remarques figurant dans le fichier `ReadMe first.rtf`.

L’installation/la désinstallation silencieuse nécessite des droits d’administration locaux sur le PC concerné. L'installation/la désinstallation silencieuse permet de consigner le déroulement dans un fichier.

Pour l’installation/désinstallation Silent, les paramètres suivants sont disponibles.

Paramètres	Composantes
`/quiet`	Démarre la procédure d’installation sans intervention de la part de l’utilisateur et sans interface utilisateur. Ce paramètre demande que le référentiel soit déjà trouvé.
`/repository`	Configure l’adresse IP ou le nom d’hôte à utiliser durant l’installation. Par exemple, `/repository=192.168.50.50`
`/installpath`	Configure le chemin des clients installés. La valeur par défaut est : `C:\Program Files(x86)\communicationsclients\`
`/autostart`	Démarre la procédure d’installation sans intervention de l’utilisateur. Ce paramètre demande que le référentiel soit déjà trouvé.
`/i`	Sélectionne un produit à installer. Les valeurs disponibles sont `OLI`, `myPortal`, `myAgent`, `FPD`, `myReports` et `all`. Par exemple : `/i="OLI,FPD"`
`/u`	Sélectionne un produit à supprimer. Par exemple : `/u="OLI,FPD"`

Paramètres	Composantes
`/set`	Sélectionne les produits devant être installés dans le système. Cette option permet d'installer les produits sélectionnés, ou de les modifier s'ils sont déjà installés. Elle permet également d'effacer les produits installés et non listés. Par exemple : `/set="OLI,FPD"`
`/repair`	Répare les produits spécifiés. Par exemple : `/repair="OLI,FPD"`

12.2.7.1 Comment effectuer l'installation silencieuse

Conditions préalables

Votre PC répond aux conditions nécessaires UC Suite PC-Clients.

Vous disposez de droits d'administration locaux sur le PC Client.

Le fichier `CommunicationsClients.exe` est disponible sur le PC client.

Remarque : Vous devez impérativement tenir compte des remarques figurant dans le fichier `ReadMe first`.

Utilisez les lignes de commande suivant les modèles suivants dans un fichier batch ou dans une fenêtre avec les invitations de saisie DOS.

Étape par étape

1) Si vous ne souhaitez pas enregistrer le déroulement, exécutez l'une des commandes suivantes :

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i=all /quiet
   ```

   Où `<IP-address>` doit être remplacé par l'adresse IP des clients UC.

2) Si vous souhaitez enregistrer le déroulement dans un fichier, par exemple, dans `C:\ccuninstall.log`, exécutez l'une des commandes suivantes :

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i="myPortal,FPD" /quiet /l="C:\ccinstall.log"
   ```

   Où `<IP-address>` doit être remplacé par l'adresse IP des clients UC. La commande ci-dessus installe uniquement myPortal for Desktop et FaxPrinter. Vous pouvez la modifier pour installer les clients que vous souhaitez.

12.2.7.2 Comment effectuer une désinstallation silencieuse

Conditions préalables

Votre PC répond aux conditions nécessaires UC Suite PC-Clients.

Vous disposez de droits d'administration locaux sur le PC Client.

Le fichier `CommunicationsClients.exe` est disponible sur le PC client.

Remarque : Vous devez impérativement tenir compte des remarques figurant dans le fichier `ReadMe first`.

Utilisez les lignes de commande suivant les modèles suivants dans un fichier batch ou dans une fenêtre avec les invitations de saisie DOS.

Étape par étape

1) Si, après la dernière installation Silent, une mise à jour du système de communication a eu lieu, répétez avec le nouveau fichier `CommunicationsClients.exe` exactement les lignes d'instruction que vous avez effectuées avec le fichier précédent `CommunicationsClients.exe` (comme si vous vouliez installer de nouveau les composantes déjà en place à l'aide du nouveau fichier `CommunicationsClients.exe`). C'est seulement ensuite que la désinstallation Silent est possible.
2) Si vous ne souhaitez pas enregistrer le déroulement, sélectionnez l'une des lignes de commande suivantes.
   - Si vous souhaitez désinstaller toutes les composantes.

     ```
     CommunicationsClients.exe /quiet /u=all
     ```
   - Si vous souhaitez désinstaller plusieurs composantes, indiquez leurs paramètres sous la forme d'une énumération, séparée par des virgules, après `/u=`, par ex. myPortal for Desktop / myAttendant et Fax Printer :

     ```
     CommunicationsClients.exe /quiet /u="myPortal,FPD"
     ```
   - Si vous souhaitez désinstaller uniquement une composante, indiquez le paramètre correspondant après `/u=`, par exemple, myPortal for Desktop / myAttendant :

     ```
     CommunicationsClients.exe /quiet /u=myPortal
     ```
3) Si vous souhaitez enregistrer le déroulement dans un fichier, par ex. `C:\ccuninstall.log`, sélectionnez l'une des lignes de commande suivantes.
   - Si vous souhaitez désinstaller toutes les composantes.

     ```
     CommunicationsClients.exe /quiet /l="C:
     \ccuninstall.log" /u=all
     ```
   - Si vous souhaitez désinstaller plusieurs composantes, indiquez leurs paramètres sous la forme d'une énumération, séparée par des virgules, après `/u=`, par ex. myPortal for Desktop / myAttendant et Fax Printer :

     ```
     CommunicationsClients.exe /quiet /l="C:
     \ccuninstall.log" /u="myPortal,FPD"
     ```
   - Si vous souhaitez désinstaller uniquement une composante, indiquez le paramètre correspondant après `/u=`, par exemple, myPortal for Desktop / myAttendant :

     ```
     CommunicationsClients.exe /quiet /l="C:
     \ccuninstall.log" /u=myPortal
     ```

12.2.8 Mise à jour automatique

Les mises à jour automatiques maintiennent les clients UC à l'état le plus récent.

Si une nouvelle version est disponible, elle est automatiquement actualisée ou bien il est fourni des informations sur la possibilité d'une actualisation. Le cas échéant, un message s'affiche précisant que l'utilisateur doit fermer une ou plusieurs applications pour être en mesure d'effectuer la mise à jour.

Remarque : Il est recommandé de toujours effectuer les mises à jour qui sont proposées. Ce cas de figure s'applique aussi aux logiciels qui sont nécessaires pour des clients UC définis.

Remarque : La mise automatique de myPortal @work n'est pas prise en charge sur MacOS.

12.3 Utilisateurs et profils utilisateur de UC Suite

Les utilisateurs de UC Suite sont des abonnés qui utilisent UC Clients de UC Suite. Les profils utilisateur enregistrent les paramètres des utilisateurs de UC Suite.

12.3.1 Utilisateurs de UC Suite

Les utilisateurs de UC Suite utilisent les clients UC de la UC Suite. Les paramètres des utilisateurs de UC Suite peuvent être configurés dans le répertoire Utilisateurs.

Le répertoire Utilisateurs contient tous les abonnés du système. Pour l'utilisation des clients UC, il faut en plus configurer des données utilisateur supplémentaires dans le répertoire Utilisateurs.

Dans le répertoire utilisateur, il est affiché les informations suivantes à propos de chaque utilisateur.

- Icône de l'état de présence

  L'administrateur peut modifier l'état de présence de chaque utilisateur.
- **Poste**
- **Nom d'utilisateur**

  Remarque : Bien qu'UCSuite autorise et prenne en charge la modification des noms d'utilisateur pour ses propres clients, de telles modifications pourraient néanmoins affecter la connexion de clients non UCSuite tels que myPortalToGo/ myPortal@Work (le cas échéant), ce qui n'est donc pas recommandé dans de telles situations.

- **Nom**

  Prénom et nom, avec la même configuration que pour l'abonné.

- **Département**

  Dans le cas où un département est affecté à l'utilisateur.
- **E-mail**

  Adresse e-mail
- **Agent actuel**

  Niveau d'agent dans le centre d'appels multimédia.
- **Boîte vocale**

  L'utilisateur peut recevoir des messages vocaux.
- **Renvoi d’appel**

  Un renvoi d'appel a été configuré pour l'utilisateur.

La fonctionnalité de recherche est également disponible pour les champs du répertoire utilisateur.

Les données d'abonné suivantes peuvent être configurées :

Valeurs et paramètres	Index
Données personnelles	
Mes données personnelles	Propre nom, nom d'utilisateur, mot de passe, adresse e-mail, département, numéros de téléphone supplémentaires
Ma photo	Ma photo Formats de fichiers pris en charge : BMP, JPG/ JPEG/JFIFI, PNG. Taille maximale du fichier: 10 Mo
Niveau utilisateur	Réception de messages Voix : voir Abonnés Utilisateur en tant que poste opérateur : voir Abonnés Utilisateur en tant qu’agent : voir Abonnés
Mes Préférences	
Représentation	Couleurs de l'habillage, langue de l'interface utilisateur
Notifications	Fenêtres contextuelles
Association au calendrier	Définition automatique de rendez-vous Outlook en cas d'absence, Actualisation automatique de l'état de présence par les rendez-vous Outlook/ iCal
Touches de raccourci	Touche de raccourci pour fonctions
Divers	Réinitialisation automatique de l'état de présence, Méthode de transfert, Durée de conservation des entrées Journal, Adresse du serveur, Touches de fonction du téléphone
Règles d'appel	
Destinations de renvoi	Renvoi d’appel en fonction de l’état
Moteur de règles	Renvoi d'appel basé sur une règle

Valeurs et paramètres	Index
Communications	
Paramètres de messagerie vocale	Mode enregistrement ou annonce, langue de la boîte vocale
Notification MV	Service de notification pour les nouveaux messages
Notification fax	Service de notification pour les nouveaux messages
Profils	
Occupé, Pas de réponse, Réunion, Maladie, Pause, Déplacement, Congé, Déjeuner, Domicile	Profil pour standard automatique personnel
Sensibilité	
Sécurité et accès	Consultation de vos messages Voix et Fax par le poste opérateur, interrogation du mot de passe de la boîte vocale.
Visibilité de l'état de présence	Visibilité de votre état de présence pour les autres
État de présence de boîte vocale	Annonce concernant votre état de présence pour appelants externes, annonce concernant votre état de présence pour certains appelants
Autoriser d’autres utilisateurs à copier ma disposition BLF	Autoriser d’autres utilisateurs à copier les groupes et boutons BLF Cette option n’est pas disponible pour les profils existants.
myAttendant	
Messages LAN	Module de texte pour messages instantanés
SDA	MSN
Communications	Destinations de renvoi

Vous trouverez des informations plus précises sur la configuration des utilisateurs dans les modes d'emploi des clients UC, en sélectionnant les mots clés figurant dans le tableau.

Le mot de passe pour clients UC compte six positions par défaut. La longueur du mot de passe peut être adaptée au propre besoin (6-10 positions). Le nombre maximal de caractères répétés est de deux et le nombre maximal de caractères consécutifs est de trois. Le nom du compte (inversé ou non) ne peut pas faire partie du mot de passe et le changement de mot de passe nécessite de connaître l'ancien mot de passe. L'utilisateur est obligé de changer le mot de passe par défaut après la première utilisation. Le nombre maximal de tentatives de connexion infructueuses est de cinq. Un administrateur de profil **Advanced** peut modifier le mot de passe d'un utilisateur (par ex. parce que l'utilisateur a oublié de le faire).

Remarque : Le prénom et le nom d'un utilisateur sont remplacés dans le répertoire utilisateur lorsqu'ils sont modifiés par un assistant ou en mode Expert. Si en revanche le prénom et le nom d'un utilisateur sont modifiés dans le répertoire utilisateur, les données de l'utilisateur, qui sont affichées via un Assistant ou en mode Expert ne sont pas écrasées. Dans ce cas, il existe deux noms d'utilisateur différents pour le même utilisateur. De plus, si la longueur du prénom et la longueur du nom de famille est supérieure à 16 caractères au total, elle sera réduite à 16 afin d'être ajustée à l'afficheur de l'appareil.

Les abonnés pour lesquels une adresse e-mail est configurée et qui utilisent myPortal for Desktop reçoivent un e-mail d'accueil avec des instructions concernant les premières étapes.

Réinitialiser les données utilisateur

Les paramètres d'un utilisateur peuvent être replacés aux valeurs par défaut. La réinitialisation des données de l'utilisateur supprime toutes les données de l'utilisateur, y compris le prénom, le nom et le nom de connexion.

Si l'utilisateur a ou non un prénom ou un nom défini via **WBM** > **Mode expert** > **Serveur de téléphonie** > **Abonné**En réinitialisant cet utilisateur via UC Suite, le numéro stocké comme extension sera également attribué dans le champ "**Nom**".

12.3.1.1 Comment configurer un utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**. Tous les utilisateurs sont présentés.
4) Sélectionnez l'utilisateur souhaité et cliquez sur **Modifier**.
5) Modifiez les données de l'utilisateur.
6) Cliquez sur **Sauvegarder**. La fenêtre est automatiquement fermée. Tous les utilisateurs sont présentés.
7) Si vous souhaitez configurer un autre utilisateur, répétez les étapes 4 à 6.

12.3.1.2 Comment réinitialiser un utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**. Tous les utilisateurs sont présentés.
4) Sélectionnez l'utilisateur souhaité et cliquez sur **Réinitialiser les utilisateurs**.
5) Cliquez sur **Sauvegarder**. La fenêtre est automatiquement fermée. Tous les utilisateurs sont présentés.
6) Si vous souhaitez réinitialiser un autre utilisateur, répétez les étapes 4 et 5.

12.3.1.3 Comment configurer un utilisateur de la suite UC comme agent

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**. Tous les utilisateurs sont présentés.
4) Cliquez dans la ligne de l'utilisateur correspondant.
5) Cliquez sur **Modifier**.
6) Dans l'arborescence du menu, cliquez sur **Données personnelles** > **Niveau utilisateur**.
7) Sélectionnez une des possibilités suivantes :

   Si l'agent doit être disponible de manière durable, coche la case **Agent disponible de manière durable**. L'agent demeure ensuite disponible pour les appels, fax et e-mails, même s'il n'a pas répondu à un appel, un fax ou un e-mail.

   Si l'agent ne doit pas être durablement disponible, décochez la case **Agent disponible de manière durable**. L'agent est désigné par l'état non disponible s'il n'a pas répondu à un appel, un fax ou un e-mail.
8) Dans la liste déroulante **Niveau**, sélectionnez le rôle souhaité pour cet agent : **Agent**, **Superviseur** ou **Administrator**.
9) Cliquez sur **Sauvegarder**.
10) Si vous souhaitez configurer un autre utilisateur en tant qu'agent, répétez les étapes 4 à 9.

12.3.1.4 Comment modifier l'état Présence pour un utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Avancé**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**. Tous les utilisateurs sont présentés.
4) Sélectionnez l'utilisateur souhaité.
5) Cliquez sur l'icône de l'état de présence et sélectionnez l'état de présence approprié dans la liste déroulante. Si nécessaire, indiquez l'heure de retour au format `aaaa/mm/jj hh:mm`, par exemple, `2012/12/12 12:00`.
6) Cliquez sur **Sauvegarder**.
7) Si vous souhaitez modifier l'état de présence d'un autre utilisateur, répétez les étapes 4 à 6.
8) Fermez la fenêtre.

12.3.1.5 Comment changer le mot de passe pour un utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**. Tous les utilisateurs sont présentés.
4) Sélectionnez l'utilisateur correspondant et cliquez sur **Modifier** > **Données personnelles** > **Mes données personnelles**
5) Dans **Mot de passe** cliquez sur **Modifier**.
6) Dans **Nouveau**, entrez le nouveau mot de passe.
7) Dans **Confirmer**, entrez le nouveau mot de passe.
8) Cliquez sur **OK**. La fenêtre est automatiquement fermée. Tous les utilisateurs sont présentés.
9) Si vous souhaitez changer le mot de passe d'un autre utilisateur, répétez les étapes 44à 8.

Étapes suivantes

Informez le/les utilisateur(s) concernés du nouveau mot de passe.

12.3.1.6 Comment modifier la longueur du mot de passe pour un utilisateur de UC Suite

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Paramètres généraux**.
5) Dans la zone **Longueurs**, entrez la longueur minimale du mot de passe (6-10) dans le champ **Longueur du mot de passe**.
6) Cliquez sur **Enregistrer**.

12.3.2 Profils utilisateur de UC Suite

Enregistrer les profils utilisateur de UC Suite Paramétrage des utilisateurs de UC Suite. Il est possible d'affecter plusieurs utilisateurs (membres) à un profil d'utilisateur. Tous les membres de ce profil ont les mêmes paramètres.

Chaque utilisateur peut être membre d'un profil utilisateur au plus. Des modifications directes apportées aux paramètres d'un utilisateur - donc pas en utilisant le profil qui représente le niveau supérieur - conduisent automatiquement à l'effacement de l'utilisateur dans le profil.

Si un utilisateur n'est pas affecté à un profil, il conserve les paramètres représentés par ce profil.

Lorsqu'un utilisateur est déjà affecté à un profil, seules les modifications apportées aux éléments de profil verrouillés s'appliquent à cet utilisateur. Si l'icône de verrouillage est déverrouillée, les modifications ne s'appliquent pas.

Si un profil entier est supprimé, les utilisateurs affectés à ce profil conservent également les paramètres de ce profil.

Les valeurs et paramètres suivants peuvent être configurés.

Options de menu	Valeur et Paramètres de
Données personnelles	
Mes données personnelles	Visibilité des numéros de téléphone
Mes Préférences	
Apparence	Couleurs de l'habillage, langue de l'interface utilisateur
Notifications	Fenêtres contextuelles
Connexion Outlook	Définition automatique de rendez-vous Outlook en cas d'absence, Actualisation automatique de l'état de présence par les rendez-vous Outlook/iCal
Touches de raccourci	Activation et configuration des combinaisons de touches pour accéder aux différentes fonctions couramment utilisées via le clavier. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.

Options de menu	Valeur et Paramètres de
Divers	Réinitialisation automatique de l'état de présence, Méthode de transfert, Durée de conservation des entrées Journal, Adresse du serveur
Règles d'appel	
Destinations de renvoi	Renvoi d'appel en fonction de l'état
Communications	
Paramètres de messagerie vocale	Mode enregistrement ou annonce, langue de la boîte vocale
Notification MV	Service de notification pour les nouveaux messages
Notification fax	Service de notification pour les nouveaux messages
Notifications d'appel manqués	Service de notification pour les appels manqués
Profils MV	
Profils MV	Profil pour standard automatique personnel. États disponibles : Occupé, Pas de réponse, Réunion, Maladie, Pause, Déplacement, Congé, Déjeuner, À domicile
Sensibilité	
Sécurité et accès	Consultation de vos messages Voix et Fax par le poste opérateur, interrogation du mot de passe de la boîte vocale.
Visibilité de l'état de présence	Visibilité de votre état de présence pour les autres
État de présence de boîte vocale	Annonce concernant votre état de présence pour appelants externes, annonce concernant votre état de présence pour certains appelants
Favoris	
Favoris	Groupes Favoris avec une liste de contacts pouvant être attribués à l'utilisateur.

Vous trouverez des informations plus précises sur les paramètres des profils utilisateur dans les modes d'emploi des clients UC, en sélectionnant les mots clés figurant dans le tableau.

12.3.2.1 Comment ajouter un profil utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Profils MV**. Tous les profils d'utilisateur existants et leurs membres sont présentés.
4) Cliquez sur **Ajouter**.
5) Indiquez dans **Nom** le nom que vous souhaitez donner au profil.
6) Cliquez sur **Sauvegarder**.
7) Configuez les paramètres souhaités du profil utilisateur.
8) Cliquez sur **Enregistrer** et fermez la fenêtre.

12.3.2.2 Comment modifier un profil utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Profils MV**. Tous les profils existants et leurs utilisateurs vous sont présentés.
4) Sélectionnez le profil souhaité.
5) Cliquez sur **Modifier**.
6) Modifiez les valeurs et paramètres souhaités.

   Remarque : Cliquez sur **Sauvegarder** avant de sélectionner une autre option de menu afin que vos modifications soient enregistrées.

7) Ensuite, cliquez sur **Enregistrer** et fermez la fenêtre.

12.3.2.3 Comment afficher les profils utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Profils MV**. Tous les profils d'utilisateur existants et leurs membres sont présentés.

12.3.2.4 Comment ajouter des membres à un profil utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Profils MV**. Tous les profils d'utilisateur existants et leurs membres sont présentés.
4) Sélectionnez le profil d'utilisateur souhaité et cliquez sur **Affecter les utilisateurs**.
5) Dans la liste **Utilisateurs disponibles**, sélectionnez les membres souhaités.
6) Cliquez sur **<-** pour les intégrer dans la liste des **Utilisateurs affectés**.

   Tous les profils d'abonné existants et leurs membres sont affichés.
7) Fermez la fenêtre.

12.3.2.5 Comment effacer des membres dans un profil utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Profils MV**. Tous les profils d'utilisateur existants et leurs membres sont présentés.
4) Sélectionnez le profil d'utilisateur souhaité et cliquez sur **Affecter les utilisateurs**.
5) Dans la liste **Utilisateurs affectés** sélectionnez les membres concernés.
6) Utilisez **->** pour les intégrer dans la liste **Utilisateurs disponibles**.

   Tous les profils d'abonné existants et leurs membres sont affichés.
7) Fermez la fenêtre.

12.3.2.6 Comment effacer un profil utilisateur de UC Suite

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Profils MV**. Tous les profils d'utilisateur existants et leurs membres sont présentés.
4) Sélectionnez le profil d'utilisateur souhaité.

5) Cliquez sur **Supprimer**.
6) Confirmez avec **OK**. Tous les profils d'abonné existants et leurs membres sont affichés.
7) Fermez la fenêtre.

12.4 Etat Présence et Service CallMe

L'état Présence et le service CallMe affichent et optimisent la disponibilité des abonnés. L'état Présence permet un renvoi d'appel simple en fonction de l'état ainsi qu'un renvoi d'appel flexible, basé sur une règle, configurable par myPortal for Desktop ou myPortal for Outlook.

12.4.1 État de présence (Présence)

L'état Présence indique dans la liste des favoris, dans le répertoire interne, dans la salle de conférence virtuelle et dans les annonces de la boîte vocale la disponibilité des abonnés internes (y compris les abonnés mobiles). De plus, l'état de présence gère la disponibilité des abonnés internes à l'aide du renvoi d'appel en fonction de l'état, du renvoi d'appel basé sur une règle et du standard automatique personnel.

En tant qu'abonné, vous pouvez modifier votre état Présence dans myPortal for Desktop, myPortal for Outlook ou via le menu de la boîte vocale. Lorsque vous désactivez le renvoi d'appel sur le téléphone, vous revenez à l'état de présence **Bureau**. Lors de chaque modification de l'état de présence, sauf pour **Bureau** et **Appelle-moi**, vous pouvez définir le moment prévu de retour à l'état **Bureau**ou **Appelle-moi**.

En tant qu'abonné, vous pouvez sélectionner les états suivants :

- **Bureau**
- **Réunion**
- **Maladie**
- **Pause**
- **Déplacement**
- **Congé**
- **Déjeuner**
- **Domicile**
- **Ne pas déranger**

Remarque : L'administrateur système peut activer/désactiver la visibilité de l'état « Maladie » dans l'administration du système. Voir OpenScape Business UC Suite > Serveur

---

Renvoi vers la boîte vocale

Lorsque l'État de présence d'un abonné n'est ni **Bureau** ni **Appelle-moi**, le système de communication renvoie les appels qui lui sont adressés vers la messagerie vocale et informe, à l'aide des annonces correspondant à l'État, sur le type de son absence et sur la date de retour prévue.

Texte d'information

Dans votre état de présence actuel, vous pouvez entrer un texte d'information quelconque, par ex. en cas de réunion "Je suis dans le bureau n° ...". Le texte d'information est affiché dans la liste des favoris, dans le répertoire interne et dans la salle de conférence virtuelle. Lorsque votre état de présence est modifié, le texte d'information est effacé.

Réinitialisation automatique de l'état de présence

En tant qu'abonné, vous pouvez, à la fin prévue de votre absence, réinitialiser automatiquement l'État de présence sur **Bureau**. Sinon, le système prolonge l'état Présence actuel par périodes de 15 minutes jusqu'à ce que vous le modifiez vous-même.

Visibilité de votre état de présence

En tant qu'abonné, vous pouvez, pour chaque abonné du répertoire interne, déterminer si celui-ci est autorisé à visualiser votre État de présence autre que **Bureau** et **Appelle-moi** ainsi que la date prévue de votre retour et le texte d'information que vous avez éventuellement inscrit.

Remarque : Les paramètres de visibilité ne s'appliquent pas aux utilisateurs de myAttendant, car ces utilisateurs peuvent toujours voir l'état de présence des autres utilisateurs.

Actualisation automatique de l'état Présence par les rendez-vous Outlook/ iCal

En tant qu'abonné, vous pouvez gérer automatiquement votre état Présence à l'aide des rendez-vous (pas ceux refusés ou uniquement proposés, toutefois) en vous servant de certains mots-clés figurant dans l'objet. Vous avez le choix entre les calendriers suivants :

- Calendrier Exchange (sur Microsoft Exchange Server)

  L'actualisation automatique de l'état de présence par les rendez-vous Outlook se produit indépendamment du fait que votre PC soit en service ou non. Pour cette fonction, l'administrateur doit configurer l'intégration du calendrier Exchange.

  Remarque : Vous trouverez des détails sur les différentes versions de Microsoft Exchange Server dans Unify Experts Wiki sous : `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

- Calendrier Outlook

  L'actualisation automatique de l'état Présence par les rendez-vous Outlook nécessite que myPortal for Desktop ou myPortal for Outlook soit démarré sur votre PC.
- Calendrier iCal (myPortal for Desktop)

Vous pouvez utiliser les mots-clés suivants :

- **Réunion**
- **Maladie**
- **Pause**
- **Déplacement**

- **Congé**
- **Déjeuner**
- **Domicile**

Les mots-clés dépendent de la langue configurée pour l'interface utilisateur. Les mots-clés peuvent figurer à n'importe quel endroit de l'objet. Lorsque l'objet contient plusieurs de ces mots-clés, seul le premier est pris en compte. Lorsque cette fonction est activée, votre état de présence est automatiquement modifié au début et à la fin du rendez-vous correspondant. La vérification des rendez-vous dans le calendrier se produit à intervalles de 30 s.

Remarque : Lorsque vous activez cette fonction, vous devez savoir que certains rendez-vous contenant certains mots-clés peuvent provoquer des modifications non souhaitées de votre état Présence. Si nécessaire, il faut modifier l'objet.

Remarque : L'état de présence Maladie peut ne pas être disponible, en fonction des paramètres système que l'administrateur a définis.

Définition automatique des rendez-vous Outlook en cas d'absence (Windows)

En tant qu'abonné, vous pouvez, durant votre absence, générer automatiquement certains rendez-vous Outlook par modification de votre état Présence. L'objet du rendez-vous Outlook correspondant se compose de l'état de présence et du texte "(Auto)", par ex. "Réunion (Auto)". Heure de début et heure de fin du rendez-vous correspondant conformément à vos indications dans myPortal for Desktop ou myPortal for Outlook. L'heure de fin du rendez-vous Outlook n'est pas modifiée même en cas de retour en retard. Vous pouvez déterminer si les rendez-vous Outlook sont enregistrés dans le fichier PST local ou dans le serveur Exchange. Dans le cas du fichier PST local, votre Outlook doit être ouvert pour créer des rendez-vous Outlook. Dans le cas du serveur Exchange, les rendez-vous Outlook sont créés, indépendamment du fait que votre Outlook est ouvert ou fermé. Pour cette fonction, l'administrateur doit configurer l'intégration du calendrier Exchange.

Remarque : Vous trouverez des détails sur les différentes versions de Microsoft Exchange Server dans Unify Experts Wiki sous : `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

Fenêtres contextuelles en cas de modification de l'état de présence

Vous pouvez faire afficher dans des fenêtres surgissantes les modifications de votre état Présence.

12.4.2 Service CallMe

Grâce au service CallMe, l'abonné peut définir comme destination CallMe un téléphone quelconque d'un autre poste de travail sur lequel il pourra être joint à l'aide de son numéro de téléphone interne. L'abonné peut utiliser myPortal for Desktop ou myPortal for Outlook sur sont poste de travail alternatif comme sur

son bureau et ainsi effectuer aussi les appels sortants à partir de la destination CallMe.

Appels entrants

Les appels entrants destinés à votre numéro de téléphone interne sont renvoyés vers la destination Appelle-moi. Chez l'appelant, il s'affiche le numéro de téléphone interne de l'abonné appelé. Les appels non répondus sont renvoyés à la boîte vocale au bout de 60 secondes.

Appels sortants

Pour les appels sortants avec myPortal for Desktop ou myPortal for Outlook, le système de communication établit deux connexions. Dans un premier temps, le système de communication appelle l'abonné sur la destination Appelle-moi. Lorsque celui-ci répond à l'appel, le système de communication appelle la destination souhaitée et établit la connexion. Le numéro de téléphone interne de l'appelant est affiché chez le destinataire (One Number Service).

Etat Présence

Lorsque le service Appelle-moi est activé, l'écran du téléphone concerné affiche "`Appelle-moi activé`" (ne concerne pas les téléphones analogiques et les téléphones DECT). Les autres abonnés voient l'état Présence **Bureau**.

Activation

En tant qu'abonné, vous pouvez activer manuellement le service Appelle-moi. De plus, si le service Appelle-moi était actif auparavant, il est de nouveau activé par la réinitialisation automatique de l'état Présence après une absence. Les types suivants de destinations Appelle-moi ne sont pas supportés :

- Groupe
- Téléphone renvoyé

Affichage de la destination CallMe dans la liste des favoris

En tant qu'abonné, à la place de votre numéro de téléphone, vous pouvez afficher le numéro de votre destination CallMe dans la liste des favoris d'autres abonnés.

Désactiver

Der service Appelle-moi demeure activé jusqu'à la modification de votre état Présence.

Remarque : La fonction Appelle-moi ne doit pas être utilisée lorsque vous composez une conférence ouverte ou vous y faites un appel.

12.4.3 Renvoi d'appel en fonction de l'état

Grâce au renvoi d'appel en fonction de l'état, vous pouvez, en fonction de votre état Présence, renvoyer l'appelant vers l'un de vos numéros de téléphone supplémentaires ou vers une boîte vocale.

En tant qu'abonné, vous pouvez configurer le renvoi d'appel en fonction de l'état pour tous les états de présence, sauf pour **Bureau**, **Appelle-moi** et **Ne pas déranger**. Lorsque vous modifiez votre état Présence, le système de communication active le renvoi d'appel en direction de la destination configurée pour le cas concerné, par ex. lorsque vous êtes en déplacement en direction de votre téléphone portable et durant vos congés en direction de votre représentant.

12.4.4 Renvoi d’appel basé sur une règle

Avec le renvoi d’appel basé sur une règle, l’abonné peut effectuer le renvoi d’appel de manière plus souple qu’avec le renvoi d’appel basé sur l’état grâce à de multiples conditions et exceptions.

De plus, le renvoi d’appel basé sur une règle prend en charge :

- toutes les destinations,
- les états de présence **Bureau**, **Réunion, Maladie, Pause, Déplacement, Congé, Déjeuner, Domicile**.

Remarque : Le renvoi d’appel fondé sur des règles ne s’applique pas à **CallMe** et **MDN**.

En tant qu’abonné, vous pouvez définir des règles et les activer ou désactiver à tout moment avec l’assistant des règles. La règle est uniquement active lorsque votre téléphone n’est pas renvoyé. Un renvoi d’appel en fonction de l’état (sauf vers la boîte vocale) désactive le renvoi d’appel basé sur une règle.

Lorsqu’une règle pour le renvoi d’appel est active, l’écran de votre téléphone affiche **Règle activée**.

À la réception d’un appel entrant, le système de communication vérifie si les règles actives peuvent s’appliquer, conformément à leur ordre dans l’assistant des règles. Seule la première règle applicable est exécutée. Dans ce cas, votre téléphone sonne une fois, avant que le système de communication ne renvoie l’appel vers la destination choisie.

Vous pouvez définir différents types de conditions et d’exceptions (sauf…) dans une règle. Cependant, vous ne pouvez pas définir une condition avec une exception du même type. Par exemple, il est impossible de définir une condition du type « Activé certains jours de la semaine°» en même temps qu’une exception du type « sauf certains jours de la semaine ».

Types des conditions et exceptions

- (sauf) pour un état Présence défini
- (sauf) de certaines personnes (dans le répertoire interne, dans le répertoire externe, dans le répertoire personnel ou d’un numéro quelconque)
- (sauf) transmis à vous par certaines personnes (dans le répertoire interne, dans le répertoire externe, dans le répertoire personnel ou d’un numéro quelconque)
- (sauf) d’un certain type c.-à-d. **Interne**, **Externe** ou **Contact inconnu**
- (sauf) à une date définie (également à plusieurs)
- (sauf) certains jours de la semaine
- (sauf) entre une date de début et une date de fin définies

- (sauf) entre une heure de début et une heure de fin définies

12.5 Répertoires et Journal

Les répertoires, la liste des favoris et le journal organisent les contacts et appels.

12.5.1 Répertoires

Les répertoires organisent les contacts des abonnés. Les abonnés peuvent accéder aux contacts avec UC Suite Clients ou avec les téléphones système avec écran.

Le système fournit les répertoires suivants qui prennent en charge les fonctions suivantes et avec la priorité indiquée ci-dessous pour le numéro de recherche (le numéro de recherche ne sera pris en charge que pour un appel externe et dans le cas où CO/ITSP ne fournit pas le nom) :

Répertoire	**myPortal for Desktop, my Attendant, myAgent, Fax Printer**	**myPortal for Outlook**	**Téléphone système avec écran**
Contacts Outlook Contacts Mac OS (myPortal for Desktop)	Si nécessaire, l'abonné peut importer les contacts Outlook/Mac OS lors du démarrage de myPortal for Desktop sur Windows.	Contient les contacts Outlook personnels d'un abonné. Seul l'abonné concerné a accès en écriture à ces données.	Contient les contacts Outlook personnels d'un abonné. Seul l'abonné concerné a accès en écriture à ces données.
Répertoire personnel	L'abonné peut soit importer les contacts Outlook/ Mac OS lors du démarrage de myPortal for Desktop, soit gérer manuellement les contacts personnels. Il n'est pas possible de modifier les contacts importés.	-	Contacts Outlook importés à l'aide de l'assistant personnel.

Répertoire	myPortal for Desktop, my Attendant, myAgent, Fax Printer	myPortal for Outlook	Téléphone système avec écran
Annuaire interne	L'annuaire interne de UC Smart propose, avec UC Suite, des fonctionnalités supplémentaires. Il contient : • Tous les abonnés internes • Groupes pour lesquels l'affichage est activé dans le système. • Numéros de téléphone supplémentaires, si l'abonné autorise leur consultation par tous les autres abonnés internes Les abonnés internes (avec téléphones système) sont représentés avec l'état de présence et peuvent être contactés à l'aide de la messagerie instantanée. La condition pour l'affichage de l'état de présence d'un abonné est que l'abonné concerné l'autorise. Le cas échéant, le moment du retour prévu est affiché. De plus, le texte d'information éventuellement créé par l'abonné s'affiche. L'abonné dispose uniquement d'un accès en lecture à cet annuaire. L'annuaire interne comprend le répertoire système. Mais les recherches effectuées dans l'annuaire interne n'incluent pas les résultats du répertoire système, uniquement les entrées de l'annuaire interne.		Comprend tous les abonnés et groupes internes pour lesquels l'affichage est activé dans le système.
Annuaire externe	Comprend les contacts d'un répertoire d'entreprise et doit être configuré par l'administrateur. L'abonné a uniquement accès en lecture à ce répertoire.		-
Exchange-Ordner public (non utilisable avec Office 365)	Contient les contacts du dossier Exchange public, si configuré par l'administrateur. Ceux-ci sont affichés dans l'annuaire externe. Vous trouverez des détails sur les différentes versions de Microsoft Exchange Server dans Unify Experts Wiki sous : `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.		-
Répertoire hors ligne externe (LDAP)	Comprend les contacts du répertoire d'entreprise LDAP et doit être configuré par l'administrateur. Le répertoire hors ligne externe n'est utilisable que lors de la recherche. L'administrateur peut activer et désactiver l'affichage du répertoire externe hors ligne pour les téléphones système.		
Répertoire système	Contient tous les numéros système, utilisateurs UC et non UC. Les utilisateurs non UC incluent des abonnés n'ayant pas de licences UC et les abonnés virtuels, tels que les fax ou le standard automatique. Le répertoire système n'est pas valable pour Fax Printer.		Comprend tous les abonnés internes et tous les numéros abrégés centraux. L'administrateur peut activer et désactiver l'affichage d'un abonné dans le répertoire système.

Remarque : Les numéros de téléphone conservés dans les paramètres utilisateurs et tous les répertoires (internes, externes, personnels, Outlook, Exchange) doivent être saisis

au format canonique pour pouvoir être joignables par UC et le périphérique.

Le code d’accès ne doit pas être dans le numéro.

Remarque : Lors de l'ajout ou de la suppression d'un contact UC, il peut s'écouler plusieurs minutes**(et** jusqu'à 30 minutes) avant que les changements ne soient appliqués à tous les clients et appareils en raison des mécanismes de mise en cache utilisés. Il est également possible de redémarrer le système pour que les modifications prennent effet **immédiatement**.

Recherche simple

En tant qu’abonné, vous pouvez effectuer une recherche dans les répertoires par **Prénom**, par **Nom de famille** ou par Numéro. La recherche de répertoires est effectuée selon l’ordre indiqué dans le tableau ci-dessus. La recherche est possible avec un mot complet comme avec une partie de mot, par exemple une partie de numéro d’appel. Les options de recherche paramétrées sont conservées par la suite jusqu’à modification. Tous les termes de recherche utilisés sont sauvegardés. Vous pouvez effacer la liste des termes de recherche utilisés.

Recherche étendue

Vous pouvez rechercher de manière ciblée dans les champs **Titre**, **Prénom**, **Nom de famille**, **Société**, **Poste**, **Tél. société**, **Tél. professionnel 1**, **Tél. professionnel 2**, **Tél. domicile 1**, **Tél. domicile 2**, **Numéro mobile** et **E-mail** et limiter le nombre maximum de résultats. L’interface moderne de myPortal for Desktop ne prend pas en charge la recherche étendue. Dans un équipement, seuls **Tél. professionnel 1**, **Tél. domicile 1**, **Numéro mobile sont pris en charge.**

Tri

Vous pouvez trier les contacts d’un répertoire de myPortal for Desktop et myPortal for Outlook selon une colonne quelconque, par ordre alphanumérique croissant ou décroissant. L’interface moderne de myPortal for Desktop ne prend pas en charge le tri.

12.5.1.1 Comment configurer les répertoires des téléphones système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Vous pouvez sélectionner les répertoires disponibles sur les téléphones système avec écran.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système** > **Affichage**.

4) Dans la liste déroulante **Annuaire**, sélectionner l'une des options ci-après.

- Si vous devez rendre disponible les contacts personnels, le répertoire interne, externe et mise en réseau ainsi que le répertoire LDAP, sélectionnez **Tout**.
- Si vous devez rendre disponible uniquement les contacts personnels, le répertoire interne, externe et mise en réseau, sélectionnez **Interne**.
- Si seul le répertoire LDAP doit être disponible, sélectionnez **LDAP**.
- Si aucun répertoire ne doit être disponible, sélectionnez **Non**.

Remarque : En sélectionnant le **répertoire téléphonique interne via le répertoire unifié**, l'utilisateur peut activer les demandes de recherche/consultation de manière à ce qu'elles soit traitées comme des demandes en direction du répertoire unifié. Lorsque l'indicateur est désactivé et en l'absence d'accès à Unified Directory, la vue de liste du menu du répertoire, établie pour le téléphone OpenScape CP 200/205, n'est pas disponible.

---

5) Cliquez sur **Appliquer**.

Étapes suivantes

Si vous avez sélectionné **Tous** ou **LDAP**, veillez à ce qu'un répertoire LDAP correspondant (par ex. Open Directory Service) soit disponible pur les téléphones système.

12.5.2 Répertoire interne

Le répertoire interne contient les détails de contact des abonnés internes du système de communication. Les clients UC Suite ont accès au répertoire système.

En tant qu'administrateur, vous avez un accès non limité à toutes les données du répertoire interne. En tant qu'abonnés, vous pouvez numéroter à partir du répertoire interne.

L'administrateur peut désactiver l'affichage de tous les abonnés analogiques pour les abonnés analogiques sans nom. Les abonnés dont le nom commence par - ne sont pas affichés dans ce dernier cas

12.5.2.1 Comment activer ou désactiver les abonnés du répertoire interne

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Dans l'arborescence du menu, cliquez sur **Serveur**.
4) Cliquez sur l'onglet **Paramètres généraux**.

5) Dans la zone **Postes analogiques**, sélectionnez dans la liste déroulante **Mode abonné analogique** l'une des possibilités suivantes.
   - Si tous les abonnés analogiques sont affichés dans le répertoire interne, sélectionnez **Afficher Tous**.
   - Si seuls les abonnés analogiques avec un nom dans le répertoire interne doivent être affichés, sélectionnez **Afficher uniquement ceux avec un nom**.

     Remarque : Les abonnés analogiques dont le nom commence par - ne sont pas affichés dans ce cas.

   - Si aucun abonné analogique ne doit être affiché dans le répertoire interne, sélectionnez **Non affiché**.
6) Cliquez sur **Sauvegarder**.

12.5.2.2 Comment activer ou désactiver la recherche du répertoire interne uniquement

Lorsque vous numérotez à partir du nom, vous pouvez décider de limiter la recherche uniquement au répertoire interne, ou rechercher dans tous les répertoires dans l'environnement réseau. Le système est configuré par défaut de manière à rechercher uniquement dans le répertoire interne.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Applications > OpenScape Business UC Suite**.
3) Dans l'arborescence du menu, cliquez sur **Serveurs**.
4) Cliquez sur l'onglet **Paramètres généraux**.
5) Pour activer la recherche uniquement dans le répertoire interne, cochez la case **Sélection par nom Recherche uniquement poste local** dans la zone **Serveur de répertoire**.

   Remarque : La case **Sélection par nom Recherche uniquement poste local** est cochée par défaut.

   Le système recherche uniquement dans le répertoire interne lorsqu'il effectue la numérotation par nom. Lorsque le poste local est atteint, le système utilise le nom du récepteur, s'il a été précédemment enregistré.
6) Pour désactiver la recherche uniquement dans le répertoire interne, décochez la case **Sélection par nom Recherche uniquement poste local** dans la zone **Serveur de répertoire**.

   Le système recherche maintenant dans tous les répertoires de l'environnement réseau lorsqu'il numérote par nom.

12.5.3 Répertoire externe

Le répertoire externe comprend des contacts situés en dehors du système de communication.

Les données du répertoire externe sont disponibles pour tous les abonnés, dans tous les clients UC Suite et sur tous les téléphones avec afficheur. Les abonnés peuvent effectuer une sélection à partir d'un répertoire externe. Les abonnés des clients UC Suite myAttendant et myAgent peuvent modifier les données du répertoire externe.

Importer un fichier CSV

En tant qu'administrateur, vous pouvez importer les contacts dans un fichier CSV avec codage UTF-8, à partir du système de données local ou à partir d'une validation de réseau en direction d'un répertoire externe.

Une ligne d'en-tête du fichier CSV permet d'affecter les noms de champ du fichier CSV aux champs du système. Le fichier CSV peut se présenter par ex. de la manière suivante.

- Lignes d'en-tête :

  "ID client", "Nom de famille", "Prénom", "Numéro de téléphone d'entreprise", "Nom de la société"
- Ligne de données :

  "987654","Dubios","Natalie","+498977712345","Company"

Lors de l'importation, vous pouvez affecter aux champs suivant du système les données du fichier CSV :

- ID client
- Titre
- Prénom
- Nom
- Société
- Tél. professionnel
- Tél. professionnel 2
- Tél. mobile
- Domicile
- Tél. fax
- E-mail
- Ville

Remarque : Le nom du contact sera affiché dans l'historique des appels uniquement si vous remplissez les champs Prénom et Nom.

Après traitement du modèle CSV, il faut enregistrer le fichier au format UTF-8 afin d'assurer l'importation correcte des caractères spéciaux éventuellement présents.

Si vous souhaitez effectuer des remplacements lors de l'importation des données, l'**ID client** correspondant doit être identique.

Remarque : Vous trouverez un modèle CSV et une description de la syntaxe nécessaire à l'importation des données pour le répertoire externe sous **Centre de service** > **Documents** > **Modèles CSV**.

12.5.3.1 Comment importer un fichier CSV depuis le système de fichiers local vers le répertoire externe

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Un fichier CSV adapté, codé UTF-8, comportant des données pour le répertoire externe, est disponible dans le système de données local.

La longueur des champs des modèles CSV est limitée. Ces limitations de longueur sont énumérées ci-dessous :

- customer_business caractère variant(50)
- customer_business2 caractère variant(50)
- customer_home caractère variable(50)
- customer_mobile caractère variable(50)
- customer_title caractère variable(20)
- customer_firstname caractère variable(50)
- customer_surname caractère variable(50)
- customer_company caractère variable(255)
- customer_id caractère variable(255)
- customer_fax caractère variable(50)
- customer_email caractère variable(255)
- customer_city caractère variable(255)
- customer_street_address caractère variable(2048)
- customer_import_source caractère variable(256)

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'**Assistant Répertoire externe**.
4) Cliquez sur l'onglet **Importer le répertoire externe**.
5) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez charger le fichier CSV à partir du système de fichiers local, cochez l'option **Fichier local** et, dans la zone **Chargement du fichier**, accédez au fichier CSV.
   - Si vous souhaitez charger le fichier CSV à partir d'un partage de réseau, sélectionnez la case d'option **Dossier public de Windows** et entrez les données d'accès au partage de réseau (nom du fichier CSV, nom de domaine ainsi que nom d'utilisateur et mot de passe pour le partage) dans la zone **Dossier public de Windows**.

     Vous pouvez vérifier si vos entrées sont correctes en cliquant sur **Test**.
6) Cliquez sur **Choisir un fichier** dans la zone de **Téléchargement un fichier** et sélectionnez le fichier souhaité.

7) Dans le champ **Lignes d'en-tête**, entrez le nombre de lignes d'en-tête du fichier CSV.
8) Indiquez le **séparateur de champs** utilisé dans le fichier CSV.
9) Sélectionner l'une des options suivantes :
   - Si vous souhaitez effacer les données existantes du répertoire externe, cochez la case **Supprimer les données avant l'importation**.
   - Si vous ne voulez pas effacer les données existantes du répertoire externe, décochez la case **Supprimer les données avant l'importation**.

Remarque : L'indicateur **Supprimer les données avant l'importation** ne supprime pas les enregistrements s'ils sont déjà utilisés dans d'autres fonctions, comme par exemple un VIP appelant, etc.

Remarque : L'indicateur **Supprimer les données avant l'importation** ne supprime que les données importées à partir d'un fichier CSV. Les données importées manuellement ne sont pas supprimées afin d'éviter toute perte de données inattendue. La seule façon de supprimer les données saisies manuellement est de les supprimer manuellement.

---

10) Dans la zone **ID client dupliqué**, indiquez comment le système doit réagir lors d'une tentative d'importation de données en cas d'ID client existant :
    - Si vous voulez remplacer les contacts existants par les données provenant du fichier CSV, sélectionnez **Mettre à jour le client existant**.

Remarque : CustomerID est l'identifiant qui détermine si deux enregistrements sont des doublons. Ainsi, on considère que les enregistrements importés avec un CustomerID existant se réfèrent à un client existant et qu'ils seront mis à jour. L'indicateur **Mettre à jour le client existant** ne fonctionne que lorsque l'CustomerID est mis en correspondance lors de l'importation. Il est fortement conseillé de s'appuyer sur le modèle fourni et d'adapter les données en fonction de celui-ci, sans omettre les identifiants uniques.

    - Si vous voulez conserver les contacts existants, sélectionnez **Arrêter l'importation de l'enregistrement actuel**.
11) Cliquez sur **Suivant**.
12) Dans la liste déroulante, sélectionnez dans l'ordre les champs du fichier CSV à attribuer aux champs correspondants du système. Si les champs appropriés n'existent pas ou si vous ne souhaitez pas importer les données, cliquez sur l'option vide.
13) Cliquez sur **Suivant**.
14) Cliquez sur **Importer**. Ne fermez pas cette fenêtre tant que les données sont en cours d'importation. Une fois l'importation terminée, le nombre d'enregistrements importés est indiqué.

12.5.3.2 Comment ajouter l'accès à une base de données externe pour le répertoire externe

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Vous disposez des données pour l'accès à la base de données externe.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Répertoire externe**.
4) Cliquez sur l'onglet **Importer le répertoire externe**.
5) Dans la zone **Chargement du fichier**, cliquez sur **Choisir un fichier** et sélectionnez le fichier souhaité.

12.5.3.3 Comment exporter un fichier CSV depuis l’annuaire externe

Conditions préalables

Vous êtes connecté à l’interface WBM avec le profil **Avancé**.

Étape par étape

1) Cliquez sur **Configuration** dans la barre de navigation.
2) Dans l’arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur l’onglet **Exporter l’annuaire externe**.
4) Sélectionnez l’une des possibilités suivantes :
   - Si vous souhaitez exporter un fichier CSV à partir d’un système de fichiers local, cochez l’option **Fichier local** et cliquez sur **Démarrer**.
   - Si vous souhaitez exporter dans un dossier Windows public, sélectionnez l’option **Dossier Windows public**. Saisissez les valeurs demandées dans les champs suivants :

     - **Nom de fichier**

     - **Nom utilisateur**

     - **Domaine**

     - **Mot de passe**

     Puis cliquez sur le bouton **Démarrer**.

12.5.4 Répertoire hors ligne externe (LDAP)

Le répertoire hors ligne externe (LDAP) contient les contacts d'un serveur LDAP pour myPortal for Desktop, myAgent, Fax Printer, myPortal for Outlook et pour les téléphones système avec afficheur.

Le système supporte LDAP Version 2 avec authentification.

LDAP (Lightweight Directory Access Protocol) est un protocole d'accès Directory basé sur TCP/IP, qui permet d'accéder aux services de répertoire

réseau. LDAP dispose d'un format univoque dans le monde entier où tous les nom peuvent être représentés. Il offre différents layouts et ainsi qu'une correspondance univoque entre le nom et sa représentation interne. De concert avec l'administrateur IT du client, l'administrateur défini ces données lors de la définition du projet. LDAP peut être utilisé sous MS Windows et sous Linux.

Dans un environnement Microsoft, le serveur ADS (Active Directory Server) ou le serveur Exchange joue simultanément le rôle de serveur LDAP. Sous Microsoft Windows, les données utilisateur peuvent être gérées à l'aide de l'application Active Directory ou ESTOS Metadir. La gestion de ces données est effectuée généralement par l'administrateur IT du client.

Sous Linux, les données utilisateur peuvent par exemple être gérées à l'aide de OpenLDAP.

Un navigateur LDAP (par ex. Freeware de Softerra) peut simplifier le paramétrage d'un service de répertoire LDAP.

Les numéros de téléphone sur le serveur LDAP doivent utiliser comme délimiteur exclusivement "-" et l'espace. Le système ne peut pas filtrer les autres délimiteurs.

Lors de la configuration d'un répertoire hors ligne externe, vous pouvez en tant qu'administrateur adapter le mapping des champs aux noms du serveur LDAP utilisé. Lors de la recherche du nom à l'aide du numéro, les champs supprimés sont ignorés. La recherche est toujours effectuée à l'aide des 4 dernières positions du numéro, précédées d'un joker. Vous pouvez désactiver la recherche du nom au moyen du numéro pour les communications entrantes.

Si le port 389 utilisé par défaut est occupé, il faut en paramétrer un autre.

Remarque : Vous trouverez des informations supplémentaires sur Internet : `http://wiki.unify.com`.

Les données du répertoire externe sont disponibles pour les abonnés dans myPortal for Desktop, myAttendant, Fax Printer et myPortal for Outlook lors de la recherche.

Téléphones système avec écran

En tant qu'abonné, vous pouvez choisir, dans le menu, entre le répertoire interne et le répertoire LDAP, dans la mesure où ceux-ci sont configurés pour les téléphones système. Le répertoire LDAP supporte la recherche parmi les contacts correspondants, puis l'appel d'un contact.

L'information sur le nom fournie par le serveur LDAP n'est pas utilisée pour l'affichage en cas d'appel ou de communication. Les numéros des appels entrants ne sont pas non plus remplacés par les informations de nom fournies par le serveur LDAP (comme c’est le cas lorsque les numéros sont remplacés par les noms correspondant aux numéros abrégés).

Un abonné du système ne peut être joignable à partir de l'annuaire LDAP que si un numéro SDA a été configuré pour lui et si ce numéro correspond à son entrée dans la base de données LDAP. Les numéros fournis par le serveur LDAP ne peuvent être acheminés en interne dans le réseau que si le numéro d'appel interne et le numéro SDA sont identiques.

12.5.4.1 Comment ajouter un répertoire hors ligne externe (LDAP) pour les client PC.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Vous disposez des données d'accès pour le serveur LDAP.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur l'onglet **Config Fournisseurs externes**.
4) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez activer la résolution des numéros de téléphone en noms dans le journal des appels entrants externes, cochez la case **Rechercher par numéro de téléphone**.
   - Si vous souhaitez désactiver la résolution des numéros de téléphone en noms dans le journal des appels entrants externes, décochez la case **Rechercher par numéro de téléphone**.
5) Cliquez sur **Ajouter** .
6) Entrez les données d'accès du serveur LDAP :
   a) Sous **Nom**, saisissez un nom pour ce répertoire hors ligne externe.
   b) Sous **Serveur**, saisissez le nom ou l'adresse IP du serveur LDAP.
   c) Sous **Port**, saisissez le numéro de port du serveur LDAP.
   d) Sous **Nom distinctif de base LDAP**, saisissez le nom distinctif de base LDAP, par ex. `dc=example-for-a-domain, dc=net`.
   e) Saisissez le **nom de l'utilisateur**.
   f) Saisissez le **mot de passe**.
7) Saisissez la désignation de champ correspondante du serveur LDAP pour les champs suivants : **Titre**, **Prénom**, **Nom de famille**, **Tél. professionnel 1**, **Tél. professionnel 2**, **Domicile**, **Mobile**, **Société**, **Tél. société**, **Adresse postale**, **Département ou Région**, **Pays**, **Code postal**, **E-mail**, **Radiomessagerie**, **Numéro fax** et **Ville**.
8) Cliquez sur **Enregistrer**.

12.5.4.2 Comment effacer un répertoire hors ligne externe (LDAP) pour les PC clients

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur l'onglet **Config Fournisseurs externes**.
4) Cliquez sur le répertoire hors ligne externe à effacer.
5) Cliquez sur **Supprimer**.

12.5.4.3 Comment ajouter un répertoire hors ligne externe (LDAP) pour les téléphones système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Vous disposez des données d'accès pour le serveur LDAP.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configur. de base**.
3) Dans l'arborescence du menu, cliquez sur **Système** > **LDAP**.
4) Entrez l'**adresse IP du serveur LDAP**.
5) Entrez le **numéro de port de l'accès LDAP**.
6) Entrez le **Nom de l'utilisateur**.
7) Entrez le **mot de passe**.
8) Dans **Confirmer le mot de passe**, entrez le mot de passe.
9) Dans **Nom distinctif de base**, indiquez le nom distinctif de base du serveur LDAP, par ex. `dc=example-for-a-domain, dc=net`.
10) Dans **Demande de recherche**, entrez la séquence de recherche pour le serveur LDAP, par ex. `cn=$*`.
11) Entrez **Attribut de résultat Nom**, pour le serveur LDAP, par ex. `cn`.
12) Entrez **Attribut de résultat Numéro de téléphone**, pour le serveur LDAP, par ex. `telephoneNumber`.
13) Pour le tri des résultats de recherche, sélectionnez l'une des possibilités suivantes.
    - Si vous souhaitez trier les résultats de recherche, cochez la case **Tri des résultats de recherche**.
    - Si vous souhaitez pas trier les résultats de recherche, décochez la case **Tri des résultats de recherche**.
14) Entrez l'**indicatif de prise de ligne LDAP**.
15) Entrez le **préfixe LDAP du numéro de téléphone**.
16) Cliquez sur **Appliquer**.

12.5.5 Répertoire système

Concernant les clients UC Suite, le répertoire système contient tous les numéros système, utilisateurs UC et non UC. Les utilisateurs non UC incluent des abonnés n’ayant pas de licences UC et les abonnés virtuels, tels que les fax ou le standard automatique. Concernant les appareils, le répertoire système contient tous les abonnés internes et tous les numéros abrégés centraux.

L’administrateur peut désactiver individuellement l’affichage pour chaque abonné ou chaque numéro abrégé avec nom.

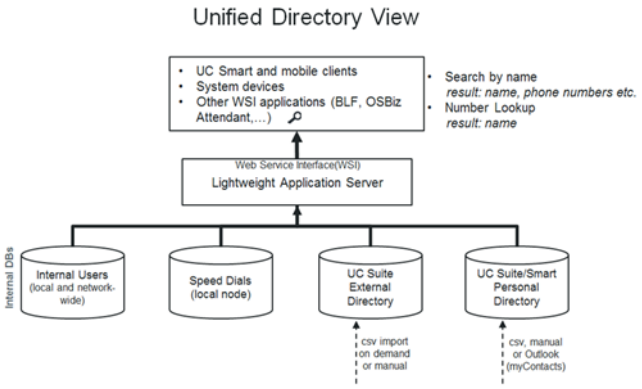
12.5.6 Annuaire unifié

OpenScape Business fournit différentes sources de données pour stocker et récupérer les données relatives aux utilisateurs ou aux contacts, en commençant par les données utilisateur internes dans la configuration utilisateur interne, via la liste de numérotation rapide interne, jusqu'aux différents répertoires des applications UC.

Chaque source de données au sein d'OpenScape Business est utilisée par une application cliente spécifique, soit située dans le logiciel système lui-même, dans les appareils téléphoniques, soit dans une application cliente de communications unifiées. En fonction des sources de données et des clients utilisés, les données récupérées et leur présentation diffèrent.

Le service « Unified Directory » d'OpenScape Business comprend les sources de données OpenScape Business existantes pour les fonctions communes de recherche et de résolution de noms. Il fournit les mêmes résultats de recherche ou informations de résolution de noms à tous les périphériques du système et aux clients OpenScape Business.

Le service d'annuaire unifié peut être accessible soit via l'interface de service Web (WSI) depuis des clients situés à l'extérieur, soit en interne via les mécanismes de traitement des appels (par exemple depuis les téléphones OpenStage).



Unified Directory utilise les bases de données et répertoires internes suivants d'OpenScape Business :

- Annuaire utilisateur interne (à l'échelle du réseau)
- Listes de numérotation rapide
- Répertoire personnel intelligent UC (facultatif)
- Répertoire externe UC Suite (facultatif)

Le service Unified Directory est disponible dans tous les systèmes OpenScape Business à partir de la version V2R2. Il ne nécessite aucun prérequis matériel, logiciel ou de licence spécifique.

Pour obtenir les meilleurs résultats lors de l'utilisation de l'annuaire unifié, certaines règles concernant le format des numéros de téléphone et l'orthographe des noms doivent être respectées.

12.5.6.1 Caractéristiques

Appareils/clients pris en charge

Le service d'annuaire unifié fournit :

- Recherche dans plusieurs sources de données internes d'OpenScape Business
- Offre unifiée des résultats de recherche à tous les clients pris en charge
- Recherche de numéros de téléphone / Résolution de noms dans plusieurs sources de données internes
- Offre unifiée de résultats de résolution de noms pour tous les clients pris en charge
- Accès aux données externes via l'interface WebServices (WSI)

Ces fonctionnalités sont disponibles pour les systèmes à nœud unique, comme décrit ci-après. Au sein des réseaux OpenScape Business, la disponibilité des fonctionnalités dépend principalement du type de connexion des liaisons, des appareils et des clients au sein du réseau.

Unified Directory prend en charge les clients/périphériques système Unify suivants via les interfaces indiquées :

Appareil/Client	Interface/Protocole utilisé	Remarques
Téléphones OpenStage	Traitement des appels / Protocole CorNet	WSI/HTTP(S) est optionnel sur OpenStage 60/80 pour les images de l'appelant
Téléphone de bureau OpenScape IP	Traitement des appels / Protocole CorNet	WSI/HTTP(S) est optionnel sur le DeskPhone IP 55 pour les images de l'appelant
Dispositifs sans fil (CMI)	Protocole de traitement des appels / CMI	
CP 100/110/200/205/210/405	Traitement des appels / Protocole CorNet	
Téléphone de bureau CP400/ 600/600E/ 700/700X/710	WSI / HTTP(S)	
myPortal au travail	WSI / HTTP(S)	

Remarque : Les clients UC Suite myPortal, myAttendant et myAgent utilisent leurs propres mécanismes pour la recherche dans l'annuaire et la résolution des noms.

Fonction de recherche

La recherche dans l'annuaire unifié est toujours effectuée à l'aide de l'interface utilisateur spécifique du périphérique/client. Les critères de recherche et le jeu de caractères utilisé peuvent être restreints, en fonction des clients utilisés.

Une fois les critères de recherche saisis, la recherche est effectuée dans les répertoires suivants.

- Annuaire utilisateur interne (à l'échelle du réseau)
- Listes de numérotation rapide
- Répertoire personnel intelligent UC (facultatif)
- Répertoire externe UC Suite (facultatif)

Tous les résultats de recherche figurant dans les répertoires ci-dessus sont affichés avec leur origine. Les correspondances contiennent soit l'ensemble complet des données de contact, soit seulement une partie de celles-ci. La profondeur des informations fournies dans les résultats dépend de la source des données.

Remarque : La recherche par nom de groupe dans myportal@work n'est pas prise en charge en mode UC Suite. Seules les recherches des utilisateurs sous licence (licence de base) et des groupes MULAP sous licence (entrées UC) sont prises en charge.

Les matchs sont affichés sur les appareils ou les clients en fonction des capacités d'affichage.

	Annuaire des utilisateurs internes	**Numéros abrégés**	**Annuaire personnel intelligent UC**	**Répertoire externe UC Suite**	**Contacts Outlook personnels (via Mes Contacts)**
Nom de famille	X	---	X	X	X
Prénom	X	---	X	X	X
Nom court/ d'affichage	X	X	---	---	---
Numéro de téléphone du bureau	---	---	X	X	X
Accueil/Ext. Numéro de téléphone	---	---	X	---	X
Numéro de téléphone portable	---	---	X	X	X
Adresse e-mail	---	---	X	X	X
Nom de l'entreprise	---	---	X	X	X
Ville	---	---	---	---	---
Photo de contact	---	---	X	---	X
Aperçu de l'image de contact	---	---	X	---	X

Recherche de numéro de téléphone

La recherche de numéro de téléphone dans l'annuaire unifié résout le problème de l'appelant transféré (CLI) par une recherche de numéro dans toutes les sources de données internes prises en charge. La recherche est effectuée dans les champs de numéro de téléphone suivants :

- Numéro de bureau
- Numéro de portable
- Numéro de téléphone fixe

La recherche de numéro de téléphone est déclenchée en cas d'appels entrants ou sortants en général, tandis que les fonctions spécifiques de routage et de transfert sont prises en compte en outre.

Une priorisation fixe des sources de données utilisées pour la recherche de numéros de téléphone est mise en œuvre afin d'obtenir le résultat le plus rapidement possible. Le résultat contient soit uniquement le nom de famille, le prénom, le nom d'affichage ou, le cas échéant, l'ensemble des données de contact associées.

Tableau 7 : Sources de données prises en charge et priorisation

Priorité	Sources de données	Remarque
1	Nom du CO/ITSP (tel qu'envoyé par le fournisseur)	La condition préalable est d'activer l'indicateur « Nom dans CO ».
2	Liste de numérotation rapide	
3	Contacts personnels	
4	Détails de l'utilisateur UC	

Les données récupérées sont présentées sur l'appareil de l'utilisateur et/ou dans le client UC. La profondeur des informations dépend des capacités d'affichage.

- **Appels entrants**

  Scénario pris en charge pour les systèmes à nœud unique :

  – Appel de base
  – Appel de groupe/Appel MULAP
  – Groupe de sonnerie
  – Transfert d'appel en une seule étape (SSCT)
  – Transfert avec présence/supervision/consultation
  – Renvoi d'appel inconditionnel (CFU)
  – Renvoi d'appel sans réponse (CFNR)
  – Renvoi d'appel occupé (CFB)
  – transfert aveugle
  – Prise d'appel

  Remarque : La prise d'appel est différente du groupe de prise d'appel. Dans le groupe de prise d'appel, lorsqu'un

numéro externe est enregistré dans l'annuaire unifié, le nom de l'appelant n'est pas affiché pour les membres du groupe.

Le scénario pris en charge pour les scénarios multi-nœuds (réseau) est un appel de passerelle.

- **Appel sortant**

  En cas d'appel sortant, la recherche du numéro de téléphone du correspondant appelé n'a lieu qu'une seule fois.

  Le scénario pris en charge pour les systèmes à nœud unique est un appel de base vers un numéro externe.

L'affichage des résultats de la recherche de numéro de téléphone dépend des capacités d'affichage des téléphones.

12.5.6.2 Règles et Conventions

Certaines conventions relatives aux formats des numéros et des noms dans les sources de données doivent être respectées pour pouvoir obtenir des résultats optimaux à l'aide du service Répertoire unifié.

Formats des numéros pris en charge

Tous les numéros de téléphone externes dans les sources de données doivent être saisis au format canonique, incluant l'indicatif pays et local, par ex. +4989700712345

La liste de numérotation abrégée prend en charge uniquement le format sélectionnable du système, par ex. 0089700712345 ou 0004989700712345

Lorsque les numéros abrégés sont configurés de façon à être accessibles via LDAP, vous devez activer l'option de conversion de nombre pour afficher le nom du contact, lorsque le numéro est au format canonique. Pour plus d'informations sur l'activation de la conversion de nombre, voir Comment ajouter une source de données externe pour Open Directory Service à la page 1120.

Formats des noms pris en charge

Les conventions suivantes relatives aux formats des noms et aux jeux de caractères doivent être respectées :

- **Format du nom pour la numérotation abrégée**

  La recherche de nom à l'intérieur de la liste de numérotation abrégée est prise en charge uniquement avec les règles de configuration spécifiques. Le prénom et le nom de famille doivent être saisis dans le champ de nom existant à l'aide du modèle suivant :

  <Nom de famille>, <Prénom> (séparés par des virgules)

- **Utilisateurs internes en cas de migrations**

  La migration vers V2R1 et versions ultérieures avec des utilisateurs internes ne suivant pas ces règles de configuration ne sera pas prise en charge de la manière prévue. En d'autres termes, l'administrateur doit convertir les noms internes selon le modèle suivant, et ce, avant la migration :

  <Nom de famille>, <Prénom> (séparés par des virgules)

Disponibilité des changements de répertoire

Après la création, mise à jour ou suppression de contacts dans les différentes sources de données, la répercussion de toutes les modifications dans les résultats de recherche de numéro de téléphone peut prendre dix minutes.

12.5.6.3 Chapitre 11.5.5.3 Limites fonctionnelles

Les limites fonctionnelles suivantes existent pour les répertoires unifiés (Unified Directories) :

Recherche de nom

- Support du nom de groupe

  Les noms de groupe (pas les noms MULAP) ne peuvent pas être recherchés dans tous les types de configurations.
- Support de caractères spéciaux

  Sur la plupart des équipements téléphoniques, l'utilisateur peut uniquement rechercher les caractères standard « a-z ». Les caractères spéciaux (diacritiques) comme les caractères allemandes Ää,Öö,Üü, ß ne sont pas accessibles via l'interface utilisateur de l'équipement téléphonique.

  Par conséquent, un résultat de recherche de caractères simples inclut aussi les caractères spéciaux. La recherche de l’un des caractères suivants : « acdegilnorstuyz », trouve aussi les caractères spéciaux correspondants : « àáâãåäăąçćčďđèéêêëêìıîíľłñńòòôõöøåêhťùúúÿ »

  dans les résultats de recherche.

  Remarque : La recherche dans l'annuaire avec le caractère générique au début de la chaîne de recherche, par exemple <*jo*> ne fonctionne que pour les utilisateurs internes.
- Support du format du nom pour la numérotation abrégée

  La recherche de nom à l'intérieur de la liste de numérotation abrégée est prise en charge uniquement avec les règles de configuration spécifiques. Le prénom et le nom de famille doivent être entrés dans le champ de nom existant à l'aide de l'un des modèles suivants

  – <Nom de famille>, <Prénom> (séparées par des virgules)
  – <Prénom> <Nom de famille> (séparateur d'espace dans ce cas)

Présentation du nom

Les contacts personnels dans UC Smart et à partir d'un répertoire hors ligne externe dont la longueur du prénom plus la longueur du nom de famille sont supérieures à 24 caractères, sont tronqués à 24 caractères pour correspondre à la longueur d'affichage de l'équipement.

Recherche de numéro de téléphone

La fonctionnalité de recherche du numéro de téléphone (retrouver le nom du contact à partir du numéro de l'appelant) n'est pas prise en charge dans Unified Directory pour les équipements SIP et S0.

12.5.6.4 Annuaire unifié dans les systèmes en réseau

Le service d'annuaire unifié est actif sur chaque nœud d'un réseau d'entreprise OpenScape et utilise les sources de données de son propre système. Les appareils téléphoniques et les clients utilisent toujours le service d'annuaire unifié au sein de leur propre nœud.

La disponibilité des contacts à l'échelle du réseau dépend donc du type de contenu de la source de données.

Tableau 8 : Source de données locale et à l'échelle du réseau

Source de données	Données locales	Données à l'échelle du réseau
Annuaire des utilisateurs internes	X	X
listes de numérotation rapide	X	---
Annuaire personnel intelligent UC	X	---

Remarque : L'annuaire unifié n'est pas entièrement pris en charge dans les environnements mixtes UC Suite/UC Smart.

Recherche de numéro de téléphone

Dans les scénarios de mise en réseau, la fonctionnalité de recherche de numéro de téléphone n'est pas utilisée. Dans de tels scénarios, le nom est transporté via les mécanismes de réseau normaux entre les nœuds du réseau.

Pour les utilisateurs internes, le nom d'affichage configuré est utilisé, la recherche n'est donc pas nécessaire.

12.5.6.5 Comment importer des contacts dans Unified Directory

L'assistant d'importation de contacts permet d'importer des contacts du répertoire à partir d'un fichier csv.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Unified Directory**.
3) Cliquez sur **Modifier** situé à côté de **Importer des contacts**, pour procéder à l'importation des contacts dans le répertoire global.

4) Sous la section **Téléchargement de fichiers**, cliquez sur **Choisir un fichier** et sélectionnez le fichier csv à télécharger.

Remarque : Le nombre maximum d'entrées par importation est de 100 000 (30 000 pour les systèmes embarqués).

---

5) Sous la section **Options**, entrez le **séparateur de fichier**. ';' ou ',' sont des entrées valides.

6) Cliquez sur **OK & Suivant**.

7) L'application dorsale traite le fichier, lit les en-têtes et présente les en-têtes avec les catégories prédéfinies du répertoire principal dans la page **Cartographie de l'en-tête CSV**. L'utilisateur peut alors faire correspondre les entrées des fichiers csv afin d'importer les données relatives dans les catégories souhaitées autres que les catégories prédéfinies.

8) Cliquez sur **OK & Suivant**.

9) Accédez à la page **Aperçu de l'importation** :

a) Sélectionnez l'une des options suivantes concernant le fichier csv importé :

- Ajouter les contacts du répertoire global
- Supprimer tous les contacts du répertoire global importés via CSV
- Supprimer tous les contacts du répertoire global

b) En ce qui concerne les **doublons d'ID client** et sélectionnez l'une des options suivantes :

- Mettre à jour le client existant
- Arrêter l'importation de l'enregistrement actuel

Les entrées qui seront ajoutées et celles qui n'ont pas été validées sont présentées dans deux tableaux correspondants.

Remarque : Les enregistrements en double sont identifiés par la combinaison des champs Prénom, Nom, Téléphone professionnel et E-mail. Ces champs ne peuvent pas être mis à jour automatiquement en choisissant "**Mettre à jour le client existant**". Pour mettre à jour ces champs, choisissez de supprimer les premiers enregistrements plus anciens à l'étape 9a.

L'indicateur **"Mettre à jour l'utilisateur existant"** ne fonctionne que lorsque l'ID client est mis en correspondance lors de l'importation.

Seul l'enregistrement ayant le même **ID Client** sera considéré comme un "client existant" et sera mis à jour.

L'indicateur "**Supprimer les données avant l'importation**" ne supprime pas les enregistrements s'ils sont déjà utilisés

dans d’autres fonctions, par exemple en tant qu'appelant VIP, etc.

L'ID client est la seule clé permettant de déterminer si l'enregistrement est dupliqué. Si l'ID client n'est pas mappé, il n'y a aucun moyen d'éviter les doublons.

Par conséquent, il est fortement conseillé aux clients de se fier au modèle fourni et d'adapter leurs données en fonction de celui-ci sans omettre les identifiants uniques.

10) Cliquez sur **OK & Suivant**. Ce processus peut prendre plusieurs minutes.
11) La page **Importation terminée** indique le nombre d'entrées qui ont été importées.
12) Cliquez sur **Terminer**.

12.5.6.6 Comment modifier ou ajouter de nouveaux contacts Unified Directory

L'assistant de modification des contacts permet de modifier les contacts déjà importés ou d'en ajouter de nouveaux.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Unified Directory**.
3) Cliquez sur **Modifier** situé à côté de **Modifier les contacts**, pour procéder à la modification des contacts dans le Répertoire global.
4) Modifiez les champs souhaités des contacts. Le bouton **Appliquer** n'est disponible que lorsqu'une entrée est modifiée.
5) Cliquez sur **Ajouter** pour ajouter manuellement un nouveau contact.
6) Remplissez les champs souhaités du nouveau contact et cliquez sur le bouton **Appliquer**.

12.5.7 Départements

Les départements regroupent les abonnés dans un répertoire interne en fonction de leur appartenance organisationnelle. Le répertoire interne permet la recherche ou le tri par département.

12.5.7.1 Comment ajouter un département

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Départements**.
4) Cliquez sur **Ajouter**.
5) Indiquez le **Nom du département**.
6) Entrez l'identificateur du **Groupe de recherche**.
7) Cliquez sur **Enregistrer**.

12.5.7.2 Comment affecter les abonnés à un département

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**.
4) Sélectionnez l'abonné correspondant.
5) Cliquez sur **Modifier** > **Données personnelles** > **mes données personnelles**.
6) Dans le champ **Département**, sélectionnez le département correspondant dans la liste déroulante.
7) Pour finir, cliquez sur **Enregistrer**.

12.5.7.3 Comment modifier le département

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Départements**.
4) Dans la liste des départements, cliquez sur le département correspondant.
5) Cliquez sur **Modifier**.
6) Indiquez le **Nom du département**.
7) Entrez l'identificateur du **Groupe de recherche**.
8) Cliquez sur **Enregistrer**.

12.5.7.4 Comment supprimer un département

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'assistant **Départements**.
4) Dans la liste des départements, cliquez sur le département correspondant.
5) Cliquez sur **Supprimer**.
6) Cliquez sur **OK**.

12.5.8 Liste des favoris

Dans la liste des favoris, vous avez en tant qu'abonné un aperçu des contacts sélectionnés. Cela vous permet de les appeler de manière très simple. Tous les abonnés internes (avec téléphone système) ainsi que les partenaires de communication externes sont indiqués avec leur état de présence et peuvent être contactés par messagerie instantanée.

Vous pouvez ajouter à la liste des favoris des contacts figurant dans les différents répertoires. Pour les favoris qui ne proviennent pas du répertoire interne, à la place de l'icône correspondant à l'état de présence, figure une icône indiquant la source du contact.

La liste des favoris gère les contacts en groupes. Il est possible de trier les contacts de tous les groupes par prénom, par nom ou selon leur ordre d'origine.

En cas d'absence d'un abonné interne, vous êtes informé du moment prévu de son retour lorsque vous positionnez le pointeur de la souris sur son entrée, à condition que cet abonné vous autorise à visualiser son état de présence.

Pour les favoris disposant de plusieurs numéros de téléphone, vous pouvez définir un numéro standard, qui vous sert à appeler l contact. Le numéro par défaut d'un favori est reconnaissable dans le menu contextuel à l'icône avec case cochée.

12.5.9 Journal

Le journal est la liste de tous les appels entrants et sortants d'un abonné. À partir du journal, l'abonné peut rappeler les contacts de manière aisée et rapide ou répondre aux appels manqués.

Dossiers pour les types d'appel

Les appels sont répartis dans les groupes suivants :

- **Ouvert**

  Contient les appels manqués non répondus pour lesquels un numéro d'appel a été transmis. Dès qu'une réponse est donnée à l'un de ces appels, toutes les entrées avec numéro de téléphone correspondant sont supprimées.
- **Tous les appels**
- **Manqué**
- **Répondu**
- **Interne**

- **Externe**
- **Entrant**
- **Sortant**
- **Programmé**

  Contient les appels programmés par vous (en tant qu'abonné) à certains moments. La fonctionnalité Appels programmés n'est pas disponible pour les agents du Centre de contacts. Pour que le système de communication effectue un appel programmé, il faut que myPortal for Desktop ou myPortal for Outlook soit ouvert au moment du rendez-vous et que votre état de présence soit défini sur **Bureau** ou **CallMe**. Vous devez également confirmer l'exécution de l'appel dans une boîte de dialogue. Si vous êtes occupé au moment d'un appel programmé, le système reporte l'appel programmé jusqu'à ce que vous soyez de nouveau libre. myPortal for Desktop ou myPortal for Outlook vous indique à la fin les éventuels appels programmés à venir. Lors du démarrage, myPortal for Desktop ou myPortal for Outlook vous indique les éventuels rendez-vous déjà dépassés concernant des appels programmés. Vous pouvez alors les effacer ou bien les enregistrer à une autre date.

Dans l'interface utilisateur moderne de myPortal for Desktop, tous les dossiers des types d'appel ne sont pas disponibles.

Au démarrage de l'interface utilisateur moderne de myPortal for Desktop, seules 100 entrées de journal sont chargées. Après cela et lorsque de nouveaux appels arrivent, le nombre dans l'historique des appels dépassera 100 enregistrements.

Durée de conservation

Le système de communication sauvegarde les appels dans le journal pour une durée maximale limitée, qui peut être configurée par l'administrateur. En tant qu'abonné, vous pouvez réduire cette durée. Une fois cette durée de conservation écoulée, le système efface automatiquement les entrées correspondantes.

Remarque : La durée de conservation définit aussi la période maximale pour les évaluations avec myReports.

Regroupement par période de temps

Dans chaque groupe, les appels sont groupés en fonction de la période, par exemple : Aujourd'hui, Hier, etc., La semaine dernière, Le mois dernier et Antérieur. Votre administrateur peut paramétrer la durée de conservation des appels dans le journal. Une fois la durée paramétrée écoulée, les entrées sont automatiquement effacées. Dans l'interface utilisateur moderne de myPortal for Desktop, le regroupement par période de temps n'est pas disponible.

Détails de l'appel

Chaque appel est affiché avec la date et l'heure et, si disponible, avec le numéro d'appel. Si, en plus du numéro d'appel, le répertoire contient d'autres informations comme **Nom de famille**, **Prénom** et **Société**, elles sont également affichées. Les colonnes suivantes sont également affichés dans la plupart des dossiers : **Sens**, **Durée** et **Communication terminée**. Tous les détails ne sont pas disponibles dans l'interface utilisateur moderne de myPortal for Desktop.

Tri

Vous pouvez trier les appels du journal selon une colonne quelconque, par ordre alphanumérique croissant ou décroissant.

Dans le journal, vous pouvez aller au premier appel dont l'entrée figurant dans la colonne de tri commence par un caractère précis que vous recherchez (par ex. aller au premier nom commençant par "P"). En entrant les caractères suivants, vous pouvez mieux cibler l'entrée recherchée. Dans l'interface utilisateur moderne de myPortal for Desktop, le tri n'est pas disponible.

Exporter

En tant qu'abonné, vous pouvez exporter le journal avec myPortal for Desktop ou myPortal for Outlook sous forme de fichier CSV :

12.5.9.1 Comment modifier la durée maximale de conservation d'un journal

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Maintenance**.
5) Entrez la durée souhaitée en jours dans le champ **Conserver l'historique des appels pendant**, sous **Maintenance des informations appels**.

   Remarque : La durée de conservation définit aussi la période maximale pour les évaluations avec myReports.

6) Cliquez sur **Enregistrer**.

12.6 Appels

Pour les appels, les abonnés disposent de fonctionnalités confortables comme la numérotation via le bureau, les fenêtres surgissantes et l'enregistrement des appels et conférences.

12.6.1 Numérotation via le bureau et numérotation à partir du presse-papiers

La numérotation via le bureau et à partir du presse-papiers permet aux utilisateurs de myPortal for Desktop (Windows) ou myPortal for Outlook d'appeler à partir de nombreuses applications Windows une destination sélectionnée ou une destination figurant le presse-papiers Windows au moyen d'une combinaison de touches, par ex. à partir d'un e-mail Outlook.

En fonction du type de séquence de caractères utilisée, la numérotation fonctionne de la manière suivante.

- Sélection d'un numéro au format canonique.
- Un numéro de téléphone dans un format composable est sélectionné, dans la mesure où le système de communication est en mesure de décider s'il s'agit d'une destination interne ou externe. Si ce n'est pas le cas, l'utilisateur est invité à procéder à la sélection correspondante.
- Une séquence de caractères contenant des lettres sert pour la recherche de prénom ou de nom de famille.

La numérotation via le bureau et la numérotation à partir du presse-papiers sont effectuées après un délai paramétrable. A l'intérieur de cette période de temps, il est possible d'interrompre la sélection. Si vous modifiez la valeur préréglée de 3 s en 0 s, la numérotation est immédiatement exécutée. La valeur est modifiée dans les paramètres des clients UC Suite.

Les applications Windows, mises en place à l'aide de composantes Windows standard, supportent généralement la numérotation via le bureau et la numérotation à partir du presse-papiers, mais pas les applications 16 bits. Numérotation via le bureau est uniquement supportée par les applications 32 bits.

12.6.2 Fenêtres surgissantes

Les fenêtres surgissantes des clients UC Suite offrent aux utilisateurs la possibilité confortable de réagir par un clic, par ex. lors d'appels entrants ou de nouveaux messages vocaux.

Les fenêtres surgissantes s'affichent dans le coin droit en bas de l'écran. Il y a différents types de fenêtres surgissantes. Les fenêtres surgissantes des appels et messages affichent le numéro de téléphone, le nom et la photo de l'appelant, s'il y en a une. Les touches des fenêtres surgissantes se modifient en fonction de la situation.

Les fenêtres surgissantes peuvent être réduites en icônes dans la barre des tâches. Dès que plus de trois fenêtres surgissantes sont ouvertes pour les appels, elles sont automatiquement réduites et placées dans la barre de tâches.

12.6.3 Enregistrement des appels

Un abonné peut enregistrer les appels. Les appels enregistrés apparaissent dans la boîte vocale.

Conseil : Notez que dans la plupart des pays, vous êtes légalement tenu d'informer votre correspondant et de lui indiquer que vous enregistrez la communication. Dans certains pays (par ex. en France), le système en informe automatiquement le correspondant.

En tant qu'administrateur, vous pouvez autoriser ou interdire l'enregistrement des appels et conférences sur l'ensemble du système. En option, vous pouvez au début de l'enregistrement, configurer la diffusion d'une annonce ou d'une tonalité d'avertissement.

En tant qu'abonné, vous pouvez gérer l'enregistrement des appels avec myPortal for Desktop ou myPortal for Outlook. Les appels enregistrés sont signalés par un point rouge dans la boîte vocale et indiquent le numéro du correspondant, s'il est disponible.

Un enregistrement en cours est interrompu par un double appel, une mise en garde, un transfert et l'ouverture d'une conférence.

Remarque : DTMF n'est pas pris en charge lorsqu'un appel est enregistré.

12.6.3.1 Comment activer ou désactiver l'enregistrement des appels

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Enregistrement en direct**.
5) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez autoriser l'enregistrement des appels, cochez la case **Enregistrement en direct**.
   - Si vous souhaitez bloquer l'enregistrement des appels, décochez la case **Enregistrement en direct**.
6) Cliquez sur **Enregistrer**.

Remarque : Les appels disposant de cette fonctionnalité ne peuvent pas être transférés ou mis en garde.

12.6.3.2 Comment activer ou désactiver l'annonce d'enregistrement

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Enregistrement en direct**.

5) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez diffuser une annonce au début de l'enregistrement, cochez la case **Émettre une annonce avant l'enregistrement**.
   - Si vous ne souhaitez pas diffuser une annonce au début de l'enregistrement, décochez la case **Émettre une annonce avant l'enregistrement**.
6) Cliquez sur **Enregistrer**.

12.6.3.3 Comment activer ou désactiver la tonalité d'avertissement pour l'enregistrement

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Enregistrement en direct**.
5) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez diffuser une tonalité d'avertissement au début de l'enregistrement, cochez la case **Émettre une tonalité d'avertissement avant l'enregistrement**.
   - Si vous ne souhaitez pas diffuser une tonalité d'avertissement au début de l'enregistrement, décochez la case **Émettre une tonalité d'avertissement avant l'enregistrement**.
6) Cliquez sur **Enregistrer**.

Remarque : Veuillez noter que ce processus s'applique uniquement à **Openscape Business S**. l'activation de la tonalité d'avertissement d'enregistrement dans **Openscape Business X** est contrôlée par le flag **Tonalité d'avertissement pendant l'enregistrement vocal**, que vous trouverez dans **Mode Expert** > **Configuration de base** > **Flags système**.

12.7 Conférences

Dans une conférence, plusieurs participants (y compris externes) peuvent téléphoner les uns avec les autres simultanément.

12.7.1 gestion des conférences

La gestion des conférences permet aux abonnés d'utiliser différents types de conférences.

Types de conférences

Les différents types de conférences présentent les caractéristiques suivantes :

	Ad-hoc	Programmé	Permanente	Ouvert
Utilisation	• gestion par le téléphone • géré(e) par l'application	• géré(e) par l'application	• géré(e) par l'application	• géré(e) par l'application
Démarrage	• Manuelle	• Programmé	• Manuelle	• Manuelle
Fin	• Manuelle	• Programmé • Manuelle	• Manuelle	• Manuelle
Durée de réservation des canaux de la conférence	• par défaut 1 heure	• Programmé	• jusqu'à désactivation ou suppression de la conférence	• jusqu'à désactivation ou suppression de la conférence
Poste	x	x	-	-
Récurrence	• Manuelle	• Programmé	-	-
Sens de l'établissement de la connexion du point de vue du système de communication	• Sortant	• Sortant • Entrant	• Entrant	• Entrant
Groupe des participants	• fixe	• fixe	• fixe	• Ouvert
Authentification des participants à la conférence	-	• ID de conférence individuel (option) • Mot de passe (option)	• ID de conférence individuel (option) • Mot de passe (option)	• ID de conférence commun (option)
Enregistrement aussitôt activé dans le système	• manuellement (On Demand Conference Recording)	• automatique (Auto Conference Recording) • manuellement (On Demand Conference Recording)	• automatique (Auto Conference Recording) • manuellement (On Demand Conference Recording)	• automatique (Auto Conference Recording) • manuellement (On Demand Conference Recording)
Invitation par e-mail avec :	• Nom de la conférence	• Nom de la conférence • Numéro d'accès • ID conférence • Mot de passe • Date et heure du début et de la fin de conférence	• Nom de la conférence • Numéro d'accès • ID conférence • Mot de passe	• Nom de la conférence • Numéro d'accès • ID conférence • Mot de passe

	Ad-hoc	Programmé	Permanente	Ouvert
Rendez-vous Outlook comme pièce jointe d'e-mail (.ics)	-	x	-	-

conférence gérée par l’application

En tant qu'abonné vous pouvez lancer, gérer et administrer une conférence à l'aide de la gestion des conférences de myPortal for Desktop ou myPortal for Outlook.

Conférence gérée par téléphone

En tant qu'abonné, vous pouvez lancer une conférence gérée par le téléphone de la manière suivante et ensuite la gérer au téléphone :

- Appeler les participants souhaités et les associer à la conférence
- Transformer un double appel en conférence
- Transformer un deuxième appel en conférence

Salle de conférence virtuelle

Dans la salle de conférence virtuelle, vous pouvez suivre en temps réel une conférence avec le cercle des participants représenté de manière graphique et aussi la diriger en tant que directeur de conférence. La salle de conférence virtuelle indique le numéro de téléphone, le nom et l'état Présence des participants, pour autant qu'ils sont disponibles.

Numéro d'accès

L'administrateur peut modifier les numéros d'accès aux conférences définies lors de l'installation de base. Vous pouvez afficher le numéro de sélection d'une conférence.

Directeur de conférence

Jusqu'à présent, l'initiateur d'une conférence devient le directeur de conférence. Celui-ci peut (en fonction du type de conférence) :

- Ajouter ou supprimer des participants à la conférence (pour les conférences contrôlées par l'application) :

  Les participants supprimés ne restent pas dans la conférence.
- déconnecter ou reconnecter des participants à la conférence :

  Les abonnés déconnectés peuvent rester dans la conférence. Pendant que le directeur de conférence connecte un participant à la conférence, le participant à la conférence unique entend la musique d'attente ou bien les autres participants à la conférence sont reliés les uns aux autres.
- enregistrer la conférence

  Les conférences enregistrées sont identifiées dans la boîte vocale par un point rouge et indiquent le numéro d'appel du premier participant à la conférence, le cas échéant. Les conférence où l'un des participants a été mis en garde ne peuvent pas être enregistrées.
- Définir un autre abonné interne comme directeur de conférence
- Prolongation de la conférence

- quitter la conférence sans y mettre fin :

  Le participant interne qui est connecté depuis le plus longtemps devient automatiquement directeur de conférence.
- terminer la conférence

Participants à la conférence

Les participants à la conférence peuvent quitter la conférence ou bien y entrer de nouveau (conférence programmée et conférence permanente). Tant qu'une conférence ne comprend qu'un seul participant, celui-ci entend une musique d'attente. L'administrateur peut déterminer si plusieurs participants externes sont admis ou non dans la conférence. Le nombre maximum des participants à la conférence externes est limité notamment par le nombre des lignes réseau disponibles.

Tonalité de conférence

Lors de la connexion ou de la déconnexion d'un participant à la conférence, les autres participants à la conférence entendent une tonalité d'avertissement. L'administrateur peut activer ou désactiver la tonalité de conférence.

Terminer automatiquement sans directeur de conférence

Lorsque seuls des participants externes demeurent dans la conférence, ils entendent au bout d'un certain temps une tonalité d'avertissement. Une fois qu'une seconde période de temps s'est écoulée, le système de communication met fin automatiquement à la conférence. En tant qu'administrateur, vous pouvez modifier ces valeurs de temps.

Notification par e-mail et rendez-vous Outlook

Le système peut automatiquement notifier les participants à la conférence par e-mail et, pour les conférences programmées, par le biais d'un rendez-vous Outlook en pièce jointe (.ics) :

Événement	participants à la conférence avertis	Rendez-vous Outlook
Nouvelle conférence	Tous	création automatique
Effacer la conférence		effacement automatique
Déplacer la conférence		Actualisation automatique
Ajouter des participants à la conférence	concernés	création automatique (concernés)
Supprimer des participants à la conférence		effacement automatique (concernés)

cela nécessite que l'administrateur ait configuré l'envoi d'e-mails. De plus, le participant à la conférence interne doit avoir défini son adresse e-mail. Pour les participants à la conférence externes, l'initiateur de la conférence doit avoir entré leur adresse e-mail.

Autres appels

En cours de participation à une conférence le fait d'effectuer un autre appel ou de recevoir un autre appel coupe le participant de la conférence.

Parcage, Va-et-vient

Dans une conférence, les fonctionnalités Parcage et Va-et-vient ne sont pas disponibles.

Taxes

Les taxes sont imputées au correspondant qui est à l'origine de la communication soumise à taxation. Lors de la transmission à une autre directeur de conférence, la suite des taxes sont imputées à ce dernier.

Charge du système

En tant qu'administrateur, vous pouvez afficher les conférences actives et enregistrées. Les conférences inactives peuvent être supprimées.

Conseil : Les conférences permanentes occupent les ressources du système en permanence. Étant donné que chaque abonné peut configurer des conférences permanentes avec myPortal for Desktop ou myPortal for Outlook, vous devez, en tant qu'administrateur, revoir régulièrement les conférences enregistrées pour éviter les goulots d'étranglement des ressources.

Transmission vidéo

Une transmission vidéo éventuellement en cours doit être terminée avant la participation à une conférence.

12.7.1.1 Comment modifier le numéro de sélection pour salle de conférence virtuelle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, allez à **Abonnés** > **UC Applications** > **Conférence**.

   Dans l'espace de travail, les numéros des salles de conférence virtuelles sont affichés. Le dernier d'entre eux correspond aux conférences planifiées et aux conférences permanentes.
4) Dans l'arborescence du menu, cliquez sur l'élément concerné (index - numéro - nom).
5) Cliquez sur l'onglet **Modifier les paramètres de l'abonné**.
6) Dans le champ **Numéro**, entrez le nouveau numéro de sélection. Le numéro de sélection ne doit comporter que les chiffres 0-9.
7) Cliquez sur **Appliquer** puis sur **OK**.

12.7.1.2 Autoriser ou interdire plusieurs participants externes à la conférence

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, allez à **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez autoriser plusieurs participants externes à la conférence, cochez la case **Plus d'1 participant à la conférence externe**.
   - Si vous souhaitez éviter plusieurs participants externes à la conférence, décochez la case **Plus d'1 participant à la conférence externe**.
5) Cliquez sur **Appliquer** puis sur **OK**.

12.7.1.3 Comment activer ou désactiver la tonalité de conférence

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, allez à **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la tonalité de conférence, cochez la case **Tonalité de conférence**.
   - Si vous souhaitez désactiver la tonalité de conférence, décochez la case **Tonalité de conférence**.
5) Cliquez sur **Appliquer** puis sur **OK**.

12.7.1.4 Comment modifier l'intervalle de temps pour la fin automatique des conférences

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.

3) Dans l'arborescence du menu, allez à **Système** > **Temporisations**.
4) Dans la ligne **Temps avant tonalité pour aboutement LR analogiques**, **Base** et **Facteur**, sélectionnez l'intervalle de temps souhaité entre le moment où le dernier directeur de conférence quitte la conférence et la tonalité d'avertissement.
5) Dans la ligne **Durée entre la tonalité d'avertissement et la fin...**, sélectionnez la durée souhaitée entre la tonalité d'avertissement et la fin automatique de la conférence.
6) Cliquez sur **Appliquer** puis sur **OK**.

12.7.1.5 Comment afficher les détails concernant une conférence enregistrée

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Conférence**.
4) Cliquez sur la conférence concernée.
5) Cliquez sur **Afficher**.

12.7.1.6 Comment supprimer la conférence enregistrée

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Conférence**.
4) Cliquez sur la conférence concernée.
5) Cliquez sur **Effacement** et confirmez la question de sécurité.

12.7.1.7 Comment configurer l'enregistrement des conférences

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Enregistrement en direct**.

5) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez autoriser l'enregistrement des conférences, cochez la case **Disponibilité de l'enregistrement en direct de conférence**.
   - Si vous souhaitez bloquer l'enregistrement des conférences, décochez la case **Disponibilité de l'enregistrement en direct de conférence**.
6) Cliquez sur **Enregistrer**.

Remarque : Les conférences disposant de cette fonctionnalité ne peuvent pas être transférées ou mises en garde.

12.7.2 Conférence Ad-hoc

Une conférence ad hoc est établie spontanément, de manière manuelle par le directeur de conférence. Le directeur de conférence peut enregistrer les conférences Ad-hoc afin de les convoquer de nouveau à un moment ultérieur quelconque.

Démarrer la conférence

Le système ouvre automatiquement chez tous les participants internes à la conférence une fenêtre avec salle de conférence virtuelle si le participant a démarré myPortal for Desktop avec l'interface utilisateur classique ou myPortal for Outlook. Le système appelle simultanément tous les participants à la conférence. Lors de l'entrée dans la conférence, les participants reçoivent un message d'accueil qui désigne le directeur de conférence.

Enregistrer la conférence

Le directeur de conférence peut enregistrer manuellement la conférence, pour lui et pour tous les participants internes connectés, à condition que l'enregistrement des communications soit activé dans le système. Les abonnés du propre noeud reçoivent l'enregistrement dans la boîte vocale, les abonnés d'autres noeuds par e-mail. La durée de l'enregistrement est uniquement limitée par la capacité de mémoire du système de communication.

Terminer la conférence

Le directeur de conférence peut terminer la conférence dans le client ou bien en raccrochant. Ou bien, la conférence est terminée lorsque tous les participants à la conférence l'ont quittée.

Extension d'une communication à une conférence

Un abonné interne en communication peut étendre la communication à une conférence Ad-hoc et associer d'autres abonnés. Pour cela, l'abonné doit posséder une licence UC Suite Conference. Cette fonctionnalité n'est pas possible avec CallMe.

12.7.3 Conférence programmée

Une conférence programmée (conférence Meet-Me) se déroule à une date définie préalablement, pendant une durée définie, avec répétition éventuelle à la même heure.

Une conférence programmée demeure activée pendant toute la période prévue, indépendamment du fait que des abonnés soient connectés ou non. Le directeur de conférence enregistre la conférence programmée sous un nom qui lui est propre.

Options de configuration d'une conférence programmée

L'initiateur de la conférence peut définir les propriétés suivantes :

- Heure de début et de fin
- tenue régulière
- Nécessité ou non de la présence du directeur de conférence
- Authentification des participants à la conférence nécessaire lors de l'entrée dans la conférence (par saisie de l'ID de conférence et du mot de passe sur le clavier du téléphone).

  Remarque : Les abonnés Mobility Entry doivent entrer l'indicatif pour Numérotation MF avant leur authentification.

  Le mot de passe par défaut pour les conférences est 123456. Le directeur de conférence peut le modifier individuellement pour chaque participant à la conférence.
- Langue des annonces au début de la conférence
- Sens d'établissement de la connexion pour chaque participant à la conférence (par défaut : **Sortant**)

Démarrer la conférence

Le système ouvre automatiquement au moment programmé, pour tous les participants à la conférence internes, la fenêtre comportant la salle de conférence virtuelle, dans la mesure où le participant à la conférence a démarré myPortal for Desktop avec l'interface utilisateur classique ou myPortal for Outlook. Si la présence du directeur de conférence est nécessaire, le système l'appelle tout d'abord puis, une fois qu'il s'est authentifié, il appelle simultanément tous les autres participants à la conférence. Les participants à la conférence qui ont programmé un renvoi vers une boîte vocale ou dont l'état Présence indique qu'ils sont absents ne sont pas appelés. Suivant le type d'établissement de la liaison configuré, le système appelle les participants à la conférence ou ceux-ci peuvent s'inviter eux-mêmes. Le système de communication annonce par son nom chaque nouveau participant : "… `participe à la conférence.`", à condition que l'initiateur ait enregistré son annonce de nom.

Remarque : Pour que les participants à une conférence que vous avez programmée sans authentification entendent une annonce avec le nom du directeur conférence, il faut que celui-ci ait lancé une fois, à une date antérieure, une conférence avec authentification.

Sélection

A l'aide du numéro de sélection, chaque participant à la conférence peut s'inviter dans la conférence durant la période de temps programmée, indépendamment du sens d'établissement de la connexion configuré pour lui. Si la sélection est opérée en dehors de la période prévue, une annonce correspondante est diffusée. Lors de la sélection via un ITSP, il faut que celui-ci supporte RFC 2833 (caractères DTMF).

Authentification forcée avec la touche *

Le directeur de conférence peut configurer la conférence de manière à ce que chaque participant doive au moins s'authentifier en appuyant sur la touche *. Ainsi, seuls les abonnés présents sont reliés à la conférence, à l'exclusion des boîtes vocales.

Prolongation de la conférence

Dix minutes avant la fin de la conférence programmée, les participants à la conférence entendent une annonce indiquant que la conférence va bientôt se termine et qu'ils peuvent prolonger la conférence en sélectionnant un chiffre. Un participant à la conférence quelconque peut prolonger la conférence en sélectionnant le chiffre correspondant. Le directeur de conférence peut prolonger la conférence jusqu'à une heure quelconque dans.

Enregistrer la conférence

Le directeur de conférence peut enregistrer automatiquement ou manuellement la conférence, pour lui et pour tous les participants internes connectés, à condition que l'enregistrement des communications soit activé dans le système. Les abonnés du propre noeud reçoivent l'enregistrement dans la boîte vocale, les abonnés d'autres noeuds par e-mail. La durée de l'enregistrement est uniquement limitée par la capacité de mémoire du système de communication.

Terminer la conférence

La conférence se termine au moment de la fin programmée, mais elle peut être arrêtée avant lorsque le directeur de conférence la termine.

12.7.4 Conférence permanente

Une conférence permanente est illimitée dans le temps. Les participants à la conférence peuvent s'inviter à tout moment.

Le directeur de conférence enregistre la conférence Permanente sous un nom qui lui est propre. Elle demeure établie jusqu'à ce qu'il l'efface.

Options de configuration d'une conférence permanente

L'initiateur de la conférence peut définir les points suivants :

- Nécessité ou non pour les participants à la conférence d'entrer l'ID de conférence et le mot de passe sur le clavier du téléphone afin de s'authentifier.

  Remarque : Les utilisateurs Mobility Entry doivent entrer le code de numérotation de suffixe DTMF avant leur authentification.

  Le mot de passe par défaut des conférences est 123456. Le directeur de conférence peut le modifier individuellement pour chaque participant à la conférence.
- Langue dans laquelle les annonces sont diffusées au début de la conférence.

Démarrer la conférence

Dès que le premier participant à la conférence se connecte, le système ouvre automatiquement chez tous les participants à la conférence interne la fenêtre de la salle de conférence virtuelle dans la mesure où le participant à la conférence a démarré celle-ci avec myPortal xA0;for xA0;Desktop ou myPortal xA0;for xA0;Outlook. Tous les participants à la conférence s'inscrivent eux-mêmes. Le système de communication présente chaque nouveau participant par l'annonce : « … participe à la conférence. »

Sélection

À l'aide du numéro de sélection, chaque participant à la conférence peut s'inviter à tout moment dans la conférence. Lors de la sélection via un ITSP, il faut que celui-ci supporte RFC 2833 (caractères DTMF).

Enregistrer la conférence

Le directeur de conférence peut enregistrer la conférence, pour lui et pour tous les participants internes connectés, à condition que l'enregistrement des communications soit activé dans le système. Les abonnés du propre nœud reçoivent l'enregistrement dans la boîte vocale, les abonnés d'autres nœuds par e-mail. La durée de l'enregistrement est uniquement limitée par la capacité de mémoire du système de communication.

L'enregistrement automatique d'une conférence permanente démarre lorsque deux participants ou plus sont présents et il s'arrête lorsqu'il en reste moins de deux. Une fois l'enregistrement terminé, tous les participants obtiennent le même fichier d'enregistrement de la conférence entière.

12.7.5 Conférence ouverte

Une conférence ouverte est pour un nombre défini d'abonnés quelconque. Chaque abonné disposant des données d'accès peut y entrer.

Le directeur de conférence enregistre la conférence ouverte sous un nom qui lui est propre. Elle demeure établie jusqu'à ce qu'il l'efface.

Options de configuration d'une conférence ouverte

L'initiateur de la conférence peut définir les points suivants :

- Le nombre maximum de participants à la conférence (maxi. 16).
- Nécessité ou non pour les participants à la conférence d'entrer l'ID de conférence et le mot de passe sur le clavier du téléphone afin de s'authentifier.

  Remarque : Les abonnés Mobility Entry doivent entrer l'indicatif pour Numérotation MF avant leur authentification.

  Le mot de passe par défaut pour les conférences est 123456. Le directeur de conférence peut le modifier individuellement pour chaque participant à la conférence.
- L'ID de conférence commun valide pour tous les participants à la conférence.
- Langue dans laquelle les annonces sont diffusées au début de la conférence.

Démarrer la conférence

Tous les participants à la conférence s'inscrivent eux-mêmes. Le système de communication présente chaque nouveau participant par l'annonce : "… participe à la conférence."

Sélection

A l'aide du numéro de sélection, chaque participant à la conférence peut s'inviter à tout moment dans la conférence. Lors de la sélection via un ITSP, il faut que celui-ci supporte RFC 2833 (caractères DTMF).

Enregistrer la conférence

Le directeur de conférence peut enregistrer automatiquement ou manuellement la conférence, pour lui et pour tous les participants internes connectés, à condition que l'enregistrement des communications soit activé dans le système. Les abonnés du propre noeud reçoivent l'enregistrement dans la boîte vocale, les abonnés d'autres noeuds par e-mail. La durée de l'enregistrement est uniquement limitée par la capacité de mémoire du système de communication.

12.8 Messagerie instantanée

La messagerie instantanée est un moyen de communiqué directement (chat)

12.8.1 Messagerie instantanée

Vous pouvez chatter avec d'autres partenaires de communication à l'aide des messages instantanés. Le système prend en charge la messagerie instantanée avec les utilisateurs UC Smart et les partenaires de communication externes, ainsi que le chats multi-utilisateur (et une combinaison des deux).

Les messages instantanés sont possibles avec les clients suivants.

- myPortal for Desktop
- myPortal for Outlook
- myAgent

- myAttendant

En tant qu'administrateur, vous pouvez activer ou désactiver la messagerie instantanée pour l'ensemble du système. Les messages instantanés envoyés et reçus sont affichés sous forme de dialogue chez les partenaires de communication. Lors de la sélection du destinataire, le client indique si le partenaire de communication est momentanément en ligne ou non. Si un partenaire de communication est hors ligne, la messagerie instantanée réalise l'opération ci-après, en fonction du type de destinataire sélectionné :

Destinataires	Comportement
Abonnés individuels	Le message instantané est affiché lors de l'ouverture de session suivante.
Groupe dans Favoris	Le message instantané n'est jamais affiché pour les abonnés qui sont hors ligne.

Messages instantanés externes

En tant qu'abonné, vous pouvez également discuter (chat) avec *un* partenaire de communication externe (par exemple, un utilisateur de Google Talk).

Chat multi utilisateur

Le chat multi utilisateur est l'échange de messages instantanés avec plusieurs partenaires de communication. Dans ce cas, le système prend en charge un partenaire de communication externe au maximum.

12.8.1.1 Comment activer ou désactiver les messages instantanés

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Paramètres généraux**.
5) Dans la zone **Messagerie instantanée**, sélectionnez l'une des options suivantes :
   - Si vous souhaitez activer les messages instantanés sur l'ensemble du réseau, décochez la case **Désactiver l'envoi des messages instantanés**.
   - Si vous souhaitez désactiver les messages instantanés sur l'ensemble du réseau, cochez la case **Désactiver l'envoi des messages instantanés**.

   Remarque : La désactivation des messages instantanés ne s'applique pas à la fenêtre de messages instantanés actuelle.
6) Cliquez sur **Enregistrer**.

12.9 Standard automatique

Le standard automatique donne aux appelants, en fonction de l'état Présence de l'abonné appelé, des possibilités de choix pour le renvoi des appels vocaux vers des numéros définis ou vers leur boîte vocale. Les appelants font leur choix en entrant des chiffres sur le téléphone.

12.9.1 Standard automatique personnel

Le standard automatique personnel est le standard automatique configurable par l'abonné.

Standard automatique personnel

En tant qu'abonné, vous pouvez paramétrer les tâches suivants pour votre numéro d'appel, à l'aide de myPortal for Desktop ou myPortal for Outlook :

- Enregistrer ou importer des annonces pour le standard automatique personnel
- Configurer les profils pour le standard automatique personnel

Les appels correspondants sont tout d'abord traités par le standard automatique central.

12.10 Messages Voix et Fax

Les services Messages Voix et Fax intégrés dans le système permettent aux abonnés de recevoir et gérer les messages Voix et Fax, via myPortal for Desktop et myPortal for Outlook. Avec Fax Printer, les abonnés peuvent envoyer des messages Fax.

12.10.1 Boîte vocale

La boîte vocale enregistre de manière centralisée les messages Voix et les communications enregistrées. Les abonnés peuvent y accéder par téléphone et avec les clients UC Smart.

Remarque : Le mot de passe de boîte vocale par défaut peut uniquement être modifié via un numéro de téléphone interne.

Seuls sont enregistrés les messages vocaux d’une durée de plus de deux secondes.

Gestion des messages vocaux

En tant qu’abonné, vous pouvez écouter vos messages vocaux :

- sur PC avec myPortal for Desktop ou myPortal for Outlook
- sur votre téléphone si votre état Présence est **Bureau** ou **Appelle-moi**
- sur un téléphone externe quelconque

Le standard peut accéder à l'aide de myAttendant aux messages vocaux des abonnés qui l'autorisent.

L'abonné gère les messages vocaux arrivés en utilisant différents dossiers comme Lus, Sauvegardés ou Supprimés.

Les messages vocaux peuvent aussi être rediffusés, arrêtés et transmis à un autre abonné. De plus, l'abonné peut enregistrer les messages vocaux au format .wav et les adresser à n'importe quelle adresse e-mail.

A l'aide de la boîte vocale, l'abonné gère aussi les communications enregistrées. Celles-ci sont identifiées par une icône particulière dans la boîte vocale.

Remarque : Vous trouverez des informations sur le menu téléphone dans la documentation UC Suite Interface utilisateur (TUI), mode d'emploi abrégé.

Comment Rappeler l'expéditeur d'un message Voix

En écoutant le message vocal, l'abonné peut rappeler directement la personne qui lui a laissé le message.

En tant qu'administrateur, vous pouvez configurer pour l'ensemble du système, s'il est possible ou non d'effectuer des rappels automatiques à partir de la boîte vocale

- pour n'importe quel numéro
- uniquement pour les propres numéros de l'abonné, qui sont configurés dans les clients myPortal for Desktop, myPortal for Outlook, myAttendant ou myAgent, dans les données personnelles, (**Poste**, **Numéro mobile**, **Numéro de téléphone externe 1**, **Numéro de téléphone externe 2**, **Numéro de téléphone privé** et **Numéro de l'assistant**).

Durée de conservation

En tant qu'administrateur, vous pouvez configurer la durée de conservation des messages vocaux.

Priorisation des messages vocaux

Les appelants peuvent identifier les messages vocaux en tant que normaux, urgents ou confidentiels.

Dans myPortal for Desktop et myPortal for Outlook, la priorisation des messages vocaux est indiquée par des couleurs différentes.

Si l'abonné écoute ses messages vocaux au téléphone, il reçoit comme première information une indication précisant combien il a de messages urgents, confidentiels et normaux. Les messages urgents sont diffusés en premier.

Lorsque les messages vocaux sont renvoyés comme e-mails, les messages vocaux à priorité élevée sont identifiés en tant que e-mails à priorité élevée.

Eventail de fonctions pour la boîte vocale

L'administrateur peut définir l'éventail de la boîte vocale. Il a le choix entre :

- **Pleine**

  Eventail de fonctions complet pour la boîte vocale (valeur par défaut)

- **Menu abrégé**
- Après l'annonce liée à l'état ou personnelle, une liaison avec la réception est proposée.
- **Aucun Menu**
- Après l'annonce de bienvenue, l'appelant est transféré directement à l'enregistrement des messages.

Indication des nouveaux messages au téléphone

Les nouveaux messages vocaux sont signalés au téléphone. Dès que le message vocal a été diffusé, les affichages sont effacés.

Le mode de signalisation des nouveaux messages vocaux est spécifique du terminal.

- Sur tous les téléphones, il y a une signalisation acoustique par une tonalité d'invitation à numéroter.
- Sur les téléphones système sans écran, la touche Boîte aux lettres s'allume également (si programmée).
- Sur les téléphones système avec écran, la touche Boîte aux lettres s'allume (si programmée) et l'écran affiche un message.

Service de notification

Si l'abonné utilise myPortal for Desktop ou myPortal for Outlook, il peut définir si l'information concernant l'arrivée d'un nouveau message vocal doit être transférée ou non et vers quelle destination.

L'abonné peut définir si le message doit être transféré comme e-mail. De plus, l'abonné peut définir si, à l'arrivée d'un nouveau message vocal, il est informé par un appel téléphonique ou par un SMS.

Langue de la boîte vocale

En tant qu'administrateur, vous pouvez sélectionner pour l'ensemble du système la langue par défaut de la boîte vocale pour le menu et les annonces propres au système.

Correspondances

Rubrique	Correspondance
Ecouter un message sur le téléphone	L'abonné ne peut lire les messages Voix par téléphone que lorsque l'état Présence **Bureau** ou **Appelle-moi** est paramétré. Avec tous les autres paramètres, il peut uniquement consulter le message via un PC.

12.10.1.1 Comment configurer le numéro d'appel de la boîte vocale

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Messagerie vocale**.
4) Entrez le **numéro de boîte vocale**.
5) Cliquez sur **OK&Suite** puis sur **Quitter**.

12.10.1.2 Comment configurer le renvoi temporisé vers la boîte vocale

L'Assistant **Renvoi temporisé** vous permet de configurer pour un abonné le renvoi temporisé à sa boîte vocale.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Renvoi temporisé**. Ouverture de la fenêtre **Configurer la fonctionnalité "Renvoi temporisé"**.
4) Sélectionnez l'abonné souhaité dans la zone **Sélectionner un abonné**.
5) A l'aide de la souris, sélectionnez la **Boîte vocale** et déplacez-la dans la zone **Paramétrer le renvoi temporisé pour l'abonné**.
6) Si nécessaire, modifiez le délai du renvoi temporisé (par défaut : 15 secondes).
7) Cliquez sur **OK&Suite** puis sur **Quitter**.

12.10.1.3 Comment configurer les paramètres de la boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur l'onglet **Boîte vocale**.
5) Dans la liste déroulante **Langue Messagerie vocale**, sélectionnez la langue de gestion des menus et des annonces prédéfinies de votre boîte vocale.
6) Dans le champ **Ordre de lecture des messages Voix**, définissez dans quel ordre les messages doivent être diffusés.
7) Dans le champ **Temps d'enregistrement des messages Voix**, entrez la durée en secondes.
8) Définissez dans le champ **Mode Boîte vocale** le volume de votre boîte vocale.

9) Si vous souhaitez que les rappels depuis la boîte vocale ne soient effectués que pour les numéros de téléphone inscrits dans les UC Clients, dans **Mes détails personnels**, cochez **Autoriser le rappel de la MV uniquement pour les numéros connus**.
10) Si vous souhaitez désactiver la dernière annonce lue par le système, cochez la case **Ignorer l'invite « Veuillez laisser un message après le bip »**. L'annonce du système ne sera pas diffusée même si une annonce professionnelle est utilisée.
11) Cliquez sur **Enregistrer**.

12.10.1.4 Comment configurer la durée de conservation pour les messages vocaux

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Maintenance**.
5) Dans les champs de **Message**, indiquez le temps de conservation en jours
6) Cliquez sur **Sauvegarder**.

12.10.1.5 Comment activer ou désactiver la demande de mot de passe de la boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Répertoire utilisateur**.
4) Cliquez sur l'entrée correspondante, puis cliquez sur **Modifier** > **Sensibilité**.
5) Cliquez sur **Sécurité et accès**.
6) Sélectionnez l'une des options suivantes :
   - Si vous souhaitez activer la demande du mot de passe lors de l'appel de votre boîte vocale, décochez la case **Ne pas utiliser de mot de passe lors d'appel de la messagerie vocale**.
   - Si vous souhaitez désactiver la demande du mot de passe lors de l'appel de votre boîte vocale, cochez la case **Ne pas utiliser de mot de passe lors d'appel de la messagerie vocale**.
7) Cliquez sur **Enregistrer**.

12.10.1.6 Comment configurer les informations relatives aux messages vocaux reçus

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configur. de base**.
3) Dans l'arborescence du menu, cliquez sur **Système**.
4) Dans l'arborescence du menu, cliquez sur **Ecran**.
5) Dans la zone **Commande**, cochez la case **Affichage de l'état dans information**.
6) Cliquez sur **Appliquer** puis sur **OK**.

12.10.1.7 Comment configurer la touche Boîte aux lettres pour l'interrogation des messages vocaux

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphones/ Abonnés**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Programmation des touches**.
4) Sélectionnez l'abonné correspondant.
5) Sélectionnez dans la première colonne la touche correspondante.
6) Sélectionnez dans la colonne **Fonctions des touches** la fonction **Boîte aux lettres**.
7) Cliquez sur **Appliquer** puis sur **OK**.

12.10.2 Annonces de la boîte vocale

Les annonces de la boîte vocale informent les appelants par ex. de l'état de présence d'un abonné.

Les annonces par défaut sont disponibles dans toutes les langues. En tant qu'abonné, vous pouvez enregistrer ou importer des annonces de boîte vocale personnelles. L'annonce par défaut correspondante est remplacée par l'annonce personnelle. En tant qu'administrateur, vous pouvez modifier les annonces par défaut en important d'autres annonces. Les annonces personnelles des abonnés sont écrasées lors de cette opération. Lors de l'importation des annonces, le système effectue automatiquement une limitation du niveau et une normalisation afin de répondre aux exigences de "USA / TIA 968 Signal Power Limitations".

Remarque : Lorsque vous servez d'annonces ou de musique provenant d'une autre source, assurez-vous que vous ne violez aucun copyright.

Annonces dans la langue système de la boîte vocale

La langue système de la boîte vocale est réglée lors de l'initialisation du pays. De plus, l'abonné peut paramétrer lui-même la langue de sa boîte vocale. L'appelant entend les annonces spécifiques de l'abonné dans la langue choisie par l'abonné et les annonce spécifiques du système dans la langue système.

Annonces en correspondance avec l'état Présence et le profil

En fonction de l'état Présence réglé, les annonces de la boîte vocale sont modifiées automatiquement, par ex. lorsque l'état Présence est **Réunion**, l'annonce peut par ex. être la suivante : l'abonné est en réunion aujourd'hui jusqu'à 15h00. Lorsque la fin de la réunion indiquée est atteinte et que l'abonné n'a pas modifié son état Présence en le réglant sur Bureau, l'annonce de la boîte vocale est alors adaptée automatiquement ou bien l'état Présence passe automatiquement sur Bureau (configuration par l'abonné).

Le tableau ci-après indique le message d'accueil diffusé à l'appelant en fonction de l'état Présence réglé et du profil défini. Le menu Appelant correspond au standard automatique central. Le profil correspond ici au standard automatique personnel de l'abonné. Celui-ci doit enregistrer le message d'accueil par défaut, le nom et les messages d'accueil personnalisés correspondant aux profils. En fonction de la configuration, le menu Appelant peut avoir différentes longueurs ou aussi ne pas être disponible.

	Occupé(e) Pas de réponse Ne pas déranger	Réunion Sick Pause Déplacement ...
Boîte vocale ave état Présence	Message d'accueil par défaut + Menu Appelant	Nom + Présence + Menu Appelant
Boîte vocale lorsque l'état Présence est bloqué	Message d'accueil par défaut + Menu Appelant (si activé)	
Profil avec annonce dynamique	Message d'accueil défini par l'utilisateur pour le profil	Nom + Présence + Message d'accueil défini par l'utilisateur pour le profil
Profils, lorsque l'annonce dynamique doit être sautée	Message d'accueil défini par l'utilisateur pour le profil	

Si un abonné a décidé que son état Présence ne serait pas transmis à un appelant extérieur, l'appelant extérieur reçoit alors l'état de présence "Occupé" (sauf pour "Bureau") bien que l'abonné appelé ne soit pas occupé. Dans ce cas, l'abonné doit définir pour le message d'accueil "Occupé" un message indiquant qu'il ne peut pas prendre l'appel.

12.10.2.1 Comment importer une annonce pour la boîte vocale

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Les fichiers audio à charger sont disponibles sous forme de fichiers PCM aux caractéristiques suivantes : 8 kHz, 16 bits, mono. La longueur du nom du fichier audio est de 30 caractères au maximum.

Remarque : Vous pouvez préalablement créer des fichiers audio adaptés avec l'assistant Audio et, dans ce cas, mixer deux sources, par ex. musique d'arrière-fond et annonce..

Conseil : Avant l'utilisation, assurez-vous que vous ne violez aucun copyright.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Chargement du fichier**.
4) Dans l'onglet **Gestionnaire de fichiers audio**, sélectionnez comme **Destination de téléchargement** l'entrée **Message d'accueil de la boîte vocale**.
5) Si vous souhaitez enregistre un fichier audio, procédez comme indiqué ci-après.
   a) Sélectionnez le champ d'option **Téléchargeur** et cliquez sur **Choisir un fichier** pour sélectionner le fichier audio approprié.
   b) Dans la zone **Détails du fichier audio** figurent les caractéristiques du fichier audio comme le nom du fichier, la taille du fichier, le débit binaire, etc.
   c) Cliquez sur **Charger**.
6) Si vous souhaitez enregistrer un message d'annonce à l'aide d'un téléphone, procédez comme indiqué ci-après.
   a) Sélectionnez le champ d'option **Enregistreur** puis, dans **Poste**, sélectionnez le téléphone d'enregistrement de l'annonce.
   b) Dans **Nom de fichier**, entrez le nom du fichier d'enregistrement.
   c) Cliquez sur **Appeler**. Le téléphone sélectionné sonne.
   d) Décrochez le combiné et cliquez sur **Enregistrer**.
   e) Formulez votre annonce en parlant dans le combiné, puis cliquez sur **Quitter**.
   f) Utilisez **Lecture** pour écouter l'annonce que vous avez enregistrée.

12.10.2.2 Comment modifier la langue des annonces de la boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Boîte vocale**.
5) Sélectionnez la **Langue de la boîte vocale** dans la liste déroulante.
6) Cliquez sur **Enregistrer**.

12.10.3 Boîte Fax

La boîte Fax permet aux abonnés de recevoir et d'envoyer des messages Fax sans télécopieurs via myPortal for Desktop ou myPortal for Outlook.

En tant qu'administrateur, vous pouvez configurer une boîte Fax pour les abonnés sous licence. De plus, les fax ou serveurs fax peuvent être raccordés via l'interface a/b ou RNIS.

Via myPortal for Desktop ou myPortal for Outlook, vous accédez à vos messages fax en tant qu'abonné. myAttendant peut accéder aux messages fax des abonnés qui en donnent l'autorisation.

Gestion des messages fax

L'abonné peut gérer les messages fax reçus en les déplaçant vers d'autres dossiers (Sauvegardé(s) ou Supprimé(s) par exemple). Les messages fax peuvent aussi être transférés à un autre abonné. De plus, l'abonné peut enregistrer les messages fax au format PDF ou TIFF et les transférer vers n'importe quelle adresse e-mail.

L'administrateur peut déterminer pour l'ensemble du système si les messages fax sont enregistrés comme fichiers TIFF (par défaut) ou fichiers PDF.

Remarque : Pour convertir un fichier TIFF en fichier PDF, la taille de la page doit être A4.

Durée de conservation des messages fax

Le système efface automatiquement les messages Fax dont la durée de conservation est dépassée :

Message fax	Durée de conservation (jours)
Nouveau	120
Lu(s)	365
Envoyé(e)	365
Supprimé(s)	60

12.10.3.1 Comment ajouter une boîte Fax pour des abonnés

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphones/ Abonnés**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Terminaux IP**.
4) Cliquez dans le champ **Numéro Fax** de l'abonné et entrez le numéro de fax, permettant à l'abonné de recevoir les messages fax (supprimer le trait d'union paramétré).
5) Si un numéro SDA doit être configuré pour la boîte Fax, cliquez dans le champ **SDA Fax** et entrez le SDA Fax (supprimer le trait d'union paramétré).
6) Cliquez sur **OK&Suivant**. Si nécessaire, vous pouvez, à l'aide de **Imprimer** imprimer une liste des abonnés avec les numéros de fax configurés.
7) Cliquez sur **OK & Suivant**, puis sur **Terminer** pour fermer l'Assistant.

12.10.3.2 Comment configurer le type de fichier pour les messages fax enregistrer (UC Suite)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Paramètres généraux**.
5) Si vous voulez que les messages fax puissent être enregistrés comme fichiers PDF, cochez dans la zone **Format Fax** la case **Use PDF as Fax Format** (Utiliser PDF comme format fax).
6) Si vous voulez que les messages fax puissent être enregistrés comme fichiers TIFF, cochez dans la zone **Format Fax** la case **Use TIFF as Fax Format** (Utiliser TIFF comme format fax).
7) Cliquez sur **Sauvegarder**.

12.10.4 Envoi de messages Fax avec Fax Printer

Fax Printer est une application pour l’envoi de messages Fax à partir d’applications Windows comme Microsoft Word, avec pages de garde centralisées ou pages de garde individualisées.

Fax Printer (imprimante Fax) comprend les composantes suivantes :

- Fax Printer Cover Editor

- Fax Printer Driver

Fax Printer peut être utilisé avec tous les programmes Windows courants. Les groupes fax facilitent la distribution. Les messages Fax sont envoyés comme e-mails ou directement sur le bureau. Une fenêtre contextuelle informe l'abonné de l'envoi réussi.

Lignes d'en-tête

En tant qu'administrateur, vous pouvez configurer différentes lignes d'en-tête pour les utilisateurs de Fax Printer. Vous pouvez définir une ligne d'en-tête par défaut. Les lignes d'en-tête peuvent comporter les éléments suivants :

Détails	Joker
Date/Heure	`{{date_time}}`
Nom de la société	`{{company_name}}`
Nom utilisateur	`{{user_name}}`
Tél. société	`{{company_number}}`
Numéro de page	`{{page_number}}`
Nombre de pages	`{{page_count}}`

Les lignes d'en-tête de messages Fax qui sont envoyées avec Fax Printer doivent comporter uniquement des caractères du jeu de caractères ANSI. C'est-à-dire qu'il ne doit pas y avoir de caractères spéciaux ou d'inflexions. Comme la ligne d'en-tête peut, par principe, comporter le nom de l'émetteur, les noms des abonnés ne doivent donc comporter aucun caractère spécial ou inflexion.

12.10.4.1 Comment ajouter une page de garde de fax

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Une page de garde de fax est disponible sous forme de fichier .ovp.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Chargement du fichier**.
4) Cliquez sur l'onglet **Chargement de la page de garde Fax centrale**.
5) Cliquez sur **Choisir un fichier**.
6) Sélectionnez un fichier .ocp.
7) Cliquez sur **Ouvrir**.
8) Dans **Nom**, entrez un nom pour la page de garde Fax.
9) Entrez une **Description** pour la page de garde Fax.
10) Cliquez sur **Charger**.
11) Une fois le chargement terminé, cliquez sur **OK**.

12) Si vous souhaitez que cette page de garde Fax devienne la page par défaut, cliquez dans la liste des pages de garde Fax sur cette page, puis sur **Paramétrer comme valeur par défaut**.
13) Cliquez sur **Enregistrer**.

12.10.4.2 Comment modifier la page de garde centrale

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Chargement du fichier**.
4) Cliquez sur l'onglet **Chargement de la page de garde Fax centrale**.
5) Dans la liste des pages de garde de fax cliquez sur la page de garde correspondante.
6) Cliquez sur **Modifier**.
7) Dans **Nom**, entrez un nom pour la page de garde Fax.
8) Entrez une **Description** pour la page de garde Fax.
9) Cliquez sur **Enregistrer**.

12.10.4.3 Comment ajouter la ligne d'en-tête pour Fax Printer

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Lignes d'en-tête de fax**.
4) Cliquez sur **Ajouter**.
5) Entrez le **Nom du modèle** pour la ligne d'en-tête de fax.
6) Pour ajouter des détails à la ligne d'en-tête, cliquez sur les boutons **Date/ Heure**, **Nom de la société**, **Nom d'utilisateur**, **Tél. société**, **Numéro de page** et **Nombre de pages** dans l'ordre souhaité. Pour chaque détail, un joker correspondant apparaît dans le champ **Texte**.
7) Pour supprimer un détail dans la ligne d'en-tête, sélectionnez dans le champ **Texte** le joker correspondant, par ex. `{{page_count}}` (**Nombre de pages**) et appuyez sur la touche `Suppr`.
8) Si nécessaire, saisissez le texte supplémentaire dans le champ **Texte**, par exemple "de" entre les jokers `{{page_number}}` (**Nombre de pages**) et `{{page_count}}` (**Nombre des pages**).
9) Cliquez sur **Enregistrer**.

12.10.4.4 Comment changer la ligne d'en-tête pour Fax Printer

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence du menu, cliquez sur **Applications** > **Suite UC**.
3) Cliquez sur **Lignes d'en-tête de fax**.
4) Dans la liste des lignes d'en-tête de fax, cliquez sur la ligne d'en-tête souhaitée.
5) Cliquez sur **Modifier**.
6) Entrez le **Nom du modèle** pour la ligne d'en-tête de fax.
7) Pour ajouter des détails à la ligne d'en-tête, cliquez sur les boutons **Date/ Heure**, **Nom de la société**, **Nom d'utilisateur**, **Tél. société**, **Numéro de page** et **Nombre de pages** dans l'ordre souhaité. Pour chaque détail, un joker correspondant apparaît dans le champ **Texte**.
8) Pour supprimer un détail dans la ligne d'en-tête, sélectionnez dans le champ **Texte** le joker correspondant, par ex. `{{page_count}}` (**Nombre de pages**) et appuyez sur la touche `Suppr`.
9) Si nécessaire, saisissez le texte supplémentaire dans le champ **Texte**, par exemple « de » entre les jokers `{{page_number}}` (**Nombre de pages**) et `{{page_count}}` (**Nombre des pages**).
10) Cliquez sur **Enregistrer**.

12.10.4.5 Comment effacer la ligne d'en-tête pour Fax Printer

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Lignes d'en-tête de fax**.
4) Dans la liste des lignes d'en-tête de fax, cliquez sur la ligne d'en-tête souhaitée.
5) Cliquez sur **Supprimer**.

12.10.5 Service de notification pour les nouveaux messages (UC Suite)

Le système peut vous informer, en tant qu'abonné, d'un nouveau message, au choix par e-mail, par téléphone ou par SMS.

Le service de notification travaille de la manière suivante.

Notification	pour message Voix	pour Message fax	Condition
E-mail	Vous recevez un e-mail avec le message en tant que fichier WAV joint, la date et l'heure de la réception, la durée du message et, si disponibles, le numéro et le nom de l'expéditeur. Si la taille du fichier WAV dépasse 10 MB (en moyenne, 1 Mo/min), il n'est pas joint au e-mail. Les messages Voix de priorité "Urgent" sont transmis comme e-mails d'importance "haute". Les e-mails avec message voix sont identifiés par une icône spécifique dans Outlook. Si vous utilisez une messagerie IMAP, qui indique uniquement l'en-tête de l'e-mail, il apparaît alors à sa place l'icône e-mail habituelle.	Vous recevez un e-mail avec le message en tant que fichier PDF ou TIFF joint, la date et l'heure de la réception, le nombre de pages et, si disponibles, le numéro et le nom de l'expéditeur. Si la taille du fichier PDF ou TIFF dépasse 10 MB, il n'est pas joint à l'e-mail. Les e-mails avec message fax sont identifiés par une icône spécifique dans Outlook. Si vous utilisez une messagerie IMAP, qui indique uniquement l'en-tête de l'e-mail, il apparaît alors à sa place l'icône e-mail habituelle.	L'envoi d'e-mails est configuré dans le système. L'adresse correspondante est utilisée comme expéditeur.
SMS	A la réception d'un message, vous recevez un SMS au numéro de téléphone que vous avez indiqué.		Le modèle de SMS est configuré
téléphonique	Votre boîte vocale vous appelle sous le numéro que vous avez défini vous-même et diffuse le message.	-	

En tant qu'abonné, vous pouvez activer ou désactiver séparément chaque type de notification pour chaque état Présence. Vous pouvez limiter la notification téléphonique aux horaires de travail configurés par votre administrateur. Vous pouvez définir le nombre et l'intervalle des tentatives répétées de notification téléphonique.

12.10.6 Envoi d'e-mails

L'envoi d'e-mails permet d'envoyer une notification aux abonnés lors de la réception de nouveaux messages Voix et Fax ainsi qu'à l'administrateur en cas de messages système.

12.10.6.1 Comment configurer l'envoi d'e-mails

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Un compte e-mail est configuré chez un fournisseur d’e-mail avec un mot de passe et vous connaissez les données d’accès.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Centre de service** > **Renvoi E-Mail**.
3) Saisissez le **serveur de messagerie sortant (SMTP)** pour le serveur de messagerie qui doit être utilisé pour l'envoi d'e-mails, par ex. `smtp.web.fr`. Si nécessaire, interrogez le serveur de la boîte d'envoi ou bien votre fournisseur e-mail.

   Remarque : Dans certains cas, l'envoi d'e-mails ne fonctionne pas car le nom du serveur de la boîte d'envoi ne peut pas être résolu. Pour résoudre le problème, vous devez entrer l'adresse IP du serveur à la place du nom.

4) Si une connexion sécurisée est requise, cochez la case. Demandez le cas échéant à votre fournisseur d'e-mail, si cette option doit être activée.
5) Saisissez le **Nom d'utilisateur** du compte e-mail.
6) Dans **Mot de passe** et **Répéter le mot de passe**, saisissez le mot de passe du compte e-mail.
7) Saisissez l'**Adresse e-mail**, par ex. `jean.exemple@web.fr`.
8) Si vous souhaitez tester l'envoi d'e-mails, procédez comme indiqué ci-après.
   a) Cliquez sur **Tester la connexion**.
   b) Dans **Envoyer à l'adresse e-mail**, saisissez l'adresse e-mail de la messagerie e-mail à laquelle vous avez accès.
   c) Indiquez l'**Objet** dans l'e-mail.
   d) Cliquez sur **Envoyer un e-mail de test**.
   e) Vérifiez si vous avez bien reçu l'e-mail.
   f) Si l'envoi d'e-mails ne s'est pas bien déroulé, cliquez sur **Retour** et corrigez vos paramètres e-mail (à partir du point 3).
9) Saisissez l'**adresse e-mail 1** pour obtenir un e-mail de notification lorsque la tolérance ALI a été utilisée. Vous pouvez aussi entrer une seconde adresse électronique.
10) Cliquez sur **OK & Suivant**, puis sur **Quitter**.

Exemple

Remarque : Si vous modifiez la configuration du renvoi d'e-mail sur un système OpenScape Business X avec Booster Server, vous devez redémarrer le Booster Server pour que ces modifications aient lieu.

12.10.7 Modèle de SMS

Un modèle de SMS permet d'envoyer une notification par SMS aux abonnés lors de l'arrivée de nouveaux messages Voix.

Pour la réception des e-mails SMS, il faut d'abord activer une adresse e-mail mobile personnelle du fournisseur concerné. L'abonné envoie pour cela un

SMS d'activation à un numéro abrégé. L'abonné reçoit alors par SMS son adresse e-mail personnelle qui se compose en règle générale du numéro et du nom de la passerelle. Ainsi, par exemple pour un client T-Mobile avec le numéro 0171/1234 567, l'adresse e-mail mobile serait : 01711234567@t-mobile-sms.de. Cela s'applique de manière similaire pour les autres réseaux.

Un modèle de SMS se compose des plages Détails du modèle et Détails SMS. L'administrateur doit entrer dans la plage Détails du modèle le nom du modèle, qui est généralement le nom du fournisseur d'e-mail en SMS.

Les indications concernant les détails du SMS sont fonction du fournisseur. Dans Destinataire, l'administrateur doit entrer l'adresse e-mail à laquelle le SMS doit être envoyé. Les indications de la ligne Objet peuvent être choisies librement, ou l'administrateur doit entrer ici par ex. le numéro du client.

Remarque : chaque fournisseur a besoin d'un modèle spécifique. Vous trouverez les données nécessaires chez le fournisseur de services de téléphonie mobile correspondant.

Joker

Les modèles de SMS peuvent comporter les jokers suivants dans le champ **Destinataires**, **Objet** ou **Texte** :

Détail	Joker
Le numéro mobile auquel sont adressés les envois	`{{MobileNumber}}`
Nom ou Numéro de l'émetteur	`{{Sender}}`
Message Date et heure reçu	`{{DateTime}}`
Le numéro de l'appelant	`{{CallingNumber}}`
Priorité du message	`{{Priority}}`

Informations spécifiques du système

La longueur du message est réduite aux 160 premiers caractères.

12.10.7.1 Comment ajouter un modèle de SMS

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Modèles**.
4) Cliquez sur **Ajouter**.
5) Entrez le **Nom du modèle**.

Remarque : Le nom du modèle ne doit pas inclure d'espaces.

6) Entrez le nom de l'auteur sous **Nom de l'auteur**.
7) Si vous souhaitez ajouter un joker, procédez comme suit :
   a) Cliquez dans le champ où vous souhaitez insérer le joker : **Destinataires**, **Objet** ou **Texte**.
   b) Dans la liste déroulante **Champs VSL**, sélectionnez le joker souhaité.
   c) Cliquez sur **Insérer**.
   d) Si vous souhaitez insérer d'autres jokers, répétez l'étape 7a-c.
8) Entrez le **destinataire**.
9) Entrez l'**objet**.
10) Entrez le **texte**.
11) Cliquez sur **Créer**.

12.10.7.2 Comment modifier le modèle SMS

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Modèles**.
4) Dans le tableau **Fournisseur SMS**, sélectionnez le modèle de SMS souhaité.
5) Cliquez sur **Modifier**.
6) Entrez le **Nom du modèle**.

Remarque : Le nom du modèle ne doit pas inclure d'espaces.

---

7) Entrez le nom de l'auteur sous **Nom de l'auteur**.
8) Si vous souhaitez ajouter un joker, procédez comme suit :
   a) Cliquez dans le champ où vous souhaitez insérer le joker : **Destinataires**, **Objet** ou **Texte**.
   b) Dans la liste déroulante **Champs VSL**, sélectionnez le joker souhaité.
   c) Cliquez sur **Insérer**.
   d) Si vous souhaitez insérer d'autres jokers, répétez l'étape 8a-c.
9) Entrez le **destinataire**.
10) Entrez l'**objet**.
11) Entrez le **texte**.
12) Cliquez sur **Créer**.

12.10.7.3 Comment supprimer un modèle de SMS

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Modèles**.
4) Dans le tableau **Fournisseur SMS**, sélectionnez le modèle de SMS souhaité.
5) Cliquez sur **Supprimer**.
6) Cliquez sur **OK**.

12.10.8 Fax sur IP (T.38 / G.711 Fax)

Le fax sur IP permet la transmission de messages fax sur Internet conformément aux normes G2 et G3 en utilisant le protocole réseau IFP (Internet Facsimile Protocol).

UC Suite peut généralement gérer jusqu'à 8 connexions fax simultanées. Selon le module DSP, OpenScape Business X5/X8, en tant que passerelle ISDN, peut gérer de 3 à 12 télécopies simultanées. Les deux paramètres déterminent le nombre de connexions fax T.38 ou G.711 simultanées.

Remarque : Il est fortement recommandé d'utiliser le fax T.38, si possible.

Le système prend en charge les scénarios suivants pour T.38 ou G.711 :

- Un abonné reçoit des fax via un fournisseur de services de téléphonie sur Internet (ITSP) sur sa boîte fax et envoie des fax vers des destinations externes grâce à une imprimante fax via l'ITSP.
- Un abonné reçoit des messages fax via un Mediatrix 4102S (SIP) à sa boîte fax et envoie des fax avec Fax Printer via un Mediatrix 4102S (SIP).
- Les stations peuvent recevoir des messages fax via un fournisseur de services de téléphonie sur Internet (ITSP) sur un télécopieur directement connecté à une interface analogique ou RNIS et envoyer des fax depuis ce télécopieur via l'ITSP vers des destinations externes.
- Les stations peuvent recevoir des messages fax via un ITSP sur un appareil fax connecté à un Mediatrix 4102S et envoyer des fax depuis cet appareil fax via le Mediatrix 4102S et l'ITSP vers des destinations externes.
- Les stations peuvent recevoir des messages fax via ISDN sur un télécopieur connecté à un Mediatrix 4102S et envoyer des fax depuis ce télécopieur via le Mediatrix 4102S et ISDN vers des destinations externes.
- Une station peut envoyer des messages fax depuis un appareil fax connecté à un Mediatrix 4102S vers un autre appareil fax également connecté à un Mediatrix 4102S.
- Message de fax interne d'un télécopieur sur un port ISDN vers un télécopieur sur un Mediatrix 4102S et vice versa.
- Message de fax interne entre un télécopieur connecté à un port RNIS et un télécopieur.

Remarque : Le protocole T.38 doit être activé dans le système pour le boîtier fax. Pour envoyer des fax depuis le système de communication via un ITSP, l'ITSP doit prendre en charge T.38.

Si le fournisseur de services de télécommunications (ITSP) ne peut pas passer au format T.38, le fax sera traité comme un G.711.

12.10.8.1 Comment activer ou désactiver Fax over IP (Fax T.38)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence du menu, cliquez sur **Passerelle vocale**.
4) Dans l'arborescence du menu, cliquez sur **Paramètres de Codec**.
5) Dans la zone **Fax T.38**, sélectionnez l'une des possibilités suivantes.
   - Si vous souhaitez activer Fax over IP (Fax T.38), cochez la case **Fax T.38**.
   - Si vous souhaitez désactiver Fax over IP (Fax T.38), décochez la case **Fax T.38**.
6) Cliquez sur **Appliquer** puis sur **OK**.

12.11 Présentation de l’intégration Microsoft Office 365

Vous pouvez collaborer en toute simplicité en accédant aux e-mails, aux conférences Web, aux documents et aux calendriers où que vous soyez. L’intégration inclut une sécurité de pointe et est garantie par Microsoft. Que vous soyez une petite entreprise ou une multinationale, Office 365 propose plusieurs forfaits conçus pour répondre aux besoins uniques de votre entreprise. Pour obtenir plus de détails ou une version d’essai de 30 jours, rendez-vous sur

OpenScape Business avec Microsoft Office 365

Lorsqu’un utilisateur créé un rendez-vous dans son calendrier Microsoft Outlook, le système OpenScape Business recherche automatiquement des mots-clés dans l’objet du rendez-vous du calendrier, notamment : Si un mot-clé est trouvé, le système configure automatiquement l’état de présence de l’utilisateur au moment du rendez-vous, même si la session Microsoft Outlook de cet utilisateur n’est plus active.

L’utilisateur configure les rendez-vous à l’aide de ces mots-clés et OpenScape Business définit automatiquement l’état de présence du téléphone de l’utilisateur et transfère les appels vers la boîte vocale ou, par exemple, sur le téléphone mobile, selon les paramètres définis. L’utilisateur peut également configurer un état client général pour que l’état de présence repasse à « Bureau » une fois le rendez-vous terminé.

Cela fonctionne également lorsque l’utilisateur n’utilise pas le client Outlook local et créé un rendez-vous avec les mots-clés indiqués ci-dessus directement à partir de la page Web Outlook dans le Cloud.

Renvoi d’e-mail :

OpenScape Business peut envoyer des e-mails à Microsoft Office 365, y compris via Microsoft Exchange Server.

Cela permet aux utilisateurs de recevoir des e-mails pour de nouveaux messages vocaux, télécopies ou appels de conférence.

OpenScape Business génère des e-mails pour ce type d’actions et informe les utilisateurs par e-mail dès qu’une nouvelle notification arrive dans la messagerie OpenScape Business.

L'intégration avec les services Microsoft Office 365 est effectuée à l'aide de l'API Microsoft Graph avec OAuth 2.0, en remplacement des services Web Exchange (EWS).

12.11.1 Comment connecter le système OpenScape Business à Microsoft Office 365

Vous pouvez connecter le système OpenScape Business à Microsoft Office 365 dans le cloud à l’aide de l’authentification Microsoft OAuth 2.0. À compter d’octobre 2026, les fonctionnalités OpenScape Business Exchange Calendar Integration, Email Forwarding et les contacts personnels nécessitent les autorisations de l’API Microsoft Graph.

Conditions préalables

- Microsoft Office 365 Enterprise E3 ou version ultérieure avec les applications « Microsoft 365 Apps » installées localement.
- Les utilisateurs sont présents dans Microsoft Office 365 et Microsoft Outlook, installé localement, est connecté à Microsoft Exchange Online.
- Toutes les mises à jour et tous les Service Packs Microsoft disponibles sont installés.
- Vérifiez que vous disposez des licences Microsoft Enterprise requises.
- Consultez les notes de publication d’OpenScape Business pour connaître les versions de Microsoft Office prises en charge.
- Microsoft 365 Apps doit être installé localement.

Remarques importantes :

- Modifiez la valeur du domaine Microsoft Office 365 (par exemple : test.onmicrosoft.com) afin qu’elle corresponde aux paramètres de votre environnement.
- L’enregistrement de l’application (Microsoft Entra ID) nécessite les autorisations suivantes :
  - Intégration des contacts : l’autorisation Microsoft Graph « Contacts.Read » est requise avec le consentement de l’administrateur.
  - Intégration du calendrier : l’autorisation Microsoft Graph « Calendars.ReadWrite » est requise avec le consentement de l’administrateur.
  - Transfert des e-mails : l’autorisation Microsoft Graph « SMTP.Send » est requise avec le consentement de l’administrateur.
- Accès aux dossiers publics Microsoft Exchange : l’accès programmatique aux dossiers publics est limité aux seuls clients Outlook pris en charge ainsi qu’aux opérations d’importation et d’exportation en masse effectuées

par Microsoft. À compter d'octobre 2026, Microsoft ne fournira plus d'API permettant de créer, lire, mettre à jour et supprimer des dossiers publics par programmation. https://techcommunity.microsoft.com/blog/exchange/retirement-of-exchange-web-services-in-exchange-online/3924440

- Pour les installations existantes, reportez-vous à la documentation d'administration d'OpenScape Business V3.

Étape par étape

1) Connectez-vous à votre locataire Microsoft sur le site web officiel de Microsoft.

   Un abonnement valide à **Microsoft Exchange Online** avec **Microsoft 365 Apps** installé localement est obligatoire.

2) Connectez-vous au Centre d'administration Microsoft 365, puis accédez à **Utilisateurs > Utilisateurs actifs**. Créez un utilisateur de test et attribuez-lui une adresse e-mail valide ainsi qu'une licence Microsoft 365.

3) Déconnectez-vous du Centre d'administration Microsoft 365, puis connectez-vous avec le nouvel utilisateur créé afin de modifier le mot de passe temporaire.

   Assurez-vous que l'utilisateur est présent dans le **répertoire des utilisateurs Microsoft Office 365**, qu'il s'est déjà connecté à son profil et qu'il peut se connecter à sa boîte vocale **Microsoft Office 365** à l'aide de Microsoft Outlook installé localement. Cette installation locale de Microsoft Office 365 doit être connectée au portail Microsoft Office 365 et être mise à jour avec toutes les mises à jour Microsoft disponibles.

4) Pour le transfert des e-mails, accédez à OpenScape Business WBM, puis à **Centre de service > Transfert des e-mails** afin de configurer une adresse e-mail associée à Microsoft Office 365.

   Pour cette étape, vous aurez besoin d'un enregistrement d'application, d'un compte de service disposant d'une adresse e-mail et d'une licence Microsoft 365.

   L'authentification OAuth est disponible pour les connexions POP3, IMAP4 et SMTP AUTH à Exchange Online. L'activation de l'envoi SMTP authentifié par le client dans Exchange Online est obligatoire pour ce compte de service. Vous trouverez des instructions supplémentaires en suivant le lien ci-dessous https://docs.microsoft.com/en-us/%20exchange/clients-and-mobile-in-exchangeonline/authenticated-client-smtp-submission

5) Pour l'intégration du calendrier Exchange et des contacts, accédez à OpenScape Business WBM, puis à Configuration > UC Suite > **Configuration des fournisseurs externes**, et appliquez les paramètres suivants pour vous connecter au serveur Microsoft Office 365 :

   a) Modifiez la valeur du domaine Microsoft Office 365 afin qu'elle corresponde aux paramètres de votre environnement.

   b) L'enregistrement d'application **Microsoft Entra ID** nécessite les autorisations suivantes pour accéder aux informations de calendrier et de contacts :

      - Intégration des contacts, MS Graph « Contacts.Read »
      - Intégration du calendrier, MS Graph « Calendars.Read.Write »

      Ces modifications permettront à OpenScape Business d'accéder à Microsoft Exchange.

6) Assurez-vous que la suite Microsoft Office est installée sur l'ordinateur de l'utilisateur et connectée à Microsoft Office 365 et, si ce n'est pas déjà fait, installez CommunicationsClients en sélectionnant au minimum l'option myPortal for Outlook.
   a) Ouvrez le chemin suivant dans l'Explorateur Windows selon la syntaxe suivante : \\\applications\installcommon\CommunicationsClients.exe
   b) Connectez-vous à l'aide des identifiants WBM et suivez l'Assistant de configuration pour installer au minimum l'option myPortal for Outlook.
7) Ouvrez Microsoft Outlook et connectez-vous au système OpenScape Business à l'aide des identifiants de l'utilisateur via les clients OpenScape Business. Pour plus d'informations, consultez le guide de l'utilisateur de myPortal for Outlook.

   Remarque : Vous pouvez également utiliser l'option **Installation silencieuse** pour installer CommunicationsClients de manière non assistée sur les ordinateurs des utilisateurs. Pour plus d'informations, consultez Installation/Désinstallation silencieuse pour PC client UC Suite à la page 496.

8) Accédez à **WBM > Configuration > UC Suite > Répertoire utilisateur** pour ajouter l'adresse e-mail de l'utilisateur.

   Avec cette configuration, OpenScape Business enverra automatiquement un e-mail de bienvenue à toutes les nouvelles adresses e-mail saisies.

   Remarque : Vous pouvez également effectuer cette étape dans **WBM > Configuration > UC Suite > Répertoire des utilisateurs**.

   Remarque : Une adresse e-mail valide configurée est nécessaire pour utiliser l'intégration du calendrier Exchange ainsi que pour recevoir la notification facultative par e-mail lorsqu'un utilisateur reçoit un message d'OpenScape Business.

   Répétez cette étape pour tous les utilisateurs.
9) Accédez à **WBM > Configuration > UC Suite > Profils** pour configurer la fonctionnalité d'**intégration du calendrier Exchange**.
   a) Sélectionnez l'utilisateur pour lequel vous souhaitez activer cette fonctionnalité, cliquez sur **Modifier**, puis sur **Mes préférences > Connectivité Outlook**.
   b) Sélectionnez l'option **Intégration du calendrier Exchange** dans la section **Intégration du calendrier**
   c) Cochez la case **Générer automatiquement des rendez-vous dans le calendrier à partir de mes changements de présence**
   d) Sélectionnez **Exchange PST** dans la liste déroulante.

   Répétez cette étape pour tous les utilisateurs.
10) Accédez à **WBM > Configuration > UC Suite > Profils**. Sélectionnez l'utilisateur que vous souhaitez configurer, puis cliquez sur **VM Notification** afin de définir si des notifications par e-mail concernant les messages

vocaux doivent être envoyées pour certains états de présence lorsqu'un nouveau message vocal est enregistré dans la boîte vocale de l'utilisateur.

Répétez cette étape pour tous les utilisateurs. Cette étape est facultative.

11) Accédez à **WBM > Configuration > UC Suite > Profils**. Sélectionnez l'utilisateur que vous souhaitez configurer, puis cliquez sur **Fax Notification** afin de définir si les notifications de fax concernant les messages vocaux doivent être envoyées pour certains états de présence lorsqu'un nouveau fax est enregistré dans la boîte vocale de l'utilisateur.

Répétez cette étape pour tous les utilisateurs. Cette étape est facultative.

12.11.2 Comment vérifier que les fonctionnalités de l'intégration Microsoft Office 365 sont configurées

E-mail :

Dans WBM, vous pouvez tester la fonction E-mail à l'aide du bouton **Tester le renvoi d'e-mail** sous **Centre de service > Renvoi d'e-mail**. Saisissez une adresse e-mail valide en tant que destinataire et vérifiez que l'e-mail de test est bien reçu dans la boîte de réception de ce compte de messagerie.

Intégration du calendrier Exchange :

Lorsqu'un utilisateur créé un rendez-vous dans son calendrier Microsoft Outlook, le système OpenScape Business recherche automatiquement des mots-clés dans l'objet du rendez-vous du calendrier, notamment : « Réunion », « Maladie », « Pause », « Absence du bureau », « Congé », « Déjeuner » et « Domicile ». Si un mot-clé est trouvé, le système configure automatiquement l'état de présence de l'utilisateur au moment du rendez-vous, même si la session Microsoft Outlook de cet utilisateur n'est plus active. L'utilisateur configure les rendez-vous à l'aide de ces mots-clés et OpenScape Business définit automatiquement l'état de présence du téléphone de l'utilisateur et transfère les appels vers la boîte vocale ou, par exemple, sur le téléphone mobile, selon l'état de présence défini et la cible de renvoi spécifiée par l'utilisateur. L'utilisateur peut également configurer un état client général pour que l'état de présence repasse à « Bureau » une fois le rendez-vous terminé. Cela fonctionne également lorsque l'utilisateur n'utilise pas le client Outlook local et créé le rendez-vous avec les mots-clés indiqués ci-dessus directement sur la page Web Outlook dans Outlook Web Access.

L'utilisateur qui utilise l'intégration du calendrier Exchange ou Outlook local doit disposer d'une adresse e-mail valide dans sa configuration de client UC Suite, ainsi que des paramètres Outlook de client UC Suite tels que définis dans le manuel ci-dessus. La combinaison Utilisateur UC Suite et Utilisateur Exchange doit obligatoirement s'opérer à l'aide de l'adresse e-mail renseignée.

Le paramètre de langue de la boîte vocale des utilisateurs UC Suite permet de combiner les mots-clés, tels que Réunion, Maladie, Pause, Absence du bureau, Congé, Déjeuner et Domicile, à la langue de l'utilisateur. Par exemple, si la boîte vocale est configurée en allemand, les mots-clés allemands seront recherchés dans l'objet des rendez-vous, comme Besprechung, Krank, Pause, AuEer Haus, Urlaub, Mittag ou Zu Hause uniquement.

Si l'option « Retour automatique au bureau » n'est pas sélectionnée, l'état de présence de l'utilisateur n'est pas modifié à la fin du rendez-vous, et l'heure

de retour indiquée pour les autres utilisateurs ou appelants augmente toutes les 15 minutes. Si l'option « Retour automatique au bureau » est sélectionnée, l'état de présence de l'utilisateur repasse automatiquement à « Bureau » à la fin du rendez-vous.

Les rendez-vous programmés moins de 3 minutes à l'avance sont ignorés, car le système suppose que l'utilisateur est en train de créer un nouveau rendez-vous et que la situation peut totalement changer au cours de ces 3 minutes. Le système de communication vérifie les rendez-vous dans le calendrier des utilisateurs toutes les 30 secondes. Dans ce contexte et en raison des éventuels délais de transmission entre le système de communication et Exchange Server, nous vous recommandons de définir des rendez-vous de test plus de 3 minutes et 30 secondes à l'avance. Programmer les rendez-vous de test plus de 5 minutes à l'avance permet d'éviter d'éventuels retards de transmission entre le système de communication et le serveur Exchange, et de tenir compte du délai de 30 secondes nécessaire pour lire les entrées du calendrier.

Toutes les valeurs des nouveaux rendez-vous sont lues dans la minute suivant l'heure de début de rendez-vous définie, dans le cadre des requêtes de lecture de 30 secondes susmentionnées. Par conséquent, lorsque l'heure de début est atteinte, gardez à l'esprit que le délai de requête de 30 secondes doit être effectué au cours de cette minute avant que l'état de présence soit défini. La requête définit également l'heure de retour des utilisateurs en fonction de l'heure de fin du rendez-vous.

Pour tester la fonctionnalité lorsque la session myPortal for Outlook ou myPortal for Desktop de l'utilisateur est fermée, utilisez la page Web Outlook dans Outlook Web Access. Connectez-vous avec les identifiants de l'utilisateur et ajoutez le rendez-vous avec le mot-clé dans le calendrier. Vérifiez dans un autre client UC Suite que l'état de présence change à l'heure de début du rendez-vous.

13 Fonctions du téléphone

Le système de communication offre de nombreuses fonctionnalités téléphoniques, par ex. mise en garde, va-et-vient et double appel, ou encore des signalisations d'appel diverses, sans parler du renvoi temporisé et du renvoi d'appel.

13.1 Appeler

Le système de communication offre différentes possibilités pour effectuer les appels, notamment Appel direct ou Numéro abrégé.

13.1.1 Composition de chiffres

Lors de la composition de chiffres, chaque chiffres est envoyé directement après avoir été entré.

L'établissement de la liaison débute immédiatement après la saisie des premiers chiffres. L'abonné n'a pas ainsi la possibilité de modifier la sélection.

13.1.2 Numérotation par blocs

Dans la numérotation en bloc, la communication est établie lorsque le numéro complet a été entré. Le numéro est transféré en un seul bloc.

L'émission de la numérotation peut être lancée par l'entrée du caractère de fin de numérotation #.

La sélection de bloc est obligatoire pour :

- ITSP-Raccordement réseau
- Raccordement primaire multiplex aux Etats-Unis

Si aucun chiffre n'est entré dans un délai de 5 secondes, la dernier chiffre entré est considéré comme le dernier chiffre de bloc de numéro.

13.1.3 Numérotation KEYPAD

Dans divers pays, les services des raccordements réseau numériques sont gérés par numérotation Keypad et non par une fonction. Pour activer ces services dans le RTC, il est possible d'utiliser l'interface dite Stimulus.

La fonctionnalité doit être configurée dans Manager E.

Chez l'abonné, l'acquittement du trafic de messages est réalisé au niveau des affichages écran. En conséquence, la numérotation KEYPAD est réservée aux téléphones à écran (optiPoint, OpenStage), aux téléphones mobiles (Cordless) avec gestion de menu optiPoint et aux téléphones IP avec interface Stimulus. Les téléphones RNIS ne sont pas supportés Le fournisseur de réseau concerné détermine les services pouvant être utilisés par sélection par numérotation Keypad.

Un abonné autorisé peut activer la numérotation Keypad à l'aide du menu de service ou de l'indicatif *503. Cela n'est possible qu'à partir de l'état de repos. Ensuite, il faut sélectionner une ligne réseau RNIS sur laquelle se déroulera la fonctionnalité.

En liaison avec les messages en provenance du réseau (par ex. avec Connect), la numérotation Keypad peut effectuer des entrées dans l'enregistrement des données de taxation. Il est consigné le numéro de l'abonné qui effectue l'opération, la ligne utilisée et la période d'utilisation de la fonctionnalité.

Remarque : Les actions effectuées en numérotation Keypad ne sont soumises à aucun contrôle du système. Les utilisations frauduleuses comme la falsification des taxes ou blocage de ligne réseau ne peuvent pas être empêchées par le système.

Il faut informer le client qu'il est responsable des dommages pouvant survenir en cas d'utilisation malveillante de cette fonctionnalité.

13.1.4 Détection de la fin de la numérotation

La fin de la numérotation est soit identifiée automatiquement au bout de 5 secondes, soit affichée manuellement par l'utilisateur par le caractère de fin de numérotation "#".

13.1.5 Edition numérotation (type GSM).

Avec l'édition de la numérotation, l'abonné peut modifier les chiffres entrés du numéro. Cette fonction est habituelle sur les téléphones mobiles. Un numéro ne peut être corrigé que pendant la saisie.

Une succession de chiffres entrés peut être effacée de droite à gauche, chaque pression sur une touche effaçant un chiffre. Une fois tapée entièrement la bonne suite de chiffres, l'émission de la numérotation a lieu en appuyant sur la touche Valider ou en décrochant le combiné.

La modification d'un numéro enregistré, par ex. pour la répétition de la numérotation, est impossible.

Conseil : L'édition de la numérotation peut être activée séparément pour chaque abonné.

Correspondances

Sujet	Correspondance
Avertissement	Un avertissement est possible pendant l'édition, car le téléphone se trouve en état Prêt pour la numérotation et est donc occupé pour le trafic entrant.
Double appel	Après un double appel, le téléphone se trouve à l'état Prêt pour la numérotation. L'édition des chiffres du numéro d'appel est donc possible.

13.1.5.1 Comment activer ou désactiver l'édition de la numérotation

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés**.
4) Dans l'arborescence du menu, cliquez sur l'abonné (index - numéro - nom).
5) Cliquez sur l'onglet **Modifier les flags abonné**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Edition de la numérotation**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Edition de la numérotation**.
7) Cliquez sur **Appliquer** puis sur **OK**.

13.1.6 Répétition de la numérotation

A chaque établissement de communication externe, le numéro composé est enregistré. Si la destination est occupée ou injoignable, l'abonné peut appuyer sur la touche Répétition de la numérotation pour composer à nouveau le même numéro.

Les numéros abrégés sont également inscrits dans la mémoire de répétition de la numérotation.

Le sélection des numéros internes ne concerne pas la mémoire de répétition de la numérotation.

Les chiffres éventuellement surnumérotés (également appelés caractères MF) ne sont pas considérés comme des informations de numérotation et ne sont donc pas enregistrés (par ex. chiffres qui sont envoyés à une boîte vocale raccordée).

La fonction Répétition de la numérotation ne peut être réalisée que par la touche, pas par un code d'accès.

Appuyer sur la touche Bis pour appeler ces numéros de façon ciblée et les réutiliser pour établir une communication. Presser une fois pour appeler le dernier numéro composé. Presser deux fois pour appeler l'avant-dernier numéro composé. Presser trois fois pour appeler le numéro qui a été enregistré depuis le plus longtemps.

Après appui sur la touche de répétition de la numérotation, le numéro enregistré est automatiquement composé après 2 secondes. Si vous avez besoin de plus de temps pour lire le numéro affiché, sélectionnez avec la touche de confirmation "faire défiler". Chaque fois que vous appuyez sur la touche "Suivant", le numéro enregistré suivant s'affiche. C'est seulement lorsque vous sélectionnez la commande "Appeler" que ce numéro est composé. Vous avez ainsi bien plus de temps pour contrôler si le numéro correct a été sélectionné.

En cas d'appel transféré via LCR, seul le numéro composé par l'abonné est enregistré.

Les codes affaire sont également enregistrés dans la mémoire de répétition de la numérotation. Pour cela, il faut configurer le flag système correspondant.

13.1.6.1 Comment activer ou désactiver la répétition automatique

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système**.
4) Cliquez sur **Flags système**.
5) Sélectionnez une des possibilités suivantes :
   - Pour activer la fonction, cochez la case **Répétition automatique de la numérotation**.
   - Pour désactiver la fonction, décochez la case **Répétition automatique de la numérotation**.
6) Cliquez sur **Appliquer** puis sur **OK**.

13.1.7 Numérotation abrégée centralisée

Les numéros de téléphone externe fréquemment utilisés peuvent être enregistrés dans le système de communication. Chaque numéro est représenté par un numéro abrégé qui est utilisé à la place du numéro de téléphone complet.

Les numéros abrégés sont des numéros à 4 chiffres.

Par défaut, chaque abonné se trouve dans un groupe auquel tous les numéros abrégés centralisés sont affectés. Ainsi, chaque abonné peut utiliser tous les numéros abrégés centralisés.

La numérotation abrégée centralisée (NAC) invalide les règles de la discrimination réseau. Notez que la composition d'une destination de numérotation rapide trouvée lors d'une recherche dans l’annuaire interne n'annule pas les règles de discrimination réseau.

Les numéros de la numérotation abrégée centralisée sont configurés par l'administrateur et organisés en groupes. Les abonnés peuvent être affectés à un de ces groupes. Un abonné ne peut utiliser que les numéros abrégés du groupe qui lui est affecté. Il n'est possible d'affecter à un groupe qu'une seule plage de numéros abrégés centralisés.

Les entrées dans les numéros abrégés sont consultables par le prénom et le nom si le nom est configuré au format <Nom>, <Prénom> ou <Prénom>, <Nom>.

Les numéros abrégés sélectionnés sont inscrits dans la mémoire de répétition de la numérotation.

Pour programmer une "pause de numérotation" et une commutation MF pour la surnumérotation de caractères MF (par ex. pour la commande de boîtes vocales), on utilise la touche de répétition de la numérotation (touche bis) ou la touche "#".

La clé de numérotation pour le client doit être définie comme suit : <dial_number><dtmf_digit><pause_digit><access_code>, par ex. 008007728477 # P2210344

Conversion de numéros en noms

A chaque destination de numérotation abrégée peut être affecté un nom. Dès qu'un numéro enregistré appelle, le système utilise automatiquement le nom et au lieu du numéro c'est le nom qui apparaît sur l'écran lorsque CLI est paramétré.

Suffixe

La numérotation du suffixe n'est pas prise en charge pour la transmission numérique « Envoi en bloc » (par exemple, une configuration ITSP). Elle est prise en charge pour la transmission numérique « chiffre par chiffre ».

Remarque : Le champ de transmission du chiffre peut être modifiée dans WBM par **Mode Expert > Lignes/Routage > Route**

Il est possible d'effectuer une surnumérotation :

- Surnumérotation manuelle

  Après avoir composé le code d'accès et indiqué le numéro de position (numéro abrégé), l'utilisateur peut composer d'autres chiffres. Ils sont ajoutés au numéro enregistré sous cette position et composés ensuite.
- Surnumérotation automatique

  Lors de la configuration d'un numéro abrégé centralisé, le numéro entré peut être subdivisé en 2 parties. On utilise "-" comme caractère de séparation. La première partie est émise dans tous les cas. Puis une temporisation démarre. Si l'utilisateur n'entre aucun autre chiffre avant l'expiration de la temporisation, la deuxième partie du numéro entré est automatiquement surnumérotée, sinon les chiffres composés manuellement sont envoyés.

  Par exemple : SSD = 7007–0

  Si, après avoir activé le numéro abrégé centralisé et avant expiration de la temporisation, l'abonné n'entre aucun numéro SDA (surnumérotation manuelle), le 0 est automatiquement composé (surnumérotation automatique).

Importation de numéros abrégés

Vous pouvez importer les numéros abrégés à partir d'un fichier XML au format UTF-8. Les numéros abrégés existants sont effacés avant l'importation.

Vous trouverez un modèle XML avec les explications correspondantes dans WBM, sous **Centre de service** > **Documents** > **Modèles CSV**. Dans ces modèles, vous pouvez inscrire vos numéros abrégés par ex. avec Microsoft Excel.

Remarque : L'import de listes de numéros abrégés à partir de fichiers CSV n'est pas recommandé et n'est pris en charge que dans des cas particuliers.

Exportation des numéros abrégés

En tant qu'administrateur au profil **Expert**, vous pouvez, à l'aide du **Mode Expert**, exporter des numéros abrégés au format UTF-8 dans un fichier XML. Tous les jeux de donnée sont toujours exportés.

13.1.7.1 Comment ajouter un numéro abrégé

A l'aide de l'assistant **Annuaire/N° abrégé** vous pouvez ajouter des numéros abrégés à la numérotation abrégée centralisée.

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Annuaire/Numéro abrégé**.
4) Dans une ligne libre du tableau, inscrivez le **numéro abrégé**, le **numéro de téléphone** et le **nom** de la destination de la numérotation abrégée.
5) Si vous souhaitez ajouter d'autres numéros abrégés, cliquez sur **Enregistrer les données** et répétez l'opération précédente.
6) Cliquez sur **OK&Suivant**.
7) Cliquez sur **Quitter**.

13.1.7.2 Comment importer les numéros abrégés d'un fichier XML

Avec l'assistant **Annuaire/N° abrégé**, vous pouvez importer les numéros abrégés et les numéros de téléphone à partir d'un fichier XML. Les numéros abrégés existants sont effacés avant l'importation.

Conditions préalables

Vous êtes connecté à WBM.

Un fichier XML au format UTF-8 avec numéros abrégés inscrits est disponible. Vous trouverez un modèle XML pour l'importation des numéros abrégés dans **Centre de service** > **Documents** > **Modèles CSV**.

Remarque : L'import de listes de numéros abrégés à partir de fichiers CSV n'est pas recommandé et n'est pris en charge que dans des cas particuliers.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Annuaire/Numéro abrégé**. La fenêtre **Modifier l'entrée d'annuaire centrale** s'affiche.
4) Cliquez sur **Importer les données CSV/XML**.
5) Dans la zone **Importer un fichier CSV/XML via HTTP**, cliquez sur **Parcourir** afin de sélectionner le fichier souhaité.
6) Cliquez sur **OK**. Les numéros abrégés existants sont effacés et les numéros abrégés inscrits dans le fichier XML sont importés dans le système.
7) Cliquez sur **Terminer**.

13.1.7.3 Comment exporter des numéros abrégés dans un fichier XML

Vous pouvez exporter des numéros abrégés dans un fichier XML. Toutes les données sont toujours exportées.

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Annuaire/Numéro abrégé**. La fenêtre **Modifier l'entrée d'annuaire centrale** s'affiche.
4) Cliquez sur **Importer les données CSV/XML**.
5) Dans la zone **Exporter un fichier XML par HTTP** cliquez sur **Téléchargement**. La liste des numéros abrégés est préparée pour téléchargement.
6) Sélectionnez l'endroit de sauvegarde du fichier et cliquez sur **Enregistrer**.

13.1.7.4 Comment modifier les numéros abrégés

A l'aide de l'assistant **Annuaire/N° abrégé** vous pouvez modifier les numéros abrégés.

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Annuaire/Numéro abrégé**.

4) Vous pouvez rechercher une entrée en entrant un terme de recherche dans le champ **N° abrégé** ou **N° de téléphone** ou **Nom** puis en cliquant sur la touche Return. Tous les résultats contenant le terme sont affichés. Si vous entrez `521` comme numéro de téléphone, il est affiché par ex. les résultats `+495213535` et `+498967521` ou si vous entrez `co` comme nom, les résultats `Collins`, `Mcoin` et `Branco`.

   Remarque : Toutes les entrées sont affichées lorsque rien n'a été entré dans tous les champs de recherche et que vous appuyez ensuite sur la touche Retour.

5) Dans l'entrée de tableau souhaitée, modifiez les valeurs dans les champs **N° abrégé**, **Numéro de téléphone** ou **Nom**.
6) Si vous souhaitez modifier d'autres numéros abrégés, cliquez sur **Enregistrer les données** et répétez l'opération précédente.
7) Cliquez sur **OK&Suivant**.
8) Cliquez sur **Quitter**.

13.1.8 Numéro abrégé individuel (KWI)

La numérotation abrégée individuelle permet à chaque abonné d'enregistrer, en plus de la Numérotation abrégée centralisée, 10 numéros abrégés individuels externes.

Sur les téléphones sans écran, l'abonné doit attendre la tonalité d'acquittement après l'entrée du numéro d'appel.

Dans la base KWI, les numéros externes peuvent être programmés. L'accès dépend de la discrimination de l'abonné. Avant d'entrer le numéro d'appel, l'abonné doit entrer le code d'accès C.O. (par ex. 0).

Pour programmer une pause dans la numérotation ou une commutation MF, la touche Répétition de la numérotation ou la touche Dièse (#) est utilisée.

13.1.9 Appel direct

Les touches de fonction d'un téléphone ou satellite peuvent être configurées comme touches d'appel direct. Pour cela, il est programmé le numéro d'un abonné interne ou d'un groupe. Un appui sur une touche de ce type exécute un appel immédiat de la destination programmée (appel direct). L'état actuel de l'abonné ou du groupe se voit grâce au voyant correspondant à la touche d'appel direct.

Il est aussi possible d'utiliser une touche d'appel direct (également appelée touche DSS (Direct Station Selection)) pour transférer rapidement une communication à l'abonné programmé ou au groupe programmé sur la touche. L'appui sur une touche d'appel direct en cour de communication avec un interlocuteur externe place la communication actuelle en double appel. L'abonné qui transfère peut transférer la communication à la destination de transfert en raccrochent le combiné (transfert aveugle). Il est également possible d'attente que la destination de transfert réponde et de transférer alors la communication (transfert supervisé). Si la destination du transfert ne prend pas la communication, un retour d'appel est activé.

Etats d'un voyant correspondant à une touche d'appel direct

Le voyant correspondant à une touche d'appel direct affiche l'état actuel de l'abonné programmé :

- Désactivé : l'abonné correspondant ne téléphone pas.
- Allumé : l'abonné correspondant téléphone ou activé Ne pas déranger.
- Clignote rapidement : l'abonné correspondant appelle. Pour prendre l'appel, il suffit alors d'appuyer sur la touche d'appel direct.
- Clignote lentement : l'abonné correspondant est appelé et n'a pas encore pris l'appel. Pour prendre l'appel, il suffit alors d'appuyer sur la touche d'appel direct.

Correspondances

Sujet	Correspondance
Téléphones RNIS, téléphones SIP	Il est impossible de programmer des touches d'appel direct sur les téléphones RNIS ou SIP.

Concepts associés

La configuration Team / le groupe Team à la page 654
Groupe chef/secrétaire / groupe Top à la page 658

13.1.10 Appel interphone/Réponse appel interphone

L'appel interphone permet d'établir une communication interne sans que le correspondant appelé ne décroche. Le haut-parleur de l'abonné appelé est alors automatiquement activé.

Sur les téléphones avec équipement mains-libres (microphone), la réponse sur appel interphone de l'abonné appelé est possible par l'activation du microphone. S'il décroche le combiné, il revient à une communication normale à deux.

L'appel interphone peut être utilisé grâce à une touche de fonction programmée à cet effet ou par l'entrée de menu correspondante ou l'indicatif suivi de la composition du numéro de l'abonné ou du groupe de destination. Une touche de fonction peut aussi être programmée avec le numéro de l'abonné. Après appui sur une touche de fonction de ce type, il y a aussitôt établissement d'une liaison avec la destination programmée.

L'appel interphone pour groupes permet des diffusions en direction de tous les abonnés internes d'un groupe.

La réponse/l'appel interphone peuvent être activés par l'entrée de menu proposée sur l'écran ou une touche de fonction programmée à cet effet.

L'appel interphone d'un abonné peut être empêché par l'activation de la protection contre les appels interphones. Dans ce cas, l'appel interphone est signalé comme un appel normal.

Correspondances

Sujet	Correspondance
Ne pas déranger, Forcer Ne pas déranger	Les abonnés qui ont activé la fonction Ne pas déranger ne peuvent pas recevoir d'Appel interphone. Si l'abonné qui souhaite utiliser la fonctionnalité "Appel interphone" dispose de la classe de discrimination qui permet de forcer Ne pas déranger, il entend la tonalité occupé durant cinq secondes. Le destinataire est appelé, pas par appel interphone.
Va-et-vient, Double appel, Transfert	Les fonctionnalités indiquées ne peuvent pas être utilisées dans une liaison Appel interphone/ Réponse sur appel interphone.
Téléphones RNIS, téléphones SIP	Les fonctionnalités "Appel interphone" et "Réponse sur appel interphone" ne peuvent pas être utilisées sur les téléphones RNIS ou SIP.

13.1.10.1 Comment activer / désactiver la protection contre les appels interphones pour un abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence menu, naviguez sous **Abonnés** > **Abonné** > **…** pour accéder à l'abonné souhaité (Index - Numéro - Nom).
4) Cliquez sur l'onglet **Modifier les flags abonné**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la protection contre les appels interphones pour l'abonné, décochez la case **Protection contre les appels interphones désactivée**.
   - Si vous souhaitez désactiver la protection contre les appels interphones pour l'abonné, cochez la case **Protection contre les appels interphones désactivée**.
6) Cliquez sur **Appliquer** puis sur **OK**.

13.1.11 Numérotation associée

La numérotation associée permet à un abonné autorisé de composer un numéro en représentant un autre abonné quelconque. Le résultat est le même que si l'autre abonné sélectionnait le numéro.

L'entrée est réalisée à l'aide d'un indicatif, avec indication de l'abonné pour lequel la numérotation est effectuée. Les chiffres suivants sont alors interprétés comme si l'abonné indiqué auparavant numérotait lui-même.

13.1.12 Réservation de ligne

Un abonné peut réserver une ligne occupée s'il ne dispose d'aucune ligne réseau libre. Dès qu'une ligne réseau devient libre, elle lui est proposée au moyen du retour d'appel.

Si l'abonné est occupé au moment du retour d'appel, l'abonné occupé reçoit un avertissement. Si l'avertissement ne reçoit pas de réponse, la réservation est annulée et la ligne proposée à l'abonné suivant dans la liste de la file d'attente. Si l'abonné a activé Ne pas déranger avant la présentation d'un retour d'appel d'une ligne réseau se trouvant en file d'attente, la réservation de la ligne est annulée et la ligne réseau est proposée à l'abonné suivant de la liste de la file d'attente.

Lorsque plusieurs abonnés réservent une même ligne réseau, l'affectation intervient dans l'ordre de réservation.

Une seule demande de file d'attente/réservation est possible par téléphone. Si l'abonné tente une deuxième réservation, cette dernière remplace la première.

Il est impossible d'activer la fonctionnalité Réservation de ligne si la communication souhaitée a été activée par LCR.

La fonctionnalité Réservation de ligne ignore les renvois temporisés existants. S'il n'y a pas de réponse dans les 20 secondes, la réservation de la ligne est annulée.

Une ligne réseau en retour d'appel ne peut pas être interceptée – ni par la fonctionnalité "Interception", ni par la fonctionnalité "Interception groupe".

La réservation des lignes peut être activée de l'une des façons suivantes :

- Les réservations manuelles ne fonctionnent que sur les téléphones avec écran.
- Réservation automatique (sur tous les autres téléphones)

  Lorsque ce flag est activé et qu'il n'est affecté aucune ligne libre à un abonné suite aux procédures de prise de ligne habituelles, une tonalité d'occupation est signalée côté abonné. Au bout de 5 secondes, un bip de confirmation positif retentit et la ligne est réservée dans la mesure où l'abonné dispose de la discrimination nécessaire.

Remarque : Sur les téléphones S_0, impossible de réserver une performance.

13.1.12.1 Comment activer ou désactiver la réservation de ligne

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système**.

4) Cliquez sur **Flags système**.
5) Sélectionnez une des possibilités suivantes :
   - Pour activer la fonction, cochez la case **Réservation automatique de ligne réseau**.
   - Pour désactiver la fonction, décochez la case **Réservation automatique de ligne réseau**.
6) Cliquez sur **Appliquer** puis sur **OK**.

13.1.13 Ligne privée

Une ligne privée est une ligne réseau qui est à la disposition d'un abonné spécifique.

13.2 Signalisation d'appel, affichage du numéro

Le système de communication offre diverses options de signalisation des appels et d'affichage des numéros d'appel, telles que CLIP, CLIR, COLP et COLR.

13.2.1 Différenciation de la signalisation d'appel

La différenciation de la signalisation d'appel permet de distinguer les communications internes et externes lors de la réception d'un appel.

Les appels entrants sont signalés de manière optique et acoustique sur le téléphone. Les informations suivantes s'affichent à l'écran :

- Le numéro de l'appelant
- Dans le cas d'un renvoi d'appel interne : en plus le numéro de téléphone réellement composé

L'appel entrant peut en plus être signalé par une diode électroluminescente. Il existe des signaux acoustiques différents pour les appels internes et externes.

Signalisation des appels internes

Il est possible d'affecter à chaque abonné l'une des huit signalisations acoustiques pour les appels internes. Le cas échéant, l'abonné émet une tonalité d'appel différente des autres, qui permet aux autres abonnés de l'identifier. Ainsi, il est possible d'affecter au directeur de l'entreprise une tonalité d'appel interne spéciale de manière que chaque collaborateur puisse identifier son appel.

Signalisation des appels externes

Il existe trois types d'appels qui se distinguent au plan acoustique et peuvent être affectés à un appel externe. L'affectation de signaux acoustiques différents permet, par ex., de faire la distinction entre deux groupes tels que le service des ventes et le service des stocks.

- L'administrateur configure les trois types de sonneries différents disponibles en Allemagne pour téléphones analogiques, téléphones RNIS et téléphones système.

- Dans les autres pays, les types de sonneries des téléphones analogiques sont signalés de façon identique.

13.2.2 Présentation de la ligne appelante (CLIP)

La présentation du numéro de la ligne appelante affiche le numéro de téléphone de l'appelant chez l'abonné appelé.

La Présentation du numéro de la ligne appelante CLIP (Calling Line Identification Presentation) concerne les appels entrants et elle doit être supportée par l'opérateur du réseau.

Si le nom et le numéro de l'appelant sont enregistrés comme numérotation abrégée centralisée (NAC) dans le système de communication, le nom s'affiche sur votre écran.

Les fonctionnalités Présentation du numéro de la ligne appelante (CLIP) et Refus de présentation de la ligne appelante (CLIR) s'excluent mutuellement, c'est-à-dire que dès que CLIP est activé, CLIR est désactivé ou inversement.

CLIP configurable

CLIP configurable transmet vers l'extérieur à la place du numéro de l'appelant (par ex. membre d'un groupe de recherche) un numéro spécifiquement paramétré (par ex. numéro du groupe de recherche).

Informations spécifiques du système

Pays	activé par défaut
Etats-Unis	LIN (Location Identification Number). Lorsque le service CLIP est activé pour les Etats-Unis, LIN automatiquement désactivé.
Autres pays	CLIP

13.2.2.1 Comment activer ou désactiver les CLIP configurables

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système**.
4) Cliquez sur **Flags système**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer des CLIP configurables, cochez la case **CLIP configurable**.
   - Si vous souhaitez désactiver des CLIP configurables, décochez la case **CLIP configurable**.

6) Cliquez sur **Appliquer** puis sur **OK**.

13.2.3 Calling Line Identification Restriction CLIR (restriction de présentation du numéro de l'appelant)

Le refus de présentation de la ligne appelante empêche l'affichage du numéro d'appel de l'appelant chez l'appelé.

Le refus de présentation de la ligne appelante CLIR (Calling Line Identification Restriction) concerne les appels sortants. Le RTC doit supporter cette fonctionnalité. Refus de présentation de la ligne appelante a la priorité sur la présentation du numéro.

Les fonctionnalités Présentation du numéro de la ligne appelante (CLIP) et Refus de présentation de la ligne appelante (CLIR) s'excluent mutuellement, c'est-à-dire que dès que CLIP est activé, CLIR est désactivé ou inversement.

CLIR et COLR ne peuvent être activés ou désactivés qu'ensemble.

Le refus de présentation de la ligne appelante n'est pas opérationnel avec certaines destinations d'appel (par. ex. numéro de la Police et des Pompiers).

Refus de présentation de la ligne appelante à l'échelle du système

En tant qu'administrateur, vous pouvez activer ou désactiver l'affichage du numéro CLIR pour l'ensemble du système.

Conseil : Le flag "Refus de présentation du numéro dans l'ensemble du système" ne s'applique pas aux Etats-Unis.

Refus temporaire de l'affichage du numéro

En tant qu'abonné, vous pouvez activer ou désactiver le refus temporaire de la présentation du numéro. Le refus temporaire de l'affichage du numéro est uniquement possible si vous avez désactivé le refus de l'affichage de l'ensemble du système.

Masquer le numéro de l'abonné

En tant qu'administrateur, vous pouvez, pour un faisceau, configurer le système de manière à ce que, à la place du numéro de l'abonné, il soit transmis uniquement le numéro de l'installation.

13.2.3.1 Comment activer ou désactiver le Masquage de l'affichage du numéro, de l'abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.

3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Sélectionnez le **faisceau** correspondant.
5) Sous **Numéro système sortant**, sélectionnez la case **Masquer le numéro d'appel de l'abonné**.
6) Cliquez sur **Appliquer** puis sur **OK**.

13.2.4 Présentation de l'identification de la ligne connectée (COLP)

La présentation de l'identification de la ligne connectée (COLP) transmet le numéro de téléphone de l'abonné appelé à l'appelant dès que les deux sont connectés.

La fonction COLP est utile dans le cas du transfert d'appel, par exemple, car elle permet à l'appelant de voir le numéro de téléphone de son interlocuteur réel au lieu du numéro composé à l'origine.

Les fonctions Présentation de l'identification de la ligne connectée (COLP) et Restriction de l'identification de la ligne connectée (COLR) s'excluent mutuellement, c'est-à-dire que dès que la fonction COLP est activée, la fonction COLR est désactivée, et vice versa.

13.2.4.1 Comment activer ou désactiver la présentation du numéro de la ligne connectée

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Sélectionnez le **Fsc** correspondant.
5) Cliquez sur l'onglet **Modifier les paramètres spéciaux**.
6) Sélectionnez la case **COLP**.
7) Cliquez sur **Appliquer** puis sur **OK**.

13.2.5 Non-identification de la ligne connectée (COLR)

La non présentation du numéro de la ligne connectée empêche l'affichage du numéro de l'appelé chez l'appelant.

La non présentation de la ligne connectée (COLR Connected Line Identification Restriction) concerne les appels entrants.

La non présentation de la ligne connectée (COLR) a la priorité sur la présentation du numéro de la ligne connectée chez l'appelant.

Les fonctionnalités Présentation de la ligne connectée (COLP) et Non présentation de la ligne connectée (COLR) s'excluent mutuellement, c.-à-d. lorsque COLP est activé COLR est désactivé et inversement.

CLIR et COLR ne peuvent être activés ou désactivés qu'ensemble.

13.2.6 CLIP No Screening (présentation de la ligne appelante avec transmission d'informations client spécifiques, relatives au numéro d'appel)

CLIP no screening présente à la place du numéro de l'appelant un numéro défini par l'appelant.

Il n'est pas nécessaire que le numéro système sortant soit identique au numéro système entrant.

Il est possible, pour des applications client spéciales, d'activer le flag "Masquer le numéro d'abonné". Ainsi, le numéro SDA de l'abonné n'est pas émis avec le numéro système sortant.

Exemple : un responsable technique, joignable de façon centrale par un numéro de support technique général, ne doit pas être joignable directement par ses clients. Pour masquer son numéro SDA personnel, le numéro de support technique général doit être entré comme Numéro système sortant et le flag "Masquer le numéro d'abonné" doit être activé. L'abonné appelé ne voit alors s'afficher que le numéro de support technique général comme CLIP.

Normalement, le même numéro système est utilisé pour les communications entrantes et sortantes. Le champ Numéro système sortant est donc vide ou l'entrée est identique à celle du champ Numéro système entrant. Si ce n'est pas le cas,

- un autre numéro peut être entré dans le champ Numéro système sortant.
- le paramètre faisceau 'Protocole-type de n° sortant' permet de définir si le numéro système sortant entré contient le numéro d'abonné sans préfixe de réseau local, avec préfixe de réseau local (national) ou avec en plus l'indicatif de pays international (international).

Conseil : La fonctionnalité CLIP No Screening doit être supportée par l'opérateur et être activée.

13.2.6.1 Comment configurer CLIP no screening

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Sélectionnez le **faisceau** correspondant.

5) Sous **Numéro système sortant**, entrez le **numéro PABX** requis.
6) Cliquez sur **Appliquer** puis sur **OK**.

13.2.7 CLIP pour terminaux analogiques

CLIP pour terminaux analogiques présente à l'appelé le numéro d'un terminal analogique de l'appelant et son affichage sur les terminaux adaptés – CLIP (Calling Line Identification Presentation) analogique.

La fonction de présentation du nom de l'appelant, CNIP (Calling Name Identification Presentation), peut être programmée en supplément.

Conseil : CNIP dépend du terminal. Tenez compte des indications du fabricant.

13.2.8 Appel sans sonnerie / Coupure sonnerie

La fonctionnalité Appel sans sonnerie / Coupure sonnerie signale les appels entrants avec uniquement une brève tonalité et un affichage à l'écran.

Appel sans sonnerie / Coupure sonnerie est uniquement disponible sur les téléphones à écran et n'a pas d'incidence sur la signalisation des RDV.

13.2.9 Conversion des numéros en nom avec la numérotation abrégée centralisée

Pour les appels à l'aide de la numérotation abrégée centralisée et les appels entrants provenant de destinations de la numérotation abrégée centralisée, le nom de la destination s'affiche au lieu du numéro abrégé.

13.3 Fonctions en cours de communication

Le système de communication offre les avantages suivant durant la connexion, par exemple la mise en garde, le renvoi ou le transfert.

13.3.1 Mise en garde

La Mise en garde permet de placer une communication en attente. L'appelant entend alors une musique d'attente ou une annonce.

La mise en garde se termine par la reprise de la communication en attente.

Il existe les types de mise en garde suivants :

- Mise en garde générale :

  Chaque abonné peut reprendre la communication en appuyant sur une touche de ligne ou de communication.

- Mise en garde exclusive : (uniquement avec fonction Team ou Top et pour un P.O)

  Seul l'abonné initial précédent peut reprendre l'appel.

Mise en garde et retour d'appel

Une fois que la temporisation **Temps pour parcage + Attente est écoulée** (par défaut : 160 s), la communication parquée émet un retour d'appel.

13.3.2 Parcage

Avec la fonction Parcage, l'abonné place une communication en attente. L'appelant entend alors une musique d'attente ou une annonce. Une communication en garde peut être reprise par un téléphone quelconque.

En tant qu'abonné, vous attribuez une position de parcage (0-9) pour un appel à parquer. Si la position de parcage est déjà occupée, le système émet une tonalité d'acquittement négative, le chiffre ne s'affiche pas et il est alors possible de sélectionner une autre position. Pour reprendre une communication parquée, vous devez indiquer sa position de parcage.

La reprise d'une communication parquée est réalisée à l'aide d'un indicatif ou d'une touche programmée spécifiquement ; elle est possible y compris lorsqu'un autre appel est en attente.

Parcage et retour d'appel

Une fois que la temporisation **Temps pour parcage + Attente est écoulée** (par défaut : 160 s), la communication parquée émet un retour d'appel.

Parcage et renvoi d'appel

En cas de retour d'appel, la communication parquée ne suit pas les renvois d'appel.

Parcage et DISA

Il n'est pas possible d'activer un parcage via DISA.

Parcage et conférence

Il est impossible de parquer une conférence.

Parcage et mise en réseau

Un appel parqué ne peut être repris qu'à l'intérieur du même noeud. Un appel entrant par un chemin réseau ne peut être mis en position de parcage que sur le nœud de destination.

Parcage et Ne pas déranger

Un abonné qui a activé la fonction Ne pas déranger peut affecter une position de parcage à une communication. En cas de retour d'appel de la communication parquée et si aucune autre destination n'a été définie dans la Gestion des appels, la communication est automatiquement coupée après écoulement de la temporisation prévue pour le retour d'appel.

Remarque : Vous trouverez des indications détaillées sur la manière de parquer un appel et de récupérer un appel parqué dans le chapitre correspondant du guide de l'utilisateur (Guide de l'utilisateur OpenStage X / HiPath/OpenScape 3000/4000).

13.3.3 Double appel

A l'aide du double appel, l'abonné peut, en cours de communication, établir une seconde communication à partir de son poste téléphonique ou prendre un correspondant qui a envoyé un avertissement. Pendant ce temps, la première communication est mise en garde.

Pour mettre fin à un double appel :

- Reprise de la communication en attente
- Déconnecter

  La déconnexion peut se traduire par :

  – Transférer la communication en attente ou
  – Retour d'appel immédiat de l'abonné en attente en direction de l'abonné qui a effectué la déconnexion

Double appel au moyen de la touche d'appel direct

L'appui sur une touche d'appel direct en cours de communication lance un double appel vers la destination correspondante.

Connexion de deux correspondants externes

En cours de communication externe, un double appel en direction d'une destination externe suivi d'un transfert permet de connecter les deux correspondants. Cela peut donner lieu à une taxation.

13.3.4 Va-et-vient

Le Va-et-vient permet à un abonné d'alterner entre deux communications. Pendant qu'il parle à l'un de ses correspondants, l'autre est mis en garde.

L'abonné peut passer d'une communication à l'autre en appuyant sur la touche de ligne correspondante.

Va-et-vient et mise en attente

La fonction Va-et-vient n'est pas disponible pour les abonnés en attente.

13.3.5 Transférer

Le transfert permet à un abonné de transférer la communication vers une autre destination. Dès que l'abonné lance la procédure de transfert, le correspondant en attente est mis en garde.

Il existe les types de transferts suivants :

- Transfert aveugle (aussi appelé transfert non filtré) :

  Vous pouvez transférer l’appel sans que l’abonné de la destination du transfert ne réponde. Lorsque l'abonné destinataire du transfert est occupé, il entend une tonalité d'avertissement. Si un tiers essaie de transférer une communication au destinataire occupé ou si la fonctionnalité Rejet des appels en instance a été activée, un retour d'appel se produit immédiatement. Si le destinataire ne répond pas à la communication transférée au bout d'un certain temps (Temporisation Durée de la sonnerie pour transfert avant réponse), il se produit un retour d'appel. Le transfert aveugle (également appelé transfert sans sélection) vers un agent dans un autre centre de contacts multimédia n'est pas possible.
- Transférer uniquement avec réponse :

  Vous ne pouvez transférer l'appel que si le correspondant de destination de transfert répond. Vous transférez l'appel en raccrochant le combiné.

Transférer avec renvoi d'appel

Le renvoi d'appel est suivi jusqu'à la destination du transfert L'écran affiche la destination ultime du transfert.

Transférer avec Ne pas déranger

Lorsqu'une communication est transférée à un abonné qui a activé la fonction Ne pas déranger, il se produit immédiatement un retour d'appel vers l'abonné à l'origine du transfert, même si ce dernier a activé la fonction Ne pas déranger.

Informations spécifiques du système

Temporisateur pour la « Durée de la sonnerie pour transfert avant réponse » : 45 secondes par défaut

Il est possible de transférer jusqu'à 5 communications simultanément à un abonné occupé.

Remarque : Lors d'un transfert d'appel, la mise à jour des informations d'affichage via l'interface ITSP/NATIVE-SIP n'est pas prise en charge.

13.3.6 Retour d'appel

Le retour d'appel renvoie automatiquement à l'abonné initial une communication depuis trop longtemps en attente ou parquée ou une communication dont le transfert a échoué.

Le retour d'appel se produit dans les cas suivants :

- Si une communication en attente ou parquée n'est pas reprise dans un délai fixé (temporisation Temps pour parcage + Attente).

- Lors d'un transfert aveugle, dans les cas suivants.
  - S'il n'y a pas de réponse avant écoulement d'un certain intervalle de temps (temporisation Durée de la sonnerie pour transfert avant réponse)
  - Si la destination n'existe pas
  - Si la destination est occupée au deuxième niveau
  - Si le téléphone numérique de la destination est défectueux
  - Le transfert n'est pas autorisé

Si l'abonné initial est occupé lorsque se produit le rappel, il est émis une tonalité d'avertissement. Dès que l'abonné initial est de nouveau libre, le retour d'appel est signalé. Sur l'écran de l'abonné initial il apparaît soit le numéro de l'appelant, soit celui de l'abonné de destination. Si l'abonné ne répond pas au retour d'appel avant la fin du temps alloué pour cela, il est effectué un renvoi vers le poste de renvoi si le drapeau pour un retour d'appel non répondu est placé. Si le poste de renvoi ne répond pas au retour d'appel avant la fin du temps alloué pour l'activation d'un retour d'appel vers le P.O., le retour d'appel est automatiquement coupé.

Retour d'appel et interception

Chaque abonné du groupe d'interception où figure l'abonné initial peut intercepter un retour d'appel si le drapeau AUN pour l'ensemble du système est placé après le retour d'appel.

Retour d'appel et Ne pas déranger

Le retour d'appel ignore Ne pas déranger.

Informations spécifiques du système

La temporisation Durée avant renvoi PO pour retour d'appel est réglée par défaut sur 30 s

La temporisation allouée pour l'activation d'un retour d'appel vers le P.O. est réglée par défaut sur 60 s.

13.3.7 Surveillance d'appel

La surveillance d’appel permet aux abonnés autorisés d’écouter la communication d’un abonné interne quelconque. Le microphone de l'abonné qui écoute est automatiquement coupé. Les abonnés de la liaison surveillée ne reçoivent aucune indication sur ce processus, comme une tonalité ou un affichage à l’écran.

Cette fonction est désactivée dans la configuration par défaut. Elle ne peut être activée que si la législation nationale le permet. Dans certains cas, la législation nationale en vigueur doit toujours être vérifiée avant d’activer la fonction.

Les abonnés autorisés ont besoin d'un téléphone système et de la classe de discrimination pour Entrée en tiers.

L’abonné à surveiller doit se trouver dans une communication active. Au début et à la fin de la surveillance d’appel, il peut se produire des coupures de communication allant jusqu’à deux secondes. Dès qu’un des interlocuteurs de la communication surveillée est mis en garde, transféré ou met fin à la communication, la communication d’écoute est coupée. Elle ne peut

être rétablie que lorsque l'abonné à surveiller repasse dans un état de communication actif.

Correspondances

Rubrique	Correspondance
Téléphones sans fil	Vous ne pouvez pas utiliser la surveillance d'appel sur un téléphone sans fil parce que ce type de poste n'est pas doté de la coupure automatique du microphone.
Conférences	La surveillance d'appel limite le nombre possible de participants aux conférences. Nombre maximum de conférences possibles dans le système = nombre maximum d'abonnés à la surveillance d'appel simultanés.
Surveillance d'appel	L'appel ne peut être annulé qu'en utilisant le code *944 + le numéro de l'abonné (pas à partir d'un menu).
Surveillance d'appel	Pour permettre l'utilisation des fonctions par un abonné, il faut activer à la fois l'indicateur abonné **Surveillance d'appel** et l'indicateur **Autorisation d'entrée en service**. (Cette fonction ne peut pas être utilisée avec la fonction "CSTA Monitoring")

13.3.7.1 Comment activer ou désactiver la surveillance d'appel pour un abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Pour l'abonné concerné, l'entrée en tiers est activée.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés**.
4) Dans l'arborescence du menu, naviguez sous **Abonnés** > **Abonné** > **…** pour accéder à l'abonné souhaité (Index - Numéro - Nom).
5) Cliquez sur l'onglet **Modifier les indicateurs abonné**.
6) Sélectionnez l'une des options suivantes :
   - Si vous voulez permettre à un abonné d'utiliser cette fonction, cochez la case **Surveillance des appels**.
   - Si vous voulez interdire à un abonné d'utiliser cette fonction, décochez la case **Surveillance des appels**.
7) Cliquez sur **Appliquer** puis sur **OK**.

13.3.8 Message discret

La fonctionnalité Message discret permet à un abonné C d'écouter une connexion simple entre deux abonnés A et B et de donner à l'abonné A des indications qui ne sont pas audibles par l'abonné B. Un mode de

fonctionnement typique pour les centres d'appel ou les installation chef/ secrétaire.

La fonctionnalité doit être configurée dans Manager E.

Remarque : Bien qu'il n'y ait pas de connexion entre l'abonné B et l'abonné C, l'abonné B peut, grâce à un couplage en retour sur le téléphone de l'abonné A, entendre de manière étouffée ce que dit l'abonné C.

Les équipement concernés par les messages discrets (abonné A) sont uniquement les téléphones système avec écran. Les abonnés A et C doivent se trouver sur le même noeud.

La fonctionnalité est activée par l'abonné C, à l'état Repos/Opérationnel, par la sélection d'un indicatif. Il existe sur le téléphone une touche partiellement définie (seul l'indicatif est enregistré sur la touche, le numéro de téléphone doit être composé ensuite). Dans le menu Service, il est ajouté une option de menu ; le menu Dispo/Communication n'est pas modifié.

La possibilité d'activer la fonctionnalité est associée à une classe de discrimination spécifique utilisateur. Avec une deuxième classe de discrimination, l'abonné A peut se protéger des messages discrets.

La désactivation est effectuée soit par la libération de l'abonné C soit en agissant sur la fonctionnalité.

Remarque : Si, dans la communication d'origine, il n'y a pas au moins un TDM, le champ de couplage n'est pas encore associé au moment de l'activation et la commutation provoque donc une brève interruption de la communication en place.

Remarque : Les fonctionnalités de transfert d'appel et de conférence ne sont pas disponibles à partir des produits UC Suite lorsque l'option Appel discret est activée.

Si la fonctionnalité Message discret est activée et que l'abonné A ou l'abonné B active une autre fonctionnalité, en rapport avec la liaison, la fonctionnalité Message discret est arrêtée par principe. Détails sur le comportement de certaines fonctionnalités, voir tableau suivant :

Fonctionnalité	Abonné A		Abonné B		Abonné C	
	Possible	Action	Possible	Action	Possible	Action
Double appel, Mise en garde, Parcage, Mise en garde commune	Oui	Comment quitter "Message discret"	Oui	Comment quitter "Message discret"	Non	Acquittement négatif
Transférer	--	--	--	--	--	--
Conférence	--	--	--	--	--	--
Avertissement	Oui	--	Oui	--	Oui	--

Fonctionnalité	Abonné A		Abonné B		Abonné C	
Réponse avertissement	Oui	Comment quitter "Message discret"	Oui	Comment quitter "Message discret"	Oui	Acquittement négatif
Entrée en tiers	Non	--	Non	--	Non	--
Transmission DTMF	Oui	--	Oui	--	Non	--
Compteur LM	--	--	--	--	--	--
Services associés	--	--	--	--	--	--
DISA / DISI	--	--	--	--	--	--

13.3.9 Enregistrement de l'appel en direct (enregistrement vocal)

Cette fonction est utilisée pour enregistrer les données d'une connexion vocale active entre deux abonnés (un abonné doit être interne, l'autre peut être externe), en d'autres termes, pour enregistrer des appels. Un périphérique distinct est requis pour l'enregistrement.

L'enregistrement peut être démarré et arrêté au moyen d'une touche de fonction ou d'un code numérique (téléphones analogiques). En fonction de la configuration, l'enregistrement peut aussi être arrêté à partir de l'appareil d'enregistrement.

L'équipement d'enregistrement peut être utilisé par tous les téléphones pris en charge dans un réseau CorNet-NQ. Les connexions avec CorNet-N et QSIG (ECMA, ISO) ne sont pas prises en charge. La tonalité d'enregistrement peut être désactivée pendant l'enregistrement.

Les téléphones TDM et CorNet-IP (HFA) (y compris les appareils sans écran) ainsi que OpenScape Personal Edition (HFA) et optiClient Attendant sont pris en charge. Les téléphones H.323 standard, les téléphones SIP et les abonnés EDSS1 ne sont pas pris en charge.

Remarque : L'enregistrement vocal activé est indiqué par un témoin lumineux ou une tonalité d'enregistrement pendant l'appel.

L'autorisation d'utiliser l'enregistrement vocal peut être réglée individuellement pour chaque abonné.

Correspondances/Restrictions

Objet	Correspondance/Restriction
Consultation en attente, basculement/ connexion, transfert, conférence	L'activation de l'une de ces fonctions lors de l'enregistrement d'un appel interrompt automatiquement l'enregistrement vocal.

Objet	Correspondance/Restriction
Call Hold	L'enregistrement en cours est interrompu en activant "Call Hold". L'enregistrement ne peut pas être activé lorsqu'un abonné est en attente.
Entrée en tiers	L'enregistrement vocal n'est pas possible. Vous ne pouvez pas écraser un appel en cours d'enregistrement. De même, vous ne pouvez pas activer l'enregistrement après avoir écrasé un appel.
Surveillance d'appel	L'enregistrement vocal n'est pas possible. Vous ne pouvez pas surveiller un appel en cours d'enregistrement. De même, vous ne pouvez pas lancer l'enregistrement après l'activation de la "Surveillance d'appel".

Remarque : Vous ne pouvez enregistrer que les appels entre deux abonnés, et pas les conférences ou les appels avec des tiers.

Remarque : Remarques supplémentaires :

-) Le périphérique d'enregistrement peut être adressé dans un nœud aléatoire dans un réseau CorNet NQ.

-) Seul un nombre limité d'abonnés dans un nœud peut recevoir une autorisation d'enregistrement vocal (actuellement limitée à 50 abonnés).

-) Les ressources de la conférence sont allouées pendant l'enregistrement.

-) Le code de service par défaut pour l'activation de l'enregistrement d'appel est *493.

13.4 Gérer la disponibilité

Pour la gestion de la disponibilité, le système propose des fonctionnalités comme Renvoi d'appel, Ne pas déranger et Refuser les appels.

Différents types de tables d'acheminement pour les renvois d'appel. Les tables d'acheminement indiquent comment sont traités les appels entrants pour l'abonné ou pour le groupe correspondant. Les destinations d'une table d'acheminement sont traitées l'une après l'autre. Il est possible d'avoir des entrées différentes pour les appels internes et les appels internes (Jour ou Nuit).

13.4.1 Renvois temporisés

Le renvoi temporisé transfère l'appel lorsque ce dernier n'a pas été accepté à l'issue d'un certain intervalle de temps.

Ce type de renvoi temporisé est également appelé renvoi temporisé fixe car il est configurable par l'administrateur.

Pour chaque renvoi temporisé, il existe une ou plusieurs tables d'acheminement qui peuvent être affectées aux abonnés pour les types suivants d'appels :

- appels externes de jour (durant renvoi de nuit inactif)
- appels externes de nuit (durant renvoi de nuit actif)
- Appels internes

Par table d'acheminement, vous pouvez indiquer jusqu'à 4 destinations d'appel en direction desquelles l'appel sera renvoyé successivement, une fois la temporisation réglable écoulée.

Pour la destinations d'appel, le numéro ou le nom de l'abonné appelé à l'origine ainsi que le numéro ou le nom de l'appelant sont affichés. En tant qu'administrateur, vous pouvez désactiver l'affichage supplémentaire du numéro de téléphone ou du nom de l'appelant.

Renvoi temporisé sur occupation

Le renvoi temporisé sur occupation renvoie immédiatement un appel entrant sur un poste occupé en direction de la destination d'appel suivante.

Si la destination d'appel est également occupée, l'appelant entend la tonalité d'occupation. En cas d'appel interne, l'appel reste dans ce cas présenté à la destination d'appel, dont la libération est contrôlée de façon cyclique. L'administrateur définit le cycle.

Si la destination d'appel n'est pas disponible et si aucun autre renvoi n'a été configuré, l'appel n'est pas transféré.

Correspondances

Rubrique	Correspondance
Terminaux analogiques	Ces téléphones ne permettent pas d'identifier les appels entrants comme appels renvoyés.
Appel en instance	Si un abonné a activé l'indication d’appel en instance (Avertissement), il est averti même s'il a configuré le renvoi temporisé sur occupation.
NPD	Une destination d'appel ayant activé le rejet des appels en instance est ignorée.
Renvoi d’appel	Le renvoi temporisé n'est exécuté que lorsque la destination d'un renvoi d'appel ne répond pas dans un délai défini par l'administrateur.
Renvoi de nuit	Si l'on utilise pour un abonné la possibilité de renvoi temporisé "jour / nuit" et que le renvoi de nuit est activé, les appels externes sont renvoyés selon les paramètres du renvoi de nuit. Les appels internes sont toujours effectués selon les paramètres du renvoi "de jour".

Rubrique	Correspondance
Renvoi temporisé en réseau	Le renvoi temporisé en réseau est prioritaire sur les autres renvois temporisés.
Groupement / Appel de groupe	Si vous entrez un groupe ou un groupe de recherche de ligne comme destination d'un renvoi temporisé, le programme appelle successivement tous les abonnés du groupe avant de renvoyer l'appel vers la destination suivante. L'appel de groupe et le groupe de recherche de ligne doivent être considérés comme un renvoi temporisé configuré au sein du renvoi temporisé. Un groupe de recherche de ligne est occupé lorsque tous les membres sont occupés ou se sont déconnectés du groupe de recherche. Un groupe est toujours occupé lorsque tous ses membres sont occupés.

13.4.1.1 Comment configurer un renvoi temporisé

Avec l'assistant **Renvoi temporisé** vous configurez pour les abonnés internes un renvoi temporisé pour les appels entrants.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateur**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Renvoi temporisé**. Ouverture de la fenêtre **Table d'acheminement - Définition**.
4) Définissez tout d'abord une table d'acheminement en cliquant sur l'icône **Modifier** dans la ligne de la table d'acheminement à traiter.

5) Dans les listes déroulantes **1e destination** à **4e destination**, sélectionnez les destinations souhaitées. Vous disposez des possibilités suivantes :

- **Aucune entrée**: la destination est sautée
- **Destination externe** : faisceau et numéro de téléphone externe avec code d'accès CO
- *** Abonné sélectionné** : l'abonné appelé
- **** Utilisateur défini** : destination du renvoi d'appel temporisé (si paramétré).
- **#9, recherche système** : abonné suivant disponible (à l'exception du poste du chef)
- **#201 - #260** : Distribution d'appels (groupe UCD)
- **#801 - #817** : Equipement d'annonces
- **100, 101, ...** : numéro de téléphone d'un abonné ou d'un groupe interne (par ex. boîte vocale)

Remarque : Pour retrouver plus rapidement une destination d'appel, vous pouvez entre un ou plusieurs chiffres dans les champs **1e - 4e Destination**. Ensuite, on saute directement à l'entrée de la liste qui commence par la séquence de chiffres entrée. L'entrée d'une séquence de lettres est également possible.

---

6) Dans la liste déroulante **Renvoi temporisé toujours réalisé au bout de**, indiquez la durée en secondes à l'issue de laquelle l'appel est renvoyé vers la destination suivante.

7) Cochez la case **Renvoi temporisé**, si en cas d'occupation l'appel doit être immédiatement acheminé vers la destination suivante.

8) Si l'appel doit être signalisé auprès d'un abonné interne supplémentaire ou par ex. sur un relais (actionneur) d'une sonnerie centrale, sélectionnez dans la liste déroulante **Destination seconde sonnerie** le numéro de téléphone souhaité. Avec **Type de seconde sonnerie**, indiquez si l'appel doit être signalé à l'abonné immédiatement ou bien une fois écoulée la durée de temporisation du renvoi d'appel.

9) Cliquez sur **OK&Suivant**. Vous vous trouvez de nouveau dans la fenêtre **Table d'acheminement - Définition**.

10) Si vous voulez paramétrer d'autres tables d'acheminement, répétez les étapes précédentes.

11) Cliquez sur **OK&Suivant**.

12) Affectez maintenant aux abonnés la table d'acheminement.

13) Vous pouvez rechercher un abonné en entrant un terme dans le champ **N° de téléphone** ou **Nom** puis en cliquant sur la touche Return. Tous les résultats contenant le terme sont affichés. Si vous entrez `521` comme numéro de téléphone, il est affiché par ex. les résultats `+495213535` et `+498967521` ou si vous entrez `co` comme nom, les résultats `Collins`, `Mcoin` et `Branco`.

Remarque : Toutes les entrées sont affichées lorsque rien n'a été entré dans tous les champs de recherche et que vous appuyez ensuite sur la touche Retour.

---

14) Dans la ligne de l'abonné souhaité, sélectionnez pour les cas suivants à partir des listes déroulantes, les tables d'acheminement :
    - **Jour** : Table d'acheminement pour appels externes entrants durant le temps de travail (circuit de jour)
    - **Nuit** : Table d'acheminement pour appels externes entrants lorsque le circuit de nuit est activé
    - **Interne**: table d'acheminement pour appels internes entrants
15) Enregistrez vos entrées avec **Sauvegarder** avant de passer à un abonné d'une autre page.
16) Si vous voulez affecter de manière confortable plusieurs abonnés à une table d'acheminement, cliquez sur **Copier**.
    a) Dans **Table d'acheminement**, sélectionnez la table d'acheminement à laquelle les abonnés doivent être affectés.
    b) Dans la fenêtre **Choix** marquez un ou plusieurs abonnés et les reprendre avec **Ajouter** dans la fenêtre **Membres**.
    c) A l'aide de cases à cocher **Jour**, **Nuit** et **Interne**, indiquez si la table d'acheminement pour les appels externes entrants doit s'appliquer durant les horaires de travail (renvoi Jour), lorsque le renvoi de nuit est activé ou seulement aux appels internes.
    d) Cliquez sur **OK&Suivant**.
17) Ensuite, cliquez sur **OK&Suivant**.
18) Vous pouvez ici faire afficher tous les abonnés d'une table d'acheminement. Pour cela, sélectionner dans **Afficher tous les membres de la table d'acheminement** la table d'acheminement souhaitée.
19) Cliquez sur **OK&Suivant**. Le renvoi temporisé pour abonnés internes est paramétré.
20) Cliquez sur **Quitter**.

13.4.2 Transfert d'appel (CF - Call Forwarding)

La fonction Transfert d'appel (CF) permet aux abonnés de réacheminer les appels entrants vers une destination de leur choix.

Lorsque des touches de ligne (y compris des touches de ligne MULAP) sont disponibles, il est possible d'activer le renvoi d'appel également de manière individuelle pour une ligne définie (ou pour une ligne MULAP).

Il est possible de réacheminer les types d'appels suivant :

- Tous les appels
- Uniquement les appels externes
- Uniquement les appels internes

Un renvoi d'appel peut être réacheminé vers les destinations suivantes :

- Autre téléphone (interne ou externe)
- Poste opérateur
- Messagerie vocale
- Groupement
- Groupe UCD (Universal Call Distribution/Répartition universelle des appels)

Les appels sortants demeurent possibles lorsque le renvoi d'appel est activé.

Destination externe

Si la destination du renvoi d'appel est externe, vous devez entrer l'indicatif réseau suivi du numéro externe de la destination de renvoi.

Renvoi d'appel vers des destinations externes

Si un abonné à inscrit dans sa table d'acheminement un renvoi d'appel en direction d'une destination externe, le renvoi temporisé aboutit à cette destination. Les autres destinations éventuellement inscrites dans la table d'acheminement ne sont pas prises en compte.

Si le renvoi temporisé doit être effectué vers d'autres destinations, l'indicateur système **Transfert temporisé après transfert en direction d'une destination externe** doit être activé par un technicien.

Si le transfert d'appel vers une destination externe doit être effectué en cas d'appel via une ligne réseau analogique, l'indicateur système **Transfert d'appel via LR analogique autorisé** doit être activé par un technicien.

Remarque : Lorsqu'un appel est routé par Smart AA et qu'il est dirigé vers un utilisateur A avec un transfert externe activé (*11) vers l'utilisateur B, ce n'est pas la CLI de l'appelant mais le SDA de l'utilisateur A qui est présenté à l'utilisateur B.

Correspondances

Rubrique	Correspondance
Ne pas déranger	Il est impossible de programmer un renvoi d'appel pour un téléphone lorsque la fonction Ne pas déranger (NPD) est active.
Rendez-vous, équipement de réveil	Lorsqu'un rendez-vous est échu, il est signalé sur le téléphone, indépendamment du fait qu'un renvoi d'appel ait été activé.
Groupe UCD comme destination de renvoi d'appel	Le renvoi vers un groupe UCD n'est pas suivi dans les cas suivants : • Si un groupement est appelé et si c'est le tour d'un abonné avec un renvoi d'appel vers un groupe UCD, le renvoi d'appel n'est pas suivi. Dans ce cas, c'est l'abonné suivant du groupement qui est directement appelé. • Un abonné est membre d'un groupe d'appel collectif avec la propriété "Groupe" et a activé un renvoi d'appel vers un groupe UCD. • Un abonné est membre d'un groupe d'appel collectif sur non-réponse. Si le groupe est appelé, le renvoi d'appel vers le groupe UCD n'est pas suivi. Exception : le premier abonné inscrit a activé un renvoi vers un groupe UCD. Ce renvoi est suivi.

13.4.2.1 Comment activer ou désactiver le renvoi d'appel via lignes réseau analogiques

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, allez à **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous voulez activer le renvoi d'appel via les lignes réseau analogiques, cochez la case **Renvoi via LR analogique autorisé**.
   - Si vous voulez désactiver le renvoi d'appel via les lignes réseau analogiques, décochez la case **Renvoi via LR analogique autorisé**.
5) Cliquez sur **Appliquer** puis sur **OK**.

13.4.2.2 Comment activer ou désactiver un renvoi d'appel vers une destination externe

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, allez à **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer le renvoi d'appel après un renvoi d'appel en direction d'une destination externe, cochez la case **Renvoi temporisé après renvoi en direction d'une destination externe**.
   - Si vous souhaitez activer le renvoi d'appel après un renvoi d'appel en direction d'une destination externe, cochez la case **Renvoi temporisé après renvoi en direction d'une destination externe**.
5) Cliquez sur **Appliquer** puis sur **OK**.

13.4.3 Renvoi d'appel Après tempo

Le renvoi d'appel après temporisation renvoie les appels non acceptés après un certain temps. Le renvoi temporisé est similaire à un renvoi temporisé, à la différence que l'abonné peut définir lui-même le renvoi.

L'abonné peut configurer le renvoi temporisé pour son téléphone personnel, ainsi qu'entrer des destinations et groupes externes.

La destination du renvoi n'est pas enregistrée de façon permanente : elle est effacée à la désactivation de la fonction.

Si la ligne est occupée, les règles de renvoi temporisé s'appliquent et l'appel est directement renvoyé vers la destination suivante.

Informations spécifiques du système

Trois destinations peuvent être définies pour chaque abonné. En outre, un identifiant spécial "personnalisé" permet à l'administrateur de libérer ou de verrouiller la fonction Renvoi d'appel après temporisation pour chaque abonné. La fonctionnalité est validé par défaut.

Lorsque le délai de réponse prédéfini est écoulé, le programme recherche la destination de renvoi enregistrée par l'abonné pour transférer l'appel. Si l'abonné n'a défini aucune destination de renvoi individuelle, le programme sélectionne la destination suivante dans la table d'acheminement.

L'administrateur doit valider le renvoi après temporisation pour l'abonné à l'aide des tables d'acheminement.

13.4.4 Renvoi temporisé au réseau (pas pour les Etats-Unis)

Chaque abonné auquel un numéro MSN (Multiple Subscriber Number, numéros multiples affectés à une ligne d'accès au réseau RNIS ou connexion ITSP) a été affecté comme numéro SDA peut activer ou désactiver un renvoi temporisé en réseau pour ce numéro MSN. L'abonné doit être autorisé à effectuer un renvoi temporisé externe.

Si un numéro MSN est affecté à un groupe d'abonnés, chaque abonné de ce groupe peut activer ou désactiver pour un renvoi temporisé en réseau pour ce numéro MSN.

La fonctionnalité se décline en trois variantes :

- Renvoi d'appel inconditionnel (CFU = Call Forwarding Unconditional) : l'opérateur renvoie directement tous les appels destinés à ce numéro MSN, indépendamment de leur état.
- Renvoi d'appel sur occupation (CFB = Call Forwarding Busy) : le renvoi d'appel n'est effectué que lorsque le numéro MSN sélectionné est occupé.
- Renvoi d'appel sur non-réponse (CFNR = Call Forwarding No Reply) : le renvoi d'appel n'est exécuté que lorsque l'appel entrant ne reçoit pas de réponse dans un délai prédéfini.

Remarque : Pour tous les scénarios de renvoi d'appel ci-dessus, les utilisateurs ne peuvent saisir qu'une seule destination de renvoi par MSN. Le nombre de MSN pouvant être renvoyés est limité à 10.

En cas de ITSP ou RNIS configuré avec un SDA, le nombre est 249.

Correspondances

Rubrique	Correspondance
Renvoi de nuit	Le renvoi temporisé en réseau a une priorité plus élevée que le renvoi de nuit.

13.4.5 Acheminement

L'acheminement permet un renvoi temporisé des appels entrants d'une ligne analogique ou S_0 en direction d'un abonné ou d'un groupe, en fonction du numéro de téléphone sélectionné et de l'état d'activation du renvoi de nuit.

Différentes destinations sont possible pour l'exploitation de jour et l'exploitation de nuit. L'appel entrant n'est pas signalé à l'abonné mais conformément aux tables d'acheminement pour pour l'abonné.

13.4.5.1 Comment configurer l'acheminement

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Lignes/Routage** > **Lignes**.
4) Dans Arborescence du menu, dans **Lignes** > **…** (indicatif du port Box), allez à la ligne analogique ou S_0 souhaitée.
5) Dans la liste déroulante **N° d'appel de jour**, sélectionnez le numéro de téléphone souhaité.
6) Dans la liste déroulante **N° d'appel de nuit**, sélectionnez le numéro de téléphone souhaité.
7) Cliquez sur **Appliquer** puis sur **OK**.

13.4.6 Pilotage

La fonctionnalité Pilotage permet à chaque abonné interne de gérer une liste personnelle de numéros internes qui sont appelés suite à l'appel de son numéro.

Les utilisateurs peuvent aussi entrer leurs propres numéros de poste. Ils peuvent le faire, par exemple, si un numéro de poste est acheminé en permanence vers un autre poste (Chef/Secrétaire).

Pour activer/désactiver cette fonctionnalité, il est possible de programmer une touche sur les téléphones système IP, OpenStage téléphones TDM, téléphones optiPoint 500. Pour permettre les variations, il est possible de programmer plusieurs touches de pilotage. Plusieurs touches peuvent être activées simultanément, toutefois le nombre maximum des téléphones avec signalisation d'appel ne doit pas dépasser cinq.

Cette fonctionnalité peut être activée/déactivée par l'abonné pour le propre téléphone via une connexion DISA ou pour un autre abonné, à l'aide de la fonctionnalité Services associés.

L'affichage écran Renvois... est l'un des trois affichages du menu pour l'ensemble du système Manager E, qui fournit des informations d'état

spécifiques du terminal (et non pas spécifiques du système). A l'aide de la fenêtre Renvoi, vous pouvez vérifier si la fonctions Pilotage actif a été activée sur un téléphone et savoir si le téléphone fait partie d'un groupe d'appel.

Si la fonctionnalité est utilisée fréquemment, l'utilisateur peut alors programmer pour celle-ci une touche libre sur son téléphone. Dans la programmation des touches, le nom de la touche est Activation du pilotage. Lorsque la fonctionnalité est active, la LED est allumée.

Grâce au flag d'abonné "Pas de pilotage sur occupation", il est possible de déterminer les abonnés pilotés qui doivent être appelés lorsque le "Maître" est occupé (= abonnés pilotés) et ceux qui ne doivent pas. Si plusieurs "maitres" ont piloé le même abonné, le flag s'applique à tous les pilotages de cet abonné.

Lorsque le flag n'est pas placé, le pilotage est effectué dans tous les cas, dans la mesure où l'abonné piloté est joignable (comportement par défaut).

Si ce flag est activé, le pilotage est fonction de la joignabilité du "maître" :

- "Maître" est libre - Pilotage Se produit Immédiatement

  Le "maître" peut recevoir un avertissement - pilotage après 5 secondes.

  Il n'est pas possible d'appeler un abonné qui effectue un pilotage ou de lui adresser un avertissement : il n'y a pas de pilotage.

Sujet	Correspondance/Restriction
Retour d'appel Recherche système Callback	Lors d'un retour d'appel immédiat (par ex. erreur de commande), d'une recherche système ou d'un rappel, le pilotage n'est pas effectué.
Renvoi d'appel	Si l'abonné qui a activé le pilotage lance un renvoi, le pilotage n'a pas lieu.
Ne pas déranger (DND)	Si l'abonné concerné par la demande de pilotage a activé Ne pas déranger, il n'est pas appelé.
Rendez-vous	Un appel rendez-vous ne peut pas suivre le pilotage.
Pas de pilotage sur occupation	Si le flag est posé, le pilotage n'est pas effectué lorsque l'abonné est occupé.

13.4.7 Refuser les appels

L’abonné a la possibilité de refuser des appels initiaux internes et externes. Ces appels peuvent être refusés au moyen de la touche de coupure.

L’appel refusé est ensuite renvoyé selon l’instruction de renvoi temporisé. Lorsque aucune destination de renvoi temporisé n’a été définie, les appels externes sont réacheminés vers le poste opérateur si les critères de renvoi requis ont été configurés. Lorsque aucune destination ne peut être appelée, l’appelant entend la tonalité d’occupation.

Les retours d’appel, les transferts d’appel, les rappels réservés, les communications mises en garde ou parquées ne peuvent pas être rejetées. Un appel réacheminé vers le poste de renvoi ne peut pas être refusé.

Correspondances

Rubrique	Correspondance
Appel de groupe, appel de groupe de recherche de recherche de ligne, MULAP	Dans ces cas, l’appel de groupe est annulé et l’appel est acheminé selon le renvoi temporisé paramétré. L’appel se termine s’il n’existe aucune autre destination d’appel.

13.4.8 Mise en réserve d'un appel

Les abonnés ont la possibilité de mettre un appel entrant en réserve. L'abonné appelé peut établir une connexion sans accepter l'appel entrant.

L'appel en attente est ensuite signalé comme appel en instance par un "Avertissement".

Lorsqu'un appel entrant est signalé, l'abonné appuie sur une touche de ligne ou une touche de communication pour pouvoir lancer un appel externe. Pour cela, deux touches de communication et une touche de ligne doivent être programmées. L'une des touches correspondantes doit être libre pour exécuter la fonction.

L'appelant ne remarque aucune modification de signalisation lorsque l'indication d'appels en instance a été activée.

13.4.9 Ne pas déranger

Ne pas déranger empêche la transmission des appels entrants.

Lorsqu'il décroche le combiné, l'abonné qui a activé la fonction NPD entend une tonalité d'invitation à numéroter spéciale. De plus, dans le cas de téléphones avec écran, l'indication Ne pas déranger est affichée tant que la fonction est activée. Sur tous les autres téléphones, la LED de la touche d'appel direct clignote par intermittence lorsque la fonction NPD est activée.

La fonction Ne pas déranger peut être outrepassée par le poste opérateur ou par un abonné autorisé. L'appel peut dans ce cas être directement transmis à l'abonné même si la fonction NPD est activée.

Lorsqu'un téléphone est en mode NPD, les appelants entendent la tonalité d'occupation.

Correspondances

Sujet	Correspondance
Poste opérateur/ Destination de nuit	Le poste opérateur et le poste de renvoi actuel ne peuvent pas activer la fonction Ne pas déranger.
Renvoi d'appel	La fonction NPD ne peut pas être activée sur un téléphone lorsqu'un renvoi d'appel a été activé. Le renvoi d'appel ne peut pas être activé sur un téléphone lorsque la fonction NPD a été activée.

Sujet	Correspondance
Rappel	Le rappel d'un abonné qui a activé la fonction Ne pas déranger n'est exécuté que lorsque la fonction NPD a été désactivée. Si l'abonné ayant activé la fonction NPD lance un rappel, la fonction Ne pas déranger est outrepassée.
Rendez-vous, équipement de réveil	Lorsqu'un abonné a programmé un rendez-vous et qu'il active la fonction Ne pas déranger, le téléphone émet un signal sonore à l'heure du rendez-vous.
DISA	La fonction DISA (Direct Inward System Access, connexion d'un poste distant au PABX) peut être activée par l'utilisateur pour son téléphone ou pour le téléphone d'un autre utilisateur (services associés).

13.5 Optimisation du déroulement de la communication

Le système de communication offre différentes possibilités pour gérer les appels de manière confortable et efficace, par ex. Rappel ou Avertissement.

13.5.1 Rappel

Lorsque l'abonné appelé ne répond pas ou si sa ligne est occupée, il est possible d'activer la fonction de rappel. Lorsqu'elle est activée, la fonction de rappel lance un appel dès que l'abonné appelé est de nouveau joignable.

Rappel automatique sur "Non-réponse" ou "Occupation"

Lorsqu'une communication ne peut aboutir parce que l'abonné appelé est occupé ou ne répond pas, l'abonné appelant peut activer la fonction de rappel afin d'établir la communication ultérieurement. Si l'abonné appelé est occupé, la fonction de rappel guette la fin de la communication. Lorsque l'abonné appelé est de nouveau libre, le système de communication appelle l'abonné appelant afin de le lui signaler. Si l'abonné appelant accepte l'appel, l'abonné qui était occupé est rappelé. Si la communication programmée par le biais de la fonction de rappel n'aboutit pas, cette dernière reste active. La tentative de rappel est répétée chaque fois que l'abonné appelé a achevé une communication.

Un poste téléphonique peut émettre deux demandes de rappel automatique et être le destinataire de deux demandes. Toutes les requêtes supplémentaires sont rejetées.

Les demandes de rappel automatique sont effacées dans les cas suivants :

- la communication a été établie, sinon le rappel reste actif (en cas de rappel interne),
- le rappel a été établi sans qu'une communication ait pu aboutir (en cas de rappel externe),
- l'abonné à l'origine de la demande efface le rappel automatique,
- le système efface quotidiennement tous les rappels à 23:57.

Les demandes de rappel automatique peuvent être définies pour des abonnés internes et des groupes. La demande de rappel automatique adressée à un groupe est stockée sur le premier abonné. En cas de demande de rappel définie pour un groupe, tous les téléphones libres sonnent.

Rappel automatique sur non-réponse sur l'interface réseau

Un abonné interne qui essaie de joindre un abonné externe ne répondant pas peut activer une demande de rappel dans le réseau. La ligne de l'abonné appelé est alors surveillée. Dès que l'abonné appelé établit lui-même une communication et y met à nouveau fin, le réseau tente d'établir une communication entre les deux abonnés. Cette fonctionnalité doit être supportée par le réseau.

Rappel sur occupation

Il est possible de programmer le rappel manuel d'un poste externe lorsque celui-ci est occupé. Dès que l'abonné est de nouveau libre, le réseau tente d'établir une communication entre les deux abonnés. La fonction doit être supportée et activée par le réseau et par le poste homologue.

13.5.2 Avertissement

Le service Avertissement signale à un abonné en communication l'arrivée d'un autre appel entrant.

Le signal est optique, en l'occurrence par l'intermédiaire d'un message qui s'affiche à l'écran. Le signal peut également être acoustique, en l'occurrence par le biais de la tonalité d'appel en instance. La tonalité d'appel en instance est émise toutes les 5 secondes.

L'abonné appelé peut accepter ou ignorer le deuxième appel. Pour recevoir le deuxième appel, l'abonné peut mettre fin à la première communication et accepter la deuxième communication ou bien sélectionner la fonction **Réponse avertissement** proposée à l'écran. Dans ce cas,la première communication est mise en garde.

Lorsqu'un appel est déjà signalé à un abonné, aucun appel supplémentaire ne peut lui être indiqué (au maximum 4 abonnés peuvent être en attente sur occupation). De même, si l'abonné a activé la fonction Rejet des appels en instance, aucun appel en instance ne lui est indiqué. Si la fonction Renvoi temporisé sur occupation n'a pas été configurée, l'appelant entend le signal d'occupation.

Activer l'indication d’appel en instance (Avertissement)

Avertissement parle poste opérateur

Le flag **Rejet des appels en instance** doit avoir été défini pour l'abonné afin que celui-ci puisse activer ou désactiver l'indication d'appel en instance par le biais des options de menu ou d'un code numérique. Si un abonné a activé l'indication d’appel en instance, il est averti même s'il a configuré le renvoi temporisé sur occupation.

Le paramètres par défaut est toujours Avertissement Après tempo. Mais le poste opérateur peut aussi effectuer immédiatement un avertissement.

Correspondances

Sujet	Correspondance
Avertissement sans tonalité	L'abonné peut activer et désactiver la tonalité d'appel en instance au moyen d'un code numérique. Les appels en instance continuent de s'afficher à l'écran du téléphone. La tonalité d'avertissement est activée par défaut.
Entrée en tiers	Lorsque le rejet des appels en instance est activé, aucune entrée en tiers n'est admise dans la communication de l'abonné.
Appel de groupe	Lorsqu'un ou plusieurs abonnés faisant partie d'un groupe d'appel collectif sont libres, l'appel leur est présenté. Si les abonnés sont occupés, à moins d'avoir activé le rejet des appels en instance, ils reçoivent tous le signal d'avertissement.
Appel interphone	L'appel interphone d'abonnés occupés est impossible.

13.5.2.1 Comment activer ou désactiver l'avertissement

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés**.
4) Cliquez par ex. sur **Clients IP**.
5) Cliquez par ex. sur **SystemClients**.
6) Sélectionnez l'abonné correspondant.
7) Cliquez sur l'onglet **Modifier les flags abonné**.
8) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer l'avertissement, décochez la case Protégé intrusions.
   - Si vous souhaitez désactiver l'avertissement, cochez la case **Protégé intrusions**.
9) Cliquez sur **Appliquer** puis sur **OK**.

13.5.2.2 Comment activer/désactiver l'avertissement immédiat par le P.O

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système**.
4) Cliquez sur **Retour/P.O/Hotline**.
5) Sous **Autres critères**, sélectionnez l'une des options suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Avertissement immédiat pour les appels du P.O**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Avertissement immédiat pour les appels du P.O**.
6) Cliquez sur **Appliquer**, puis sur **OK**.

Remarque :

Pour les téléphones de bureau CMI DECT - TDM, lorsqu'un abonné occupé est appelé, et que la fonction "appel en attente - avertissement" est autorisée, la tonalité d'occupation est active pendant 5 secondes, puis l'avertissement se déclenche et la tonalité de retour d'appel résonne.

Pour les téléphones IP DECT - SIP, lorsqu'un abonné occupé est appelé, et que la fonction "appel en attente - avertissement" est autorisée, l'avertissement est immédiat et la tonalité de retour d'appel résonne dès le début.

13.5.3 Entrée en tiers (Intrusion)

A l'aide de Entrée en tiers, un abonné autorisé peut intervenir dans la communication d'un abonné interne.

L'entrée en tiers se produit au moyen d'un indicatif ou d'une touche et elle est signalée aux correspondants associé par une tonalité d'avertissement ou par un affichage à l'écran.

Cette fonction peut être activée pendant le signal d'occupation ou pendant l'indication d'appel en instance.

En cas d'entrée en tiers dans une communication :

- Lorsque l'abonné appelé raccroche, il reçoit un appel de l'abonné qui transfère.
- Lorsque l'abonné qui entre en tiers (celui qui veut transférer la communication et entre en tiers) raccroche, la communication transférée est passée à l'abonné destinataire.
- Lorsque l'abonné qui était en communication avec l'abonné appelé raccroche, l'abonné appelé et l'abonné entré en tiers restent en communication.

Entrée en tiers peut être réalisée par chaque abonné interne et le poste de renvoi (poste opérateur). Afin de pouvoir utiliser cette fonctionnalité, l'abonné interne ainsi que le poste de renvoi doivent être autorisés.

Il est impossible d'interdire l'entrée en tiers sur un téléphone donné.

Correspondances

Sujet	Correspondance
Protection de la signalisation sur le canal vocal	L'entrée en tiers est impossible si l'abonné appelé ou son correspondant interne est paramétré comme poste de données (protection du canal voix contre les intrusions) ou si le correspondant appelé est en cours de numérotation.
Ne pas déranger	Si l'abonné appelé a activé la fonction Ne pas déranger (NPD), l'entrée en tiers n'est possible que s'il est en communication.
Groupe/groupe de recherche de ligne	Lorsque tous les membres d'un groupe ou d'un groupe de recherche sont occupés, l'entrée en tiers est impossible.
Abonné S_0	L'entrée en tiers visant un abonné S_0 est impossible.

13.5.3.1 Comment autoriser un abonné interne à effectuer des entrées en tiers

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés**.
4) Dans l'arborescence du menu, cliquez sur l'abonné (index - numéro - nom).
5) Cliquez sur l'onglet **Modifier les flags abonné**.
6) Cochez la case **Autorisation d'entrée en tiers activée**.
7) Cliquez sur **Appliquer** puis sur **OK**.

13.5.3.2 Comment autoriser l'entrée en tiers dans le poste de renvoi

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système** > **Renvoi/P.O/Hotline**.
4) Dans la zone **Autres critères**, cochez la case **Remplacement par P.O.**.
5) Cliquez sur **Appliquer** puis sur **OK**.

13.5.4 Textes d'absence

Le texte d'absence de l'abonné s'affiche à l'écran de l'appelant.

La fonction Textes d'absence permet également l'attribution de paramètres variables. Ces paramètres (par ex. l'heure) doivent être définis pendant l'activation. Le pavé numérique du terminal permet d'entrer les caractères complémentaires. Le texte d'absence peut être activé/désactivé sur un téléphone par le biais d'un code numérique ou d'une touche de fonction configurée au préalable.

Renvoi d'appel

En cas de renvoi d'appel le texte d'absence de l'abonné appelé est affiché et le renvoi d'appel est effectué.

13.5.4.1 Comment modifier un texte d'absence

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système**.
4) Cliquez sur **Textes**.
5) Dans la colonne **Textes message**, cliquez sur le champ correspondant et entrez le texte d'absence.
6) Cliquez sur **Appliquer** puis sur **OK**.

13.5.5 Textes messages

Les messages sont des textes système, qu'un abonné peut sélectionner et envoyer à un abonné interne.

Un texte de message (texte d'information) peut être envoyé à un ou plusieurs destinataires.

Pour envoyer le texte à tous les membres d'un groupe interne ou d'un groupe de recherche de ligne, indiquez le numéro d'appel du groupe ou du groupe de recherche de ligne à la place du numéro d'un destinataire spécifique.

Remarque : Seuls 100 téléphones peuvent recevoir des messages de masse MWI (indication de message en attente), tout message supplémentaire échouera.

Pour envoyer le message, appuyez sur la touche correspondante ou sélectionnez l'option de menu Envoyer un message.

L'envoi peut se faire lorsque le poste est à l'état inactif, en appel, en communication ou occupé. En cours d'appel, il n'est pas nécessaire d'indiquer le numéro du destinataire.

13.5.5.1 Comment modifier un texte d'information

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système**.
4) Cliquez sur **Textes**.
5) Dans la colonne **Textes message**, cliquez sur le champ correspondant et entrez votre texte.
6) Cliquez sur **Appliquer** puis sur **OK**.

13.5.6 Services associés

Un abonné autorisé peut commander certaines fonctions, comme par ex. activer/désactiver le renvoi d'appel, le code verrouillage ou le groupement de recherche de ligne, à la place d'un autre abonné. Le résultat est le même que si l'abonné activait ou désactivait ces fonctions lui-même.

Les fonctions suivantes peuvent être ainsi commandées pour un autre abonné :

- Renvoi d'appel, activer / désactiver
- Code verrouillage, activer / désactiver
- Pilotage, activer / désactiver
- Texte d'absence, activer / désactiver
- Groupe de recherche et appel collectif, activer / désactiver
- Renvoi de nuit, activer / désactiver
- Rendez-vous, activer / désactiver
- Envoyer un message / Effacer des messages envoyés
- Modifier le mot de passe de verrouillage
- Connecter / Déconnecter un agent UCD
- Agent UCD disponible / non disponible
- Agent UCD, activer / désactiver le post-traitement
- Agent UCD, renvoi de nuit activer / désactiver
- Renvoi MULAP, activer / désactiver
- Réinitialiser les fonctionnalités activées

Une procédure doit être exécutée. L'abonné doit entrer les paramètres suivants :

- L'indicatif pour les services associés
- Le numéro d'appel de l'abonné pour lequel une action doit être exécutée
- Le code numérique de la fonctionnalité à commander

Avant qu'un abonné puisse utiliser les services associés, il doit désactiver le code de verrouillage de l'autre abonné, s'il est activé.

13.5.6.1 Comment activer ou désactiver des services associés

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés**.
4) Dans l'arborescence du menu, cliquez sur l'abonné (index - numéro - nom).
5) Cliquez sur l'onglet **Modifier les flags abonné**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous voulez activer la fonction, cochez **Num./service associé**.
   - Si vous voulez désactiver la fonction, décochez **Num./service associé**.
7) Cliquez sur **Appliquer** puis sur **OK**.

13.5.7 DISA

DISA (Direct Inward System Access) permet aux abonnés autorisés d'utiliser les fonctionnalités du système de communication depuis l'extérieur, par ex. sur un téléphone mobile avec myPortal for Mobile (Mobile Callback) et Mobility.

Les abonnés peuvent, par l'intermédiaire de la fonction DISA, établir des connexions sortantes internes et externes. Chaque fois qu'un abonné utilise la fonction DISA, il doit entrer le mot de passe pour le code de verrouillage. Certaines fonctions sont alors disponibles, à l'instar d'une utilisation interne.

Le mode DISA supporte les fonctionnalités suivantes :

Fonctionnalité	par l'abonné en personne	par le biais de services associés
Renvoi d'appel, activer / désactiver	x	x
Ne pas déranger, activer / désactiver	x	x
Groupe de recherche, activer / désactiver	x	x
Texte d'absence, activer / désactiver	x	x
Pilotage, activer / désactiver	x	x
Code verrouillage, activer / désactiver	x	x
Réinitialiser les services	x	x

Fonctionnalité	par l'abonné en personne	par le biais de services associés
Numérotation abrégée centralisée	x	–
Envoyer un texte message	x	–
Renvoi de nuit, activer / désactiver	x	–

L'administrateur définit le numéro d'appel permettant aux abonnés d'accéder à la fonction DISA. Il est possible d'attribuer des numéros d'appel différents pour les communications internes et externes. Interne signifie à un autre nœud, mis en réseau via IP.

Le mot de passe que l'abonné doit entrer se compose du numéro d'appel interne et du PIN pour le code de verrouillage. Après avoir entré le mot de passe, l'abonné doit appuyer sur la touche # ou patienter jusqu'à ce que le système de communication ait identifié son entrée selon le mode de sécurité défini par l'administrateur pour la fonction DISA.

Pour exécuter une autre action par le biais de la fonction DISA, l'abonné doit ouvrir une nouvelle session.

Remarque : Dans OpenScape Business X, lorsqu'un numéro DISA est appelé, une tonalité continue se déclenche. Dans OpenScape Business S, lorsqu'un numéro DISA est appelé, une musique d'attente se déclenche.

13.5.7.1 Comment activer ou désactiver la classe de discrimination DISA pour un abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés**.
4) Dans l'arborescence du menu, cliquez sur l'abonné (index - numéro - nom).
5) Cliquez sur l'onglet **Modifier les flags abonné**.
6) Sélectionnez une des possibilités suivantes :
   - Pour activer la fonction, sélectionnez la case **Discrimination DISA**.
   - Pour désactiver la fonction, désélectionnez la case **Discrimination DISA**.
7) Cliquez sur **Appliquer** puis sur **OK**.

13.5.7.2 Comment configurer un numéro DISA

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Configur. de base** > **Système** > **DISA**.
4) Dans le champ **SDA**, entrez le numéro d'appel que les abonnés peuvent utiliser pour une connexion DISA de l'extérieur.
5) Dans le champ **Numéro d'appel**, entrez le numéro permettant aux abonnés d'utiliser la fonction DISA de façon interne.
6) Cliquez sur **Appliquer** puis sur **OK**.

13.5.7.3 Comment configurer le mode sécurisé pour la fonction DISA

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Configur. de base** > **Système** > **DISA**.
4) Dans la liste déroulante **Mode sécurité**, sélectionnez le mode sécurisé **Après tempo.** ou **Après entrée de #**.
5) Cliquez sur **Appliquer** puis sur **OK**.

13.5.8 Appel flexible/PIN mobile

Grâce à l'appel flexible (PIN mobile), le téléphone système est utilisé provisoirement, lors de la communication sortante suivante, comme s'il s'agissait du téléphone de l'abonné qui effectue cet appel.

L'appel flexible comprend le numéro d'appel, le nom, la discrimination réseau et la taxation de cet abonné.

Lorsque l'appel flexible est activé, le téléphone utilisé ne peut pas être joint sous son propre numéro. Une fois la communication terminée, cet état est supprimé.

Pour l'activation de l'appel flexible, il faut un code de verrouillage individuel pour l'abonné mobile.

Pour l'activation, effectuez l'une des opérations suivantes sur le téléphone système.

- OpenStage : Menu Service > PIN et Classe de discrimination > Appel flexible + numéro de téléphone mobile + code de verrouillage de l'abonné mobile
- Indicatif pour FlexCall + numéro de téléphone mobile + code de verrouillage de l'abonné mobile

13.5.9 Relocate

A l'aide de Relocate/Echange de numéro un abonné TDM est en mesure de modifier par procédure l'affectation entre port de connexion physique et données d'abonné logiques (profil d'utilisateur).

Relocate peut être utilisé lorsque deux abonnés décident d'échanger leurs postes de travail et qu'ils utilisent le même type de téléphone. Relocate permet la réalisation du DeskSharing pour les utilisateurs TDM. Les utilisateurs TDM sont en mesure d'effectuer le changement de numéro sans soutien de l'administrateur.

Il ne peut être échangé que des profils utilisateurs de même type de téléphone, c.-à-d. avec un clavier identique. Lors de l'échange des profils utilisateur des différents types de téléphone, les fonctions de touche programmées individuellement de l'appareil de base sont remplacées par les valeurs par défaut. Lors de la réalisation de Relocate, il se produit une défaillance/un rédémarrage des téléphones TDM associés. Le fonctionnalités activées sont traitées en conséquence, c.-à-d. que les rappels actuels et les infos envoyées sont effacés, toutes les autres fonctionnalités sont conservées.

Condition pour l'utilisation de Relocate : validation de la fonctionnalité pour l'ensemble du système. Pour l'échange de numéros, sélectionnez dans le menu Service du téléphone effectuant le remplacement Changer N° et entrez le numéro interne de l'abonné de destination ainsi que le PIN de verrouillage (le PIN de verrouillage n'est pas nécessaire lorsqu'il est encore égale à 00000, la valeur par défaut). Après entrée du numéro de destination, Relocate est verrouillé jusqu'à la fin de la procédure pour tous les autres abonnés. Lors de la réalisation de l'échange, les deux terminaux concernés sont réinitialisés. La réussite de l'échange est signalé sur les deux téléphones TDM par l'affichage du nouveau numéro (affichage écran : Nouveau N° : XXXXX).

Relocate ne peut pas être effectué sur les téléphones système avec autorisation de programmation (pour Assistant T). Donc, en règle générale, pas aux deux premiers téléphones système activés.

13.5.9.1 Comment valider pour l'ensemble du système un relocate/échange de numéro d'appel

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Configuration de base** > **Système**.

3) Dans l'arborescence du menu, cliquez sur **Flags système**.
4) Cochez la case **Changement de terminal autorisé**.
5) Cliquez sur **Appliquer** puis sur **OK**.

13.5.10 Réinitialisation des fonctionnalités activées

Vous pouvez réinitialiser des fonctions spécifiques sur votre terminal à l'aide d'indicatifs.

C'est possible pour les Fonctionnalités suivantes :

- Renvoi d'appel
- Effacer les informations reçues
- Texte d'absence, activer / désactiver
- Pilotage, activer / désactiver
- Groupe de recherche, activer / désactiver
- Refus de présentation de la ligne appelante, activer / désactiver
- Avertissement sans tonalité, activer / désactiver
- Ne pas déranger, activer / désactiver
- Coupure sonnerie, activer / désactiver
- Rendez-vous
- Effacer tous les rappels

13.5.11 Procédures

Le système de communication permet aux abonnés de programmer une touche avec des codes numériques, des numéros d'appel, ainsi que d'autres informations d'appel. Si l'abonné appuie sur la touche de procédure comme suffixe ou pendant une communication, le système transmet les signaux DTMF (multifréquence bitonalité) correspondants.

Exemples d'application :

- Code numérique pour le rappel
- Code numérique pour l'indication d’appel en instance
- Code numérique pour l'entrée en tiers
- Séquence de chiffres pour la messagerie vocale ou le répondeur
- Indicatif flashing réseau + numéro de destination
- Code numérique pour la commande d'un service + Numéro de destination, par ex. code numérique pour Envoi / Interrogation message (Message Waiting) + numéro d'appel + numéro de texte
- CA (Code Affaire) + indicatif faisceau + numéro de destination

Les procédures requérant l'entrée d'un PIN ne peuvent pas être enregistrées.

Seul le premier niveau de touches supporte les procédures.

Selon la situation, un abonné peut exécuter les fonctions suivantes sous forme de procédures :

Fonctionnalité	Prêt pour la numérotatio	Occupé	En communicat	Appel sortant	Appel entrant
Interception, ciblée	x	–	x	–	–
Renvoi, activer (pas pour les systèmes multi-sociétés ; pas pour les différents MSN d'une connexion réseau S_0)	x	–	x	x	–
Renvoi en réseau, activer / désactiver ; fonction de commutation (pas avec les systèmes multi-sociétés) ;	x	–	x	x	–
Répartition des appels, ouverture / fermeture de session ; fonction de commutation	x	–	x	x	–
Répartition des appels, activer / désactiver la destination de nuit ; fonction de commutation	x	–	x	x	–
Renvoi d'appel par Configuration Team	x	x	x	x	x
Texte d'absence, activer / désactiver ; fonction de commutation	x	–	x	x	–
Numérotation associée	x	x	x	x	x
Services associés	x	–	x	x	–
Appel interphone	x	–	x	–	–
Libération de lignes (Emergency Trunk Access)	x	–	x	x	–
Messages (Message Waiting), envoyer	x	–	x	x	–
NAI, émettre	x	–	x	x	–
NAC, émettre	x	–	x	x	–
Transfert DTMF	–	–	x	–	–
Transfert DTMF en cours de communication avec la touche de procédure	x	x	x	x	x
Renvoi de nuit, activer / désactiver ; fonction de commutation	x	–	x	x	–
Parcage / Reprise ; fonction de commutation	–	x	x	x	–
Code affaire CA	x	–	x	–	–
Code affaire CA en préfixe	x	–	x	–	–
Demandes de rappel, afficher / effacer ; fonction de commutation	x	–	–	–	–
Pilotage, activer / désactiver ; fonction de commutation	x	–	x	x	–
Sélection langue	x	x	x	x	x
Telephone Data Service TDS	x	–	x	x	–
Ouverture porte via boîtier adaptateur	x	x	x	x	x
Rendez-vous, activer / désactiver ; fonction de commutation	x	x	x	x	x
Reprise d'une communication externe à partir d'une mise en garde générale	x	x	x	x	x
Code de verrouillage central	x	–	x	–	–

Informations spécifiques du système

Une touche de procédure peut enregistrer 32 caractères au maximum.

13.5.12 Equipement de réveil et rendez-vous

Chaque abonné a la possilité de programmer un rendez-vous. Au moment programmé, un appel est émis. L'appel peut être unique (au cours des 24 heures suivantes) ou répété (c.-à-d. quotidien).

L'entrée de l'heure du rendez-vous de fait à l'aide de quatre chiffres, les deux premiers correspondent aux heures, les deux derniers aux minutes. Un mode d'horloge 12 heures est pris en charge pour les États-Unis : les utilisateurs saisissent les quatre chiffres, puis sélectionnent « am » (touche 2) ou « pm » (touche 7). En l'absence d'indication, "am" est retenu.

Les téléphones analogiques, optiPoint entry ou téléphones CMI peuvent uniquement programmer des rendez-vous uniques.

Un appel de rendez-vous dure par défaut 20 secondes ; il est répété jusqu'à cinq fois avec chaque fois une pause d'une minute. L'effacement de l'opération se produit automatiquement lorsque le combiné est décroché ou bien en cas d'appui de la touche haut-parleur durant l'appel ou bien après la cinquième répétition (nombre configurable). Un appel de rendez-vous peut aussi être effacé grâce à une procédure. Sur les terminaux à écran, il existe de plus une possibilité d'interrogation.

Si un appel de rendez-vous à échéance ne peut pas être signalé (par ex. abonné occupé), il est mis en réserve jusqu'au cycle suivant.

Conseil : Des rappels temporisés peuvent être programmés pour un maximum de 50 utilisateurs, par système.

13.6 Vue d’ensembles des fonctions et des codes

Indicatif de service	Description
*0	Reprise d'une communication en attente
*1	Renvoi d’appel
*2	Va-et-vient
*3	Conférence
*44	Renvoi de nuit activé
*51	Flashing réseau
*52	Coupure micro
*53	Numérotation MF
*55	Réponse avertissement
*56	Parcage

Indicatif de service	Description
*57	Interception dans un groupe d'interception
*58	Activer un rappel automatique
*59	Interception d'un poste
*60	Code affaire
*61	Ouverture de porte
*62	Entrée en tiers
*64	Activer renvoi externe (canal D)
*65	Interroger les coûts
*66	Verrouillage du poste
*67	Numérotation associée
*68	Envoyer un message
*69	Activer un texte d'absence
*7	Envoyer un No abrégé centralisé ou individuel
*80	Appel interphone
*90	Activer un relais
*91	Programmation des touches
*92	Modifier un numéro abrégé
*93	Modifier le code PIN
*940	Test du terminal
*95	Gestion du système
*97	Activer ne pas déranger
	Activer babyphone
*81	Pilotage
#1	Annuler un renvoi
#44	Renvoi de nuit désactivé
#52	Activer le micro
#56	Reprise parcage
#58	Consulter/annuler les rappels automatiques
#64	Annuler le renvoi externe (canal D)
#66	Déverrouillage du poste
#68	Lire/effacer un message
#69	Annuler un texte d'absence
#97	Annuler Ne Pas Déranger

Indicatif de service	Description
*96	Réponse automatique sur appel interphone
#96	Annuler réponse automatique sur appel interphone
#90	Désactiver un relais
#81	Annuler pilotage : effacer tous les abo. de la liste
#0	Réinitialiser tous les services
#3	Annuler conférence
#82	Consultation de la liste des appelants
*83	Services associés
*84	Appel malveillant
*85	Intégrer groupement
#85	Appel collectif désactivé
*82	Mémoriser dans la liste des appelants
*86	Activation masquage du N° SDA
#86	Désact. du masquage du N° SDA
*87	Suppression tonalité d'avertissement
#87	Activation tonalité d'avertissement
*98	Désactivation sonnerie poste
#98	Activation sonnerie poste
*991	Télégestion DTMF
*992	Autorisation télégestion DTMF
*993	Autorisation télégestion par accès RNIS (obsolète)
*994	Autorisation interro. à distance des données système
*89	Ouverture porte par code DTMF
#89	Ouverture porte par code DTMF verrouillée
*63	Reprise com. externe après touche mise en garde
*41	Attribuer N° SDA
*401	UCD - Intégration agents
#401	UCD - Retrait agent
*402	UCD - Agent disponible
#402	UCD - Agent indisponible
*403	UCD Activer post-traitement

Indicatif de service	Description
#403	UCD Désactiver post-traitement
*404	UCD Activer renvoi de nuit
#404	UCD Désactiver renvoi de nuit
*405	UCD Interroger file d'attente
*42	Telephone Data Service (TDS)
*43	Valider la ligne
*45	Recherche de personne : Rechercher
#45	Recherche de personne : Rencontre
*46	Appel de RDV : Activer
#46	Appel de RDV : Désactiver
*9419	Activer déménagement poste
#9419	Désactiver déménagement poste
*942	Déclaration combinés sans fil (CMI)
*943	Verrouillage centralisé
*944	Surveillance d’appel
	Drop Last Conference Party within CO (USA only)
*490	Activer autoriser les avertissements
#490	Désactiver autoriser les avertissements
*48	Sélection langue
*508	Appel flexible
*502	Activer le filtrage pour MULAP
#502	Désactiver le filtrage pour MULAP
*501	Activer renvoi pour MULAP
#501	Désactiver renvoi pour MULAP
*509	Geler le traçage
*47	DISA interne
*503	Numérotation KEYPAD
*54	Annuaire interne
*491	Terminal analogique d'hôtel
#943	Code verrouillage centralisé / redéfinir code
*9411	Renvoi d'appel client en mode urgence activé
#9411	Renvoi d'appel client en mode urgence désactivé

Indicatif de service	Description
*493	Enregistrement vocal act.
#493	Enregistrement vocal dés.
*495	Renvoi temporisé activé
#495	Renvoi temporisé désactivé
*945	Message discret
*494	Data I/O
*996	Autoriser les Smart Services via HTTPS pour l’administration à distance
#996	Désactiver les Smart Services via HTTPS pour l’administration à distance
*997	Arrêt contrôlé

14 Travailler en équipe (groupes)

Le système de communication propose de nombreuses fonctionnalités pour le travail en équipe. En dehors des groupes d'interception d'appel, groupes d'appel collectif et groupements, il faut aussi citer les groupes avec fonctions Team et Chef/Secrétaire ainsi que les groupes Boîte vocale et boîte Fax. La fonctionnalité "UCD (UCD Uniform Call Distribution)" assure une répartition équilibrée des appels entrants à l'intérieur d'un groupe de participants (groupe UCD).

Conseil : Lors de la configuration des groupes, il faut tenir compte du fait que les trois premiers groupes sont réservés :

Le premier groupe est utilisé par défaut comme groupe de recherche pour la messagerie vocale externe.

Le deuxième groupe est utilisé par défaut comme groupe de recherche pour OpenScape Business Smart VoiceMail.

Le troisième groupe est utilisé par défaut comme groupe de recherche pour le Company AutoAttendant d'OpenScape Business Smart VoiceMail.

14.1 Groupe d'interception, appel de groupe et groupe de recherche

Le système de communication offre différentes possibilités pour réunir les abonnés en groupes, afin que plusieurs abonnés et téléphones puissent par exemple être joints sous un même numéro ou qu'un appel destiné à un abonné soit aussi signalé chez les autres abonné.

Dans un groupe d'interception, l'appel pour un membre est toujours signalé également pour tous les autres membres du groupe.

Lors d'un appel de groupe, tous les membres sont joignables à l'aide du même numéro de téléphone (numéros des appels de groupe). Le premier abonné qui décroche est relié à l'appelant.

Dans un groupe de recherche, un appel entrant est signalé à un des membres. Si celui-ci ne prend pas l'appel, la communication est adressée au membre suivant. Tous les membres du groupement peuvent être joints sous un numéro unique.

14.1.1 Groupe d'interception

Un appel destiné à un membre d'un groupe d'interception est signalé également chez tous les autres membres du groupe. L'appel peut être pris par tous les autres membres du groupe grâce à une touche de fonction programmée à cet effet ou par l'entrée de menu correspondante du téléphone ou par la composition d'un indicatif.

Chez l'abonné du groupe d'interception appelé initialement, l'appel est signalé de façon acoustique et optique (écran). Si cela est programmé, l'appel est signalé également par la LED de la touche de fonction.

Les autres membres du groupe reçoivent d'abord uniquement une signalisation optique de l'appel. L'écran affiche le numéro ou le nom de l'abonné appelé initialement et le numéro ou le nom de l'appelant. L'affichage du numéro ou du nom de l'appelant peut être désactivé par un administrateur avec le profil **Expert** via le **Mode Expert**. Si cela est programmé, l'appel est signalé également par la LED de la touche de fonction.

Si l'appel n'est pas pris durant quatre sonneries (4 x 5 secondes), les autres membres du groupe sont avertis par une tonalité d'avertissement (signalisation acoustique). L'intervalle de temps entre la signalisation de l'appel et la tonalité d'avertissement n'est pas variable. La tonalité d'avertissement peut être désactivée par un administrateur avec le profil **Expert** via le **Mode Expert** pour tous les membres du groupe.

S'il y a plusieurs appels pour le groupe d'interception, la signalisation se fait dans l'ordre d'arrivée des appels.

Si les retours d'appel pour les membres d'un groupe AUN (groupe d'interception) doivent pouvoir être interceptés par les autres membres, cette fonction doit être activée par un administrateur avec le profil **Expert** via le **Mode Expert**.

Un abonné peut être uniquement membre dans un groupe d'interception.

Les taxes incombant éventuellement pour un appel intercepté sont affectées à l'abonné qui a intercepté l'appel.

Remarque : Les guillemets doubles (") ne sont pas supportés pour nommer un groupe d'interception.

Téléphones SIP

Il est possible d'intégrer des téléphones SIP dans un groupe d'interception.

Conseil : De plus, il est possible de programmer pour les téléphones SIP une touche de fonction pour le groupe d'interception d'appel ; les messages spécifiques d'un groupe d'interception peuvent être affichés sur l'écran des téléphones SIP. Pour cela, la fonctionnalité "Groupe d'interception" du téléphone SIP doit être activée (voir Mode d'emploi du téléphone SIP).

Interception d'appel à l'extérieur d'un groupe d'interception

Une variante de la fonctionnalité est "l'interception d'appel à l'extérieur d'un groupe d'interception". Cela permet l'interception d'appels pour les abonnés internes qui ne font pas partie du même groupe d'interception. L'interception de l'appel est possible par une touche de fonction programmée à cette effet ou par l'entrée de menu correspondante ou par sélection de l'indicatif d'interception ciblée, suivi de l'entrée du numéro de l'abonné appelé.

Correspondances

Rubrique	Correspondance
Rappel	Les retours d'appel et rappels ne sont signalés chez les autres membres du groupe que si le drapeau système **Interception après retour d'appel**.
Ne pas déranger	Les abonnés qui ont activé la fonctionnalité Ne pas déranger ne reçoivent pas de signalisation d'interception.
Téléphones RNIS	L'intégration de téléphones RNIS dans les groupes d'interception est impossible.
MULAP	L'intégration de numéros MULAP aux groupes d'interception est impossible.

Tâches associées

Configurer les groupes d'interception à la page 641
Comment ajouter ou supprimer des membres dans un groupe d'interception à la page 641
Comment activer ou désactiver l'affichage du numéro et du nom de l'appelant à la page 649
Comment activer ou désactiver la tonalité d'avertissement à la page 650
Comment activer ou désactiver l'interception de retour d'appel à la page 650

14.1.2 Appel de groupe

S'il faut que plusieurs abonnés puissent être joints sous un même numéro (numéro d'appel collectif), il est possible de définir un groupe d'appel collectif. Les appels externes et internes entrants sont signalés simultanément chez tous les membres du groupe. Le premier abonné qui décroche est relié à l'appelant.

Chaque membre d'un groupe d'appel collectif peut aussi être joint sous son propre numéro d'abonné.

Une des propriétés suivantes doit être affectée au groupe :

- Groupe

  Les appels entrants sont signalés simultanément chez tous les membres du groupe disponibles. Les membres du groupe disponibles sont les abonnés qui ne sont pas occupé. Chez les membres du groupe occupés, un appel en attente est signalé immédiatement par un bip d'avertissement. Si un abonné raccroche, l'appel continue à être signalé chez tous les membres du groupe (bip d'avertissement chez les abonnés occupés).

  L'appelant entend la tonalité d'occupation si tous les membres du groupe sont occupés et ont activé la fonction NPD. Si un renvoi temporisé est défini pour ce groupe, l'appelant ne reçoit pas de tonalité d'occupation, mais est directement acheminé vers la destination de renvoi temporisé suivante.
- RNA

  Les appels entrants sont signalés simultanément chez tous les membres du groupe. Si un membre du groupe est occupé, l'ensemble du groupe d'appel

collectif est identifié comme occupé. Les autres appelants entendent la tonalité d'occupation.

Remarque : L'état de présence d'une destination externe appartenant au groupe ne peut pas être détecté.

- Appel en attente

  Les appels entrants sont signalés simultanément chez tous les membres du groupe disponibles. Les membres du groupe disponibles sont les abonnés qui ne sont pas occupé. Un appel est signalé par une tonalité d'occupation pour les membres du groupe qui sont occupés.

  La fonction Ne pas déranger doit être désactivée chez tous les membres du groupe.

Les appels de groupe sont traités par le renvoi temporisé comme des abonnés. En d'autres termes, si un appel ne peut être pris par aucun membre d'un groupe d'appel collectif, il est renvoyé à une destination de renvoi temporisé conformément à la table d'acheminement. Vous pouvez spécifier si le renvoi d'appel doit être effectué sur RNA (sonnerie sans réponse) ou sur occupation.

Si un appel n'a été accepté par aucun membre d'un appel collectif, il est affiché comme appel manqué dans le journal des clients UC de tous les membres. Un appel accepté est affiché uniquement dans le journal du membre qui a accepté l'appel.

Un abonné peut faire partie de plusieurs groupes. Pour les groupes de type Appel de groupe, Groupe de recherche, Configuration Team / Groupe Team et Groupe Chef/Secrétaire / Groupe Top : La somme de tous les membres de ces groupes ne doit pas dépasser 32.

L'écran de l'abonné interne appelant affiche le nom affecté au groupe. Après la réception d'un appel, le nom de l'abonné qui a pris l'appel s'affiche.

Si un membre a défini des règles à l'aide de l'AutoAttendant, par exemple pour transférer des appels, ces règles ne s'appliqueront qu'aux appels destinés à son propre numéro de poste. Dans le cas d'un appel collectif, ces règles sont ignorées.

Il est possible de configurer jusqu'à 20 abonnés par appel collectif.

Il est possible d'affecter à chaque groupe d'appel collectif un nom de 16 caractères maximum.

Boîte vocale pour un appel de groupe

Lors de la configuration d'un appel de groupe, une messagerie vocale est automatiquement créée. Le numéro de cette boîte vocale du groupe d'appel correspond toujours au numéro du groupe d'appel. Si aucun membre n'accepte un appel de groupe, le renvoi est effectué en direction de la boîte vocale du groupe d'appel. Pour ce faire, la boîte vocale de l'appel de groupe doit avoir été définie comme destination CFNA (renvoi d'appel sans réponse) de cet appel de groupe.

Si un membre ne prend pas l'appel entrant de son propre numéro d'abonné, cet appel est renvoyé vers une destination de renvoi conformément à la table d'acheminement de cet abonné.

Exemple d'un appel de groupe de type RNA (sonnerie sans réponse) avec le numéro d'appel de groupe 404 et les membres A (numéro d'appel 200), B (201) et C (202). Pour l'appel de groupe, un renvoi temporisé en direction de la boîte vocale du groupe d'appel collectif a été configuré. Chaque membre a défini le renvoi d'appel sans réponse (CFNA) après le délai d'attente vers sa propre boîte vocale.		
Appel entrant pour le membre A (200)	Tous les membres sont libres.	Le membre A ne prend pas l'appel. Un renvoi temporisé vers la boîte vocale du membre A est effectué.
	Le membre A a défini le renvoi d'appel inconditionnel (CFU) vers sa propre boîte vocale. Les membres B et C sont libres.	L'appel est immédiatement transféré (CFU) vers la boîte vocale du membre A.
Appel entrant pour l'appel de groupe (404)	Tous les membres sont libres.	L'appel est signalé à tous les membres du groupe. Aucun membre ne prend l'appel. Un renvoi temporisé vers la boîte vocale du groupe d'appel collectif est effectué.
	Le membre A a défini le renvoi d'appel inconditionnel (CFU) vers sa propre boîte vocale. Les membres B et C sont libres.	L'appel est signalé aux membres B et C. Aucun membre ne prend l'appel. Un renvoi temporisé vers la boîte vocale du groupe d'appel collectif est effectué.
	Le membre A a défini un renvoi d'appel inconditionnel (CFU) vers une destination externe. Les membres B et C sont libres.	L'appel est signalé aux membres B et C ainsi qu'à la destination externe. Aucun membre ne prend l'appel. Un renvoi temporisé vers la boîte vocale du groupe d'appel collectif est effectué.
	Le membre A a défini les règles CFNA à l'aide de l'AutoAttendant. Les membres B et C sont libres.	L'appel est signalé à tous les membres du groupe. Aucun membre ne prend l'appel. Un renvoi temporisé vers la boîte vocale du groupe d'appel collectif est effectué.

Activation et désactivation du groupe d'appel collectif

Si un abonné est membre d'un groupe d'appel collectif, il peut se retirer de ce groupe et y retourner grâce à des indicatifs.

Si un abonné est membre aussi bien de plusieurs groupements que de plusieurs groupes d'appel collectif, il peut se retirer de tous les groupements et groupes d'appel collectif et y retourner grâce à des indicatifs. Le retrait et le retour dans un groupement ou groupe d'appel collectif précis est possible par

l'entrée des indicatifs suivie de la sélection des groupements et groupes d'appel collectif affichés sur l'écran.

Il est aussi possible de programmer des touches de fonction avec fonction de commutation pour l'intégration et le retrait. Dans ce cas, une touche de fonction peut être programmée pour s'appliquer à un groupement ou groupe d'appel collectif précis ou à tous les groupements et groupes d'appel collectif. Une programmation variable est également possible. Lorsque l'utilisateur appuie sur une touche de fonction de ce type, il doit ensuite définir en le sélectionnant dans les groupes d'appel collectif et groupements affichés à l'écran, pour quel groupement ou groupe d'appel collectif le retrait/retour doit s'appliquer.

Type de sonnerie

Pour chaque appel collectif, un administrateur ayant le profil **Expert** peut définir la signalisation acoustique des appels externes entrants via le réglage du type de sonnerie. Vous disposez des possibilités suivantes :

- Sonnerie à deux tons (paramètre par défaut)
- Sonnerie à trois tons
- sonnerie courte-longue-courte

Sur les téléphones analogiques, seul le paramètre par défaut est possible. Les modifications n'ont pas d'influence.

Téléphones SIP

L'intégration de téléphones SIP dans un groupe d'appel collectif est possible.

Remarque : Sur les téléphones SIP, il n'est pas possible de programmer des touches de fonction. Les messages d'affichage spécifiques d'un groupe de recherche ne sont pas pris en charge.

Correspondances

Rubrique	Correspondance
Renvoi d'appel	Si un membre du groupe active un renvoi d'appel pour tous les appels, tous les appels sont signalés sur le téléphone de destination.
Ne pas déranger	Si un membre du groupe active la fonction Ne pas déranger, les appels entrants adressés à son téléphone ne sont pas remis. Cela concerne les appels qui passent par le numéro de groupe et le numéro de l'abonné.
Entrée en tiers	Si tous les membres d'un groupe d'appel collectif sont occupés, aucune entrée en tiers n'est possible.
Téléphones RNIS	L'intégration de téléphones RNIS au groupe d'appel collectif est impossible.

Concepts associés

Répertoire interne à la page 466

Tâches associées

Comment ajouter un groupe d'appel collectif à la page 642

Comment modifier un groupe d'appel collectif (groupe) à la page 643
Comment effacer un groupe d'appel collectif à la page 644
Comment ajouter ou effacer un membre dans un groupe d'appel collectif à la page 645
Comment ajouter un groupe d'appel collectif (non-réponse ou avertissement) à la page 650
Comment afficher ou modifier l'appel collectif (non-réponse ou avertissement) à la page 651
Comment effacer l'appel collectif (non-réponse ou avertissement) à la page 652
Comment ajouter ou effacer un membre du groupe d'appel collectif (non-réponse ou avertissement) à la page 652
Comment activer ou désactiver le rejet des appels en instance pour les membres d'un groupe à la page 653

14.1.3 Groupe de recherche

Les groupes de recherche de personnes permettent de distribuer les appels entrants aux abonnés associés (membres). Si un abonné est occupé ou n'accepte pas un appel entrant, l'appel est automatiquement transféré au prochain membre libre du groupe de recherche. Tous les membres du groupe de recherche peuvent être joints au même numéro de téléphone.

Chaque membre d'un groupe de recherche peut également être joint à son propre numéro de poste.

L'une des propriétés suivantes doit être attribuée au groupe de recherche.

- Linéaire

  Un appel entrant est toujours signalé en premier lieu au premier membre d'un groupe de recherche. La suite de la signalisation est effectuée en fonction de l'ordre dans lequel les membres sont entrés dans le tableau des groupes.
- Cyclique

  Un appel entrant est toujours signalé en premier au membre qui suit l'abonné qui a répondu au dernier appel. La suite de la signalisation est effectuée en fonction de l'ordre dans lequel les membres sont entrés dans le tableau des groupes.

L'appel est automatiquement transféré au prochain membre libre du groupe de recherche de personnes à l'expiration du délai de transfert, à condition qu'il n'y ait pas de réponse à l'appel, qu'un membre soit occupé ou que la fonction NPD soit activée.

Vous pouvez programmer une destination de renvoi d'appel (liste de destination d'appel) si un appel ne peut être pris par aucun des membres du groupe de recherche.

Un abonné peut faire partie de plusieurs groupes. Pour les groupes de type Appel de groupe, Groupe de recherche, Configuration Team / Groupe Team et Groupe Chef/Secrétaire / Groupe Top : La somme de tous les membres de ces groupes ne doit pas dépasser 32.

Le nom attribué au groupe de recherche est affiché sur l'écran de l'appelant interne. Après la réception d'un appel, le nom de l'abonné qui a pris l'appel s'affiche.

Si un membre a défini des règles à l'aide de l'AutoAttendant, par exemple pour transférer des appels, ces règles ne s'appliqueront qu'aux appels destinés à son propre numéro de poste. Les règles sont ignorées pour les appels de groupe de recherche de personnes.

Il est possible de configurer jusqu'à 20 abonnés par groupe de recherche.

Chaque groupe de recherche peut se voir attribuer un nom contenant jusqu'à 16 caractères.

Boîte vocale pour groupe de recherche

Lors de la configuration d'un groupe de recherche, une boîte vocale est automatiquement créée pour ce groupe. Le numéro d'appel de cette boîte vocale pour le groupe de recherche correspond toujours à celui du groupe de recherche. Si un appel destiné à un groupe de recherche n'est accepté par aucun membre, l'appel est transféré vers la boîte vocale du groupe de recherche. Pour ce faire, la boîte vocale du groupe de recherche doit avoir été définie comme destination CFNA (renvoi d'appel sur non-réponse) de ce groupe de recherche.

Si un membre ne prend pas l'appel entrant de son propre numéro d'abonné, cet appel est renvoyé vers une destination de renvoi conformément à la table d'acheminement de cet abonné.

Exemple d'un groupe de recherche linéaire avec le numéro d'appel 404 et les membres A (numéro d'appel 200), B (201) et C (202). Le renvoi d'appel sans réponse après le délai d'attente vers la boîte vocale du groupe de recherche a été configuré pour le groupe de recherche. Chaque membre a défini le renvoi d'appel sans réponse (CFNA) après le délai d'attente vers sa propre boîte vocale.		
Appel entrant pour le membre A (200)	Tous les membres sont libres.	Le membre A ne prend pas l'appel. Un renvoi temporisé vers la boîte vocale du membre A est effectué.
	Le membre A a défini le renvoi d'appel inconditionnel (CFU) vers sa propre boîte vocale. Les membres B et C sont libres.	L'appel est immédiatement transféré (CFU) vers la boîte vocale du membre A.
Appel entrant pour le groupe de recherche (404)	Tous les membres sont libres.	L'appel est signalé d'abord au membre A, puis au membre B et enfin au membre C. Aucun membre n'accepte l'appel. Le renvoi d'appel sans réponse après le délai se produit vers la boîte vocale du groupe de recherche.

	Le membre A a défini le renvoi d'appel inconditionnel (CFU) vers sa propre boîte vocale. Les membres B et C sont libres.	L'appel est signalé d'abord au membre B, puis au membre C. Aucun membre n'accepte l'appel. Le renvoi d'appel sans réponse après le délai se produit vers la boîte vocale du groupe de recherche.
	Le membre A a défini un renvoi d'appel inconditionnel (CFU) vers une destination externe. Les membres B et C sont libres.	L'appel est signalé d'abord au membre B, puis au membre C. Aucun membre n'accepte l'appel. Le renvoi d'appel sans réponse après le délai se produit vers la boîte vocale du groupe de recherche.
	Le membre A a défini les règles CFNA à l'aide de l'AutoAttendant. Les membres B et C sont libres.	L'appel est signalé d'abord au membre A, puis au membre B et enfin au membre C. Aucun membre n'accepte l'appel. Le renvoi d'appel sans réponse après le délai se produit vers la boîte vocale du groupe de recherche.

Activation/désactivation du groupe de recherche

Si un abonné est membre d'un groupe de recherche, il peut utiliser des codes pour quitter et rejoindre le groupe de recherche.

Si un abonné est membre de plusieurs groupes de recherche et de plusieurs appels collectifs, il peut utiliser des codes pour quitter et rejoindre tous les groupes de recherche et tous les appels collectifs. Les abonnés sont ajoutés ou retirés d'un groupe de recherche ou d'un appel collectif spécifique en entrant des codes, puis en faisant une sélection parmi les groupes de recherche et les appels collectifs affichés.

Il est aussi possible de programmer des touches de fonction avec fonction de commutation pour l’intégration et le retrait. Vous pouvez programmer ici une touche de fonction qui s'applique à un groupe spécifique ou à tous les groupes de recherche de personnes et aux appels de groupe. Une programmation variable est également possible. Après avoir appuyé sur une telle touche de fonction, vous devez sélectionner l'un des groupes de recherche et d'appels collectifs affichés pour définir le groupe de recherche ou l'appel collectif que vous souhaitez quitter ou rejoindre.

Type de sonnerie

Pour chaque groupe de recherche, un administrateur ayant le profil **Expert** peut définir la signalisation acoustique des appels externes entrants via le réglage du type de sonnerie. Vous disposez des possibilités suivantes :

- Sonnerie à deux tons (paramètre par défaut)
- Sonnerie à trois tons
- sonnerie courte-longue-courte

Sur les téléphones analogiques, seul le paramètre par défaut est possible. Les modifications n'ont pas d'influence.

Téléphones SIP

Les téléphones SIP peuvent être intégrés dans un groupe de recherche.

Conseil : Sur les téléphones SIP, il n'est pas possible de programmer des touches de fonction. Les messages d'affichage spécifiques d'un groupe de recherche ne sont pas pris en charge.

Correspondances

Rubrique	Correspondance
Renvoi d'appel	Si un membre du groupe de recherche active le renvoi d'appel pour tous les appels, tous les appels sont signalés sur le téléphone de destination.
Ne pas déranger	Si un membre d'un groupe de recherche active la fonction Ne pas déranger, les appels entrants destinés à son téléphone ne sont pas transmis. Cela s'applique aux appels destinés au groupe de recherche et au numéro de poste du membre.
File d'attente	Pour les groupes de recherche cycliques et linéaires, il n'est pas possible de créer une file d'attente.
Téléphones RNIS	Il n'est pas possible d'inclure des téléphones RNIS dans les groupes de recherche.

Tâches associées

Comment ajouter un groupe de recherche à la page 645
Comment modifier un groupe de recherche à la page 647
Comment effacer un groupe de recherche à la page 648
Comment ajouter ou effacer un membre dans un groupe de recherche à la page 648

14.1.4 Configuration des groupes d'interception d'appel, des groupes d'appel collectif et des groupements à l'aide des assistants

Différents assistants permettent la configuration aisée des groupes d'interception d'appel, des groupes d'appel collectif et des groupements.

A l'aide de l'assistant **Interception d'appel** vous pouvez regrouper des abonnés afin de permettre la réception mutuelle des appels reçus. Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide de l'Assistant :

- Configurer les groupes d'interception
- Comment ajouter ou supprimer des membres dans un groupe d'interception

L'Assistant **Appel de groupe/Groupe d'appel collectif** permet de configurer des appels collectifs de type Groupe et Groupe de recherche. Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide de l'Assistant :

- Comment ajouter un groupe d'appel collectif
- Comment modifier un groupe d'appel collectif (groupe)
- Comment effacer un groupe d'appel collectif
- Comment ajouter ou effacer un membre dans un groupe d'appel collectif
- Comment ajouter un groupe de recherche
- Comment modifier un groupe de recherche
- Comment effacer un groupe de recherche
- Comment ajouter ou effacer un membre dans un groupe de recherche

14.1.4.1 Configurer les groupes d'interception

L'Assistant **Interception d'appel** vous permet de regrouper des abonnés en un groupe avec la possibilité de prise réciproque des appels.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Interception**. La liste de tous les groupes d'interceptions possibles s'affiche.
4) Pour configurer un groupe d'interception, cliquez dans la ligne du groupe d'interception souhaité sur **Modifier**.
5) Si vous souhaitez ajouter des membres au groupe d'interception, cochez la case **Affectation Groupe <numéro>** du numéro/nom souhaité.
6) Si vous voulez supprimer des membres dans le groupe d'interception, décochez la case **Affectation Groupe <numéro>** du numéro/nom souhaité.
7) Cliquez sur **OK** pour valider les entrées.
8) Dans le champ **Nom** entrez le nom du nouveau groupe d'interception d'appel qui vient d'être configuré.
9) Si vous souhaitez configurer un autre groupe d'interception, répétez les étapes 4 à 8.
10) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Concepts associés

Groupe d'interception à la page 631

14.1.4.2 Comment ajouter ou supprimer des membres dans un groupe d'interception

Avec l'assistant **Interception d'appel**, vous pouvez ajouter ou supprimer des membres dans le groupe d'interception d'appel.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Interception**.
4) Dans la ligne du groupe d'interception souhaité, cliquez sur **Modifier**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter des membres au groupe d'interception, cochez la case **Affectation Groupe <numéro>** du numéro/nom souhaité.
   - Si vous voulez supprimer des membres dans le groupe d'interception, décochez la case **Affectation Groupe <numéro>** du numéro/nom souhaité.
6) Cliquez sur **OK** pour valider les entrées.
7) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Concepts associés

Groupe d'interception à la page 631

14.1.4.3 Comment ajouter un groupe d'appel collectif

L'Assistant **Appel de groupe/Groupe d'appel collectif** permet de configurer des appels collectifs de type Groupe et Groupe de recherche.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Appel de groupe/ Groupement de recherche de ligne**.
4) Cliquez sur **Ajouter** pour configurer un nouveau groupe d'appel collectif.
5) Dans le champ **Numéro d'abonné du groupe**, indiquez le numéro du nouveau groupe d'appel collectif.
6) Dans le champ **Numéro SDA**, indiquez le numéro SDA du nouveau groupe d'appel collectif.

   : Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

7) Dans le champ **Nom du groupe**, indiquez le nom du nouveau groupe d'appel collectif.
8) Dans la liste déroulante **Type**, sélectionnez l'entrée **Groupe**.

9) Sélectionnez une des possibilités suivantes pour intégrer dans le répertoire interne le numéro d'appel collectif.
   - Pour afficher les numéros des appels collectifs dans un répertoire interne, cochez la case **Annuaire**.
   - Pour ne pas afficher les numéros des appels collectifs dans le répertoire interne, décochez la case **Annuaire**.
10) Dans la liste déroulante **Numéro de l'abonné qui doit être affecté au groupe**, sélectionnez le numéro de l'abonné souhaité.
11) Cliquez sur **OK & Suivant**.

Conseil : Si le numéro de téléphone et/ou le numéro SDA que vous avez composé sont déjà présents, vous pouvez ouvrir le plan de numérotation actuel pour identifier un numéro de téléphone et/ou numéro SDA libre.

12) Cliquer dans la ligne du groupe d'appel collectif souhaité sur **Modifier** pour affecter au groupe des abonnés supplémentaires.
13) Dans la liste déroulante **Numéro**, sélectionnez le numéro de l'abonné qui doit être affecté au groupe d'appel collectif.
14) Cliquez sur **Ajouter**.
15) Si vous souhaitez ajouter d'autres abonnés au groupe d'appel collectif, répétez les étapes 13 et 14.
16) Cliquez sur **OK** pour valider les entrées.
17) Si vous souhaitez paramétrer un autre groupe d'appel collectif, répétez les étapes 4 à 16.
18) Cliquez sur **OK&Suivant** puis sur **Quitter**.

Concepts associés

Appel de groupe à la page 633

14.1.4.4 Comment modifier un groupe d'appel collectif (groupe)

A l'aide de l'Assistant **Appel de groupe/Groupement de recherche de ligne**, vous pouvez modifier les groupes d'appel collectif de type Groupe.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Appel de groupe/Groupe de recherche de ligne**.
4) Cliquez dans la ligne du groupe d'appel collectif à modifier sur **Modifier**.
5) Modifiez les paramètres de groupe souhaités.

6) Uniquement pour UC Smart : affectez si nécessaire une boîte vocale à l'appel de groupe :
   a) Uniquement pour UC Smart : sélectionnez dans la liste déroulante **Type de boîte de messagerie UC Smart** si l'appel de groupe doit recevoir une boîte de messagerie standard ou une boîte de messagerie de diffusion (AutoAttendant).
   b) Uniquement pour boîte de messagerie standard : si un appelant peut laisser un message sur la boîte vocale, activez la case **Enregistrement**.
   c) Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.
   d) Si le mot de passe de la boîte vocale doit être rétabli, cochez la case **Réinitialisation mot de passe**.

   Remarque : La case à cocher **Réinitialisation mot de passe** ne doit pas être sélectionnée lors de la reconfiguration d'une boîte vocale. Cela provoque la réinitialisation du mot de masse de la boîte vocale. Lors d'une nouvelle configuration, l'abonné doit de toute manière, lors du premier accès à sa boîte vocale, modifier le mot de passe initial.

   ---

7) Si vous souhaitez ajouter un membre à l'appel de groupe, dans la liste déroulante **[N° appel].**, sélectionnez le numéro du membre souhaité. Cliquez sur **Ajouter**.
8) Si vous souhaitez supprimer un membre dans l'appel collectif, cliquez dans la ligne du membre souhaité sur **Effacer** puis sur **OK**.
9) Cliquez sur **OK** pour valider les entrées.
10) Cliquez sur **OK&Suite** puis sur **Quitter**.

Concepts associés

Appel de groupe à la page 633

14.1.4.5 Comment effacer un groupe d'appel collectif

A l'aide de l'Assistant **Appel de groupe/Groupe d'appel collectif**, vous pouvez effacer les groupes d'appel collectif de type Groupe.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Appel de groupe/Groupe de recherche de ligne**.
4) Cliquez dans la ligne de l'appel collectif à effacer sur **Modifier**.
5) Cliquez sur **Effacer les données**.
6) Cliquez sur **OK** pour confirmer la suppression.

7) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Concepts associés

Appel de groupe à la page 633

14.1.4.6 Comment ajouter ou effacer un membre dans un groupe d'appel collectif

L'assistant **Appel de groupe/Groupe d'appel collectif** permet d'ajouter ou supprimer des membres au groupe d'appel.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Appel de groupe/Groupe de recherche de ligne**.
4) Dans la ligne de l'appel collectif souhaité, cliquez sur **Modifier**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter un membre à l'appel de groupe, dans la liste déroulante **[N° appel].**, sélectionnez le numéro du membre souhaité. Cliquez sur **Ajouter**.
   - Si vous souhaitez supprimer un membre dans l'appel collectif, cliquez dans la ligne du membre souhaité sur **Effacer** puis sur **OK**.
6) Cliquez sur **OK** pour valider les entrées.
7) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Concepts associés

Appel de groupe à la page 633

14.1.4.7 Comment ajouter un groupe de recherche

Avec l'assistant **Appel de groupe/Groupement de recherche de ligne**, vous pouvez configurer des groupements de recherche de ligne.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Appel de groupe/ Groupement de recherche de ligne**.
4) Cliquez sur **Ajouter** pour configurer un nouveau groupe de recherche.

5) Dans le champ **Numéro d'abonné du groupe**, indiquez le numéro du nouveau groupe de recherche.
6) Dans le champ **Numéro SDA**, indiquez le numéro SDA du nouveau groupe de recherche.

: Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

---

7) Dans le champ **Nom du groupe**, indiquez le nom du nouveau groupe de recherche.
8) Dans la liste déroulante **Type**, indiquez le type du nouveau groupe de recherche. Vous disposez des possibilités suivantes :
   - Lorsque l'appel doit toujours être signalé d'abord sur le premier membre du groupe de recherche, sélectionnez **Groupe de recherche linéaire**.
   - Lorsque l'appel doit être signalé d'abord au membre du groupe qui suit le membre ayant répondu au dernier appel, sélectionnez **Groupe de recherche cyclique**.
9) Sélectionnez une des possibilités suivantes : pour reprendre le numéro du groupe d'appel collectif dans le répertoire interne :
   - Pour afficher les numéros des groupes de recherche dans un répertoire interne, cochez la case **Annuaire**.
   - Si le numéro du groupe de recherche ne doit pas apparaître dans le répertoire interne, décochez la case **Annuaire**.
10) Dans la liste déroulante **Numéro de l'abonné qui doit être affecté au groupe**, sélectionnez le numéro de l'abonné souhaité.
11) Cliquez sur **OK & Suivant**.

Conseil : Si le numéro de téléphone et/ou le numéro SDA que vous avez composé sont déjà présents, vous pouvez ouvrir le plan de numérotation actuel pour identifier un numéro de téléphone et/ou numéro SDA libre.

---

12) Cliquer dans la ligne du nouveau groupe de recherche sur **Modifier** pour affecter au groupe de recherche des abonnés supplémentaires.
13) Dans la liste déroulante **Numéro**, sélectionnez le numéro de l'abonné qui doit être affecté au groupe de recherche.
14) Cliquez sur **Ajouter**.
15) Si vous souhaitez affecter d'autres membres au groupe de recherche, répétez les étapes 13 et 14.
16) Cliquez sur **OK** pour valider les entrées.
17) Si vous souhaitez paramétrer un autre groupe de recherche, répétez les étapes 4 à 16.
18) Cliquez sur **OK&Suivant** puis sur **Quitter**.

Concepts associés

Groupe de recherche à la page 637

14.1.4.8 Comment modifier un groupe de recherche

Avec l'assistant **Appel de groupe/Groupe d'appel collectif**, vous pouvez modifier les groupes d'appel collectif.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Appel de groupe/Groupe de recherche de ligne**.
4) Cliquez dans la ligne du groupe de recherche à modifier sur **Modifier**.
5) Modifiez les paramètres souhaités du groupe de recherche.
6) Uniquement pour UC Smart : affectez si nécessaire le groupe de recherche à une boîte vocale :
   a) Sélectionnez dans la liste déroulante **Type de boîte de messagerie UC Smart** si le groupe de recherche doit recevoir une boîte de messagerie standard ou une boîte de messagerie de diffusion (AutoAttendant).
   b) Uniquement pour boîte de messagerie standard : si un appelant peut laisser un message sur la boîte vocale, activez la case **Enregistrement**.
   c) Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.
   d) Si le mot de passe de la boîte vocale doit être rétabli, cochez la case **Réinitialisation mot de passe**.

   Remarque : La case à cocher **Réinitialisation mot de passe** ne doit pas être sélectionnée lors de la reconfiguration d'une boîte vocale. Cela provoque la réinitialisation du mot de masse de la boîte vocale. Lors d'une nouvelle configuration, l'abonné doit de toute manière, lors du premier accès à sa boîte vocale, modifier le mot de passe initial.
7) Si vous souhaitez ajouter un membre à un groupe de recherche, sélectionnez dans la liste déroulante **N° appel** le numéro du membre souhaité. Cliquez sur **Ajouter**.
8) Si vous souhaitez supprimer un membre dans l'appel collectif, cliquez dans la ligne du membre souhaité sur **Effacer** puis sur **OK**.
9) Si vous souhaitez modifier la position des membres à l'intérieur d'un groupe d'appel collectif, cliquez sur **Modifier l'ordre**. Dans le champ **Position** entrez pour chaque membre le numéro de position souhaité. Cliquez sur **OK&Suite**.
10) Cliquez sur **OK** pour valider les entrées.
11) Cliquez sur **OK&Suite** puis sur **Terminer**.

Concepts associés

Groupe de recherche à la page 637

14.1.4.9 Comment effacer un groupe de recherche

Avec l'assistant **Appel de groupe/Groupe d'appel collectif**, vous pouvez effacer les groupes d'appel collectifs.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Appel de groupe/Groupe de recherche de ligne**.
4) Cliquez dans la ligne du groupe de recherche à effacer sur **Modifier**.
5) Cliquez sur **Effacer les données**.
6) Cliquez sur **OK** pour confirmer la suppression.
7) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Concepts associés

Groupe de recherche à la page 637

14.1.4.10 Comment ajouter ou effacer un membre dans un groupe de recherche

Avec l'assistant **Appel de groupe/Groupe d'appel collectif**, vous pouvez ajouter ou supprimer des membres aux groupes d'appel collectifs.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Appel de groupe/Groupe de recherche de ligne**.
4) Dans la ligne du groupe de recherche souhaité, cliquez sur **Modifier**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter un membre à un groupe de recherche, sélectionnez dans la liste déroulante **N° appel** le numéro du membre souhaité. Cliquez sur **Ajouter**.
   - Si vous souhaitez supprimer un membre dans l'appel collectif, cliquez dans la ligne du membre souhaité sur **Effacer** puis sur **OK**.
6) Cliquez sur **OK** pour valider les entrées.
7) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Concepts associés

Groupe de recherche à la page 637

14.1.5 Configuration des groupes d'interception d'appel, des groupes d'appel collectif et des groupements à l'aide du mode Expert

En dehors des possibilités de configuration offertes par les assistants, l'administrateur de profil **Expert** dispose de possibilités supplémentaires de configuration en **Mode Expert**.

Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide du **Mode Expert** :

- Comment activer ou désactiver l'affichage du numéro et du nom de l'appelant
- Comment activer ou désactiver la tonalité d'avertissement
- Comment activer ou désactiver l'interception de retour d'appel
- Comment ajouter un groupe d'appel collectif (non-réponse ou avertissement)
- Comment afficher ou modifier l'appel collectif (non-réponse ou avertissement)
- Comment effacer l'appel collectif (non-réponse ou avertissement)
- Comment ajouter ou effacer un membre du groupe d'appel collectif (non-réponse ou avertissement)
- Comment activer ou désactiver le rejet des appels en instance pour les membres d'un groupe

14.1.5.1 Comment activer ou désactiver l'affichage du numéro et du nom de l'appelant

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si le numéro et le nom de l'appelant doivent être affichés, cochez la case **Numéro A dans groupes d'interception / Pilotage / Destination de renvoi/ Destination de renvoi temporaire**.
   - Si le numéro et le nom de l'appelant doivent être affichés, cochez la case **Numéro A dans groupes d'interception / Pilotage / Destination de renvoi/ Destination de renvoi temporaire**.
5) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe d'interception à la page 631

14.1.5.2 Comment activer ou désactiver la tonalité d'avertissement

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la tonalité d'avertissement, vous devez cocher la case **Tonalité d'avertissement pour groupes d'interception**.
   - Si vous souhaitez désactiver la tonalité d'avertissement, vous devez décocher la case **Tonalité d'avertissement pour groupes d'interception**.
5) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe d'interception à la page 631

14.1.5.3 Comment activer ou désactiver l'interception de retour d'appel

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous voulez que l'interception des retours d'appel soit possible, cochez la case **Interception après retour d'appel**.
   - Si vous ne voulez pas que l'interception des retours d'appel soit possible, décochez la case **Interception après retour d'appel**.
5) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe d'interception à la page 631

14.1.5.4 Comment ajouter un groupe d'appel collectif (non-réponse ou avertissement)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Cliquez sur **Appels entrants** > **Groupes/Groupement** dans l'arborescence du menu.
4) Cliquez sur l'onglet **Ajouter un groupe**.
5) Dans le champ **Numéro**, indiquez le numéro du nouveau groupe d'appel collectif.
6) Dans le champ **Numéro SDA**, indiquez le numéro SDA du nouveau groupe d'appel collectif.

   : Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

7) Dans le champ **Nom**, indiquez le nom du nouveau groupe d'appel collectif.
8) Dans la liste déroulante **Type**, sélectionner l'une des possibilités suivantes :
   - Si vous souhaitez paramétrer un groupe d'appel collectif de type Non-réponse, sélectionnez **Non-réponse**.
   - Si vous souhaitez paramétrer un groupe d'appel collectif de type Avertissement, sélectionnez l'entrée **Avertissement**.
9) Dans la liste déroulante **Numéro**, sélectionnez le numéro de l'abonné qui doit être affecté au groupe d'appel collectif.
10) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Appel de groupe à la page 633

14.1.5.5 Comment afficher ou modifier l'appel collectif (non-réponse ou avertissement)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le groupe d'appel collectif souhaité.
4) Cliquez sur l'onglet **Modifier les paramètres du groupe**. Les réglages actuels des paramètres du groupe sont affichés.
5) Si nécessaire, modifiez les paramètres souhaités de l'appel collectif.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Appel de groupe à la page 633

14.1.5.6 Comment effacer l'appel collectif (non-réponse ou avertissement)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le groupe d'appel collectif souhaité.
4) Cliquez sur l'onglet **Effacer le groupe**.
5) Cliquez sur **Effacer** et ensuite sur **OK**.

Concepts associés

Appel de groupe à la page 633

14.1.5.7 Comment ajouter ou effacer un membre du groupe d'appel collectif (non-réponse ou avertissement)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Sélectionnez une des possibilités suivantes :
   - Si vous voulez ajouter un membre au groupe d'appel collectif, naviguez dans l'arborescence menu, sous **Appels entrants** > **Groupes/Groupes de recherche** > **…** vers le groupe d'appel collectif souhaité. Cliquez l'onglet **Ajouter un membre**. Dans la liste déroulante **Numéro**, sélectionnez le numéro de l'abonné souhaité. Cliquez sur **Appliquer** puis sur **OK**.
   - Si vous souhaitez supprimer un membre dans le groupe d'appel collectif, naviguez dans l'arborescence menu sous **Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le membre souhaité du groupe d'appel collectif ((Membre du groupe) Numéro, Nom). Cliquez sur l'onglet **Effacer un membre**. Cliquez sur **Effacer** et ensuite sur **OK**.

Concepts associés

Appel de groupe à la page 633

14.1.5.8 Comment activer ou désactiver le rejet des appels en instance pour les membres d'un groupe

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence menu, naviguez sous **Abonnés** > **Abonné** > **…** pour accéder à l'abonné souhaité (Index - Numéro - Nom).
4) Cliquez sur l'onglet **Modifier les flags abonné**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la protection, cochez la case **Protégé intrusions**.
   - Si vous souhaitez désactiver le rejet des appels en instance, décochez la case **Protégé intrusions**.

   Remarque : Lorsqu'un groupe est configuré en tant que groupe de standard, tous ses membres existants sont automatiquement configurés avec le "Drapeau de rejet d'appel en attente" réglé sur faux. Cela s'applique également à tous les nouveaux membres du groupe Standard. L'utilisateur peut configurer manuellement "rejet d'appel en attente" sur vrai pour n'importe quel membre du groupe Standard de manière à activer la tonalité d'occupation pour ce membre, mais ce n'est pas le comportement par défaut.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Appel de groupe à la page 633

14.2 Configuration Team / groupe Team et Groupe chef/secrétaire / groupe Top

Une configuration Team / un groupe Team offre des fonctions d'équipe conviviales. Les numéros de téléphone de tous les membres d'une équipe (Team) ont été programmés sur les touches MULAP (touches de ligne). Ainsi, chaque membre d'une équipe (Team) a accès à toutes les lignes (par ex. pour interception d'appel) et il peut téléphoner simultanément sur plusieurs lignes. Un groupe Chef/Secrétaire / Top offre des fonctions Chef/Secrétaire conviviales (fonction Top) pour jusqu'à trois chefs et jusqu'à trois secrétaires.

Remarque : Lors de la création d'un MULAP à partir des options Team / Top dans WBM / Manager E, il n'est pas permis d'entrer un nombre commençant par ** ou ***.

14.2.1 La configuration Team / le groupe Team

Sur un téléphone avec fonctions Team, le numéro propre et les numéros des autres membres de l'équipe sont programmés sur des touches MULAP (Multiple Line Appearance) (touches de ligne). Chaque membre de l'équipe a accès à toutes les lignes (par ex. pour l'interception d'appel) et peut aussi simultanément téléphoner par plusieurs lignes. En outre, les touches DSS avec lesquelles les membres de l'équipe peuvent s'appeler directement sont programmées automatiquement.

Grâce aux touches MULAP, les membres Team ont accès aux numéros de tous les membres.Un appel destiné à un membre de l'équipe peut par conséquent également être pris par tous les autres membres par pression sur la touche MULAP qui clignote.Le va-et-vient entre plusieurs lignes est également possible.Il suffit à un membre de l'équipe d'appuyer sur une touche MULAP pour émettre un appel sortant par la ligne correspondante. Le numéro correspondant à cette ligne apparaît sur l'écran pour l'appelé.

Les appels entrants sont signalés visuellement et simultanément sur tous les téléphones des membres de l'équipe par la DEL de la touche MULAP. Pour chaque membre Team, il est possible d'indiquer également si les appels entrants doivent être également signalés de façon acoustique.

Une touche d'appel collectif permet à chaque membre Team d'activer ou désactiver la signalisation des appels entrants pour chacune des lignes.

Un administrateur avec le profil **Advanced** peut configurer jusqu'à trois abonnés par configuration Team/groupe Team via l'assistant **Configuration Team**. Un administrateur avec le profil **Expert** peut configurer jusqu'à dix abonnés par configuration Team/groupe Team par le biais du **mode Expert**.

Un seul abonné peut faire partie de plusieurs groupes. Pour les groupes de type Appel de groupe, Groupe de recherche, Configuration Team / Groupe Team et Groupe Chef/Secrétaire / Groupe Top : La somme de tous les membres de ces groupes ne doit pas dépasser 32.

Il est possible d'affecter à chaque configuration/groupe Team un nom de 16 caractères maximum.

Lors de la définition d'une configuration Team ou d'un groupe Team, les caractéristiques suivantes sont affectées aux membres (ces paramètres peuvent être modifiés par un administrateur avec le profil **Expert** via le **mode Expert**) :

- **Maître**

  Ce paramètre transforme un membre en maître de la configuration Team / du groupe Team. Si un maître active un renvoi d'appel, celui-ci s'applique à tous les membres (téléphones) de la configuration Team / du groupe Team.

  Paramètre par défaut : le maître est le premier membre de la configuration Team / du groupe Team.
- **Sonnerie acoustique**

  Si ce paramètre est activé, les appels entrants sont signalés de manière acoustique.

  Paramètre par défaut : le paramètre est activé.
- **Prise automatique sortante**

  Si ce paramètre est activé, lorsque le combiné est décroché, l'appel a lieu automatiquement par la ligne MULAP de ce membre. Si le paramètre n'est

pas activé, l'abonné doit appuyer sur la touche MULAP avant de pouvoir numéroter.

Paramètre par défaut : le paramètre est activé.

- **Pas de prise d'appel automatique entrante**

  Si ce paramètre est activé, il n'est pas possible de prendre l'appel entrant en décrochant le combiné. Pour accepter l'appel entrant, il faut appuyer sur la touche MULAP.

  Paramètre par défaut : le paramètre n'est pas activé.

- **Autorisation conférence automatique**

  Lorsque ce paramètre est activé, une pression sur la touche MULAP valide la ligne MULAP pour la conférence. Chez tous les autres participants, la validation est signalée par le clignotement de la touche MULAP. Pour rejoindre la conférence, les participants appuient sur la touche MULAP.

  Paramètre par défaut : le paramètre n'est pas activé.

- **Touche MULAP configurée**

  Lorsque ce paramètre est activé, une touche MULAP est configurée sur le téléphone correspondant. Appuyez sur la touche pour configurer un appel sortant via la ligne MULAP du maître. Le numéro du poste MULAP du maître s’affiche sur l’écran de la personne appelée.

  Paramètre par défaut : le paramètre n'est pas activé.

Utilisation des touches MULAP

Une ligne propre (ligne MULAP) est affectée à chaque membre Team. La ligne propre et les lignes de tous les autres membres sont configurées chez chaque membre Team comme touches MULAP (touches de ligne). Ainsi, chaque membre Team peut utiliser toutes les lignes MULAP existantes.

La LED d'une touche MULAP (touche de ligne) a la signification suivante :

- Désactivée : la ligne correspondante est libre et peut être utilisée.
- Allumée : la ligne correspondante est occupée.
- Clignote rapidement : appel sur la ligne correspondante.
- Clignote lentement : une communication mise en garde attend sur la ligne correspondante.

Utilisation des touches DSS

Chaque membre de l'équipe dispose d'une touche DSS pour chaque autre membre de l'équipe. Ainsi, les membres Team peuvent se joindre l'un l'autre directement par pression sur une touche.

Une touche de sélection directe du poste (DSS) peut également être utilisée pour transférer rapidement un appel existant au membre de l'équipe programmé sur cette touche.

La DEL d'une touche DSS peut avoir différents états avec les significations suivantes :

- Désactivée : le membre d'équipe correspondant ne téléphone pas.
- Allumée : le membre d'équipe correspondant téléphone ou a activé Ne pas déranger.
- Clignote rapidement : le membre d'équipe correspondant appelle. L'appel peut être accepté en appuyant sur la touche de sélection directe du poste (DSS).

- Clignote lentement : le membre Team correspondant est appelé et n'a pas encore pris l'appel. L'appel peut être accepté en appuyant sur la touche de sélection directe du poste (DSS).

Type de sonnerie

Pour chaque configuration Team ou groupe Team, un administrateur avec le profil **Expert** peut définir la signalisation acoustique des appels entrants externes en réglant le type de sonnerie.Vous disposez des possibilités suivantes :

- Sonnerie à deux tons (paramètre par défaut)
- Sonnerie à trois tons
- sonnerie courte-longue-courte

Sur les téléphones analogiques, seul le paramètre par défaut est possible. Les modifications n'ont pas d'influence.

Boîte Fax pour configuration Team / groupe Team

Pour chaque configuration Team / groupe Team il est possible de définir une boîte Fax permettant à chaque membre de recevoir des messages Fax directement via myPortal for Desktop ou myPortal for Outlook.

Si une boîte fax a déjà été configurée pour le maître (le premier membre) de la configuration Team / du groupe Team, cette boîte fax est reprise lors du paramétrage de la configuration Team / du groupe Team. Les boîtes Fax déjà configurées des autres membres sont effacées.

Après résolution de la configuration Team / du groupe Team, seul l'ancien maître (le premier membre) peut utiliser la boîte fax.

Commande de dispositifs membres du Mulap

Les téléphones SIP peuvent être intégrés dans un MULAP de base, à condition qu'un dispositif TDM/HFA ait été défini comme premier membre du MULAP de base. Les téléphones IP peuvent être intégrés dans un MULAP de base, à condition qu'un dispositif TDM/HFA ait été défini comme premier membre du MULAP de base.

Il est possible d'intégrer par exemple des téléphones mobiles dual mode, configurés comme abonnés Mobility Entry. Les téléphones mobiles bimodes prennent en charge à la fois les réseaux GSM/ UMTS et les réseaux WLAN. Via WLAN, il est possible d'enregistrer un téléphone mobile dual mode comme abonné IP (client SIP) sur le système de communication.

Les utilisateurs mobiles, y compris les utilisateurs mobiles GSM, les clients Unify Phone et Microsoft Teams, peuvent être intégrés dans un MULAP de base, à condition qu'un dispositif TDM/HFA ait été défini comme premier membre du MULAP de base.

Remarque : La description étendue ci-dessus s'applique aux systèmes OpenScape Business X et OpenScape Business S, mais se limite à Team et Basic Mulap, et non aux sous-chapitres avec des déclarations similaires comme Executive/Secretary / Top Group.

Conseil : Aucune programmation de touches MULAP n'est possible pour les téléphones SIP. De plus, aucune fonctionnalité ne peut être activée ou désactivée à l'aide d'indicatifs. Les messages d'affichage spécifiques du MULAP de base ne sont pas pris en charge.

Remarque : Les téléphones haut de gamme, tels que les CP 400/600/600E/700/700X/710, conservent leurs propres entrées de journal et peuvent présenter davantage d'informations. Mais pour les configurations de groupe, ils utilisent les données du système car les groupes sont configurés au niveau du système et non des téléphones. Il est donc possible que les informations sur les groupes ne s'affichent pas dans les entrées de journal car elles doivent se conformer aux limitations et à la configuration du système.

Correspondances

Rubrique	Correspondance
Renvoi d'appel	Un membre Team a activé un renvoi pour tous les appels. Dans ce cas, tous les appels sont renvoyés pour son propre numéro d'abonné.
Ne pas déranger	Si un membre Team active la fonction Ne pas déranger, les appels entrants ne sont pas remis. **Remarque :** Une équipe entière n'est occupée que si tous les membres de l'équipe ont activé la fonction Ne pas déranger.
Téléphones RNIS	L'intégration de téléphones RNIS dans les configurations/groupes Team est impossible.
Groupe/Groupe de recherche	Il est impossible d'ajouter un maître MULAP de base/chef dans les configurations ou groupes Team.

Concepts associés

Appel direct à la page 585

Tâches associées

Comment ajouter une configuration Team / un groupe Team à la page 662
Comment modifier la configuration Team / le groupe Team à la page 663
Comment effacer la configuration Team / le groupe Team à la page 664
Comment ajouter ou effacer un membre à la configuration Team / au groupe Team à la page 668
Comment modifier un membre d'une configuration Team / d'un groupe Team à la page 669
Comment modifier les propriétés des membres d'une configuration Team / d'un groupe Team à la page 669
Comment modifier la programmation des touches du téléphone pour la configuration Team/le groupe Team à la page 670

Comment ajouter une boîte Fax à une configuration Team / un groupe Team à la page 670

14.2.2 Groupe chef/secrétaire / groupe Top

Les groupes Top peuvent être configurés si des fonctions chef et secrétaire (fonction Top) conviviales sont nécessaires.

Des fonctions chef-secrétaire peuvent être configurées pour groupes de jusqu'à trois chefs et jusqu'à trois secrétaires.

Conseil : Les formulations "le chef" et "la secrétaire" s'appliquent aussi aux groupes de plus d'un chef et plus d'un secrétaire. Dans ce texte, "le chef" correspond à un chef homme ou femme et "la secrétaire" correspond à un secrétaire, homme ou femme.

Il est affecté à membre Top (chaque chef et chaque secrétaire) une ligne propre, la ligne MULAP (Multiple Line Appearance). La ligne propre et les lignes MULAP de tous les autres membres sont configurées chez chaque membre Top comme touches MULAP (touches de ligne). Pour les appels entrants par la ligne MULAP, le numéro MULAP apparaît sur l'écran des appelés. La secrétaire peut passer les appels sortants par sa propre ligne ou par la ligne MULAP de tous les chefs et autres secrétaires. Si, par exemple, une communication doit être établie pour un chef, il est possible d'utiliser pour cela la ligne MULAP de ce chef.

De plus, des touches d'appels direct sont programmées par lesquelles le chef peut appeler directement le secrétaire et inversement.

Les appels entrants sont signalés simultanément chez tous les membres Top de façon optique, par le voyant de la touche de ligne. Pour chaque membre Top, il est possible d'indiquer également si les appels entrants doivent être également signalés de façon acoustique. Dans ce cas, la signalisation acoustique se fait en fonction de la touche de déviation d'appel.

Grâce à la touche de déviation d'appel, la signalisation des appels entrants peut être commutée. Les appels entrants sont signalés soit chez le chef, soit au secrétaire. Si le chef appuie sur la touche de déviation d'appel, les appels qui arrivent continuent à lui être affichés par des fenêtres surgissantes. La prise d'un appel ne peut se faire que par une touche correspondante sur le téléphone et pas par la fenêtre surgissante.

Les téléphones secrétaire peuvent quitter et rejoindre le groupe Chef/Secrétaire à l'aide d'une touche d'appel collectif. Dans ce cas, la déviation d'appel est prioritaire.

Conseil : Si la secrétaire se retire de la configuration Chef/Secrétaire / du groupe Top avec la touche Appel collectif, sans activer le renvoi d'appel pour le chef, les appels entrants ne sont signalés ni au chef, ni à la secrétaire.

Un administrateur avec le profil **Advanced** peut définir jusqu'à deux chefs et jusqu'à deux secrétaires par configuration Chef/Secrétaire / groupe Top

via l'assistant via l'assistant **Chef / Secrétaire**. Un administrateur avec le profil **Expert** peut définir jusqu'à trois chefs et jusqu'à trois secrétaires par configuration Chef/Secrétaire / groupe Top via le **mode Expert**.

Pour chaque chef, il est possible de configurer au maximum trois téléphones et pour chaque secrétaire, au maximum deux téléphones.

Un seul abonné peut faire partie de plusieurs groupes. Pour les groupes de type Appel de groupe, Groupe de recherche, Configuration Team/Groupe Team et Chef/Secrétaire/Groupe Top, la règle suivante s'applique : le total des participation à ces groupes des abonnés ne doit pas dépasser 32.

Il est possible d'affecter à chaque configuration Chef/Secrétaire / groupe Top un nom de 16 caractères maximum.

Lors de la définition d'une configuration Chef/Secrétaire / d'un groupe Top, les caractéristiques suivantes sont affectées aux membres (les modifications des réglages peuvent être effectuées par un administrateur avec le profil **Expert** via le **mode Expert**.) :

- **Maître**

  Ce paramètre sert à donner à un membre des fonctions de chef. Lorsque le combiné est décroché, il y a automatiquement appel par la ligne MULAP de ce membre. Les appels entrants par le numéro MULAP chef correspondant sont par défaut signalés exclusivement de façon optique.

  Paramètre par défaut : les fonctions Chef sont affectées à tous les chefs de la configuration Chef/Secrétaire / du groupe Top.
- **Sonnerie acoustique**

  Si ce paramètre est activé, les appels entrants sont signalés de manière acoustique.

  Paramètre par défaut : le paramètres est activé pour tous les membres avec fonction secrétaire.
- **Prise automatique sortante**

  Si ce paramètre est activé, lorsque le combiné est décroché, l'appel a lieu automatiquement par la ligne MULAP de ce membre. Si le paramètre n'est pas activé, l'abonné doit appuyer sur la touche MULAP avant de pouvoir numéroter.

  Paramètre par défaut : le paramètre est activé pour tous les membres.
- **Pas de prise d'appel automatique entrante**

  Si ce paramètre est activé, il n'est pas possible de prendre l'appel entrant en décrochant le combiné. Pour accepter l'appel entrant, il faut appuyer sur la touche MULAP.

  Paramètre par défaut : le paramètre n'est pas activé.
- **Autorisation conférence automatique**

  Lorsque ce paramètre est activé, une pression sur la touche MULAP valide la ligne MULAP pour la conférence. Chez tous les autres participants, la validation est signalée par le clignotement de la touche MULAP. Pour entrer dans la conférence, appuyez sur la touche MULAP.

  Paramètre par défaut : le paramètre n'est pas activé.
- **Touche MULAP configurée**

  Lorsque ce paramètre est activé, une touche MULAP est configurée sur le téléphone correspondant. L'appui sur la touche provoque une prise sortante

par la ligne MULAP chef. Le numéro MULAP chef apparaît sur l'écran de l'appelé.

Paramètre par défaut : le paramètre est activé.

Utiliser les touches MULAP

Une ligne propre (ligne MULAP) est affectée à chaque membre Top. La ligne propre et les lignes de tous les autres membres sont configurées chez chaque membre Top comme touches MULAP (touches de ligne). Ainsi, chaque membre Top peut utiliser toutes les lignes MULAP existantes.

La LED d'une touche MULAP (touche de ligne) a la signification suivante :

- Désactivée : la ligne correspondante est libre et peut être utilisée.
- Allumée : la ligne correspondante est occupée.
- Clignote rapidement : appel sur la ligne correspondante.
- Clignote lentement : une communication en garde attend sur la ligne correspondante ou la ligne correspondante a été validée pour une conférence.

Utiliser les touches d'appel direct

Chaque membre Top a une touche d'appel direct pour chaque autre membre Top. Ainsi, les membres Top peuvent se joindre l'un l'autre directement par pression sur une touche.

La touche d'appel direct peut aussi être utilisée pour transférer rapidement une communication en cours au membre Top programmé sur la touche.

La LED d'une touche d'appel direct a la signification suivante :

- Désactivée : le membre Top correspondant ne téléphone pas.
- Allumée : le membre Top correspondant téléphone ou a activé Ne pas déranger.
- Clignote rapidement : le membre Top correspondant appelle. Pour prendre l'appel, il suffit alors d'appuyer sur la touche d'appel direct.
- Clignote lentement : le membre Top correspondant est appelé et n'a pas encore pris l'appel. Pour prendre l'appel, il suffit alors d'appuyer sur la touche d'appel direct.

Type son.

Pour chaque configuration Chef/Secrétaire / chaque groupe Top, un administrateur avec le profil **Expert** peut définir la signalisation acoutisque des appels externes entrants via le réglage du type de sonnerie. Vous disposez des possibilités suivantes :

- Sonnerie à deux tons (paramètre par défaut)
- Sonnerie à trois tons
- Sonnerie courte/longue/courte

Sur les téléphones analogiques, seul le paramètre par défaut est possible. Les modifications n'ont pas d'influence.

Boîtes Fax pour configuration Chef/Secrétaire / groupe Top

Pour chaque membre d'une configuration Chef/Secrétaire / d'un groupe Top, il est possible de configurer une boîte Fax permettant au membre de recevoir les messages Fax directement via myPortal for Desktop ou myPortal for Outlook.

Si pour le premier chef de la configuration Chef/Secrétaire / du groupe Top une boîte Fax a déjà été configurée, cette boîte Fax est reprise lors du paramétrage de la configuration Chef/Secrétaire / du groupe Top. Les boîtes Fax déjà configurées des autres membres sont effacées.

Après résolution d'une configuration Chef/Secrétaire / d'un groupe Top, seule l'ancien premier chef peut utiliser sa boîte Fax.

Téléphones SIP

Il est possible d'intégrer des téléphones SIP dans une configuration Chef/Secrétaire / groupe Top. Condition : le premier membre (chef 1) de la configuration Chef/Secrétaire / du groupe Top doit avoir été défini comme téléphone système (par exemple téléphone IP, HFA ou SIP).

Il est possible d'intégrer par exemple des téléphones mobiles dual mode, configurés comme abonnés Mobility Entry. Les téléphones mobiles dual mode supporte les réseaux GSM/UMTS et les réseaux WLAN. Via WLAN, il est possible d'enregistrer un téléphone mobile dual mode comme abonné IP (client SIP) sur le système de communication.

Conseil : Sur les téléphones SIP, il et impossible de programmer des touches MULAP et des touches d'appel direct. De plus, aucune fonctionnalité ne peut être activée ou désactivée à l'aide d'indicatifs. Les messages d'affichage spécifiques de la configuration Chef/Secrétaire/du groupe Top ne sont pas supportés.

Correspondances

Sujet	Correspondance
Renvoi d'appel	Un membre Top a activé un renvoi pour tous les appels. Dans ce cas, tous les appels sont renvoyés pour son propre numéro d'abonné.
Ne pas déranger	Si un membre Top active la fonction Ne pas déranger, les appels entrants ne sont pas remis.
Téléphones RNIS	L'intégration de téléphones RNIS dans les configurations Chef/Secrétaire / groupes Top est impossible.
Groupes/Groupe de recherche	Il n'est pas possible d'inclure un MULAP maître Basique/Chef dans les configurations Chef/Secrétaire ou groupes Top.

Concepts associés

Appel direct à la page 585

Tâches associées

Comment ajouter le groupe Chef/Secrétaire / groupe Top à la page 665
Comment modifier le groupe Chef/Secrétaire / groupe Top à la page 666
Comment effacer un groupe Chef/Secrétaire / Top à la page 667
Comment ajouter ou effacer un membre au groupe Chef/Secrétaire / groupe Top à la page 671
Comment modifier un membre d'un groupe Chef/Secrétaire / groupe Top à la page 671

Comment modifier les caractéristiques des membres d'un groupe Chef/Secrétaire / groupe Top à la page 672
Comment ajouter une boîte Fax à un groupe Chef/Secrétaire / un groupe Top à la page 672

14.2.3 Configuration des équipes (Team) / groupes Team et fonctions Chef/Secrétaire / groupes Top à l'aide des assistants

Différents assistants permettent la configuration confortable des équipes (Team) (groupes Team) et des fonctions Chef/Secrétaire (fonction Top).

Avec l'Assistant **Configuration Team**, vous pouvez définir des configurations Team (groupes Team). Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide de l'Assistant :

- Comment ajouter une configuration Team / un groupe Team
- Comment modifier la configuration Team / le groupe Team
- Comment effacer la configuration Team / le groupe Team

L'Assistant **Chef / Secrétaire** permet de configurer des fonctions Chef et Secrétaire conviviales (fonction Top). Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide de l'Assistant :

- Comment ajouter le groupe Chef/Secrétaire / groupe Top
- Comment modifier le groupe Chef/Secrétaire / groupe Top
- Comment effacer un groupe Chef/Secrétaire / Top

Concepts associés

Configuration de l'entrée de mobilité à la page 894

14.2.3.1 Comment ajouter une configuration Team / un groupe Team

Avec l'Assistant **Configuration Team**, vous pouvez définir des configurations Team (groupes Team).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Configuration Team**.
4) Cliquez sur **Ajouter** pour configurer une nouvelle configuration Team.
5) Dans la liste déroulante **Premier téléphone**, sélectionnez le numéro du premier téléphone de la nouvelle configuration Team.
6) Cliquez sur **OK & Suivant**.
7) Dans **Nom**, entrez le nom de la configuration Team lorsqu'aucun nom n'est affiché ou lorsqu'une modification du nom affiché est nécessaire.

   Remarque : Le **nom** est déjà occupé par le nom du premier téléphone de la configuration Team si un nom a été attribué à ce téléphone.

8) Dans le champ **Numéro interne**, entrez le numéro interne de la nouvelle configuration Team, si une modification du numéro affiché est nécessaire.

   Le **numéro interne** est déjà occupé par le numéro interne du premier téléphone de la configuration Team.

   : Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

9) Entrer dans le champ **Numéro SDA** le numéro SDA de la nouvelle configuration Team s'il est nécessaire de modifier le numéro SDA affiché.

   Remarque : Le champ **numéro SDA** est déjà occupé par le numéro SDA du premier téléphone de la configuration Team.

10) Dans **Fax** dans le champ **Numéro interne**, entrez le numéro interne de la boîte Fax pour la nouvelle configuration Team, si aucun numéro n'est affiché ou si une modification du numéro affiché est nécessaire.

    Le champ **Numéro interne** est déjà occupé par le numéro interne de la boîte Fax du premier téléphone de la configuration Team, à condition toutefois qu'une boîte Fax ait été configurée pour ce téléphone.

11) Dans **Fax** dans le champ **Numéro SDA**, entrez le numéro SDA de la boîte Fax pour la nouvelle configuration Team, si aucun numéro SDA n'est affiché ou si une modification du numéro SDA affiché est nécessaire.

    Le champ **Numéro SDA** est déjà occupé par le n° SDA de la boîte Fax du premier téléphone de la configuration Team, à condition toutefois qu'une boîte Fax ait été configurée pour ce téléphone.

12) Activez l'indicateur **Team en tant que membre du groupe**.

    L'indicateur **Team en tant que membre du groupe** peut être configuré uniquement lorsque des membres du groupe Team possèdent le même type de poste, ce qui crée un seul groupe MULAP. Lorsque cet indicateur est activé, le groupe MULAP peut être ajouté en tant que membre dans les groupes.

13) Sélectionnez dans la liste déroulante **Deuxième téléphone** le numéro du deuxième téléphone de la nouvelle configuration Team.

14) Sélectionnez dans la liste déroulante **Troisième téléphone** le numéro du troisième téléphone de la nouvelle configuration Team.

15) Cliquez sur **OK & Suivant**.

16) Si vous souhaitez paramétrer une autre configuration Team, répétez les étapes 4 à 15 .

17) Cliquez sur **OK&Suivant** puis sur **Quitter**.

Concepts associés

La configuration Team / le groupe Team à la page 654

14.2.3.2 Comment modifier la configuration Team / le groupe Team

Avec l'Assistant **Configuration Team**, vous pouvez définir des configurations Team (groupes Team).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Configuration Team**.
4) Cliquez dans la ligne de la configuration Team à modifier sur **Modifier**.
5) Modifiez les paramètres souhaités.
6) Uniquement pour UC Smart : si nécessaire, affectez une boîte vocale à la configuration team :
   a) Sélectionnez dans la liste déroulante **Type de boîte de messagerie UC Smart** si la configuration Team doit recevoir une boîte de messagerie standard ou une boîte de messagerie de diffusion (AutoAttendant).
   b) Uniquement pour boîte de messagerie standard : si un appelant peut laisser un message sur la boîte vocale, activez la case **Enregistrement**.
   c) Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.
   d) Si le mot de passe de la boîte vocale doit être rétabli, cochez la case **Réinitialisation mot de passe**.

   Remarque : La case à cocher **Réinitialisation mot de passe** ne doit pas être sélectionnée lors de la reconfiguration d'une boîte vocale. Cela provoque la réinitialisation du mot de masse de la boîte vocale. Lors d'une nouvelle configuration, l'abonné doit de toute manière, lors du premier accès à sa boîte vocale, modifier le mot de passe initial.
7) Cliquez sur **OK&Suivant**.
8) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Concepts associés

La configuration Team / le groupe Team à la page 654

14.2.3.3 Comment effacer la configuration Team / le groupe Team

Avec l'Assistant **Configuration Team**, vous pouvez effacer des configurations Team (groupes Team).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Configuration Team**.
4) Cliquez dans la ligne de la configuration Team à effacer sur **Modifier**.
5) Cliquez sur **Effacer les données**.
6) Cliquez sur **OK** pour confirmer la suppression.

7) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Remarque : Dans les applications utilisant l'interface CSTA (UC, OSCC, etc.) : Lorsqu'un groupe Team ou un membre d'un groupe Team est supprimé, un redémarrage du système est nécessaire.

Concepts associés

La configuration Team / le groupe Team à la page 654

14.2.3.4 Comment ajouter le groupe Chef/Secrétaire / groupe Top

L'Assistant **Chef / Secrétaire** permet de configurer des fonctions de chef et de secrétaire conviviales (fonction Top).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Chef / Secrétaire**.
4) Cliquez sur **Ajouter** pour configurer une nouvelle configuration Chef/ Secrétaire (groupe Top).
5) Dans le champ **Nom**, entrez le nom de la nouvelle configuration Chef/ Secrétaire.
6) Dans la liste déroulante correspondante, sélectionnez les numéros de téléphone souhaités de la nouvelle configuration Chef/Secrétaire.
7) Cliquez sur **OK & Suivant**.
8) Dans Fax dans le champ **Numéro**, entrez le numéro interne de la boîte **Fax** pour la nouvelle configuration Chef/Secrétaire, si aucun numéro n'est affiché ou si une modification du numéro affiché est nécessaire.

   Le champ **Numéro** est déjà occupé par le numéro interne de la boîte Fax du premier chef de la configuration Chef/Secrétaire, à condition toutefois qu'une boîte Fax ait été configurée pour ce téléphone.
9) Dans **Fax** dans le champ **N° SDA**, entrez le numéro SDA de la boîte Fax pour la nouvelle configuration Chef/Secrétaire, si aucun numéro SDA n'est affiché ou si une modification du numéro SDA affiché est nécessaire.

   Le champ **N° SDA** est déjà occupé par le n° SDA de la boîte Fax du premier chef de la configuration Chef/Secrétaire, à condition toutefois qu'une boîte Fax ait été configurée pour ce téléphone.

: Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

10) Sélectionnez une valeur par défaut pour la programmation des touches :
    - Si vous voulez paramétrer les touches des fonctions Chef/Secrétaire sur le premier ou le deuxième satellite, cochez la case sur la **1re/2e console**.
    - Si vous voulez paramétrer les touches des fonctions Chef/Secrétaire sur les premières touches de fonction libres du téléphone, cochez la case sur les **1res touches libres**.
11) Cliquez sur **OK & Suivant**.
12) Si vous souhaitez configurer une autre configuration Chef/Secrétaire, répéter les étapes 4 à 11.
13) Cliquez sur **OK&Suivant** puis sur **Quitter**.

Concepts associés

Groupe chef/secrétaire / groupe Top à la page 658

14.2.3.5 Comment modifier le groupe Chef/Secrétaire / groupe Top

L'Assistant **Chef / Secrétaire** permet d'éditer des fonctions Chef et Secrétaire conviviales (fonction Top).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Chef / Secrétaire**.
4) Dans la ligne de la configuration Chef/Secrétaire à modifier cliquez sur **Modifier**.
5) Modifiez les paramètres souhaités.
6) Uniquement pour UC Smart : attribuez si nécessaire une boîte vocale au groupe Top :
    a) Sélectionnez dans la liste déroulante **Type de boîte de messagerie UC Smart** si le groupe Top doit recevoir une boîte de messagerie standard ou une boîte de messagerie de diffusion (AutoAttendant).
    b) Uniquement pour boîte de messagerie standard : si un appelant peut laisser un message sur la boîte vocale, activez la case **Enregistrement**.
    c) Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.
    d) Si le mot de passe de la boîte vocale doit être rétabli, cochez la case **Réinitialisation mot de passe**.

Remarque : La case à cocher **Réinitialisation mot de passe** ne doit pas être sélectionnée lors de la reconfiguration d'une boîte vocale. Cela provoque la réinitialisation du mot de masse de la boîte vocale. Lors d'une nouvelle configuration, l'abonné doit de

toute manière, lors du premier accès à sa boîte vocale, modifier le mot de passe initial.

7) Cliquez sur **OK&Suite**.
8) Modifiez les indications souhaitées pour la Boîte Fax (**Fax**) et l'**Assignation des touches**.
9) Cliquez sur **OK&Suite**.
10) Cliquez sur **OK&Suite** puis sur **Quitter**.

Concepts associés

Groupe chef/secrétaire / groupe Top à la page 658

14.2.3.6 Comment effacer un groupe Chef/Secrétaire / Top

L'Assistant **Chef / Secrétaire** permet de configurer des fonctions de chef et de secrétaire conviviales (fonction Top).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Chef / Secrétaire**.
4) Cliquez dans la ligne de la configuration Chef/Secrétaire (groupe Top) à effacer sur **Modifier**.
5) Cliquez sur **Effacer les données**.
6) Cliquez sur **OK** pour confirmer la suppression.
7) Cliquez sur **OK&Suivant** puis sur **Terminer**.

Remarque : Dans les applications utilisant l'interface CSTA (UC, OSCC, etc.) : Lorsqu'un groupe Chef/Secrétaire ou Top ou un membre d'un groupe Chef/Secrétaire ou Top est supprimé, un redémarrage du système est nécessaire.

Concepts associés

Groupe chef/secrétaire / groupe Top à la page 658

14.2.4 Configuration des équipes (Team) / groupes Team et fonctions Chef/ Secrétaire / groupes Top à l'aide du mode Expert

En plus des possibilités de configuration offertes par les assistants, un administrateur de profil **Expert** dispose de possibilités supplémentaires pour la configuration des équipes (Team) / groupes Team et fonctions Chef/ Secrétaire / groupes Top à l'aide du **mode Expert**.

Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide du **Mode Expert** :

- Comment ajouter ou effacer un membre à la configuration Team / au groupe Team
- Comment modifier un membre d'une configuration Team / d'un groupe Team
- Comment modifier les propriétés des membres d'une configuration Team / d'un groupe Team
- Comment modifier la programmation des touches du téléphone pour la configuration Team/le groupe Team
- Comment ajouter une boîte Fax à une configuration Team / un groupe Team
- Comment ajouter ou effacer un membre au groupe Chef/Secrétaire / groupe Top
- Comment modifier un membre d'un groupe Chef/Secrétaire / groupe Top
- Comment modifier les caractéristiques des membres d'un groupe Chef/Secrétaire / groupe Top
- Comment ajouter une boîte Fax à un groupe Chef/Secrétaire / un groupe Top

14.2.4.1 Comment ajouter ou effacer un membre à la configuration Team / au groupe Team

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Conseil : Avec l'assistant **Configuration Team** un administrateur avec profil **Advanced** peut définir jusqu'à trois membres (téléphones) d'une configuration Team (Groupe Team). Pour ajouter des membres supplémentaires, il faut faire intervenir un Administrateur avec profil **Expert** qui les ajoute via le **Mode Expert** (voir description ci-après).

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter un membre au groupe Team, naviguez dans l'arborescence menu sous **Appels entrants** > **Team/Top** > **…** vers le groupe Team souhaité (configuration Team). Cliquez sur l'onglet **Ajouter un membre Team/Top**. Dans la liste déroulante **Type**, sélectionnez le type d'abonné. Dans la liste déroulante **N° appel**, sélectionnez le numéro de l'abonné souhaité. Cliquez sur **Appliquer** puis sur **OK**.
   - Si vous souhaitez supprimer un membre du groupe Team (configuration Team), naviguez dans l'arborescence menu sous **Appels entrants** > **Team/Top** > **…** vers le membre du groupe Team souhaité (configuration Team) ((Membre du groupe) Numéro, Nom). Cliquez sur l'onglet **Effacer le membre Team/Top**. Cliquez sur **Effacer** et ensuite sur **OK**.

Concepts associés

La configuration Team / le groupe Team à la page 654

14.2.4.2 Comment modifier un membre d'une configuration Team / d'un groupe Team

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence menu, en passant par **Appels entrants** > **Team/Top** > **...** sélectionnez le membre du groupe Team (configuration Team) souhaité ((Membre groupe) Numéro, Nom).
4) Cliquez sur l'onglet **Modifier le membre Team/Top**.
5) Modifiez les paramètres souhaités.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

La configuration Team / le groupe Team à la page 654

14.2.4.3 Comment modifier les propriétés des membres d'une configuration Team / d'un groupe Team

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence menu, en passant par **Appels entrants** > **Team/Top** > **...** sélectionnez le membre du groupe Team (configuration Team) souhaité ((Membre groupe) Numéro, Nom).
4) Cliquez sur l'onglet **Modifier les paramètres du groupe Team/Top**.
5) Modifiez les propriétés souhaitées.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

La configuration Team / le groupe Team à la page 654

14.2.4.4 Comment modifier la programmation des touches du téléphone pour la configuration Team/le groupe Team

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous **Appels entrants** > **Team/Top** > **…** vers le groupe Team souhaité (configuration Team).
4) Cliquez sur l'onglet **Modifier le groupe Team/Top**.
5) Sélectionnez une valeur par défaut pour la programmation des touches :
   - Lorsque les touches doivent être paramétrées sur le premier ou le deuxième satellite, cochez la case **sur première / deuxième console**.
   - Si vous voulez paramétrer les touches sur les premières touches de fonction libres du téléphone, cochez la case **sur les 1ères touches libres**.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

La configuration Team / le groupe Team à la page 654

14.2.4.5 Comment ajouter une boîte Fax à une configuration Team / un groupe Team

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous **Appels entrants** > **Team/Top** > **…** vers le groupe Team souhaité (configuration Team).
4) Cliquez sur l'onglet **Ajouter la boîte Fax**.
5) Entrez dans le champ **Numéro Fax.** du membre souhaité du groupe Team (configuration Team) le numéro interne de la boîte Fax.
6) Dans le champ **SDA Fax** du membre souhaité du groupe Team (Configuration Team), entrez le numéro SDA de la boîte Fax activé.
7) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

La configuration Team / le groupe Team à la page 654

14.2.4.6 Comment ajouter ou effacer un membre au groupe Chef/Secrétaire / groupe Top

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Conseil : Avec l'assistant **Chef / Secrétaire**, un administrateur avec le profil **Advanced** peut définir jusqu'à deux chefs et jusqu'à deux secrétaires par configuration Chef/Secrétaire (groupe Top). Pour ajouter des membres supplémentaires, il faut faire intervenir un Administrateur avec profil **Expert** qui les ajoute via le **Mode Expert** (voir description ci-après).

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter un membre au groupe Top (configuration Chef/Secrétaire), naviguez dans l'arborescence menu sous **Appels entrants** > **Team/Top** > **…** vers le groupe Top souhaité (configuration Chef/Secrétaire). Cliquez sur l'onglet **Ajouter un membre Team/Top**. Dans la liste déroulante **Type**, sélectionnez le type d'abonné. Dans la liste déroulante **N° appel**, sélectionnez le numéro de l'abonné souhaité. Cliquez sur **Appliquer** puis sur **OK**.
   - Si vous souhaitez supprimer un membre du groupe Top (configuration Chef/Secrétaire), naviguez dans l'arborescence menu sous **Appels entrants** > **Team/Top** > **…** vers le membre du groupe Top souhaité (configuration Chef/Secrétaire) ((Membre du groupe) Numéro, Nom). Cliquez sur l'onglet **Effacer le membre Team/Top**. Cliquez sur **Effacer** et ensuite sur **OK**.

Concepts associés

Groupe chef/secrétaire / groupe Top à la page 658

14.2.4.7 Comment modifier un membre d'un groupe Chef/Secrétaire / groupe Top

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence menu, en passant par **Appels entrants** > **Team/Top** > **...** sélectionnez le membre du groupe Top (configuration Chef/Secrétaire) ((Membre groupe) Numéro, Nom).
4) Cliquez sur l'onglet **Modifier le membre Team/Top**.

5) Modifiez les paramètres souhaités.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe chef/secrétaire / groupe Top à la page 658

14.2.4.8 Comment modifier les caractéristiques des membres d'un groupe Chef/ Secrétaire / groupe Top

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence menu, en passant par **Appels entrants** > **Team/Top** > **...** sélectionnez le membre du groupe Top (configuration Chef/Secrétaire) ((Membre groupe) Numéro, Nom).
4) Cliquez sur l'onglet **Modifier les paramètres du groupe Team/Top**.
5) Modifiez les propriétés souhaitées.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe chef/secrétaire / groupe Top à la page 658

14.2.4.9 Comment ajouter une boîte Fax à un groupe Chef/Secrétaire / un groupe Top

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence menu, naviguez sous **Appels entrants** > **Team/Top** > **…** vers le groupe Top souhaité (configuration Chef/Secrétaire).
4) Cliquez sur l'onglet **Ajouter la boîte Fax**.
5) Dans le champ **Numéro Fax** du membre souhaité du groupe Top (configuration Chef/Secrétaire) entrez le numéro interne de la boîte Fax.
6) Dans le champ **SDA Fax** du membre souhaité du groupe Top (configuration Chef/Secrétaire), entrez le numéro SDA de la boîte Fax.
7) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe chef/secrétaire / groupe Top à la page 658

14.3 MULAP de base et MULAP chef

Un MULAP de base permet à un abonné qui utilise plusieurs téléphones (par exemple téléphone fixe et téléphone mobile) d'être joint sous un seul numéro de téléphone. Les MULAP chefs peuvent être configurés si des fonctions chef et secrétaire limitées doivent être utilisées.

14.3.1 MULAP de base

Les MULAP de base peuvent être configurés lorsqu'un abonné utilise plusieurs téléphones différents (par exemple, un téléphone fixe et un téléphone mobile) mais souhaite être joint à un seul numéro de téléphone (numéro de téléphone MULAP de base).

Si un appelant sonne au numéro de téléphone MULAP de base, l'appel est signalé visuellement sur tous les téléphones appartenant au MULAP de base. L'abonné peut également définir si les appels entrants doivent également être signalés acoustiquement pour chaque membre individuel. Le statut du MULAP de base passe à occupé et les autres appelants entendent le signal d'occupation lorsqu'ils répondent à un appel.

Le numéro de téléphone du MULAP de base est affiché sur l'écran de l'appelé pour les appels sortants via la ligne MULAP de base.

Il est possible de configurer jusqu'à 20 membres par MULAP de base.

Chaque MULAP de base peut se voir attribuer un nom contenant jusqu'à 16 caractères.

Chaque téléphone de l'abonné est un membre du MULAP de base et les propriétés suivantes peuvent être attribuées à chaque membre :

- **Maître**

  Ce paramètre permet de transformer un membre en maître du MULAP de base. Si le maître active le renvoi d'appel, cette fonction s'applique à tous les membres (téléphones) du MULAP de base. Si le maître active un rappel automatique sur un MULAP de base, le rappel est lancé dès que tous les maîtres sont libres.

  Un abonné ne peut pas être inclus plus de 25 fois en tant que maître MULAP dans des groupes de recherche.

  Réglage par défaut : le maître est le premier membre du MULAP de base.
- **Sonnerie acoustique**

  Si ce paramètre est activé, les appels entrants sont signalés de manière acoustique.

  Réglage par défaut : le paramètre est actif pour tous les maîtres.
- **Prise automatique sortante**

  Si ce paramètre est activé, la ligne MULAP de base est automatiquement appelée lorsque l'abonné décroche le combiné. Si le paramètre n'est pas activé, l'abonné doit appuyer sur la touche MULAP avant de pouvoir numéroter.

  Réglage par défaut : la saisie automatique des appels sortants est attribuée à tous les maîtres.

- **Pas de prise d'appel automatique entrante**

  Si ce paramètre est activé, il n'est pas possible de prendre l'appel entrant en décrochant le combiné. Pour accepter l'appel entrant, il faut appuyer sur la touche MULAP.

  Paramètre par défaut : le paramètre n'est pas activé.
- **Autorisation conférence automatique**

  Lorsque ce paramètre est activé, une pression sur la touche MULAP valide la ligne MULAP pour la conférence. Chez tous les autres participants, la validation est signalée par le clignotement de la touche MULAP. Pour rejoindre la conférence, les participants appuient sur la touche MULAP.

  Paramètre par défaut : le paramètre n'est pas activé.
- **Touche MULAP configurée**

  Lorsque ce paramètre est activé, une touche MULAP est configurée sur le téléphone correspondant. Vous pouvez appuyer sur cette touche pour établir un appel sortant via la ligne MULAP de base. Le numéro MULAP de base s'affiche sur l'écran de l'appelé.

  Paramètre par défaut : le paramètre est activé.

Affichage du numéro/nom

Lorsqu'un appel sortant est établi, un numéro de poste est attribué (numéro de poste local ou numéro de groupe MULAP).

Lorsqu'un appel MULAP entrant est pris, le numéro de groupe MULAP est attribué.

Dans le cas d'un appel vers un MULAP :

- Avant de répondre à l'appel, l'écran de l'appelant affiche le nom MULAP et/ou le numéro du MULAP appelé.
- Après avoir répondu à un appel, l'écran de l'appelant indique le nom du poste et/ou le numéro MULAP de l'appelant.
- Dans le cas d'appels provenant d'un poste MULAP (touche MULAP ou préférence), l'afficheur de l'appelé et celui du répondant indiquent toujours le nom du poste et/ou le numéro MULAP.
- Ce qui suit s'applique généralement aux saisies sortantes : Si un poste effectue un appel en utilisant le numéro de poste local et que la préférence sortante diffère du numéro de poste local, l'écran de l'appelé affiche toujours le numéro de poste de la préférence sortante.

Utilisation des touches MULAP

Le DEL d'une touche MULAP peut avoir différents statuts avec la signification suivante :

- Désactivée : la ligne correspondante est libre et peut être utilisée.
- Allumée : la ligne correspondante est occupée.
- Clignote rapidement : appel sur la ligne correspondante.
- Clignotement lent : un appel en attente est en train de se dérouler sur la ligne concernée ou la ligne concernée a été libérée pour une conférence.

Type de sonnerie

Pour chaque MULAP de base, un administrateur ayant le profil **Expert** peut définir la signalisation acoustique des appels externes entrants via le réglage du type de sonnerie. Vous disposez des possibilités suivantes :

- Sonnerie à deux tons (paramètre par défaut)
- Sonnerie à trois tons
- sonnerie courte-longue-courte

Sur les téléphones analogiques, seul le paramètre par défaut est possible. Les modifications n'ont pas d'influence.

Commande de dispositifs membres du Mulap

Les téléphones SIP peuvent être intégrés dans un MULAP de base, à condition qu'un dispositif TDM/HFA ait été défini comme premier membre du MULAP de base. Les téléphones IP peuvent être intégrés dans un MULAP de base, à condition qu'un dispositif TDM/HFA ait été défini comme premier membre du MULAP de base.

Il est possible d'intégrer par exemple des téléphones mobiles dual mode, configurés comme abonnés Mobility Entry. Les téléphones mobiles bimodes prennent en charge à la fois les réseaux GSM/ UMTS et les réseaux WLAN. Via WLAN, il est possible d'enregistrer un téléphone mobile dual mode comme abonné IP (client SIP) sur le système de communication.

Les utilisateurs mobiles, y compris les utilisateurs mobiles GSM, les clients Unify Phone et Microsoft Teams, peuvent être intégrés dans un MULAP de base, à condition qu'un dispositif TDM/HFA ait été défini comme premier membre du MULAP de base.

Remarque : La description étendue ci-dessus s'applique aux systèmes OpenScape Business X et OpenScape Business S, mais se limite à Team et Basic Mulap, et non aux sous-chapitres avec des déclarations similaires comme Executive/Secretary / Top Group.

Conseil : Aucune programmation de touches MULAP n'est possible pour les téléphones SIP. De plus, aucune fonctionnalité ne peut être activée ou désactivée à l'aide d'indicatifs. Les messages d'affichage spécifiques du MULAP de base ne sont pas pris en charge.

Correspondances

Rubrique	Correspondance
Ne pas déranger	Lorsque la fonction « Ne pas déranger » est activée, les appels entrants ne sont plus transmis.
Téléphones RNIS	Il n'est pas possible d'inclure des téléphones RNIS dans les MULAP de base.

Tâches associées

Comment ajouter un MULAP de base à la page 679
Comment afficher ou modifier le MULAP de base à la page 679

Comment effacer le MULAP de base à la page 680
Comment ajouter ou effacer un membre du MULAP de base à la page 680
Comment modifier le membre d'un MULAP de base à la page 681

14.3.2 MULAP chef

Les MULAP chefs peuvent être configurés si des fonctions chef et secrétaire limitées doivent être utilisées.

Tous les membres d'un MULAP chef peuvent être joints sous le numéro MULAP chef et sous leurs numéros de poste personnels.

Conseil : Dans ce texte, "le chef" correspond à un chef homme ou femme et "la secrétaire" correspond à un secrétaire, homme ou femme.

Il est possible de configurer jusqu'à 20 membres par MULAP chef.

Il est possible d'affecter à chaque MULAP chef un nom de 16 caractères maximum.

Les paramètres décrits ci-après permettent de définir quels membres d'un MULAP chef peuvent utiliser les fonctions de chef et lesquels peuvent utiliser les fonctions de secrétaire.

Si un appelant compose le numéro MULAP chef, l'appel est signalé de façon optique chez tous les téléphones faisant partie du MULAP chef. Chez les membres avec fonctions de secrétaire, les appels entrants sont aussi signalés de façon acoustique.

Pour les appels entrants par la ligne MULAP chef, le numéro MULAP chef apparaît sur l'écran des appelés.

Les membres d'un MULAP chef peuvent se voir affecter les caractéristiques suivantes :

- **Maître**

  Ce paramètre permet d'affecter à un membre des fonctions de chef. Lorsque le combiné est décroché, il y a automatiquement appel par la ligne MULAP chef. Les appels entrants par le numéro MULAP chef sont signalés exclusivement de façon optique.

  Un abonné ne peut pas être enregistré plus de 25 fois en tant que maître MULAP dans des groupes de recherche.

  Paramètre par défaut : le premier membre du MULAP chef reçoit les fonctions de chef.
- **Sonnerie acoustique**

  Si ce paramètre est activé, les appels entrants sont signalés de manière acoustique.

  Paramètre par défaut : le paramètres est activé pour tous les membres avec fonction secrétaire.

- **Prise automatique sortante**

  Si ce paramètre est activé, lorsque le combiné est décroché, l'appel a lieu automatiquement par la ligne MULAP chef. Si le paramètre n'est pas activé, l'abonné doit appuyer sur la touche MULAP avant de pouvoir numéroter.

  Ce paramètre ne peut pas être utilisé par les membres avec la fonction de secrétaire.

  Paramètre par défaut : le paramètres est activé pour tous les membres avec fonction chef.
- **Pas de prise d'appel automatique entrante**

  Si ce paramètre est activé, il n'est pas possible de prendre l'appel entrant en décrochant le combiné. Pour accepter l'appel entrant, il faut appuyer sur la touche MULAP.

  Paramètre par défaut : le paramètre n'est pas activé.
- **Autorisation conférence automatique**

  Lorsque ce paramètre est activé, une pression sur la touche MULAP valide la ligne MULAP pour la conférence. Chez tous les autres participants, la validation est signalée par le clignotement de la touche MULAP. Pour rejoindre la conférence, les participants appuient sur la touche MULAP.

  Paramètre par défaut : le paramètre n'est pas activé.
- **Touche MULAP configurée**

  Lorsque ce paramètre est activé, une touche MULAP est configurée sur le téléphone correspondant. Vous pouvez appuyer sur la touche pour configurer un appel sortant via la ligne MULAP chef. Le numéro MULAP chef s’affiche sur l’écran de la personne appelée.

  Paramètre par défaut : le paramètre est activé.

Utiliser les touches MULAP

La LED d'une touche MULAP a la signification suivante :

- Désactivée : la ligne correspondante est libre et peut être utilisée.
- Allumée : la ligne correspondante est occupée.
- Clignote rapidement : appel sur la ligne correspondante.
- Clignote lentement : une communication en garde attend sur la ligne correspondante ou la ligne correspondante a été validée pour une conférence.

Type de sonnerie

Pour chaque MULAP chef, un administrateur avec le profil **Expert** peut définir la signalisation acoustique des appels entrants externes en réglant le type de sonnerie. Vous disposez des possibilités suivantes :

- Sonnerie à deux tons (paramètre par défaut)
- Sonnerie à trois tons
- Sonnerie courte/longue/courte

Sur les téléphones analogiques, seul le paramètre par défaut est possible. Les modifications n'ont pas d'influence.

Téléphones SIP

Il est possible d'intégrer des téléphones SIP dans un MULAP chef. Condition : le premier membre du MULAP chef (Chef 1) doit être un téléphone système (par ex. téléphone HFA ou UP0).

Il est possible d'intégrer par exemple des téléphones mobiles dual mode, configurés comme abonnés Mobility Entry. Les téléphones mobiles dual mode supportent les réseaux GSM/UMTS et les réseaux WLAN. Via WLAN, il est possible d'enregistrer un téléphone mobile dual mode comme abonné IP (client SIP) sur le système de communication.

Conseil : Sur les téléphones SIP, aucune programmation des touches MULAP n'est possible. De plus, aucune fonctionnalité ne peut être activée ou désactivée à l'aide d'indicatifs. Les messages d'affichage spécifiques du MULAP chef ne sont pas supportés.

Correspondances

Rubrique	Correspondance
Ne pas déranger	Après l'activation de la fonction Ne pas déranger, les appels entrants ne sont pas délivrés.
Téléphones RNIS	L'intégration de téléphones RNIS dans des MULAP chef est impossible.

Tâches associées

Comment ajouter un MULAP chef à la page 681
Comment afficher ou modifier le MULAP chef à la page 682
Comment effacer le MULAP chef à la page 682
Comment ajouter ou effacer un membre du MULAP chef à la page 683
Comment modifier un membre d'un MULAP chef à la page 683

14.3.3 Configuration de MULAP de base et MULAP chef

La configuration de MULAP de base et de MULAP chef est réservée exclusivement à un administrateur de profil **Expert**, à l'aide du **Mode Expert**.

Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide du **Mode Expert** :

- Comment ajouter un MULAP de base
- Comment afficher ou modifier le MULAP de base
- Comment effacer le MULAP de base
- Comment ajouter ou effacer un membre du MULAP de base
- Comment modifier le membre d'un MULAP de base
- Comment ajouter le MULAP chef
- Comment afficher ou modifier le MULAP chef
- Comment effacer le MULAP chef
- Comment ajouter ou effacer un membre du MULAP chef
- Comment modifier un membre d'un MULAP chef

14.3.3.1 Comment ajouter un MULAP de base

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Cliquez sur **Appels entrants** > **Groupes/Groupement** dans l'arborescence du menu.
4) Cliquez sur l'onglet **Ajouter un groupe**.
5) Dans le champ **Numéro d'appel**, saisissez le numéro du nouveau MULAP de base.
6) Dans le champ **Numéro SDA**, saisissez le numéro SDA du nouveau MULAP de base.

   : Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

7) Dans les champs **Nom** et **Prénom**, saisissez le nom du nouveau MULAP de base.
8) Dans la liste déroulante **Type**, sélectionnez **MULAP de base**.
9) Dans la liste déroulante **Numéro d'appel** sélectionnez le numéro d'appel de l'abonné auquel vous souhaitez affecter le nouveau MULAP de base.
10) Cliquez sur **Appliquer** puis sur **OK**.

Remarque : Dans les applications utilisant l'interface CSTA (UC, OSCC, etc.), lorsqu'un groupe MULAP de base ou un membre d'un groupe MULAP de base est créé, un redémarrage du système est nécessaire.

Concepts associés

MULAP de base à la page 673

14.3.3.2 Comment afficher ou modifier le MULAP de base

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le MULAP de base souhaité.

4) Cliquez sur l'onglet **Modifier les paramètres du groupe**. Les réglages actuels des paramètres du groupe sont affichés.
5) Si nécessaire, modifiez les paramètres souhaités du MULAP de base.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

MULAP de base à la page 673

14.3.3.3 Comment effacer le MULAP de base

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le MULAP de base souhaité.
4) Cliquez sur l'onglet **Effacer le groupe**.
5) Cliquez sur **Effacer** et ensuite sur **OK**.

Remarque : Dans les applications utilisant l'interface CSTA (UC, OSCC, etc.): Lorsqu'un groupe MULAP basique ou un membre d'un groupe MULAP basique est supprimé, un redémarrage du système est nécessaire.

Concepts associés

MULAP de base à la page 673

14.3.3.4 Comment ajouter ou effacer un membre du MULAP de base

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter un membre au MULAP de base, naviguez dans l'arborescence menu sous **Appels entrants** > **Groupes/Groupes de recherche** > **…** vers le MULAP de base souhaité. Cliquez sur l'onglet **Ajouter un membre**. Dans la liste déroulante **Numéro**, sélectionnez le numéro de l'abonné souhaité. Cliquez sur **Appliquer** puis sur **OK**.

- Si vous souhaitez supprimer un membre dans le MULAP de base, naviguez dans l'arborescence menu sous **Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le membre souhaité du MULAP de base ((Membre du groupe) Numéro, Nom). Cliquez sur l'onglet **Effacer un membre**. Cliquez sur **Effacer** et ensuite sur **OK**.

Concepts associés

MULAP de base à la page 673

14.3.3.5 Comment modifier le membre d'un MULAP de base

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence menu, en passant par **Appels entrants** > **Groupes/ Groupes de recherche** > **…**, sélectionnez le membre du MULAP de base (Membre du groupe) Numéro, Nom).
4) Cliquez sur l'onglet **Modifier le membre**.
5) Modifiez les paramètres souhaités.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

MULAP de base à la page 673

14.3.3.6 Comment ajouter un MULAP chef

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Cliquez sur **Appels entrants** > **Groupes/Groupement** dans l'arborescence du menu.
4) Cliquez sur l'onglet **Ajouter un groupe**.
5) Dans le champ **Numéro d'appel**, saisissez le numéro du nouveau MULAP chef.

6) Dans le champ **Numéro SDA** saisissez le numéro SDA du nouveau MULAP Chef.

: Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

7) Dans les champs **Nom** et **Prénom**, saisissez le nom du nouveau MULAP chef.
8) Dans la liste déroulante **Type**, sélectionnez l'entrée **MULAP chef**.
9) Dans la liste déroulante **Numéro d'appel** sélectionnez le numéro d'appel de l'abonné auquel vous souhaitez affecter le nouveau MULAP chef.
10) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

MULAP chef à la page 676

14.3.3.7 Comment afficher ou modifier le MULAP chef

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/ Groupe de recherche** > **…** vers le MULAP Chef souhaité.
4) Cliquez sur l'onglet **Modifier les paramètres du groupe**. Les réglages actuels des paramètres du groupe sont affichés.
5) Si nécessaire, modifiez les paramètres souhaités du MULAP chef.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

MULAP chef à la page 676

14.3.3.8 Comment effacer le MULAP chef

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/ Groupe de recherche** > **…** vers le MULAP Chef souhaité.

4) Cliquez sur l'onglet **Effacer le groupe**.
5) Cliquez sur **Effacer** et ensuite sur **OK**.

Remarque : Dans les applications utilisant l'interface CSTA (UC, OSCC, etc.): Lorsqu'un groupe Chef MULAP ou un membre d'un groupe Chef MULAP est supprimé, un redémarrage du système est nécessaire.

Concepts associés

MULAP chef à la page 676

14.3.3.9 Comment ajouter ou effacer un membre du MULAP chef

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter un membre au MULAP Chef, naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/Groupe de recherche** > **…** vers le MULAP Chef souhaité. Cliquez sur l'onglet **Ajouter un membre**. Dans la liste déroulante **Numéro**, sélectionnez le numéro de l'abonné souhaité. Cliquez sur **Appliquer** puis sur **OK**.
   - Si vous souhaitez supprimer un membre dans le MULAP Chef, naviguez dans l'arborescence menu sous **Appels entrants** > **Groupes/Groupe de recherche** > **…** vers le membre souhaité du MULAP Chef ((Membre du groupe) Numéro, Nom). Cliquez sur l'onglet **Effacer un membre**. Cliquez sur **Effacer** et ensuite sur **OK**.

Concepts associés

MULAP chef à la page 676

14.3.3.10 Comment modifier un membre d'un MULAP chef

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence menu, en passant par **Appels entrants** > **Groupes/ Groupes de recherche** > **…**, sélectionnez le membre du MULAP de base (Membre du groupe) Numéro, Nom).

4) Cliquez sur l'onglet **Modifier le membre**.
5) Modifiez les paramètres souhaités.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

MULAP chef à la page 676

14.3.3.11 Comment ajouter un MULAP de base dans un groupe

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Appels entrants**.
3) Cliquez sur le MULAP de base souhaité dans l'arborescence du menu sous **Appels entrants > Groupes/Groupements**.
4) Cliquez sur l'onglet **Modifier les paramètres du groupe**. Les réglages actuels des paramètres du groupe sont affichés.
5) Activez l'indicateur **MULAP en tant que membre du groupe**.
6) Cliquez sur le groupe souhaité dans l'arborescence du menu sous **Appels entrants > Groupes/groupements** pour ajouter un MULAP de base en tant que membre du groupe.
7) Cliquez sur l'onglet **Ajouter un membre** et sélectionnez le MULAP de base à partir du menu déroulant dans le champ **numéro d' appel**.
8) Cliquez sur **Appliquer**, puis sur **OK**.

Restrictions :

- Tous les membres MULAP de base doivent être configurés avec les paramètres M, R, A.
- Le nombre maximum de membres du groupe doit être de 20, en comptant les membres du MULAP de base.
- Les membres du MULAP de base ne peuvent pas déjà être membres du groupe.
- Vous pouvez ajouter un MULAP à :
  1) Groupement linéaire
  2) Groupement cyclique
  3) Groupe
- Il n'est pas autorisé d'ajouter un MULAP à :
  1) Appel en attente
  2) Non réponse
- L'état d'un groupe ne peut pas être modifié en Avertissement ou Non réponse s'il contient un MULAP.

14.4 Groupes Messagerie vocale et Boîte Fax

Un groupe Boîte vocale (groupe Répondeur) peut permettre à un groupe d'abonnés d'accéder aux messages vocaux. Ce numéro du groupe Boîte vocale n'appelle pas les membres de ce groupe, mais joint directement la boîte vocale (le répondeur) du groupe. Un groupe Boîte Fax (groupe Fax) peut permettre à un groupe défini d'abonnés d'accéder aux messages Fax. Le numéro du groupe Boîte Fax permet d'accéder directement à la boîte Fax du groupe.

14.4.1 Groupe Boîte vocale

Un groupe Boîte vocale (groupe Répondeur) peut permettre à un groupe défini d'abonnés d'accéder aux messages vocaux. Ce numéro du groupe Boîte vocale n'appelle pas les membres de ce groupe, mais joint directement la boîte vocale (le répondeur) du groupe. Une fois qu'un message voix a été déposé dans la boîte vocale du groupe, ce message est renvoyé vers les boîtes vocales de tous les membres.

Tous les membres reçoivent simultanément le message Voix. Si un membre du groupe efface un message vocal, ce message est effacé dans toutes les boîtes vocales des autres membres et dans la boîte vocale du groupe. Les messages Voix personnels de tous les membres ne sont pas influencées par cela.

Chaque membre d'un groupe Boîte vocale est joignable via son propre numéro d'abonné.

Il est possible de configurer jusqu'à 20 membres par groupe Boîte vocale.

Il est possible d'affecter à chaque groupe Boîte vocale un nom de 16 caractères maximum.

Au moins un abonné d'un Groupe Boîte vocale doit disposer d'une licence Messagerie vocale.

Correspondances

Sujet	Correspondance
Pilotage	L'utilisation de la fonctionnalité *Pilotage* est impossible.

Tâches associées

Comment ajouter un groupe Boîte vocale à la page 686
Comment afficher ou modifier le groupe Boîte vocale à la page 687
Comment effacer un groupe Boîte vocale à la page 687
Comment ajouter ou effacer un membre dans le groupe Boîte vocale à la page 688
Comment modifier le membre d'un groupe Boîte vocale à la page 688

14.4.2 Groupe Boîte Fax

Un groupe Boîte Fax (groupe Fax) peut permettre à un groupe défini d'abonnés d'accéder aux messages Fax. Le numéro du groupe Boîte Fax permet d'accéder directement à la boîte Fax du groupe. Une fois qu'un message Fax

a été déposé dans la boîte Fax du groupe, ce message est renvoyé vers les boîtes Fax de tous les membres.

Tous les membres reçoivent simultanément le message Fax. Si un membre du groupe efface un message Fax, ce message est effacé dans toutes les boîtes Fax des autres membres et dans la boîte Fax du groupe.

Chaque membre d'un groupe Boîte Fax est joignable via son propre numéro d'abonné.

Il est possible de créer jusqu'à 20 groupes Boîte Fax.

Il est possible d'affecter à chaque groupe Boîte Fax un nom de 16 caractères maximum.

Au moins un abonné d'un Groupe Boîte Fax doit disposer d'une licence Fax.

Tâches associées

Comment configurer un groupe Boîte Fax à la page 689
Comment afficher ou modifier le groupe Boîte Fax à la page 690
Comment ajouter ou effacer un membre dans le groupe Boîte Fax à la page 690

14.4.3 Configuration des groupes de boîtes vocales et groupes de boîtes Fax

La configuration des groupes de boîtes vocales et des groupes Boîte Fax est exclusivement réservée à un administrateur de profil **Expert**, à l'aide du **Mode Expert**.

Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide du **Mode Expert** :

- Comment ajouter un groupe Boîte vocale
- Comment afficher ou modifier le groupe Boîte vocale
- Comment effacer un groupe Boîte vocale
- Comment ajouter ou effacer un membre dans le groupe Boîte vocale
- Comment modifier le membre d'un groupe Boîte vocale
- Comment configurer un groupe Boîte Fax
- Comment afficher ou modifier le groupe Boîte Fax
- Comment effacer un groupe Boîte Fax
- Comment ajouter ou effacer un membre dans le groupe Boîte Fax

14.4.3.1 Comment ajouter un groupe Boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.

3) Cliquez sur **Appels entrants** > **Groupes/Groupement** dans l'arborescence du menu.
4) Cliquez sur l'onglet **Ajouter un groupe**.
5) Dans le champ **Numéro**, indiquez le numéro du nouveau groupe Boîte vocale.
6) Dans le champ **Numéro SDA**, indiquez le numéro SDA du nouveau groupe Boîte vocale.

: Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

---

7) Dans le champ **Nom** indiquez le nom du nouveau groupe Boîte vocale.
8) Dans la liste déroulante **Type**, sélectionnez l'entrée **Répondeur**.
9) Dans la liste déroulante **Numéro**, sélectionnez le numéro de l'abonné auquel doit être affecté le nouveau groupe Boîte vocale.
10) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe Boîte vocale à la page 685

14.4.3.2 Comment afficher ou modifier le groupe Boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le groupe Boîte vocale souhaité.
4) Cliquez sur l'onglet **Modifier les paramètres du groupe**. Les réglages actuels des paramètres du groupe sont affichés.
5) Si nécessaire, modifiez les paramètres souhaités du groupe Boîte vocale.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe Boîte vocale à la page 685

14.4.3.3 Comment effacer un groupe Boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le groupe Boîte vocale souhaité.
4) Cliquez sur l'onglet **Effacer le groupe**.
5) Cliquez sur **Effacer** et ensuite sur **OK**.

Concepts associés

Groupe Boîte vocale à la page 685

14.4.3.4 Comment ajouter ou effacer un membre dans le groupe Boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter un membre au groupe Boîte vocale, naviguez dans l'arborescence menu sous **Appels entrants** > **Groupes/Groupes de recherche** > **…** vers le groupe Boîte vocale souhaité. Cliquez sur l'onglet **Ajouter un membre**. Dans la liste déroulante **Numéro**, sélectionnez le numéro de l'abonné souhaité. Cliquez sur **Appliquer** puis sur **OK**.
   - Si vous souhaitez supprimer un membre dans le groupe Boîte vocale, naviguez dans l'arborescence menu sous **Appels entrants** > **Groupes/ Groupes de recherche** > **…** vers le membre souhaité du groupe Boîte vocale ((Membre du groupe) Numéro, Nom). Cliquez sur l'onglet **Effacer un membre**. Cliquez sur **Effacer** et ensuite sur **OK**.

Concepts associés

Groupe Boîte vocale à la page 685

14.4.3.5 Comment modifier le membre d'un groupe Boîte vocale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence menu, en passant par **Appels entrants** > **Groupes/ Groupes de recherche** > **…**, sélectionnez le membre souhaité du groupe Boîte vocale ((Membre du groupe) Numéro, Nom).

4) Cliquez sur l'onglet **Modifier le membre**.
5) Modifiez les paramètres souhaités.
6) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe Boîte vocale à la page 685

14.4.3.6 Comment configurer un groupe Boîte Fax

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés** > **Applications UC** > **Groupe Fax**. Les groupes boîte Fax déjà configurés sont affichés.
4) Sélectionnez la rangée libre suivante et, dans le champ **Numéro**, entrez le numéro du nouveau groupe Boîte Fax.
5) Dans le champ **SDA**, entrez le numéro SDA du nouveau groupe Boîte Fax.

   : Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

6) Dans le champ **Nom** entrez le nom du nouveau groupe Boîte Fax.
7) Dans la liste déroulante **Type**, sélectionnez l'entrée **Groupe fax**.
8) Cliquez sur **Appliquer** puis sur **OK**.
9) Fermez la fenêtre **Groupe Fax**.
10) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
11) Cliquez sur **Groupes**.
12) Cliquez sur l'onglet **Groupes Fax**.
13) Sélectionnez le nouveau groupe Boîte Fax et cliquez sur **Modifier**.
14) Sélectionnez l'une des options suivantes :
    - Si vous souhaitez ajouter un membre au groupe Boîte Fax, sélectionnez le membre choisi dans la liste **Utilisateurs**.
    - Si vous souhaitez ajouter plusieurs membres au groupe Boîte Fax, appuyez sur <Ctrl> et marquez les membres choisis dans la liste **Utilisateurs**.
15) Cliquez sur **Enregistrer**.

Concepts associés

Groupe Boîte Fax à la page 685

14.4.3.7 Comment afficher ou modifier le groupe Boîte Fax

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés** > **Applications UC** > **Groupe Fax**.
4) Dans l'arborescence du menu, cliquez sur le groupe Boîte Fax souhaité.
5) Cliquez sur l'onglet **Modifier les paramètres de l'abonné**.
6) Si nécessaire, modifiez les paramètres souhaités du groupe Boîte Fax.
7) Cliquez sur **Appliquer** puis sur **OK**.

Concepts associés

Groupe Boîte Fax à la page 685

14.4.3.8 Comment effacer un groupe Boîte Fax

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Groupes**.
4) Cliquez sur l'onglet **Groupes Fax**.
5) Sélectionnez le groupe Boîte Fax souhaité et cliquez sur **Effacer**.

14.4.3.9 Comment ajouter ou effacer un membre dans le groupe Boîte Fax

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Groupes**.
4) Cliquez sur l'onglet **Groupes Fax**.
5) Sélectionnez le groupe Boîte Fax souhaité et cliquez sur **Modifier**. Il est affiché la liste **Utilisateurs** où les membres existants sont marqués.

6) Sélectionnez l'une des options suivantes :

- Si vous souhaitez ajouter un membre au groupe Boîte Fax, appuyez sur <Ctrl> et sélectionnez le nouveau membre en plus des membres déjà présents dans la liste **Utilisateurs**.
- Si vous souhaitez supprimer un membre dans le groupe Boîte Fax, appuyez sur <Ctrl> et supprimez la maque du membre concerné dans la liste **Utilisateurs**.

7) Cliquez sur **Enregistrer**.

Concepts associés

Groupe Boîte Fax à la page 685

14.5 Appel interphone pour groupes

L'appel interphone pour groupes permet des diffusions en direction des abonnés internes d'un groupe.

14.5.1 Diffusion à un groupe

La diffusion à un groupe permet d'effectuer un appel interphone avec les abonnés internes d'un groupe. Cette fonctionnalité est également appelée "Diffusion interne". Les membres du groupe qui sont occupés ou ont activé la fonction Ne pas déranger activé, ne reçoit pas le paging interne. Pour les membres de groupe appelés, il n'y a pas de possibilité de réponse sur appel interphone. La réponse n'est possible que par décrochage du combiné, ce qui entraîne le passage à une communication à deux normale.

La diffusion au groupe (diffusion interne ou paging interne) peut être utilisée grâce à une touche de fonction programmée à cet effet ou par l'entrée de menu correspondante **Appel interphone** ou l'indicatif correspondant, suivi du numéro du groupe de destination. Une touche de fonction peut aussi être programmée avec le numéro de groupe. Après appui sur une touche de fonction de ce type, il y a aussitôt établissement d'une liaison avec le groupe programmé.

Correspondances

Sujet	Correspondance
Ne pas déranger	Les membres du groupe qui ont paramétré Ne pas déranger ne bénéficient pas de la diffusion.
Téléphones RNIS, téléphones SIP	La fonctionnalité "Diffusion à un groupe (Paging interne)" ne peut pas être utilisée par les téléphones RNIS ou SIP.

14.5.2 Transférer à un groupe à partir d'une diffusion

Une communication qui se trouve en double appel peut être transférée par transfert à partir de la diffusion à un groupe. Pour cela, la diffusion au groupe est activée (Paging interne). Dès qu'un abonné décroche le combiné ou active

le haut-parleur et que l'abonné qui a transféré raccroche, il y a communication à deux. Pour les autres membres du groupe, la liaison est coupée.

La diffusion au groupe (diffusion interne ou paging interne) peut être utilisée grâce à une touche de fonction programmée à cet effet ou par l'entrée de menu correspondante **Appel interphone** ou l'indicatif correspondant, suivi du numéro du groupe de destination. Une touche de fonction peut aussi être programmée avec le numéro de groupe. Après appui sur une touche de fonction de ce type, il y a aussitôt établissement d'une liaison avec le groupe programmé.

Correspondances

Sujet	Correspondance
Ne pas déranger	Les membres du groupe qui ont paramétré Ne pas déranger ne bénéficient pas de la diffusion.
Téléphones RNIS, téléphones SIP	La fonctionnalité "Transfert à un groupe à partir d'une diffusion" ne peut pas être utilisée par les téléphones RNIS ou SIP.

14.6 UCD (Uniform Call Distribution, distribution uniforme des appels)

La fonctionnalité UCD (Uniform Call Distribution) permet au système de communication de répartir équitablement les appels entrants à l'intérieur d'un groupe de participants (groupe UCD).

Les groupes UCD sont utilisés notamment dans l'environnement des hotline techniques (par exemple hotline du service clients), par la gestion des plaintes, dans la prospection du marché, la réception des commandes (par ex. maison de vente par correspondance, service de facturation) ou dans les services d'urgence.

En général, la distribution des appels se passe de telle sorte qu'un appel entrant adressé à un groupe UCD est transféré à l'abonné (agent) du groupe dont la dernière communication remonte le plus loin. Il est également possible de définir d'autres règles de distribution.

Si aucun agent n'est libre pour prendre un appel entrant, l'appel est automatiquement transféré à une file d'attente. En fonction de la priorité et du temps d'attente, les appels en attente sont distribués entre les agents libérés.

Il est possible de diffuser des annonces ou de la musique aux appelants qui se trouvent en attente.

Configuration

Avec l'Assistant **UCD**, vous pouvez configurer les groupes et abonnés pour une distribution intelligente des appels (UCD). Sont décrites les procédures correspondant aux applications suivantes, paramétrées à l'aide de l'Assistant :

- Comment configurer le renvoi d'appel / les groupes UCD
- Comment ajouter ou effacer des agents UCD
- Comment modifier les annonces/la musique d'attente pour UCD

En dehors des possibilités de configuration offertes par les assistants, l'administrateur de profil **Expert** dispose de possibilités supplémentaires de configuration en **Mode Expert**.

14.6.1 Distribution d'appels / Groupe UCD

Un groupe UCD comprend des agents (abonnés) qui font partie d'un groupe de travail et peuvent être joints sous un même numéro. Un appel entrant interne ou externe est automatiquement affecté à l'agent qui se trouve depuis le plus longtemps inactif.

Chaque groupe UCD peut être configuré par WBM (**mode Expert**) de telle sorte que les appels adressés chez un agent soient automatiquement pris en charge par le système de communication (Automatic Incoming Call Connection AICC).

Si tous les agents d'un groupe UCD sont occupés, les appels entrants peuvent être entrés dans une file d'attente. Pour chaque groupe UCD, le nombre maximum des appels en file d'attente peut être défini individuellement. Si le nombre maximum d'appels en attente est dépassé, les autres appels peuvent être acheminés à une destination de débordement (une destination externe, un autre groupe UCD, un abonné interne ou un groupe).

Si la destination de débordement est un autre groupe UCD et si tous les agents de ce groupe UCD sont également occupés, l'appel reste dans la file d'attente du groupe d'origine et il est également inscrit dans la file d'attente de l'autre groupe UCD (destination de débordement).

Des annonces ou de la musique peuvent être diffusées aux appelants en attente.

Il est possible d'affecter à chaque groupe UCD un nom de 16 caractères maximum.

Correspondances

Sujet	Correspondance
Renvoi d'appel	Le renvoi vers un groupe UCD n'est pas suivi dans les cas suivants : • Si un groupe de recherche est appelé et si c'est le tour d'un abonné avec un renvoi d'appel vers un groupe UCD, le renvoi d'appel n'est pas suivi. Dans ce cas, c'est l'abonné suivant du groupe de recherche qui est directement appelé. • Un abonné est membre d'un groupe d'appel collectif avec la propriété "Groupe" et a activé un renvoi d'appel vers un groupe UCD. • Un abonné est membre d'un groupe d'appel collectif sur non-réponse. Si le groupe est appelé, le renvoi d'appel vers le groupe UCD n'est pas suivi. Exception : le premier abonné inscrit a activé un renvoi vers un groupe UCD. Ce renvoi est suivi.

14.6.1.1 Comment configurer le renvoi d'appel / les groupes UCD

Avec l'Assistant **UCD**, vous pouvez configurer une distribution intelligente des appels dans un groupe avec certains abonnés.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **UCD**. Le système affiche la liste de tous les groupes UCD possibles.
4) Pour configurer un groupe UCD, cliquez dans la ligne du groupe UCD souhaité sur **Modifier**.
5) Dans le champ **Numéro**, entrez le numéro du groupe UCD.
6) Dans le champ **Numéro SDA**, entrez le numéro SDA du groupe UCD.

: Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

---

7) Dans le champ **Nom**, entrez le nom du groupe UCD.
8) Cliquez sur **OK & Suivant**. La fenêtre **Affectation des agents UCD** s'affiche.
9) Sélectionnez les ID d'agents UCD souhaités dans la **sélection** et affectez-les au groupe UCD en cliquant sur **Ajouter**.
10) Cliquez sur **OK & Suivant**. La fenêtre **Modifier Annonce/débordement** s'affiche.
11) Sélectionnez le **système d'annonces** du groupe UCD. Vous avez la possibilité de sélectionner une annonce (si configurée) ou la musique d'attente interne (Music On Hold MOH). Après la sélection d'un système d'annonces, le champ **Retard annonce** apparaît.
12) Dans le champ **Retard annonce**, indiquez le temps en secondes durant lequel l'appelant placé dans la file d'attente doit entendre une annonce.
13) Dans la liste déroulante **Délai d'attente entre agents**, sélectionnez l'intervalle de temps à l'issue duquel un appel sera transmis à l'agent UCD suivant du groupe UCD.
14) Sélectionnez la **destination du débordement** du groupe UCD. Vous avez la possibilité de sélectionner une destination externe, un autre groupe UCD, un abonné interne ou un groupe.

    Si vous sélectionnez **Destination externe** comme destination de débordement, le champ **Destination externe** et la liste déroulante **Faisceau** s'affiche.

    a) Dans le champ **Destination externe**, entrez le numéro de la destination externe de débordement.
    b) Lorsque la destination de débordement externe doit être atteinte par un faisceau déterminé, sélectionnez le faisceau correspondant dans la liste déroulante **Faisceau**.
15) Cliquez sur **OK** pour valider les entrées.
16) Si vous souhaitez configurer d'autres groupes UCD, répétez les étapes 4 à 15.
17) Cliquez sur **OK&Suivant** puis sur **Quitter**.

14.6.2 Agents UCD

Les abonnés d'un groupe CD (agents) constituent un groupe de travail qui peut être utilisé par exemple pour les hotlines techniques ou dans la réception des commandes. Tous les appels entrants sont répartis équitablement entre les abonnés disponibles d'un groupe UCD.

L'affectation des agents aux groupes UCD se fait par des identifications (ID). Une ID peut être affectée au maximum à un groupe UCD. Plusieurs ID peuvent être affectées à un agent. Il est ainsi possible pour un agent de travailler dans plus d'un groupe UCD. Un agent ne peut toutefois être connecté et donc actif que dans un groupe UCD à la fois.

Pour pouvoir utiliser les fonctions UCD de façon efficace, les agents doivent disposer de téléphones avec écran, touches de fonction et casque.

Connexion / Déconnexion

Un agent peut se connecter avec son ID (identification) sur n'importe quel téléphone du système de communication (sauf téléphones RNIS et SIP). Lorsque la connexion a abouti, l'agent est disponible et affecté de façon permanente au téléphone correspondant jusqu'à sa déconnexion. Une autre connexion sur un autre téléphone est impossible. Après sa déconnexion, l'agent n'est plus pris en compte par la distribution des appels.

Les fonctions UCD Connexion, Déconnexion et Modification de l'état de l'abonné peuvent être activées par les agents sur le téléphone grâce aux touches de fonction programmées à cet effet ou aux entrées de menu correspondantes ou aux indicatifs.

Etats des abonnés

Lorsque la connexion a abouti, l'agent se trouve dans l'état d'abonné **Disponible**. Si besoin est, l'agent peut paramétrer lui-même un autre état d'abonné ou l'état de l'abonné se modifie automatiquement, en fonction de l'activité de l'agent. L'état d'abonné actualisé s'affiche sur l'écran du téléphone.

Les affichages suivants sont possibles :

Affichage	Signification
Disponible	L'agent est disponible et peut prendre les appels UCD.
Non disponible	L'agent s'est déconnecté temporairement de son poste de travail (par exemple pour une pause).
Post-traitement	L'agent se trouve dans le délai de post-traitement. Au sein du délai de post-traitement, il ne reçoit pas d'appel UCD. Selon la configuration, il peut s'agir d'un délai de post-traitement individuel (l'agent détermine lui-même la longueur du délai de post-traitement en modifiant son état d'abonné) ou d'un délai de post-traitement automatique (tous les agents disposent automatiquement d'un délai de post-traitement après un appel UCD).
Pour <nom du groupe UCD>	L'agent reçoit un appel UCD.

A la fin de sa période de travail, l'agent se déconnecte et n'est plus disponible pour les appels UCD. Il peut continuer à être joint par son numéro d'abonné personnel.

Si tous les agents d'un groupe UCD se trouvent dans l'état d'abonné **Non disponible**, il y a un renvoi temporisé des appels entrants vers une destination de débordement (une destination externe, un autre groupe UCD, un abonné interne ou un groupe).

Si un agent ne prend pas un appel alors qu'il est connecté et disponible, il est automatiquement placé par le système de communication à l'état d'abonné **Non disponible**.

Correspondances

Sujet	Correspondance
Renvoi d'appel	Si un agent active la fonctionnalité "Renvoi d'appel", il est automatiquement déconnecté et n'est plus disponible pour les appels UCD.
Téléphones RNIS, téléphones SIP	L'utilisation de téléphones RNIS et SIP est impossible.

14.6.2.1 Comment ajouter ou effacer des agents UCD

Avec l'assistant **UCD** vous pouvez ajouter des agents UCD sous forme de groupe UCD ou les effacer dans un groupe UCD.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **UCD**. Le système affiche la liste de tous les groupes UCD possibles.
4) Pour ajouter/effacer des agents UCD dans un groupe UCD, cliquez dans la ligne du groupe UCD souhaitée sur **Modifier**.
5) Cliquez sur **OK&Suivant** pour accéder à la fenêtre **Affectation des agents UCD**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter des agents UCD, sélectionnez les ID des agents UCD souhaités dans **Sélection** et affectez-les au groupe UCD en cliquant sur **Ajouter**.
   - Si vous souhaitez effacer des agents UCD, sélectionnez les **membres** souhaités et effacez-les du groupe UCD en cliquant sur **Effacer**.
7) Cliquez sur **OK&Suivant** pour valider les entrées.
8) Cliquez sur **OK**.
9) Si vous souhaitez modifier les agents UCD d'un autre groupe UCD, répétez les étapes 4 à 8.

10) Cliquez sur **OK&Suivant** puis sur **Terminer**.

14.6.3 Post-traitement

Cette fonctionnalité permet d'exempter temporairement un agent de la distribution des appels afin qu'il puisse réaliser des opérations de post-traitement pour l'appel qui vient de s'achever. Durant le délai de post-traitement, l'agent ne reçoit pas d'appel UCD.

Une distinction est établie entre

- le délai de post-traitement individuel

  L'agent détermine lui-même la longueur du délai de post-traitement en modifiant son état d'abonné.
- le délai de post-traitement automatique

  Pour cela, la fonctionnalité "UCD (Uniform Call Distribution)" est configurée de telle sorte que tous les agents de tous les groupes UCD disposent automatiquement après un appel UCD d'un délai de post-traitement. La définition du délai de post-traitement automatique se fait par cycles d'appels, c'est-à-dire par paliers de 5 secondes.

  Un agent peut prolonger manuellement le délai de post-traitement automatique en modifiant son état d'abonné.

Durant le délai de post-traitement, un agent peut continuer à être joint par son numéro d'abonné personnel.

14.6.3.1 Comment modifier le délai de post-traitement automatique

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.

3) Dans l'arborescence du menu, cliquez sur **Appels entrants** > **UCD**.

4) Cliquez sur l'onglet **Modifier les paramètres UCD**.

5) Dans la liste déroulante **Mode Post-traitement (cycles)** sélectionnez le temps dont devront disposer tous les agents UCD pour le post-traitement. L'indication se fait en cycles de sonneries, c'est-à-dire par paliers de 5 secondes.

6) Cliquez sur **Appliquer** puis sur **OK**.

14.6.4 Distribution des appels avec priorité

Les appels internes et externes entrants pour un groupe UCD peuvent recevoir une priorité. Les appels présents dans la file d'attente sont affectés en fonction de la priorité et du délai d'attente aux agents du groupe UCD.

Un appel en attente avec une priorité plus élevée reçoit une réponse avant un appel en attente depuis plus longtemps avec une priorité plus faible. Un appel en attente avec une priorité plus faible est acheminé plus tôt à une destination de débordement qu'un appel en attente avec une priorité plus élevée.

Pour les appels externes, l'affectation de priorité se fait en fonction de la ligne (par canal B), qu'il s'agisse de lignes IP ou TDM.

Exemples :

- Système de communication avec raccordement multiplex primaire RNIS (interface S_{2M}) et raccordement multiposte RNIS (interface S_0)

  Les appels arrivant par le raccordement multiplex primaire RNIS sont des appels clients normaux. Tous les canaux B de l'interface S_{2M} reçoivent par conséquent une priorité moyenne. Les appels qui passent par le raccordement multiposte RNIS sont des appels urgents, par exemple des commandes de pièces de rechange. Tous les canaux B de l'interface S_0 reçoivent par conséquent une priorité élevée.
- Système de communication avec raccordement système vers un fournisseur de services de téléphonie sur Internet ITSP et raccordement multiposte RNIS (interface S_0)

  Les appels entrants par le numéro de l'installation pour la téléphonie IP sont des appels clients normaux. Tous les canaux B de l'interface LAN reçoivent par conséquent une priorité moyenne. Les appels qui passent par le raccordement multiposte RNIS sont des appels urgents, par exemple des commandes de pièces de rechange. Tous les canaux B de l'interface S_0 reçoivent par conséquent une priorité élevée.

Pour les appels internes, la priorité est paramétrée à l'échelle du système et s'applique dont de façon équilibrée à tous les appels internes.

10 niveaux de priorité (1 = élevée, 10 = basse) sont disponibles.

Par défaut, la priorité pour les appels internes = 10 et la priorité pour les appels externes = 1.

14.6.4.1 Comment modifier la priorité de la file des appels

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Dans l'arborescence du menu, cliquez sur **Appels entrants** > **UCD**.
4) Cliquez sur l'onglet **Modifier les paramètres UCD**.
5) Dans la liste déroulante **priorité interne**, sélectionnez la priorité qui doit s'appliquer à tous les appels internes de tous les groupes UCD (1 = priorité la plus élevée, 10 = priorité la plus faible).
6) Sélectionnez pour chaque ligne (canal B) la **priorité** qui doit s'appliquer aux appels externes arrivant sur cette ligne pour tous les groupes UCD (1 =

priorité la plus élevée, 10 = priorité la plus faible). Pour chaque canal B, une priorité individuelle peut être paramétrée.

7) Cliquez sur **Appliquer** puis sur **OK**.

14.6.5 Prendre automatiquement les appels UCD

Grâce à cette fonctionnalité, les agents peuvent prendre les appels entrants sans opérations supplémentaires (Automatic Incoming Call Connection AICC).

Pour que la fonctionnalité puisse être utilisée, le téléphone de l'agent doit être équipé d'un casque et d'une touche Coupure. L'agent est averti par un bip dans le casque de l'arrivée d'un appel, qui lui est automatiquement et immédiatement transféré.

L'agent peut mettre fin à une communication en cours en appuyant sur la touche Coupure.

Par défaut, la fonctionnalité "AICC" n'est pas activée. L'activation est spécifique du groupe et s'applique à tous les agents d'un groupe UCD, que le téléphone de l'agent soit équipé d'un casque ou pas.

14.6.5.1 Comment modifier la réception automatique des appels UCD

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **UCD** > **…** vers le groupe UCD souhaité.
4) Cliquez sur l'onglet **Modifier le groupe UCD**.
5) Sélectionnez une des possibilités suivantes :
   - Si les agents UCD de ce groupe UCD doivent accepter les appels entrants sans effectuer d'opérations de commande supplémentaires, sélectionnez dans la liste déroulante **AICC** la mention **Oui**.
   - Si les agents UCD de ce groupe UCD ne doivent pas prendre les appels entrants sans effectuer les étapes de commande classiques (par exemple soulever le combiné), sélectionnez dans la liste déroulante **AICC** l'élément **non**.
6) Cliquez sur **Appliquer** puis sur **OK**.

14.6.6 File d'attente UCD

Si tous les agents d'un groupe UCD sont occupés, les appels entrants peuvent être entrés dans une file d'attente. Des annonces ou de la musique peuvent être diffusées aux appelants en attente.

Si un appel qui se trouve dans la file d'attente depuis un certain temps (sonnerie principale) n'est pas pris par l'agent qui se trouve depuis le plus de temps dans l'état **Disponible**, cet agent est placé dans l'état **Non disponible**. L'appel est ensuite transféré à l'agent suivant. Si l'appel n'est pas non pris par cet agent dans un certain délai (sonnerie secondaire), cet agent est également placé dans l'état **Non disponible**. Si tous agents se trouvent à l'état **Non disponible**, l'appel peut être acheminé à une destination de débordement.

Pour chaque groupe UCD, il est possible de définir individuellement quel est le nombre maximum d'appels autorisés en file d'attente. Si le nombre maximum d'appels en attente est dépassé, les appels suivants peuvent être acheminés à une destination de débordement.

Vous pouvez définir comme destination de débordement une destination externe, un autre groupe UCD, un abonné interne ou un groupe. Si la destination de débordement est un autre groupe UCD et si tous les agents de ce groupe UCD sont également occupés, l'appel reste dans la file d'attente du groupe d'origine et il est également inscrit dans la file d'attente de l'autre groupe UCD (destination de débordement).

Un agent peut consulter le nombre d'appels qui se trouvent dans la file d'attente de son groupe UCD par une touche de fonction programmée à cet effet ou par l'entrée de menu correspondante ou par un indicatif.

Appels dans une file d'attente

Le nombre maximum d'appels en file d'attente est de 30 pour les groupes UCD 1 à 59 et 72 pour le groupe UCD 60.

Le nombre minimum d'appels en file d'attente est de zéro. Si zéro est configuré comme nombre minimum, il n'y a pas de file d'attente. Les appels sont transférés directement à une destination de débordement ou refusés si aucun agent n'est disponible.

14.6.6.1 Comment modifier la file d'attente UCD

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **UCD** > **…** vers le groupe UCD souhaité.
4) Cliquez sur l'onglet **Modifier le groupe UCD**.
5) Dans la liste déroulante **Cycl. prim.** sélectionnez le nombre des cycles de sonnerie primaires. L'indication se fait en cycles de sonneries, c'est-à-dire par paliers de 5 secondes. Vous paramétrez le temps pendant lequel un appel reste en file d'attente s'il n'est pas pris par l'agent qui se trouve à l'état Disponible depuis le plus de temps. Ensuite, l'appel est transféré à l'agent disponible suivant.
6) Dans la liste déroulante **Cycl. sec.** sélectionnez le nombre des cycles de sonnerie secondaires. L'indication se fait en cycles de sonneries, c'est-à-

dire par paliers de 5 secondes. Vous paramétrez le temps pendant lequel un appel reste en file d'attente s'il n'est pas pris par l'agent disponible suivant.

7) Sélectionnez si un changement d'annonce doit avoir lieu :
   - Si les appelants se trouvant dans la file d'attente doivent entendre une annonce unique, sélectionnez dans la liste déroulante **Changement annonce** l'élément **Unique**..
   - Si les appelants se trouvant dans la file d'attente doivent entendre des annonces qui changent cycliquement, sélectionnez dans la liste déroulante **Changement annonce** l'élément **Cyclique**.
8) Dans le champ **Retard annonce**, indiquez l'intervalle de temps que doit attendre un appelant se trouvant dans la file d'attente avant d'entendre une annonce. L'indication est fournie en secondes.
9) Cliquez sur **Appliquer** puis sur **OK**.

14.6.7 Débordement UCD

Les appels UCD peuvent être acheminés à une destination de débordement, s'ils ne sont pas pris par les agents d'un groupe UCD et si aucune file d'attente n'a été configurée ou le nombre maximum d'appels en file d'attente a été atteint.

Remarque : Le concept de débordement UCD définit une seule destination de débordement, la deuxième entrée CDL. Donc, les annonces ne sont diffusées que lorsque l'appel se trouve sur la destination de débordement UCD et non pour l'ensemble du cycle de sonnerie. Lorsqu'un appel quitte la destination de débordement UCD, la MOH (musique d'attente) par défaut est ouverte.

Pour chaque groupe UCD, le nombre maximum des appels en file d'attente peut être défini individuellement. Si ce nombre est dépassé, les autres appels peuvent être acheminés à une destination de débordement.

Si aucune file d'attente n'est souhaitée, zéro peut être défini comme nombre maximum d'appels en fil d'attente. Les appels non pris sont alors immédiatement acheminés à une destination de débordement.

Correspondances

Sujet	Correspondance
Standard automatique	L'utilisation d'un standard automatique comme destination de débordement n'est pas possible.

14.6.7.1 Comment modifier le débordement UCD

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.
3) Naviguez dans l'arborescence menu sous**Appels entrants** > **UCD** > **…** vers le groupe UCD souhaité.
4) Cliquez sur l'onglet **Modifier le groupe UCD**.
5) Dans le champ **File d'attente**, indiquez le nombre maximum des appels en attente. Les appels qui se situent au-delà sont envoyés vers une destination de débordement.
6) Dans le champ **Temps débordement**, entrez la durée souhaitée. L'indication est fournie en secondes.

   Remarque : ce paramétrage a un intérêt uniquement si une application UCD externe est raccordée. Si un appel en attente n'est pas pris par l'application UCD dans le délai de débordement, l'appel continue à être traité par le système de communication grâce aux indications de la Gestion des appels.
7) Cliquez sur **Appliquer** puis sur **OK**.

14.6.8 Renvoi de nuit UCD

Pour chaque groupe UCD, il est possible de configurer un renvoi de nuit individuel. Chaque agent d'un groupe UCD peut activer et désactiver le renvoi de nuit. Après l'activation, tous les appels pour ce groupe UCD sont acheminés à la destination de nuit.

Vous pouvez définir comme destination du renvoi de nuit par exemple un abonné interne, un autre groupe, une annonce/musique d'attente, la boîte vocale du système de communication ou une destination externe.

Activation / Désactivation

L'activation ou la désactivation du renvoi de nuit UCD peuvent se faire par une touche de fonction programmée à cet effet ou par les entrées de menu correspondantes ou par des indicatifs. Avec l'activation, il faut entrer le numéro de la destination de renvoi de nuit souhaitée.

Informations sur le renvoi de nuit du système de communication, voir Renvoi de nuit.

Correspondances

Sujet	Correspondance
Etat de l'abonné	L'activation du renvoi de nuit UCD ne modifie pas l'état actuel de chaque agent. Il n'y a pas de déconnexion forcée des agents encore connectés.
Renvoi de nuit du système de communication	Le renvoi de nuit UCD et le renvoi de nuit du système de communication peuvent être activés et désactivés indépendamment l'un de l'autre. Exemple : un groupe UCD a été entré comme destination du renvoi de nuit du système de communication. Les appels qui joignent ce groupe UCD par le renvoi de nuit du système de communication restent dans ce groupe UCD, indépendamment d'un renvoi de nuit UCD.

Sujet	Correspondance
Communications en cours	Les communications en cours ne sont pas influencées par l'activation du renvoi de nuit UCD.

14.6.9 Annonces/musique d'attente pour UCD

Il est possible de diffuser aux appelants une musique d´attente (Music On Hold MOH) ou des annonces s'ils ne sont pas mis en relation immédiatement aux agents d'un groupe UCD. La musique d'attente et les annonces peuvent être affectées séparément à chaque groupe UCD.

Les possibilités suivantes sont offertes :

- Musique d'attente (Music On Hold, MoH)

  Il est possible de diffuser aux correspondants en attente une musique provenant de la source intégrée du système de communication. Des fichiers de musique d'attente supplémentaires peuvent être chargés depuis le PC vers le système de communication.

  Informations supplémentaires, voir Musique d'attente
- Annonces

  Il est possible de diffuser aux correspondant en attente des annonces intégrées. Des annonces supplémentaires peuvent être chargés du PC vers le système de communication.

  Informations supplémentaires, voir Annonces

La durée avant le démarrage de l'annonce est paramétrable (**Retard annonce**). Pour supprimer l'annonce, vous pouvez paramétrer la valeur maximum (600 secondes). On suppose que l'appel aura reçu une réponse durant cet intervalle.

14.6.9.1 Comment modifier les annonces/la musique d'attente pour UCD

Avec l'assistant **UCD** vous pouvez configurer des annonces et/ou une musique d'attente pour les groupes UCD.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **UCD**. Le système affiche la liste de tous les groupes UCD possibles.
4) Pour modifier les annonces/la musique d'attente d'un groupe UCD, cliquez dans la ligne du groupe UCD souhaitée sur **Modifier**.
5) Cliquez autant de fois que nécessaire sur **OK&Suivant** pour afficher la fenêtre **Modifier Annonce/débordement**.
6) Sélectionnez le **système d'annonces** du groupe UCD. Vous avez la possibilité de sélectionner une annonce (si configurée) ou la musique

d'attente interne (Music On Hold MOH). Après la sélection d'un système d'annonces, le champ **Retard annonce** apparaît.

7) Dans le champ **Retard annonce** indiquez le temps en secondes durant lequel l'appelant placé dans la file d'attente doit entendre une annonce.
8) Cliquez sur **OK** pour valider les entrées.
9) Si vous souhaitez modifier les annonces / la musique d'attente (MoH) d'un autre groupe UCD, répétez les étapes 4 à8.
10) Cliquez sur **OK&Suivant** puis sur **Terminer**.

14.6.10 Transfert aux groupes UCD

Les groupes UCD peuvent transférer des appels internes et externes. Si un appel n'est pas pris dans un certain délai, il y a un retour d'appel.

Le délai de retour d'appel est défini par la temporisation **Surveillance d'un transfert avant réponse à un groupe UCD**. Le paramètre par défaut est de 300 secondes. Ce réglage peut être modifié par une administrateur avec le profil **Expert** via le **Mode Expert**.

Correspondances

Sujet	Correspondance
Annonces	Des annonces peuvent être diffusées aux communications externes transférées. C'est impossible pour les communications internes.
Délai de retour d'appel	Pour un transfert aux groupes UCD, un autre délai de retour d'appel s'applique que pour un transfert aux abonnés.

14.6.10.1 Comment modifier le délai de retour d'appel pour les communications transférées aux groupes UCD

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configuration de base** > **Système** > **Temporisations**.
4) Sélectionnez pour la temporisation **Surveillance d'un transfert avant réponse à un groupe UCD** le délai de retour d'appel souhaité (paramètre par défaut = 300 secondes). Si la communication n'est pas prise après l'écoulement de ce délai, il y a un retour d'appel.
   a) Dans la liste déroulante **Base**, sélectionnez la base de temps souhaitée.
   b) Dans le champ **Facteur** indiquez la valeur de multiplication de la base de temps.

5) Cliquez sur **Appliquer** puis sur **OK**.

14.6.11 Libération des appels UCD via lignes analogiques

Lorsque les appels UCD arrivant sur des lignes analogiques ne sont pas pris dans un délai déterminé, ces appels sont libérés. Cela empêche le blocage des lignes analogiques.

Le temps de libération est défini par la temporisation **Surveillance appel UCD sur ligne analogique**. Le paramètre par défaut est de 300 secondes. Ce réglage peut être modifié par une administrateur avec le profil **Expert** via le **Mode Expert** (entre 0 et 255 minutes).

14.6.11.1 Comment modifier l'heure de libération des appels UCD via lignes analogiques

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configuration de base** > **Système** > **Temporisations**.
4) Indiquez pour la temporisation **Surveillance appel UCD sur ligne analogique (voir aide)** la durée d'attente souhaitée (réglable de 0 à 255 minutes, paramètre par défaut = 300 secondes). Si l'appel n'a pas été pris durant cet intervalle de temps, il est libéré.
   a) Dans la liste déroulante **Base**, sélectionnez la base de temps souhaitée.
   b) Dans le champ **Facteur** indiquez la valeur de multiplication de la base de temps.
5) Cliquez sur **Appliquer** puis sur **OK**.

15 Routage de l'appel

Le système de communication offre plusieurs possibilités pour affecter une destination souhaitée : discriminations (contrôle de la numérotation), renvois de jour et de nuit, Least Cost Routing et service de gestion des appels. La réalisation des appels d'urgence est possible à partir de toutes les configurations.

15.1 Discriminations (contrôle de la numérotation)

Les discriminations (contrôle de la numérotation) règlent l'accès des abonnés aux connexions externes, éventuellement payantes.

Concepts associés

Configuration des abonnés à la page 403

15.1.1 Groupes de discrimination et classes de service

Il est attribué à chaque abonné un groupe de discrimination qui définit les autorisations dont dispose l'abonné pour les appels entrants et sortants.

Dans le groupe de discrimination, il est défini pour chaque faisceau l'une des classes de service suivantes :

- **Interne**

  L'abonné peut uniquement téléphoner en interne.
- **Appels entrants**

  L'abonné peut uniquement recevoir des appels externes.
- **Liste des numéros autorisés** 1-6

  L'abonné n'est autorisé à composer que les numéros externes définis dans la liste des numéros autorisés. Si aucun numéro n'est inscrit, l'abonné bénéficie de la catégorie Appels entrants uniquement.
- **Liste des numéros interdits** 1-6

  L'abonné n'est pas autorisé à composer les numéros externes définis dans la liste des numéros interdits. Si aucun numéro n'est inscrit, l'abonné bénéficie de la catégorie Accès total au réseau.
- **Réseau**

  L'abonné peut recevoir des communications entrantes et effectuer des appels sortants sans aucune restriction.

Quelques-uns des 15 groupes de discrimination possibles sont prédéfinis pour tous les faisceaux appartenant à la même classe de services et sont qualifiés de pertinents (par ex. groupe de discrimination **International** avec la classe de service **Réseau** ou groupe de discrimination **Entrant** avec la classe de service **Appels entrants**. Les noms de tous les groupes de discrimination peuvent être modifiés par l'administrateur.

Remarque : Par défaut, chaque station appartient à la classe COS 7 ; cela peut être modifié. Chaque ligne appartient

également à la classe COS 7, mais cela n'est pas configurable, de sorte que la classe COS 7 ne doit pas être utilisée et dispose d'un accès illimité à chaque groupe de lignes réseau.

Correspondances

Sujet	Correspondance
Numéros abrégés	Les numéros abrégés centraux peuvent être sélectionnés indépendamment de la catégorie d'accès (discrimination réseau).
LCR	Groupes de discrimination (contrôle de la numérotation) et discrimination LCR sont différents.
Renvoi d'appel	Dans un renvoi d'appel, on tient compte de la classe de discrimination de l'appelant.

15.1.1.1 Comment modifier le nom d'un groupe de discrimination

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Cliquez dans l'arborescence du menu sur **Jour:groupe de discrimination**.

   Remarque : Dans l'arborescence du menu, vous pouvez aussi cliquer sur **Nuit:groupe de discrimination**, cela conduit au même résultat.
4) Dans l'arborescence du menu, cliquez sur le groupe de discrimination souhaité.
5) Cliquez sur l'onglet **Modifier le groupe de discrimination**.
6) Modifiez dans le champ **Groupe de discrimination** le nom du groupe de discrimination.
7) Cliquez sur **Appliquer** puis sur **OK**.

15.1.1.2 Comment modifier les discriminations d'un groupe de discrimination

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.

3) Cliquez dans l'arborescence du menu sur **Jour:groupe de discrimination**.
4) Dans l'arborescence du menu, cliquez sur le groupe de discrimination souhaité.
5) Cliquez sur l'onglet **Modifier le groupe de discrimination**.
6) Pour le mode Jour, pour chaque faisceau utilisé, sélectionnez à partir de la liste déroulante la classe de discrimination souhaitée.
7) Si nécessaire, sélectionnez l'autorisation de **Mise en réseau** pour le mode Jour.
8) Dans l'arborescence du menu, cliquez sur **Nuit:groupe de discrimination**.
9) Dans l'arborescence du menu, cliquez sur le groupe de discrimination traité auparavant.
10) Cliquez sur l'onglet **Modifier le groupe de discrimination**.
11) Sélectionnez maintenant pour le mode Nuit, pour chaque faisceau utilisé, à partir de la liste déroulante, la classe de service souhaitée.
12) Ici aussi, sélectionnez si nécessaire l'autorisation de **Mise en réseau** pour le mode Nuit.
13) Cliquez sur **Appliquer** puis sur **OK**.

15.1.1.3 Comment afficher tous les membres d'un groupe de discrimination

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Cliquez dans l'arborescence du menu sur **Jour:groupe de discrimination**.

Remarque : Dans l'arborescence du menu, vous pouvez aussi cliquer sur **Nuit:groupe de discrimination**, cela conduit au même résultat.

---

4) Dans l'arborescence du menu, cliquez sur le groupe de discrimination souhaité.
5) Cliquez sur l'onglet **Afficher les membres du groupe**. Tous les abonnés auxquels le groupe de discrimination sélectionné est affecté sont présentés avec leur numéro de téléphone et leur nom.

15.1.2 Listes des numéros autorisés et des numéros interdits

Avec les listes des numéros autorisés et des numéros interdits, il est possible de déterminer quels numéros externes les abonnés peuvent composer et quels numéros ils ne peuvent pas.

Les listes des numéros autorisés contiennent les séquences de chiffres autorisées en début de numéro. L'abonné n'est autorisé à composer que les

numéros externes définis dans la liste des numéros autorisés. Bien vérifier que les numéros d'urgence nécessaires figurent bien dans la liste !

Les listes des numéros interdits contiennent les séquences de chiffres interdites en début de numéro. L'abonné n'est pas autorisé à composer les numéros externes définis dans la liste des numéros interdits. Bien vérifier que la liste ne comporte pas de numéros d'urgence !

La **liste des numéros d'urgence** est un cas particulier de la liste des numéros autorisés. L'abonné ne peut composer que les numéros d'urgence figurant dans la liste. Bien vérifier que tous les numéros d'urgence nécessaires figurent bien dans la liste !

Il n'est pas nécessaire d'inscrire les numéros de téléphone complets dans les listes. Par exemple, pour donner l'autorisation aux abonnés de composer tous les numéros 0800xxx (gratuits), il suffit d'inscrire ici `0800`. Comme les listes concernent uniquement les communications externes sortantes, le code d'accès CO n'a pas besoin d'être indiqué dans les numéros inscrits. Le caractère `#` placé en tête dans un numéro interdit empêche de contourner le contrôle de la numérotation pour les téléphones système qui occupent une ligne réseau analogique avec numérotation MF et veulent basculer sur MF en cours de numérotation.

A l'aide d'un **filtre d'analyse**, l'administrateur peut, pour une liste des numéros interdits quelconque, déterminer quels sont les chiffres qui doivent être comparés avec la liste des numéros interdits correspondante. Le système de communication masque la plage de numéros définis avant l'évaluation de la numérotation. L'interdiction des caractères `*` et `#` permet à l'abonné de contourner le contrôle de la numérotation en entrant ces caractères.

Limites de configuration

Caractéristique	Nombre
Liste de numéros autorisés 1 : liste longue, 100 entrées	1
Listes de numéros autorisés 2-6 : courts, 10 entrées	5
Liste de numéros interdits 1 : liste longue, 50 entrées	1
Listes des numéros interdits 2-6 : courts, 10 entrées	5
Longueurs de caractères des entrées de la liste (chiffres 0 - 9 ainsi que les caractères * et #)	26

15.1.2.1 Comment établir une liste des numéros d'urgence

Avec l'assistant **Classe de discrimination** vous pouvez créer une liste des numéros d'urgence pour le groupe de discrimination "Numéros d"urgence".

Conditions préalables

Vous êtes connecté à WBM.

Votre système de communication est raccordé à une ligne réseau.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Classe de discrimination**.
4) Dans le champ de saisie, entrez un numéro d'urgence et cliquez sur **Ajouter**. Le numéro est intégré dans la Liste de numéros d'urgence.
5) Si vous voulez inscrire d'autres numéros de téléphone dans la liste des numéros d'urgence, répétez l'étape précédente.
6) Cliquez plusieurs fois sur **OK&Suivant** et terminez la configuration avec **Terminer**.

15.1.2.2 Comment créer une liste des numéros autorisés et une liste des numéros interdits

Avec l'assistant **Classe de service**, vous pouvez créer une liste des numéros autorisés et une liste des numéros interdits.

Conditions préalables

Vous êtes connecté à WBM.

Votre système de communication est raccordé à une ligne réseau.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs** .
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Classe de service**.
4) Cliquez sur **OK & Suivant**.
5) Dans le champ de saisie, entrez un numéro autorisé sans code d'accès CO et cliquez sur **Ajouter**. Le numéro est intégré dans la liste des numéros autorisés.
6) Si vous voulez inscrire d'autres numéros de téléphone dans la liste des numéros autorisés, répétez l'étape précédente.
7) Cliquez sur **OK & Suivant**.
8) Dans le champ de saisie, entrez un numéro interdit sans code d'accès CO et cliquez sur **Ajouter**. Le numéro est intégré dans la liste des numéros interdits.
9) Si vous voulez inscrire d'autres numéros de téléphone dans la liste des numéros interdits, répétez l'étape précédente.
10) Cliquez plusieurs fois sur **OK & Suivant** et terminez la configuration avec **Terminer**.

15.1.2.3 Comment établir d'autres listes de numéros autorisés

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Classes de discrimination** > **Listes de numéros autorisés**.
4) Dans l'arborescence du menu, cliquez sur la liste de numéros autorisés souhaitée.
5) Cliquez sur l'onglet **Ajouter un numéro**.
6) Indiquez le **numéro** externe sans indicatif de faisceau.
7) Cliquez sur **Appliquer** puis sur **OK**.
8) Si vous souhaitez ajouter d'autres numéros de téléphone, répétez les opérations 6 et 7.
9) Si vous souhaitez configurer d'autres listes de numéros autorisés, répétez les opérations 4 à 7.
10) Dans l'onglet **Afficher la liste**, vous pouvez visualiser tous les numéros de téléphone de la liste des numéros autorisés sélectionnée.

15.1.2.4 Comment établir des listes de numéros interdits

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Classes de discrimination** > **Listes de numéros interdits**.
4) Dans l'arborescence du menu, cliquez sur la liste de numéros interdits souhaitée.
5) Cliquez sur l'onglet **Ajouter un numéro**.
6) Indiquez le **numéro** externe sans indicatif de faisceau.
7) Cliquez sur **Appliquer** puis sur **OK**.
8) Si vous souhaitez ajouter d'autres numéros de téléphone, répétez les opérations 6 et 7.
9) Si vous souhaitez configurer d'autres listes de numéros interdits, répétez les opérations 4 à 7.
10) Dans l'onglet **Afficher la liste**, vous pouvez visualiser tous les numéros de téléphone de la liste des numéros interdits sélectionnée.

15.1.2.5 Comment afficher tous les numéros de téléphone d'une liste des numéros interdits

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Classes de discrimination** > **Listes de numéros interdits**.
4) Dans l'arborescence du menu, cliquez sur la liste des numéros interdits comportant le numéro souhaité.

15.1.2.6 Comment afficher tous les numéros de téléphone d'une liste des numéros autorisés

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Classes de discrimination** > **Listes de numéros autorisés**.
4) Dans l'arborescence du menu, cliquez sur la liste des numéros autorisés comportant le numéro souhaité.

15.1.2.7 Comment modifier le filtre d'analyse pour les numéros interdits

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Classes de discrimination** > **Listes de numéros interdits**.
4) Dans l'arborescence du menu, cliquez sur la liste des numéros interdits comportant le numéro souhaité.
5) Cliquez sur l'onglet **Modifier le filtre d'analyse**.
6) Dans les listes déroulantes **Du chiffre** et **Au chiffre**, sélectionnez une plage de valeurs.

   Il est ainsi possible de configurer une zone à l'intérieur d'un numéro de téléphone. La position de départ de la plage est sélectionnée dans la liste déroulante **Du chiffre**, la position de fin dans **Au chiffre**. .

   La préconfiguration de ce champ avec ***** et **#** sert à bloquer ces caractères car * et # peuvent être utilisés comme caractères "factices" qui ne sont pas évalués par le réseau et contournent ainsi le contrôle de la numérotation.

Lorsque l'on entre * et # dans les numéros interdits, ces caractères n'ont aucune influence et seuls les chiffres sélectionnés sont évalués.

7) Entrez Dans le champ **Caractère** le ou les caractère(s) à masquer.
8) Cliquez sur **Appliquer** puis sur **OK**.

15.1.3 Liste noire

Une liste noire est disponible dans le système OpenScape Business qui permet de bloquer les appels entrants de numéros d'appelant spécifiques (CLI) et d'appels sans numéro d'appelant ou une présentation restreinte du numéro de l'appelant.

La liste noire contient jusqu'à 100 numéros avec un maximum de 25 chiffres, au format canonique (par exemple, +4989) ou au format international (par exemple, 004989). Les caractères supportés sont les chiffres 0 à 9 et le caractère '+'. Le caractère '+' fait référence au préfixe international configuré dans le système. Il doit toujours être entré à la première position. Les fragments de numéro commençant au début du numéro de l'appelant (CLI) sont autorisés. Une vérification logique est effectuée lors de la saisie d'un numéro dans la liste noire. Le numéro est refusé s'il a déjà été saisi ou s'il est couvert par un fragment de numéro.

La vérification des numéros d’appelants est toujours effectuée selon le format international. Les numéros d'appelant sont convertis au format international en fonction des données de routage, s'ils sont transmis dans d'autres formats.

La liste noire s'applique à toutes les liaisons du standard configurées dans le système. Il prend en charge plusieurs fournisseurs de standard/téléphonie avec des indicatifs régionaux différents.

Une entrée du journal d'événement est créée par la liste noire pour chaque appel bloqué.

Dans un réseau OpenScape Business, la liste noire doit être configurée dans chaque nœud connecté aux fournisseurs de standard/téléphonie, respectivement dans les passerelles. Les appels internes au réseau ne sont pas limités par la liste noire.

La liste noire peut être activée/désactivée par l'administrateur système. De plus, un indicateur séparé peut être défini pour le blocage des appels anonymes.

Les entrées du **Journal de service** contiennent des informations sur les numéros d'appels bloqués. Les entrées du journal qui correspondant aux numéros appelés bloqués contiennent le texte d'événement **!BlackListed Call:** (appel mis sur la liste noire). Pour trouver le numéro appelé qui a été bloqué, vous devez vérifier les deux derniers chiffres de l’entrée du journal. Ces chiffres (sous forme hexadécimale) correspondent à la position dans la liste noire qui contient le numéro bloqué. Si ces chiffres sont ff, l'appel bloqué est anonyme.

Correspondances

Les appels avec suppression de la CLI ne sont pas bloqués comme appels anonymes par le système si l'indicateur **Annulation de la suppression du numéro d'appel** est défini dans le système. Le numéro de l'appelant doit être entré clairement dans la liste noire, dans ce cas. L’indicateur **Annulation de la**

suppression du numéro d'appel est désactivé par défaut dans les paramètres d'usine. Il ne peut être activé qu'à l'aide du gestionnaire E.

Entrer des numéros mobiles d'utilisateurs de mobilité dans la liste noire peut affecter la fonctionnalité de mobilité du système. Dans ce cas, l'appel vers le port DISA en mode « Call Through » est bloqué par la liste noire.

15.1.3.1 Comment créer une liste noire pour les appels entrants en Mode expert

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie > Catégories de service.**
3) Cliquez sur **Catégories de service > Liste noire** dans l'arborescence.
4) Cliquez sur l'onglet **Ajouter le numéro d'appel**.
5) Entrez le **Numéro d'appel**.
6) Cliquez sur **Appliquer**, puis sur **OK**.
7) Si vous souhaitez ajouter d'autres numéros de téléphone, répétez les opérations 5 et 6.
8) Les numéros de téléphone ajoutés à la liste noire sont affichés dans l'onglet **Liste d'affichage** sous la zone **Liste noire** ou dans l'arborescence du menu sous **Liste noire** .

   L'administrateur système doit pouvoir bloquer les appelants indésirables de manière permanente.

   - Activez la case à cocher **Bloquer les appels anonymes** dans la zone Appels anonymes pour bloquer un appel entrant anonyme.

     Remarque : Les appels anonymes sont définis comme les appels dont le numéro de l'expéditeur ne sera pas visible par l'utilisateur.

   - Cochez la case**Fonction liste noire activée** dans la zone Liste noire pour bloquer des numéros d'appel spécifiques.

     Remarque : La fonction de liste noire est basée uniquement sur le numéro de l'appelant (initiateur de l'appel) donné par le fournisseur de service.

15.1.3.2 Comment modifier/supprimer tous les numéros de téléphone d'une liste noire

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie > Catégories de service**.
3) Cliquez sur **Catégories de service > Liste noire** dans l'arborescence.
4) Cliquez sur le numéro souhaité dans la liste noire dans l'arborescence.
5) L'administrateur peut modifier ou supprimer l'entrée sélectionnée.

   Pour modifier l'entrée sélectionnée :

   - Cliquez sur l'onglet **Modifier le numéro de poste**.
   - Entrez le numéro à appeler dans le champ **Numéro d'appel**.
   - Cliquez sur **Appliquer**, puis sur OK.

   Pour supprimer l'entrée sélectionnée :

   - Cliquez sur l'onglet **Supprimer le numéro d'appel**.
   - Entrez le numéro à appeler dans le champ **Numéro d'appel**.
   - Cliquez sur **Appliquer**, puis sur OK.
6) L'administrateur système doit pouvoir bloquer les appelants indésirables de manière permanente.

   - Cochez la case **Bloquer les appels anonymes** dans la zone **Appels anonymes** pour bloquer un appel entrant anonyme.

     Remarque : Les appels anonymes sont définis comme les appels dont le numéro de l'expéditeur ne sera pas visible par l'utilisateur.

   - Cochez la case **Fonction liste noire activée** dans la zone **Liste noire** pour bloquer des numéros d'appel spécifiques.

     Remarque : La fonction de liste noire est basée uniquement sur le numéro de l'appelant (initiateur de l'appel) donné par le fournisseur de service.

15.1.3.3 Comment afficher tous les numéros de téléphone d'une liste noire

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie > Catégories de service**.
3) Cliquez sur **Catégories de service > Liste noire** dans l'arborescence.
4) Les numéros de téléphone sont affichés dans l'onglet **Liste noire** dans l'arborescence ou l'onglet **Afficher la Liste** sous la zone **Liste noire**.

15.1.3.4 Comment créer une liste noire pour les appels entrants dans la configuration

Vous pouvez créer une liste noire avec l'assistant **Liste noire pour les appels entrants**.

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Liste noire pour les appels entrants**.
4) Dans le champ de saisie, entrez un numéro d'appel autorisé et cliquez sur **Ajouter**. Le numéro d'appel est ajouté à la liste noire.
5) Cliquez sur OK & Suivant.
6) Si vous voulez inscrire d'autres numéros à la liste noire, répétez les étapes 4 et 5.
7) Si vous souhaitez vraiment effacer un numéro d'appel, cliquez sur **Supprimer**.
8) Cliquez plusieurs fois sur **OK & Suivant** et terminez la configuration avec **Terminer**.

15.1.4 Renvoi de nuit

Durant la nuit, les appels entrants et sortants peuvent être traités de manière différente que durant la journée. Les appels entrants peuvent être dirigés vers une destination de renvoi de nuit et les abonnés internes peuvent avoir d'autres autorisations pour leur téléphone que durant le jour. La commutation de l'ensemble du système du jour vers la nuit est effectuée automatiquement à une heure définie par l'administrateur.

Renvoi de nuit avec programmation temporelle

Renvoi de nuit variable

N'importe quel téléphone peut servir de destination de renvoi de nuit pour autant qu'il possède le groupe de discrimination correspondante pour les appels entrants. Un téléphone qui peut uniquement prendre les appels internes ne peut pas servir de destination de renvoi de nuit. Si la destination de renvoi de nuit a activé un renvoi d'appel, l'appel suit ce renvoi.

Durant la nuit, il peut être affecté à un groupe de discrimination d'autres classe de service que celles affectées durant la journée afin, par ex. de lutter contre l'emploi abusif.

Pour le mode Nuit, vous pouvez en plus définir un autre poste de renvoi que pour le mode Jour. Le poste de renvoi distinct peut être un abonné ou un groupe d'abonnés.

Le système de communication active et désactive le renvoi de nuit conformément à un programme horaire défini par l'administrateur.

Conseil : Dans le renvoi de nuit avec programmation temporelle, la règle définie s'applique à TOUS les abonnés du système de communication. Il existe aussi un changement de catégorie d'accès automatique en fonction du temps, dans ce cadre les abonnés sont formés en groupes (profils).

Le renvoi de nuit variable est activé et désactivé manuellement par un abonné autorisé. Les appels se conforment aux listes des destinations configurées par l'administrateur.

Normalement, le premier abonné du système de communication (numéro d'appel "100") peut activer et désactiver le renvoi de nuit. L'administrateur peut autoriser jusqu'à cinq abonnés à activer ou désactiver le renvoi de nuit.

Renvoi de nuit UCD

Pour chaque groupe UCD, vous pouvez configurer un renvoi de nuit individuel. Celui-ci peut être activé et désactivé indépendamment du renvoi de nuit de l'ensemble du système. Chaque agent d'un groupe UCD peut l'activer et le désactiver. L'état actuel de chaque agent ainsi que les communications en cours ne sont pas affectés. Après activation, tous les appels destinés à ce groupe UCD sont dirigés vers la destination de renvoi de nuit.

Il est possible de sélectionner comme destination de renvoi de nuit un autre groupe UCD, un abonné interne ou une destination externe.

15.1.4.1 Comment attribuer les discriminations relatives au renvoi de nuit manuel

A l'aide de l'assistant **Discriminations** vous attribuez les autorisations aux différents abonnés, qui peuvent ainsi faire basculer leur téléphone du renvoi de jour au renvoi de nuit (et inversement). Le passage du renvoi de jour au renvoi de nuit est commandé par le téléphone, à l'aide d'un indicatif.

Conditions préalables

Vous êtes connecté à WBM. Votre système de communication est raccordé à une ligne réseau.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Classe de discrimination**.
4) Cliquez plusieurs fois sur **OK&Suivant** jusqu'à ce que la fenêtre **Abonnés autorisés pour renvoi de nuit** s'affiche.
5) Sélectionnez l'abonné dans la liste **Abonnés** et cliquez sur **Ajouter**. L'abonné apparaît ensuite dans la liste sous **Abonnés autorisés**.
6) Cliquez sur **OK&Suivant**.
7) Dans la fenêtre **Vue d'ensemble** vous voyez une liste de toutes les discriminations définies.
8) Cliquez sur **Terminer**.

15.1.4.2 Comment effacer les discriminations pour le renvoi de nuit manuel

A l'aide de l'assistant **Discriminations**, vous pouvez effacer la discrimination des abonnés pour le passage du renvoi de jour au renvoi de nuit.

Conditions préalables

Vous êtes connecté à WBM. Votre système de communication est raccordé à une ligne réseau.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Classe de discrimination**.
4) Cliquez plusieurs fois sur **OK&Suivant** jusqu'à ce que la fenêtre **Abonnés autorisés pour renvoi de nuit** s'affiche.
5) Dans la liste **Abonnés autorisés**, sélectionnez l'abonné souhaité (dont vous souhaitez effacer la discrimination) et cliquez sur **Effacer**.
6) Cliquez sur **OK&Suivant**.
7) Dans la fenêtre **Vue d'ensemble** vous voyez une liste de toutes les discriminations définies.
8) Cliquez sur **Terminer**.

15.1.4.3 Comment configurer le renvoi de nuit avec programmation temporelle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Classes de discrimination**.
3) Dans l'arborescence du menu, cliquez sur **Renvoi de nuit automatique** > **Lundi** (lundi est donné en exemple ; tous les jours de la semaine sont possibles).
4) Dans **Modifier zone**, sélectionnez l'une des quatre zones possibles pour laquelle une classe de discrimination définie doit s'appliquer.
5) A l'aide de **Début** et **Fin**, définissez la durée (en heures et minutes) de cette classe de discrimination.
6) Dans **Numéro Nuit**, sélectionnez l'abonné autorisé.

   Dans le champ **Renvoi de nuit auto.**, votre réglage pour la zone concernée est affiché.
7) Cliquez sur **Appliquer**, puis sur **OK**.
   Lorsque le renvoi de nuit est actif, un message **Le système fonctionne actuellement en mode nuit** s'affiche sur la page d'accueil du portail d'administration.

15.1.4.4 Comment configurer un jour spécial pour le renvoi de nuit avec programmation temporelle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Discriminations** > **Jours spéciaux**.
4) A l'aide de **>>** ou **<<**, sélectionnez l'année pour laquelle vous désirez défini un jour férié.
5) A l'aide de **>>** ou **<<**, sélectionnez le mois pour lequel vous désirez défini un jour férié.
6) Dans le calendrier, cliquez sur le jour que vous désirez définir comme jour férié.
7) Dans **Nom**, indiquez la désignation du jour férié.
8) Cliquez sur **Appliquer** puis sur **OK**.

15.1.4.5 Comment effacer un jour spécial pour le renvoi de nuit avec programmation temporelle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Discriminations** > **Renvoi de nuit automatique** > **Jours spéciaux**.
4) Dans **Jour** cliquez sur la corbeille à gauche du jour férié à supprimer.
5) Cliquez sur **Appliquer** puis sur **OK**.

15.1.5 Changement de catégorie d'accès automatique en fonction du temps

En cas de changement automatique de catégorie d'accès en donction du temps, les abonnés sont regroupés par profils d'abonnés qui définissent les catégories d'accès en fonction des intervalles de temps de la semaine. Pour chaque profil d'abonné, il est possible de configurer un calendrier.

Correspondances

Différences entre le changement automatique de catégorie d'accès en fonction du temps et le renvoi de nuit avec programmation temporelle :

- Le changement automatique de catégorie d'accès en fonction du temps s'applique uniquement au fonctionnement de jour et non au renvoi de nuit.
- Atteindre la destination d'appel avec Call Management (gestion des appels) :

  La procédure a lieu à l'aide de Call Management et elle est indépentante du changement automatique de catégorie d'accès en fonction du temps. Il existe des listes d'appel différetes selon le jour et la nuit.
- Dans le renvoi de nuit avec programmation temporelle, il est uniquement possible de faire la distinciton entre le renvoi de jour et le renvoi de nuit, et cela s'applique à TOUS les abonnés.
- Destinations de renvoi distinct

  La destination de renvoi distinct est déterminée uniquement par le renvoi de nuit avec programmation temporelle.
- Groupe d'autorisation :

  Durant la nuit, le groupe de discrimination est en relation constante (configurable) avec l'abonné, le changement de catégorie d'accès automatique en fonction du temps n'a aucune influence sur cela.

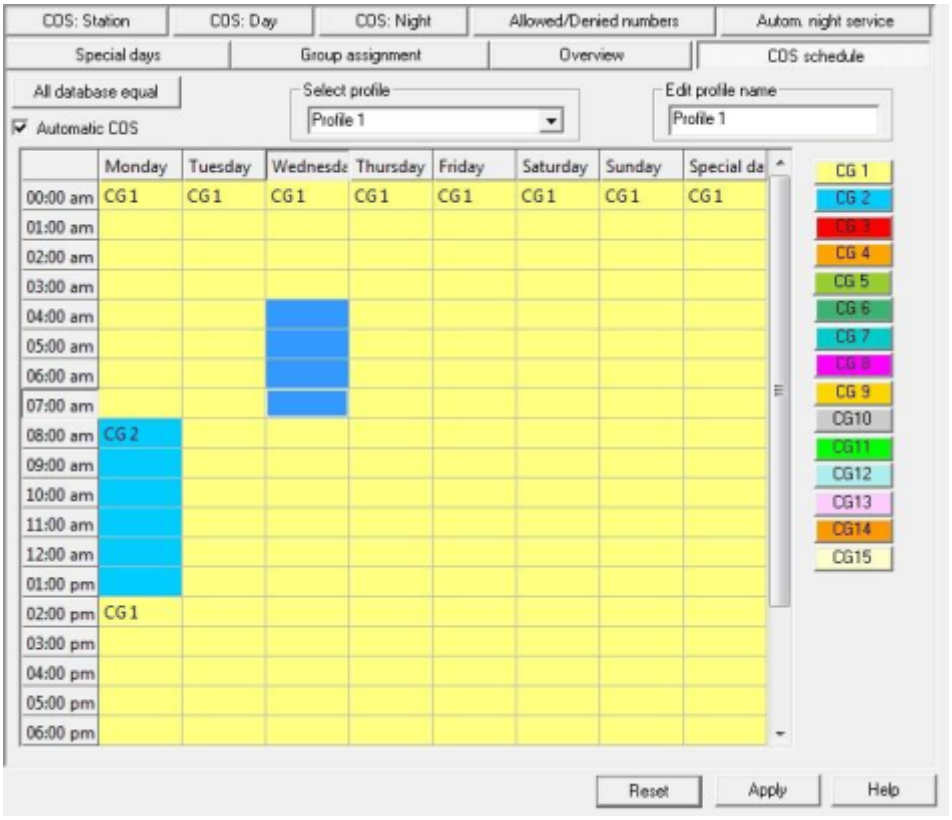
  Durant la journée, le groupe de discrimination peut varier entre plusieurs moments de la journée ou il est également en relation fixe (configurable) avec l'abonné.

Sujet	Correspondances
Renvoi de nuit	La fonctionnalité "Renvoi de nuit" a la priorité sur la fonctionnalité "Changement de catégorie d'accès automatique en fonction du temps". Si le renvoi de nuit est activé, le groupe de discrimination est géré de la manière habituelle et le groupe de discrimination pour la nuit est repris. Le calendirer ne s'applique que durant la journée.
Mise en réseau	Le changement de catégorie d'accès automatique en fonction du temps et la commutation de nuit ne fonctionnent pas au-delà du noeud.

15.1.5.1 Calendrier

Le calendrier sert à gérer les classes de service lors du changement automatique de catégorie d'accès en fonction du temps. Il est possible de configurer jusqu'à huit changements de catégorie d'accès par jour pour chaque jour de la semaine.

Chaque jour commence à 00h00. L'entrée de l'heure de fin dans les différentes colonnes spécifie les fuseaux horaires. Dans l'exemple suivant de calendrier, les changements de catégorie d'accès sont désignées par CG2, CG4 et CG5.



Un abonné peut disposer des différents groupes de discrimination pour le jour et la nuit.

Si, pour l'ensemble du système, le changement de catégorie d'accès automatique pour la jour est défini, l'abonné dispose du groupe de discrimination qui lui est attribué, en fonction du profil et du calendrier. Durant la nuit, l'abonné dispose du groupe de discrimination qui lui était attribué jusqu'ici (par le renvoi de nuit).

Le changement automatique de catégorie d'accès en fonction du temps est désactivé par défaut

Le système de communication supporte un seul fuseau horaire (temps universel). Les groupes d'abonnés qui travaillent dans des fuseaux horaires différents sont placés sur le fuseau horaire du système de communication.

Le calendrier peut uniquement être configuré à l'aide de Manager E.

15.1.6 VBZ (matrice de connexion)

La fonctionnalité VBZ (matrice de connexion) détermine les connexions entre utilisateurs du système de communication. Cette fonctionnalité est par ex. utilisée pour les installations secondaires.

La fonctionnalité VBZ (matrice de connexion) permet également de paramétrer les lignes utilisables par les différents abonnés pour les appels entrants et les appels sortants..

La fonctionnalité VBZ n'a pas d'incidence sur les applications ; elle n'a d'importance que pour la téléphonie. La représentation de l'état Présence, par ex., n'est pas gênée par une restriction d'accès provoquée par la VBZ.

La fonctionnalité Matrice de connexion VBZ est réalisée en deux étapes.

- Créer des groupes de restriction de trafic
- Configurer la matrice VBZ

Conseil : La fonctionnalité Matrice VBZ ne doit pas être utilisée en connexion avec la fonctionnalité UC car cela entraîne des restrictions.

15.1.6.1 Groupes de restriction de trafic (groupes de matrices de connexion)

Les groupes de restriction de trafic (groupes de matrices de connexion) règlent les connexions autorisées et interdites entres les abonnés et les lignes du système de communication.

A l'aide des groupes de restriction de trafic, certains abonnés et certaines lignes peuvent être constitués en groupes.

A l'aide de l'affectation de groupes VBZ, vous affectez aux différentes lignes du système de communication un groupe VBZ. Lors du codage de la matrice de connexion, vous pouvez utiliser ces groupes et déterminer quels abonnés peuvent accéder à quelles lignes.

Par défaut, tous les abonnés et toutes les lignes réseau sont affectés au groupe de restriction de trafic 1. Donc, tous les abonnés ont un accès sans restriction aux autres abonnés ainsi qu'aux lignes, entrantes comme sortantes. La matrice des connexions indique quels sont les groupes de restriction de trafic qui peuvent établir une connexion avec les autres groupes de restriction de trafic et lesquels.

Il est possible de configurer au maximum 64 groupes de restriction de trafic (VBZ).

15.1.6.2 Affectation des numéros KWZ aux groupes de restriction de trafic

A chaque groupe de restriction de trafic correspond une plage de destinations de numéros abrégés centralisés (KWZ). Lorsqu'un abonné sélectionne un numéro abrégé centralisé, le système contrôle s'il est autorisé à le faire en se référant au groupe de restriction de trafic. Si le numéro abrégé centralisé correspond au groupe de numéros abrégés centralisés du groupe de restriction de trafic, la sélection est effectuée, sinon un message d'erreur est diffusé.

Si un abonné sélectionne un numéro abrégé, le groupe VBZ correspondant est déterminé. On détermine ainsi si l'abonné est autorisé ou non à composer ce numéro abrégé. S'il n'a pas l'autorisation, la numérotation est rejetée avec un message d'erreur

Les plages de numéros abrégés peuvent se recouper dans les groupes de matrices de connexion.

Par défaut, toutes les numéros abrégés sont affectés au groupe VBZ 1.

Les plages de numéros abrégés peuvent se recouper dans les groupes de matrices de connexion. Sont par exemple admissibles :

Groupe VBZ	Plage de numéros abrégés centralisés
1	0000-7999
2	0050-0150
3	0200-0500

Il n'est toutefois pas autorisés d'inscrire dans un groupe de restriction de trafic, à la place d'une plage de numéros, des numéros individuels ou plusieurs plages de numéros. Ne sont pas admissibles, par exemple :

Groupe VBZ	Plage de numéros abrégés centralisés
1	0000, 0005, 0010
2	0050-0100, 0300-0500

15.1.6.3 Comment affecter une ligne à un groupe de restriction de trafic

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Discriminations** > **Affectation à un groupe de restriction de trafic** > **Affectation à un groupe de restriction de trafic**.
4) Pour la ligne figurant dans la colonne **Abonnés**, sélectionnez dans la liste déroulante **Groupe** l'entrée correspondant au groupe de restriction de trafic souhaité.
5) Cliquez sur **Appliquer** puis sur **OK**.

15.1.6.4 Comment affecter une ligne à un groupe de restriction de trafic

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Discriminations** > **Affectation à un groupe de restriction de trafic** > **Affectation de la ligne à un groupe de restriction de trafic**.

4) Pour la ligne figurant dans la colonne **Lignes**, sélectionnez dans la liste déroulante **Groupe** l'entrée correspondant au groupe de restriction de trafic souhaité.
5) Cliquez sur **Appliquer** puis sur **OK**.

15.1.6.5 Comment modifier la matrice de connexions

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Discriminations**.
3) Dans l'arborescence du menu, cliquez sur **Discriminations** > **Matrice de connexions**.
4) Modifiez les possibilités de connexion de la manière suivante :
   - Si vous souhaitez bloquer toutes les possibilités de connexion, cliquez sur **Interdire tout**.
   - Si vous souhaitez autoriser toutes les possibilités de connexion, cliquez sur **Autoriser tout**.
   - Si vous souhaitez autoriser uniquement les possibilités de connexion internes aux groupes, cliquez sur **Groupes entres eux**.
   - Si vous souhaitez traiter une possibilité de connexion entre deux groupes de restriction de trafic cliquez dans le champ au croisement de ces groupes de restriction de trafic, dans la matrice de connexions. Cliquez de nouveau dans le champ afin de valider ou de bloquer les possibilités de connexion dans une direction, dans l'autre direction ou dans les deux directions.
5) Cliquez sur **Appliquer** puis sur **OK**.

15.1.7 Code de verrouillage centralisé, changement de catégorie d'accès

Le code de verrouillage centralisé permet un large verrouillage des foncitons téléphoniques par un abonné autorisés (évent. l'administrateur) pour un autre abonné. Seules les fonctionnalités suivantes restent alors disponibles : Appels internes, Numérotation abrégée centralisée et Conférence avec des abonnés internes. L'abonné verrouillé peut désactiver ce code de verrouillage en entrant son code de verrouillage téléphone ou de nouveau l'abonné autorisé.

Le code de verrouillage téléphonique du téléphone pour lequel le code de verrouillage de l'abonné autorisé doit être activé ou désactivé n'est pas nécessaire pour un blocage.

L'abonné autorisé est par défaut l'abonné qui porte le numéro de téléphone "100" (reconfiguré).

15.1.8 Code de verrouillage individuel (verrouiller le téléphone)

Le code de verrouillage individuel du téléphone permet de garantir qu'aucune communication externe ne peut être effectuée depuis cet appareil et que les paramètres utilisateur ne peuvent pas être modifiés.

Malgré le verrouillage du téléphone, il est possible d'émettre des appels d'urgence.

Il reste possible d'effectuer des communications internes.

Les appels entrants peuvent être acheminés vers les abonnés internes.

Lorsqu'un téléphone est verrouillé, les fonctions disponibles sont celles qui ne requièrent pas une numérotation externe. La fonction Numérotation abrégée centralisée (NAC) fait exception à cette règle.

L'abonné entend une tonalité continue (tonalité d'invitation à numéroter spéciale) qui lui rappelle que le téléphone est verrouillé. De plus, le message "Déverrouiller le téléphone" est affiché sur les téléphones avec écran.

Un abonné peut verrouiller et déverrouiller son téléphone à l'aide d'une touche ou d'un indicatif en entrant son code de verrouillage personnel.

Avant la première utilisation du verrouillage du téléphone, il faut configurer le code de verrouillage du téléphone. Le code de verrouillage de téléphone défini pour tous les téléphones est 00000 et peut être modifié individuellement. Pour cela, le téléphone doit être déverrouillé. Le code de verrouillage de téléphone doit toujours comprendre 5 positions. Seuls les chiffres de 0 à 9 sont autorisés. Lorsque l'abonné a oublié le code de verrouillage du téléphone, il est possible de réinitialiser ce code à la valeur par défaut 100 ; pour cela, un abonné autorisé doit intervenir (1er abonné du système dont le numéro est "100" ou administrateur).

15.1.8.1 Comment réinitialiser le code de verrouillage individuel

L'Assistant **Nom et version d'abonné** permet de réinitialiser le code de verrouillage individuel d'un téléphone.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Nom et version d'abonné**. La fenêtre **Configuration du nom et déverrouillage pour les abonnés et groupes** s'affiche.
4) Sélectionnez la case **Réinitialiser le code de verrouillage**.
5) Cliquez sur **OK&Suite** puis sur **Quitter**.

15.1.9 Protection appel PCV par ligne réseau (Brésil uniquement)

La protection appel PCV par ligne réseau permet le déclenchement automatique des appels PCV entrants. Cette fonctionnalité est exclusivement disponible lorsque le pays réglé est le Brésil. Dans tous les autres pays, ce paramétrage est ignoré.

La configuration individuelle pour chaque ligne réseau analogique est possible. La protection appel PCV peut être configurée individuellement pour chaque ligne réseau analogique. Si la fonctionnalité pour une ligne réseau est validée, la boucle est ouverte durant 2 s (valeur par défaut) 1 s (valeur par défaut) après l'acceptation d'un appel entrant. Ainsi, les appels PCV sont supprimés sur le réseau, les autres communications ne sont pas modifiées.

15.1.10 Protection appel PCV par abonné (uniquement pour le Brésil)

Avec la protection appel PCV par abonné, il est possible de paramétrer pour chaque abonné individuellement une protection contre les appels PCV et donc de supprimer automatiquement les appels PCV. Cela vaut également pour le renvoi d'appels, les interceptions, les retours d'appels, etc.

De plus, il existe la possibilité de configurer une protection contre les appels PCV sur l'ensemble du système. Celui-ci est utile lorsque l'appel ne concerne pas un abonné individuel, mais par exemple un groupe de recherche (ou lorsqu'il s'agit d'une erreur de numérotation).

15.2 LCR (Least Cost Routing)

La fonction Acheminement (LCR, Least Cost Routing) gère automatiquement par quelle voie une communication sortante est connectée. La voie empruntée peut être le réseau public, différents opérateurs réseau (ITSP) ou un réseau privé. La voie de connexion la plus appropriée pour la communication est recherchée à l'aide du plan de numérotation, des tables de routage et des règles de numérotation.

Les connexions sont des communications, des liaisons de données analogiques par fax et modem et des communications de données RNIS.

15.2.1 Fonctionnalité LCR

La fonction LCR permet de définir l'opérateur utilisé par ex. pour les communications réseau, les communications par téléphone mobile ou les communications à l'étranger. Vous définissez par le système de communication l'opérateur le plus économique et passez toutes les communications correspondantes par cette route définie.

Si le système trouve dans le plan de numérotation un modèle qui correspond au numéro d'appel composé, il recherche dans les tables de routage un faisceau adéquat (Un faisceau est affecté à chaque ligne. Voir Accès réseau via lignes numériques et analogiques). Le système contrôle si la discrimination LCR correspond bien à l'entrée de la table de routage. La discrimination LCR et la différence par rapport à la classe de discrimination (contrôle de la numérotation) sont décrites dans le chapitre Discrimination LCR.

Ainsi, grâce à la fonctionnalité LCR, il est possible de contrôler l'utilisation des faisceaux ou des lignes par les abonnés du système de communication (afin, par ex., de s'assurer que les fax sont transmis exclusivement par les lignes réseau TDM et non par les lignes ITSP). Il est également contrôlé si l'appelant dispose bien de la classe de discrimination nécessaire selon contrôle de la numérotation pour utiliser le faisceau considéré actuellement par LCR. Ce contrôle pour être désactivé par configuration pour le trafic interautomatique (lignes PABX).

Les chiffres composés sont mis en mémoire temporaire jusqu'à ce que les tables de routage avec les classes de service LCR aient été vérifiées. La communication n'est établie que lorsque cette vérification est achevée, en tenant compte des règles de numérotation. Une tonalité d'invitation à numéroter peut être émise pour signaler à l'abonné qu'il peut composer son numéro.

Lors de la configuration des règles de numérotation, vous pouvez entrer une information pour l'abonné qui effectue la sélectionné afin de lui signaler par ex. que la connexion est établie par le biais d'un fournisseur de services téléphoniques défini (en indiquant le fournisseur) ou que les frais de communication seront élevés. Cette information peut s'afficher à l'écran, être émise sous forme de tonalité ou encore lui être communiquée à la fois par affichage et par une tonalité.

Par principe :

- Si le routage LCR est activé, le contrôle intervient pour chaque numérotation externe. Exception : en cas de sélection d'un indicatif de ligne spécifique ou d'une touche de ligne.
- Si la fonction LCR détermine que la ligne préférentielle ne peut pas utilisée, le système de communication recherche un faisceau alternatif (éventuellement plus coûteux) dans la table de routage.
- Selon le mode d'accès et la table de routage, les chiffres sont transmis individuellement ou en bloc.
- Si la table des numéros SDA et vide, on utilise en remplacement la table des numéros internes. On applique les règles correspondantes pour cette table.

Conseil : Même sur les systèmes de communication avec lignes réseau analogiques (HKZ), il faut configurer un numéro de site (indicatif national / le cas échéant indicatif du réseau local / le cas échéant un numéro de l'installation).

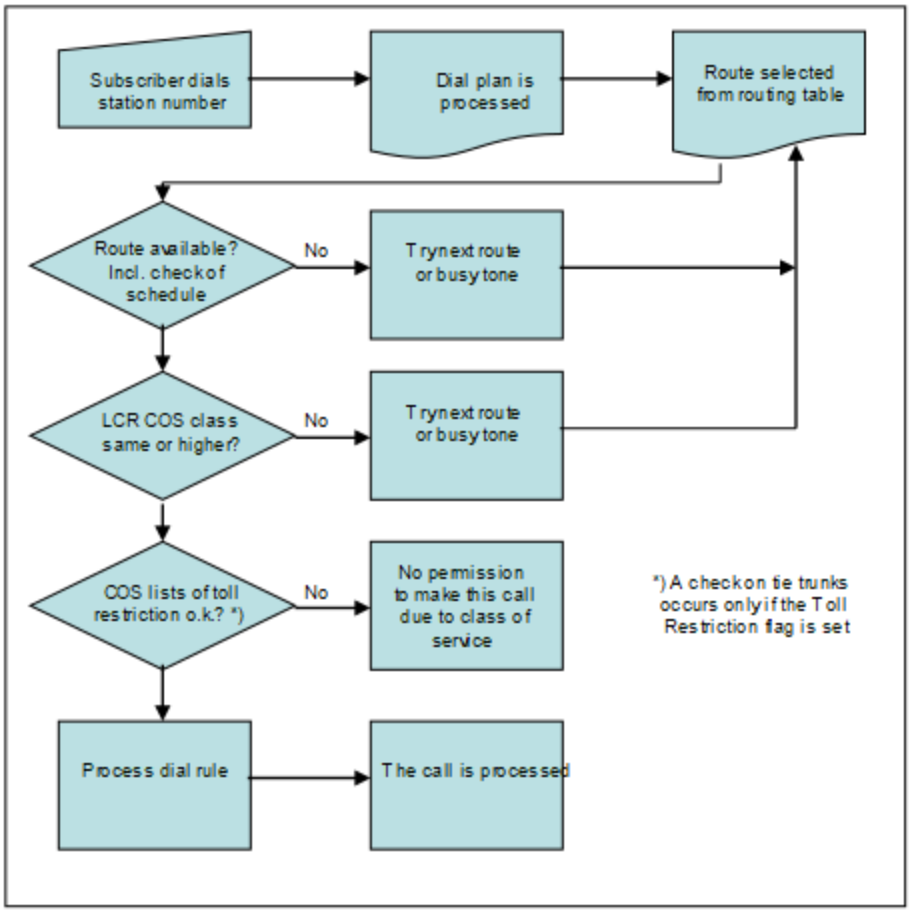
De plus, il faut configurer un numéro SDA ou bien, dans le cas où la table des numéros SDA est vide, un numéro SDA du propre raccordement réseau analogique (HKZ). C'est seulement ainsi que l'on peut garantir l'accessibilité à toutes les destinations externes.

Informations spécifiques du système

Le système de communication évalue au total 24 caractères.

Le système de communication peut gérer jusqu'à 1000 plans de numérotation et 254 tables de routage, avec chacune 15 entrées.

Organigramme LCR



Emission de la numérotation

Il existe deux types de transmission de la numérotation : la transmission par chevauchement ou par blocs. En mode chevauchement, chaque chiffre est émis et traité directement après la sélection. (Condition : l'évaluation LCR est complète, c.-à-d. l'entrée du plan de numérotation a été identifiée de manière univoque et les discriminations ont été contrôlées). En mode numérotation par blocs, des blocs de chiffres sont constitués et envoyés (c.-à-d. que la prise de ligne et la sélection interviennent de manière temporisée ou lorsque l'identification explicite de fin de sélection est disponible.

L'émission de la numérotation pour les faisceaux ITSP doit toujours avoir lieu en blocs. Le paramétrage du faisceau s'applique à l'ensemble de la table de routage.

Etats-Unis uniquement : Carrier Select Override

Carrier Select Override peut être réalisé à l'aide d'une prise de ligne ciblée (indicatif, touche). Dans ce cas, le mécanisme LCR est entièrement contourné.

Correspondances

Sujet	Correspondance
Calendrier	S'il existe dans un système résultant d'une migration de HiPath 3000 une configuration LCR avec calendrier, ces entrées demeurent opérationnelles et peuvent être administrées avec Manager E.
Numérotation abrégée centralisée	Pour garantir le fonctionnement correct des destinations de numérotation abrégée centralisée, le code d'accès LCR doit être entré dans la destination de numérotation abrégée, suivi du numéro de la destination.
Touches nominatives	Les touches nominatives pour destinations externes doivent être programmées avec le code d'accès LCR pour pouvoir fonctionner correctement.
Classe de discrimination (contrôle de la numérotation)	Les classes de service de la restriction d'accès à l'interurbain sont également utilisées pour le routage LCR. Pour les lignes PBX, le contrôle de la numérotation peut être désactivé, la configuration est réalisée à l'aide d'un flag.
Prime Line	Si la "Prise de ligne automatique" (Prime Line) sur le réseau est activée, LCR est impossible. Ces deux fonctionnalités s’excluent l’une l’autre.

15.2.1.1 Comment valider LCR

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Conseil :

Certaines entrées, telles que le préfixe du réseau local ou le numéro de l'abonné, ont déjà été définies dans l'Assistant pendant **l'installation de base**. Ces entrées ne doivent être modifiées manuellement que par des techniciens qualifiés. Une configuration incorrecte du mode LCR risque de rendre impossibles ou de restreindre les connexions sortantes.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l’arborescence de navigation, cliquez sur **Serveur de téléphonie** > **LCR** .
3) Cliquez sur l'onglet **Flags LCR**.
4) Cochez la case **Autoriser LCR**.
5) Cliquez sur **Appliquer** puis sur **OK**.

15.2.2 LCR-Plan de numérotation

Le système recherche dans le plan de numérotation des modèles qui correspondent aux chiffres composés (séquence de numérotation). Le résultat obtenu sert de critère pour la sélection de la table de routage. Dans ce cadre, le système contrôle si la discrimination LCR de l'abonné correspond bien à l'entrée du plan de numérotation.

Le modèle d'une séquence de numérotation est, dans le plan de numérotation, mise en correspondance avec une table de routage qui défini les autres paramètres pour l'établissement de cette connexion.

Le plan de numérotation est divisé en champs individuels destinés à l'identification et à la configuration. Le tableau ci-dessous représente les numéros 4922000 et 1603656260 entrés dans le plan de numérotation.

Champ 1		Champ 2		Champ 3		Champ 4		Champ 5
0	C	492	–	2000				
0	C	160	–	365	–	62	–	60

Les entrées suivantes s'appliquent aux numéros de téléphone :

0 . . . 9	Chiffres autorisés
–	Séparateurs de champs
C	Tonalité d'invitation à numéroter simulée (peut être entrée max. trois fois). Cette entrée est également interprétée comme séparateur de champs.
Signe global	
X	Chiffre quelconque entre 0 et . 9
N	Chiffre quelconque entre 2 et . 9
Z	Un ou plusieurs chiffres suivent jusqu'à la fin de la numérotation

Une séquence de chiffres peut être divisée en 10 champs au maximum.

Less séparateurs de champs permettent de subdiviser la séquence de chiffres en champs individuels pouvant être traités séparément. Exemple : après le premier chiffre composé, un séparateur de champs est ajouté pour qu'un 0 (zéro) composé soit identifié comme champ individuel afin de simuler la discrimination réseau.

La séparation permet de répéter ces champs dans le plan de numérotation ou de les agencer différemment. Les champs délimités par les caractères de séparation "–" et "C" du plan de numérotation peuvent être commandés séparément pour répéter, masquer, échanger ou insérer des chiffres.

Un caractère '#' ou '*' dans la séquence de chiffres composée par l'abonné indique la fin de la numérotation et/ou la commutation du procédé de numérotation. Ces caractères ne sont donc pas des entrées valides dans le plan de numérotation.

Les entrées avec caractères globaux doivent toujours être précédées d'un chiffre univoque pour éviter les conflits entre différentes entrées de caractères globaux.

Dans certains plans de numérotation, l'entrée du code affaire peut être obligée. On applique la procédure de contrôle du code affaire.

Si plusieurs entrées du plan de numérotation correspondent à un séquence de numérotation, celle qui correspond le mieux est utilisée. Exemple : 00894711 a été composé, les entrées de plan de numérotation 0CZ et 0C089Z sont disponibles -> 0C089Z est retenu. La position des entrées dans le plan de numérotation ne joue pas un rôle, il n'est pas nécessaire de disposer d'une entrée "triée".

OpenScape Business est en mesure d'évaluer une séquence de numérotation d'une longueur atteignant 24 caractères.

Entrées LCR lors de la première configuration du système de communication

Lors de la première mise en service du système de communication, des entrée part défaut, spécifiques de chaque pays, sont effectuées dans le plan de numérotation LCR. Jusqu'au plan de numérotation 34, il y a une prédéfinition des entrées côté système pour les appels d'urgence, les renseignements, les numéros spéciaux, les prises de ligne par défaut pour RTC et ITSP, pour UC Suite, activation d'annonce et networking et il est pris en compte la numérotation au format international sur les lignes RNIS. Cette zone peut être influencée par des modifications de configuration à un autre niveau (par ex. modification du flag **Numéro de site**). Il faut donc s'assurer que la prise de ligne réseau par défaut avec modification du numéro de site continue à fonctionner (cela est important pour la numérotation avec des numéros publics).

Conseil : A partir du plan de numérotation 36, les entrées sont librement disponibles.

15.2.2.1 Comment modifier le plan de numérotation

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Cliquez sur **Plan de numérotation**.
4) Les différents plans de numérotation sont listés sous **Modifier le plan de numérotation** et vous pouvez modifier les champs suivants :
   - **Nom**
   - **Chiffres composés**
   - **Table de routage**
   - **Code affaire**
   - **Contrôle de la numérotation**

     Le flag Contrôle de la numérotation se rapporte exclusivement au type de faisceau PABX. Pour le faisceau Réseau, cela n'a pas d'importance

c.-à-d. qu'il n'est pas possible de désactiver à ce niveau le contrôle de la numérotation pour les lignes réseau.

- **Fonctionnement d'urgence**

Remarque : Cliquer sur la flèche bleue à côté du champ **Table de routage** pour ouvrir directement la table de routage correspondante.

---

5) Cliquez sur **Appliquer** puis sur **OK**

15.2.3 Table de routage LCR

Le routage au moindre coût (LCR) est réalisé en recherchant un faisceau adéquat dans les tables de routage (un faisceau est attribué à chaque ligne). Le système contrôle si la discrimination (contrôle de la numérotation) correspond à ce faisceau. La règle de numérotation dépend également de la voie d'acheminement sélectionnée.

La table de routage décrit

- le faisceau affecté à la voie correspondante,
- la règle de numérotation,
- la classe de service LCR requise pour une prise (classe de service COS),
- la possibilité d'avertissement en cas de liaison coûteuse (signal d'avertissement).
- la passerelle dédiée et
- l'ID de noeud de passerelle.

La table est analysée du haut vers le bas, par ordre hiérarchique. Le système vérifie si le faisceau est libre ou si l'abonné dispose de la classe de service LCR requise. Si c'est le cas, la numérotation est exécutée conformément à la règle de numérotation entrée dans la table de routage, à condition que la classe de discrimination (contrôle de la numérotation) et l'affectation VBZ entre abonnés et lignes le permettent.

Si la voie de communication principale de la table de routages est occupée, LCR peut choisir la voie de communication suivante (et éventuellement plus onéreuse) configurée dans le tableau. Cela peut être signalé à l'utilisateur par un signal acoustique et/ou optique.

Il est possible de créer jusqu'à 254 tables de routage de respectivement 16 voies d'acheminement.

Passerelle dédiée

Dans une interconnexion de réseaux, une passerelle dédiée est un noeud partenaire défini de manière fixe (passerelle dédiée -> Forcé). Si une une passerelle dédiée est inscrite avec l'ID de noeud de passerelle pour le faisceau de Networking IP, l'acheminement se fait obligatoirement vers cette passerelle.

Dans une configuration multipasserelle, une passerelle dédiée est déterminéeà l'aide de la configuration des abonnés.

15.2.3.1 Comment modifier les tables de routage

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Cliquez sur **Table de routage**.
4) Toutes les tables de routage s'affichent :
   - **1-Table**
   - **2-Table**
   - **Table nn**

   Conseil : Les tables de routage 1 à 15 sont prévues pour les entrées par défaut ou pour une configuration à l'aide des assistants. Lors d'une migration, les entrées existantes sont automatiquement inscrites dans ces tables de routage.

   Ce mécanisme n'empêche pas toutefois les doublons lors de entrées. Il est recommandé de contrôler ensuite manuellement les tables de routage.
5) Cliquez sur la table de routage de votre choix. La table de routage sélectionnée s'affiche, avec l'onglet **Modifier la table de routage**.
6) Les différentes tables de routage sont listées sous **Modifier la table de routage** et vous pouvez modifier les champs suivants :
   - **Faisceau**
   - **Règle de numérotation**

     Remarque : En cliquant sur la flèche bleue à côté de la règle désirée, vous pouvez visualiser et modifier les propriétés de la règle de numérotation.
   - **Dis. min. (Discrimination LCR)**
   - **Avertissement**
   - **Passerelle dédiée**
   - **ID noeud Passerelle**
7) Cliquez sur **Appliquer** puis sur **OK**.

15.2.4 Classe de service LCR

Une classe de service LCR (Class Of Service, COS) individuelle est attribuée à chaque abonné. Un abonné ne peut utiliser une voie d'acheminement que si sa classe de discrimination est supérieure ou égale à la classe de service LCR figurant dans la table de routage. Par conséquent, un abonné auquel la classe de discrimination 7 a été attribuée ne peut pas utiliser une voie avec la classe de discrimination 8. Par défaut, tous les abonnés sont inscrits avec la discrimination LCR maximale (15).

Correspondances

Sujet	Correspondance
Contrôle de la numérotation	La classe de discrimination (contrôle de la numérotation) a la priorité par rapport à la discrimination LCR. La classe de discrimination (contrôle de la numérotation) peut être activée et désactivée pour les lignes interautomatiques.
Affectation à la matrice de connexions	La sélection n'est effectuée que si la matrice de connexions le permet.

15.2.4.1 Comment attribuer et modifier une classe de service LCR

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Cliquez sur **Classes de service**.
4) Dans **Modifier la classe de discrimination LCR** dans le champ **Classe de discrimination** attribuez une discrimination LCR ou modifiez une classe de discrimination existante.

   Il s'agit en l'occurrence uniquement d'autoriser un abonné à accéder à la classe de service LCR. Le champ n'a pas d'influence sur la discrimination réseau.
5) Cliquez sur **Appliquer** puis sur **OK**.

15.2.5 LCR-Règles de numérotation

Les règles de numérotation LCR permettent de convertir les numéros d'appel entrés en de nouvelles séquences de chiffres aléatoires pour un traitement supplémentaire. La conversion des chiffres permet d'accéder à divers opérateurs. La règle de numérotation utilisée est déterminée par la voie d'acheminement ou le faisceau dans la table de routage.

Informations spécifiques du système

Le système de communication est en mesure de gérer jusqu'à 254 règles de numérotation dans la table des règles de numérotation LCR. Le nom de chaque règle de numérotation est limité à 16 caractères.

Les règles commandent de façon sélective les différents champs du plan de numérotation pour les procédures suivantes :

- Répétition de chiffres
- Suppression de chiffres

- Echange de chiffres
- Ajout de chiffres
- Changement de type de numérotation
- Identification d'une tonalité de numérotation
- Ajout de pauses interchiffres

Règle de numérotation

Vous pouvez définir ici jusqu'à 254 règles de numérotation avec une longueur de 40 caractères maximum.

La table des règles de numérotation LCR est également nommée table de routage.

Définition des règles de numérotation (format de la règle de numérotation)

- A:

  Répéter les champs restants (envoyer). "A" provoque l'émission de tous les champs de chiffres suivants. Le point de référence est le dernier séparateur de champs dans le champ Chiffres composés dans le plan de numérotation.

  Si "A" est inscrit sans référence explicite, cela correspond à tous les chiffres qui suivent le code d'accès, c.-à-d. que "A" correspond à "E2A"
- B:

  Utilisé pour la mise en réseau multi passerelle lorsque le numéro appelé de l'extérieur est du type TON (type de numéro) "unknown" afin d'assurer le routage vers le noeud multi passerelle. Afin que ce numéro de téléphone soit univoque, il est complété en National ou International conformément au type TON dans LCR. Cela est nécessaire lorsque les n° SDA ne sont pas univoques et doivent être configurés au format national ou international.
- D (n) :

  composer une séquence de chiffres (1 à 25 chiffres). "D" peut apparaître plusieurs fois, en un endroit quelconque, dans la chaîne de caractères.
- E (n) :

  Expédition du contenu du champ (1 à 10). "E" peut apparaître plusieurs fois, en un endroit quelconque, dans la chaîne de caractères. La position de "E" par rapport à (n) est libre. Un champ spécifique peut être appelé plusieurs fois, y compris successivement. Exception faite de "E1", "E" peut être encadré par n'importe quels autres paramètres.

  En cas de numérotation par chevauchement (par opposition à la numérotation par blocs), le dernier élément de la règle de numérotation ne doit pas être E(n) mais E(n)A.
- M (n) :

  code d'autorisation (1 à 16). Cette lettre ne doit pas se trouver en dernière position.
- P (n) :

  P (n) peut être présent plus d'une fois dans la séquence et placé dans n'importe quelle position. P (n) peut être entouré par n'importe quel autre paramètre (1 à 60 fois l'unité de pause de l'ensemble du système).
- S:

  Switch, commutation du type de numérotation de DC à DTMF (avec CONNECT, PROGRESS ou CALL PROC avec PI). "S" ne doit apparaître

qu'une seule fois dans la chaîne de caractères, et ne doit pas se trouver en dernière position. Après "S", on ne doit plus utiliser le paramètre "C".

- C:

  "C" ne doit apparaître qu'une seule fois dans la chaîne de caractères. Les caractères suivants sont envoyés sans pause interchiffre et utilisés pour l'accès à l'opérateur pour les modes "Single Stage", "Two Stage", "DICS" et "PRI".

- U:

  utilisation du type de numérotation Adresse SUB. "U" ne doit apparaître qu'une seule fois dans la chaîne de caractères et ne doit pas se trouver en dernière position. Les paramètres "S", "P", "M" et "C" ne doivent pas être utilisés après "U".

- N (N)(uniquement pour les Etats-Unis) :

  groupe SFG de réseau (1 à 5) ou numéro de bande (1).

- L (uniquement pour les Etats-Unis!) :

  "L" ne peut apparaître qu'à la fin de la séquence de caractères. "L" fait que l'appel est traité comme un appel d'urgence.

Exemple :

Le système doit ajouter automatiquement un indicatif de fournisseur d'accès au début de la séquence.

Signification de la règle de numérotation D010xxA : le système compose d'abord l'indicatif du fournisseur d'accès (010xx), puis tous les chiffres après le code d'accès que l'abonné a composés (A).

15.2.5.1 Comment modifier les règles de numérotation

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Cliquez sur **Règle de numérotation**. Toutes les règles de numérotation s'affichent.
4) Cliquez sur la règle de numérotation de votre choix dans l'arborescence.
5) Vous pouvez modifier les champs suivants :
   - **Nom de la règle**
   - **Format de la règle de numérotation**
   - **Procédures de l'opérateur** (**Inconnue**, **Opérateur principal**, **MCL Single Stage**, **MCL Two Stage**, **Réseau d'entreprise**, **Serveur de contrôle de numérotation**, **Interface primaire**)
   - **Type** (**Inconnu**, **Indicatif national**, **Préfixe de réseau local**, **Numéro de l'installation**)
6) Cliquez sur **Appliquer** puis sur **OK**.

15.2.6 Opérateur

Vous pouvez attribuer un opérateur à chaque faisceau. Le choix de l'opérateur est défini par les règles de numérotation LCR (Least Cost Routing/routage au moindre coût).

Inconnu(e)

Aucune indication explicite sur un opérateur.

Opérateur principal

En cas de prise via l'opérateur principal, la sélection simple se fait par numérotation par blocs ou par la sélection de chiffres individuels dans le réseau public.

MCL Single Stage

Avec MCL Single Stage, l'opérateur souhaité est sélectionné à l'aide d'un préfixe puis le numéro est composé. La sélection est effectuée pour le RNIS dans le canal D ou bien sous forme de numérotation normale sur LR.

MCL Two Stage

Avec MCL Two Stage, l'opérateur souhaité est sélectionné à l'aide d'un préfixe. Après une phase de synchronisation, il est tout d'abord envoyé, sous forme de caractères DTMF, le code d'autorisation (également configurable) puis le numéro de destination.

Pour la synchronisation par le temps, une pause comprise entre 2 et 12 s doit être programmée.

Réseau d'entreprise

Un réseau d'entreprise est directement raccordé au système de communication. La fonction LCR détermine à partir du numéro composé par l'abonné la faisceau correspondant et achemine la communication soit via le faisceau du réseau public soit via le faisceau du réseau de l'entreprise.

Serveur Dial-In Control

Dans ce type de LCR, l'opérateur souhaité est sélectionné avec un préfixe à l'aide d'un serveur DICS (Dial-In Control Server) ; le numéro d'appel et un code d'autorisation configurable sont transmis dans la sous-adresse. La sélection est opérée dans le canal D.

Primary Rate Interface (interface primaire) (Seulement pour Etats-Unis)

Avec l'interface primaire, la sélection de l'opérateur ou du Calling Service intervient dans le message de SETUP avec les éléments d'information Network Specific Facility, Operator System Access et Transit Network Selection.

Correspondances

Sujet	Correspondance
Réception/renvoi des informations d'appel	Le masquage, temporaire ou permanent, du numéro d'appel ne doit pas être activé.

Sujet	Correspondance
RNIS/Sous-adressage	La fonctionnalité RNIS "SUB" doit être demandée dans le réseau public ou déjà validée.

15.2.7 Prise ciblée des lignes réseau

Les lignes réseau peuvent être occupées de manière ciblée par les abonnés.

Normalement, la priorisation pour l'indicatif réseau est fixée par Least Cost Routing. Le plus souvent, le fournisseur le plus économique est indiqué en premier, le second en prix est indiqué en second, etc.

Si un abonné souhaite établir une communication via un fournisseur d'accès qui ne figure pas en première place (par ex. parce qu'il est encore plus avantageux pour les liaisons grande distance), il peut le sélectionner en entrant l' indicatif correspondant ou à l'aide d'une touche de ligne.

De la même manière, en procédant à une sélection par indicatif, l'abonné a la possibilité de composer un numéro dont le choix est uniquement possible via le RNIS (cas où le fournisseur est Vodafone, par ex.).

Par défaut, il est programmé un indicatif (88) pour une prise de ligne ciblée via le RNIS. Tous les indicatifs peuvent être définis ou modifiés a posteriori par l'administrateur.

15.2.7.1 Comment configurer l'indicatif pour une prise ciblée de la ligne RNIS

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Cliquez sur **Plan de numérotation**. Les différents plans de numérotation sont listés.
4) Indiquez dans **Nom** le nom que vous souhaitez donner au plan de numérotation.
5) Dans **Chiffres composés**, entrez exactement l'indicatif et les abréviations (par exemple **88CZ**).

Remarque : 88 est l'indicatif attribué par défaut par le système pour la prise ciblée d'une ligne réseau RNIS.

Information sur les abréviations C et Z, voir LCR-Plan de numérotation.

---

6) Dans **table de routage**, entrez **1**.
7) Cliquez sur **Appliquer** puis sur **OK**.

15.2.7.2 Comment afficher les indicatifs pour la prise réseau ciblée

Avec l'assistant **Ligne réseau RNIS / Analogique / ITSP** vous pouvez afficher les indicatifs servant à la prise réseau RNIS ciblée.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Votre système de communication est raccordé à une ligne réseau analogique.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Ligne réseau RNIS/ analogique/ITSP**.
4) Cliquez plusieurs fois sur **OK&Suivant** jusqu'à ce que la fenêtre **Indicatifs pour la prise de ligne réseau ciblée** s'affiche.
5) Par défaut, vous voyez les indicatifs correspondant à la prise réseau RNIS ciblée. Pour les ITSP configurés, les indicatifs correspondants sont présentés.
6) Cliquez sur **OK&Suivant** puis sur **Terminer**.

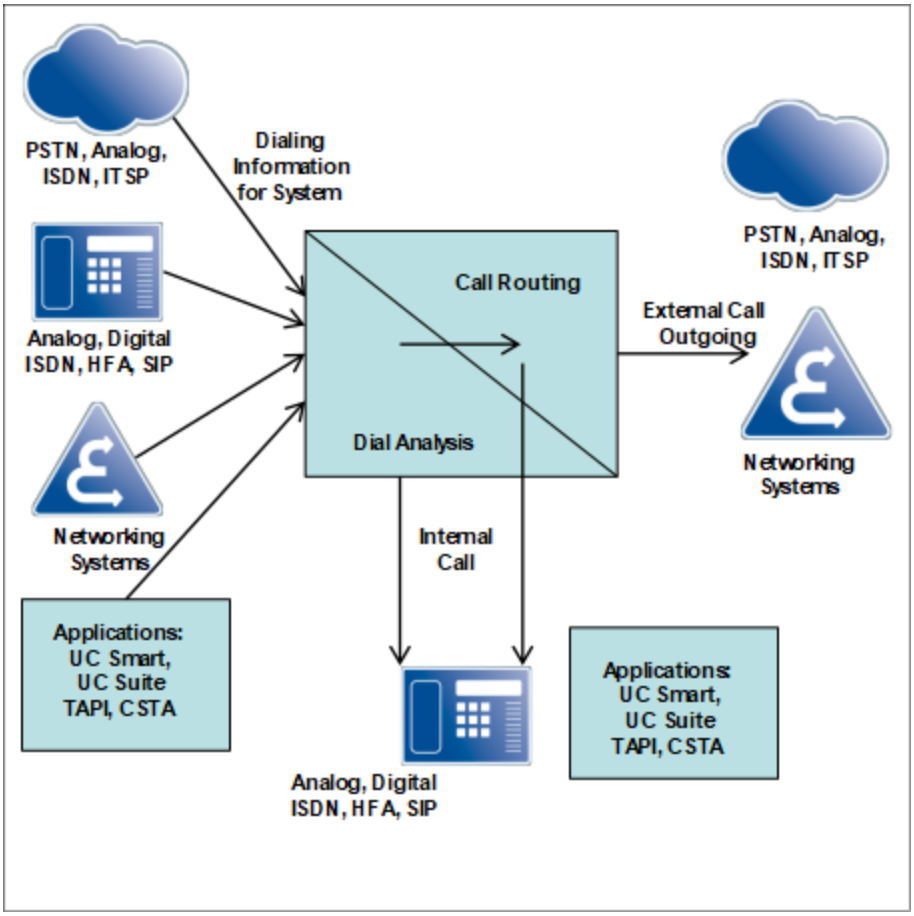
15.3 Evaluation de la numérotation et routage de l'appel

Ce chapitre indique la relation existant entre l'évaluation de la numérotation et le routage de l'appel. Il explique comment le système de communication évalue les numéros de téléphone qui sont composés par les abonnés, lignes et applications diverses pour la sélection d'une destination quelconque et comment se produit le routage une fois l'évaluation de la numérotation achevée. Les fonctions système concernées ici ont déjà pour une grande partie été décrites dans les chapitres précédents. La numérotation à l'aide de numéros de téléphone public à l'intérieur d'un noeud/d'un réseau est décrite de manière détaillée dans cette partie.

L'évaluation de la numérotation

- du système de communication saisie et évalue tous les numéros composés à l'aide des données de configuration
- elle contrôle les discriminations (par ex. sur la base des classe de service des abonnés, des flags d'abonnés, du jour/de la nuit, des numéros autorisés et interdits, des discriminations LCR, des calendriers, des matrices de commutation, etc.)
- elle décide si le numéro de téléphone composé est fourni en interne ou si une ligne doit pour cela être occupée. Cela s'applique à la numérotation de numéros internes, de numéros publics et de numéros internes au réseau.
- elle normalise les numéros de téléphone, c.-à-d. qu'elle rend les numéros sélectionnables pour le système de communication. (par ex., format canonique : "+49nnn" devient "00049nnn", où le premier "0" est l'indicatif d'accès principal du PBX)

- elle abrège si nécessaire les numéros (les premiers chiffres du numéro de destination sont supprimés lors de la prise de ligne entrante afin de déterminer les destinations SDA au format court).



15.3.1 Aperçu du routage d'appel / LCR

Un appel entrant est soumis à différents contrôles dans le système de communication et il est acheminé en conséquence.

Contrôle 1 (destination d'appel interne)

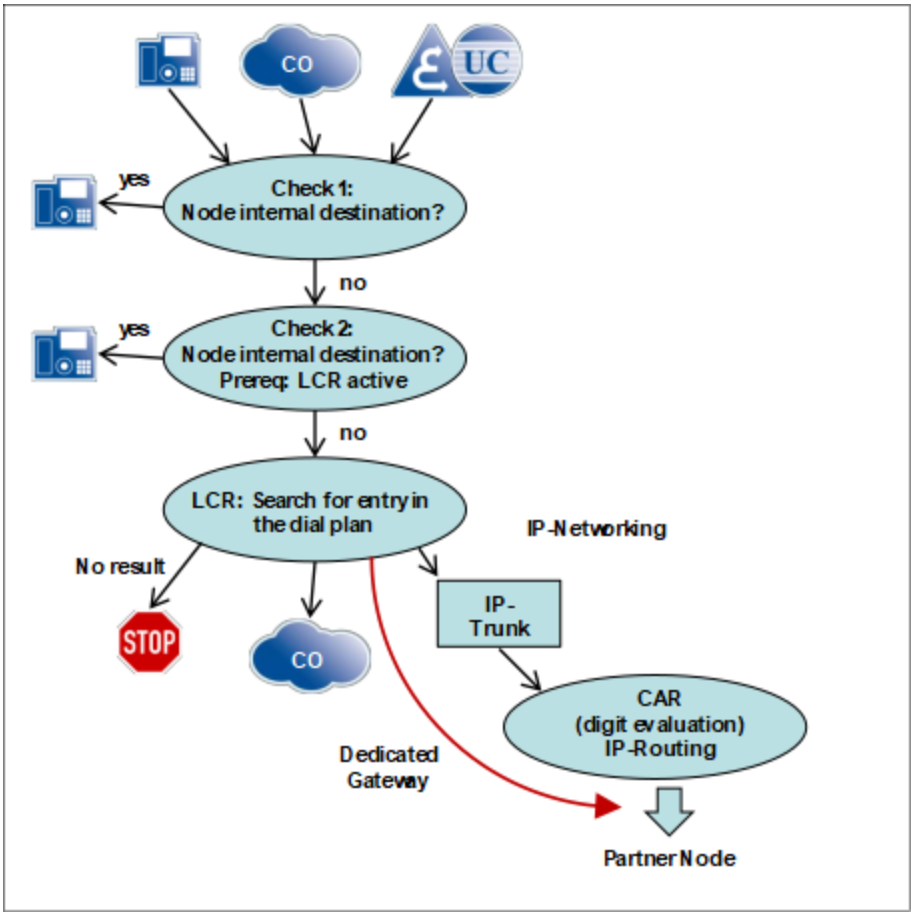
- Les destinations avec numéro canonique sont tout d'abord converties en numéro composables (au niveau de l'interface utilisateur) ou identifiées par TON=International (interface ITSP).
- Les numéros de destination des lignes sont, si nécessaire, raccourcis de la partie du numéro de l'installation correspondant au faisceau.
- Les numéros internes sont évalués à l'aide du plan de numérotation interne, les appels venant de l'extérieur le sont à l'aide du plan de numérotation des numéros SDA.

Contrôle 2 (destination d'appel interne)

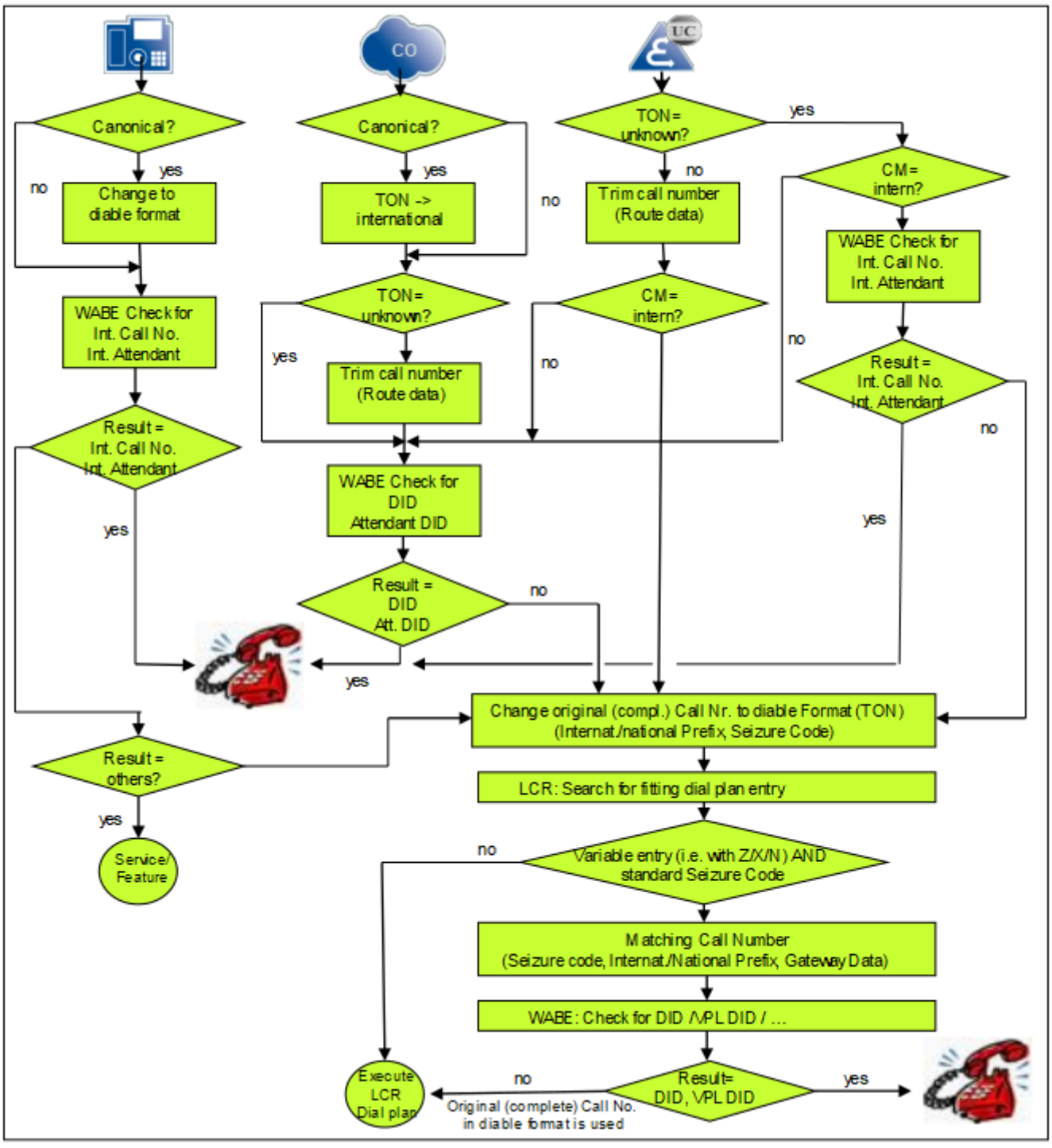
- Les abonnés, applications, clients ou autres systèmes de communication sélectionnent les numéros de destination au format public (par ex. 0 0049nnn)
- Condition : le code d'accès CO par défaut (par ex. "0") est paramétré

- Le numéro de destination est raccourci des parties du numéro de site (site passerelle) et évalué en fonction du plan de numérotation des numéros SDA, indépendamment du fait qu'il s'agit d'un appel interne ou externe.
- Si aucune destination d'appel interne n'a été trouvée, le numéro composable, non raccourci (!) est traité dans LCR et l'appel est routé en conséquence sur une ligne.

A l'intérieur d'un réseau IP, le paramètre "Passerelle dédiée - Dedicated Gateway" de la table de routage LCR permet l'adressage direct d'un noeud pour un numéro sélectionné, en contournant l'évaluation de la numérotation CAR.



15.3.2 Organigramme Evaluation de la numérotation



Explications à propos de l'organigramme

Allemand	Anglais	Explication
WABE		Evaluation de la numérotation

Allemand	Anglais	Explication
CM	CM	Classmark identifie l'appelant en tant qu'appelant externe ou appelant interne (réseau)
TON	TON	Type Of Number Type de numéro: Unknown (inconnu), Subscriber (abonné), National ou International, utilisé aussi bien pour les numéros de destination que pour les numéros d'origine.
SDA	DID (SDA)	Numéro de sélection directe à l'arrivée
TNR RNR	N° d'appel int.	Numéro d'appel interne
Assistant int.	VPL Int	Numéro de poste opérateur pour appels internes
SDA PO	SDA PO	Numéro de poste opérateur pour appels externes
SERVICE	SERVICE	Indicatif de service
LCR	LCR	Least Cost Routing

En ce qui concerne l'évaluation de la numérotation, les clients UC se comportent de la même manière que les abonnés qui sont gérés par CSTA.

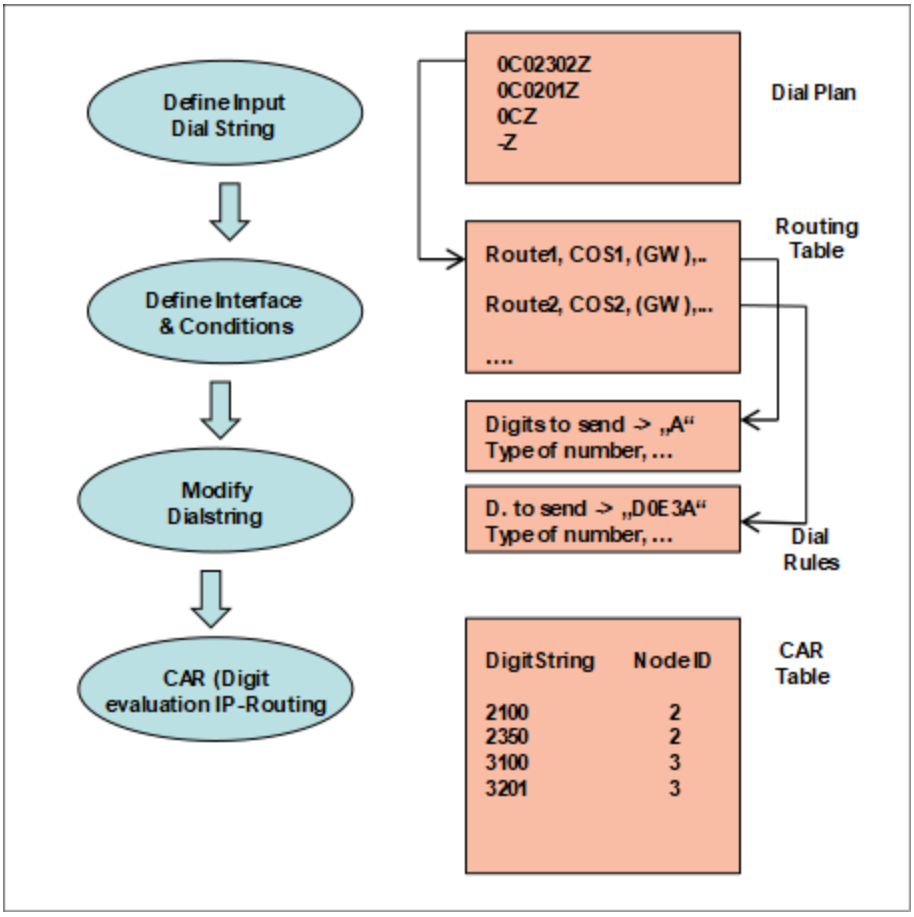
En ce qui concerne l'évaluation de la numérotation, la UC Suite se comporte comme une ligne SIP-Q.

15.3.3 Routage d'appel et LCR en interconnexion de réseaux

Dans la mise en réseau, le routage d'appel et LCR jouent un rôle important. Les appels sont routés à l'aide du plan de numérotation et des règles de numérotation. La passerelle dédiée joue un rôle particulier.

LCR Basics

Entrées LCR lors de la première configuration



Les entrées dans la table de routage (Routing table) sont traitées successivement, en boucle, si aucune prise de ligne réussie n'intervient.

Remarque : -règle z à supprimer dans la configuration des systèmes indépendants.

Lors de la première mise en service du système de communication, différentes entrées par défaut sont consignées dans le plan de numérotation LCR, en fonction du pays. Jusqu'au plan de numérotation 35, il y a une prédéfinition des entrées côté système pour les appels d'urgence, les renseignements, les numéros spéciaux, les prises de ligne par défaut pour RTC et ITSP, l'UC Suite, la mise en réseau et il est pris en compte la numérotation au format international sur les lignes RNIS.

Cette plage peut être influencée par des modifications de configuration (par ex. modification du flag **Numéro de site**). Il faut donc s'assurer que la prise de ligne réseau par défaut avec modification du numéro de site continue à fonctionner (cela est important pour la numérotation avec des numéros publics).

Conseil : A partir du plan de numérotation 36, les entrées sont librement disponibles.

15.3.3.1 Passerelle dédiée

La passerelle dédiée n'est pertinente que pour un réseau IP.

Pourquoi une passerelle dédiée est-elle nécessaire ?

Comment paramétrer de manière durable les destinations, lors de la configuration ?

Cas d'utilisation d'une passerelle dédiée

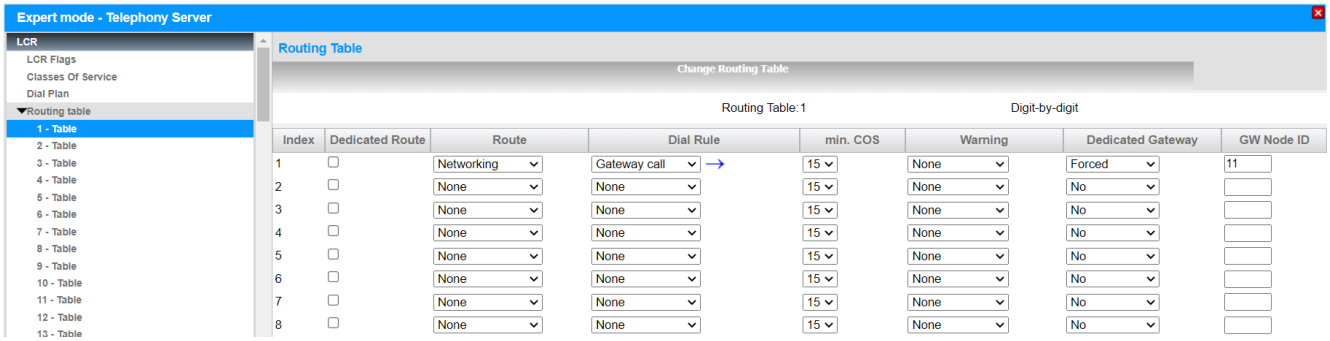
la passerelle dédiée dans WBM

Les valeurs suivantes peuvent être définies :

- La table CAR de chaque système de communication contient des numéros présent dans l'ensemble du réseau, dans les autres noeuds et elle est périodiquement automatiquement actualisée (écrasée) de manière cyclique. Donc les tables CAR ne conviennent pas pour une utilisation durable d'entrées ajoutées manuellement.
- Il est inscrit des numéros valides sur l'ensemble du réseau, donc cela rend impossible un routage individualisé par noeud (par ex. "0" pour le noeud de passerelle correspondant).
- En se servant d'un adressage direct dans LCR
- La Passerelle dédiée s'adresse directement au noeud de destination à l'aide de l'ID de noeud (adresse IP)
- Lorsque l'on utilise la passerelle dédiée, on saute les tables CAR (voir figure précédente).

Adressage direct

- des passerelles TDM pour occuper les lignes réseau ("0CZ")
- des passerelles TDM pour réaliser des éclatements avec des indicatifs séparés
- des noeuds internes au réseau, qui doivent être atteints à l'aide de numéros publics
- des passerelles TDM auxquelles les abonnés d'un réseau multi-passerelle (sur un OpenScape Business S) sont affectés (par ex. Abonné 1 appartient par définition à la passerelle 1 et l'abonné 2 appartient à la passerelle 2).
- des passerelles et appels dont l'origine, à l'intérieur d'une configuration multi-passerelle, NE PEUT PAS être affectée à une passerelle définie (par ex. le groupe fax d'un centre de contacts UC)



N°	L’analyse des numéros d’appel est effectuée à l’aide de la table CAR (pas besoin de renseigner le champ **ID nœud Passerelle**)
Forcé	Est directement acheminé vers la passerelle correspondante (ID noeud Passerelle = n)
Multi-emplacement (Multi Location)	À n’utiliser qu’avec des configurations multipasserelles : Selon la configuration multipasserelle des abonnés OpenScape Business S, le système de communication connaît l’affectation à leur passerelle respective et peut donc ainsi acheminer les appel sortants de manière ciblée en direction de la passerelle concernée. Dans la configuration **multi-emplacement**, l’ID de nœud de passerelle est utilisé uniquement s’il n’est pas possible d’identifier une passerelle par l’affectation des abonnés (par défaut).

15.3.4 Scénarios : évaluation de la numérotation et routage de l'appel

Dans les scénarios, il est décrit les correspondances et les paramètres de configuration nécessaires permettant d'expliquer les différentes déroulements dans le système de communication. Les scénarios représentés peuvent se combiner en fonction du cas d'application.

Système unique

Système en réseau en tant que sous-installation (sans ligne réseau)

Interconnexion de réseaux avec multi-passerelle

1) Abonné A appelle abonnés B via numéro d'appel interne
2) Abonné A appelle abonnés B à l'aide d'un numéro public
3) Abonnés A appelle abonné externe via le réseau
4) Réseau RNIS appelle abonné A
5) Configurations spéciales et conséquences :

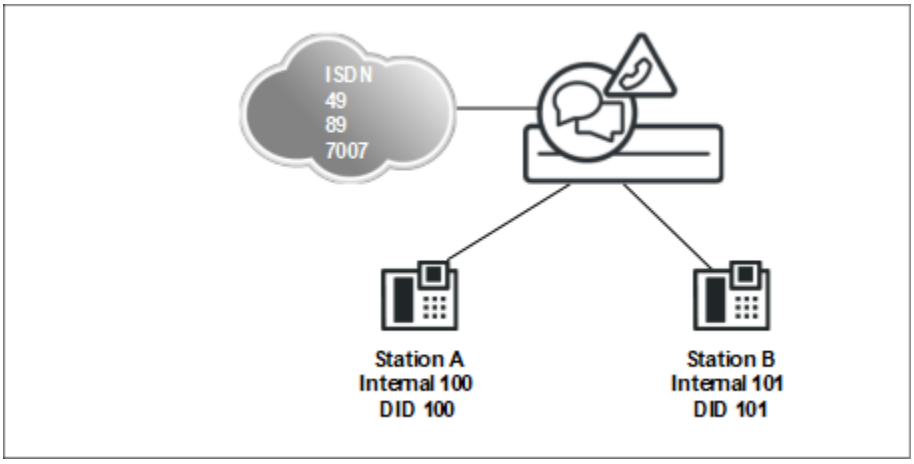
2 lignes réseau

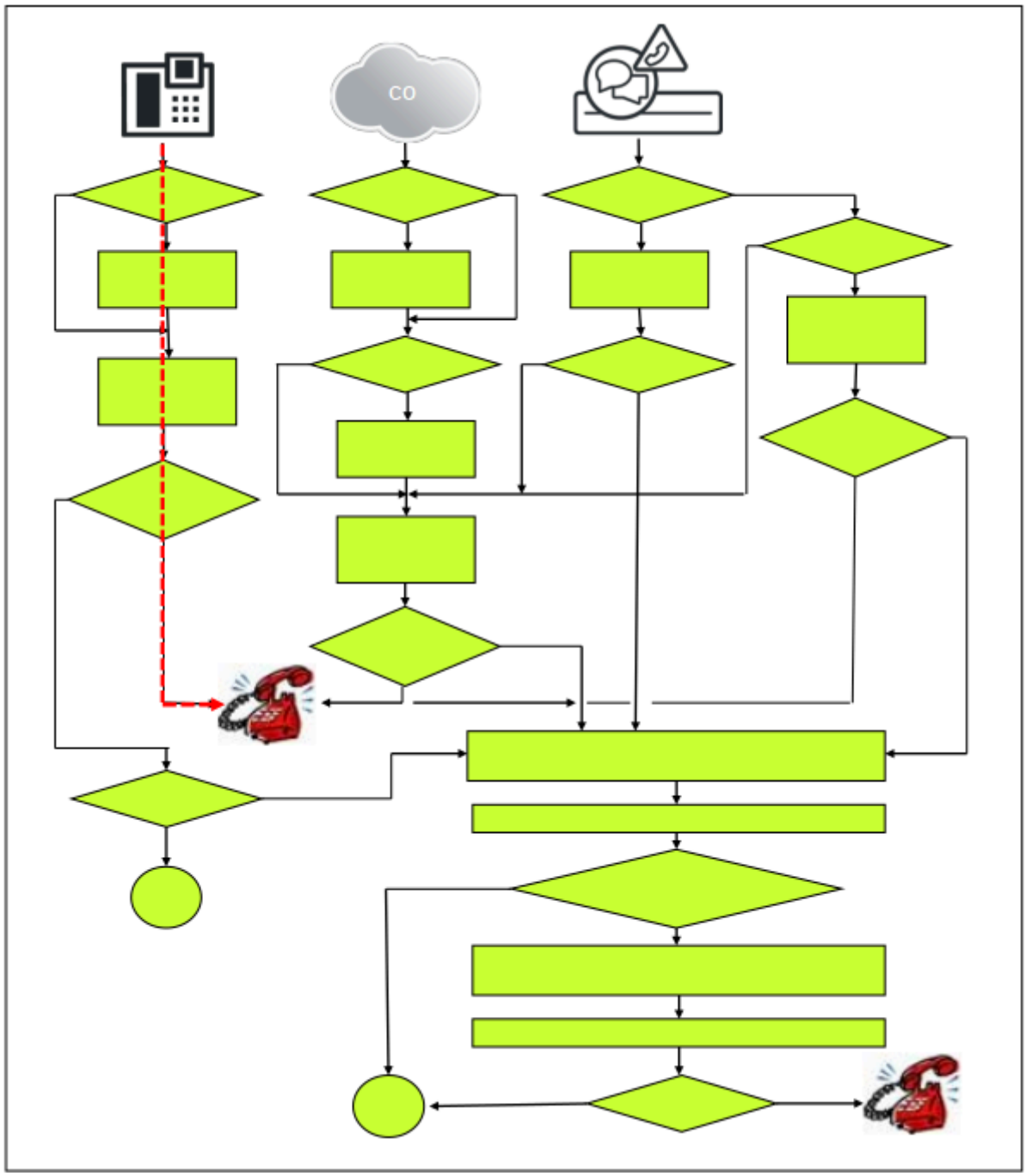
1) Abonné A appelle abonné C via numéro d'appel interne
2) Abonné A appelle abonné C via numéro public d'une interconnexion de réseaux
3) Réseau RNIS appelle abonné C

1) Passerelle 1 réseau RNIS appelle abonné D
2) Abonnés D appelle abonné externe via le réseau

15.3.4.1 Abonné A appelle abonnés B via numéro d'appel interne

Configuration des deux numéros internes



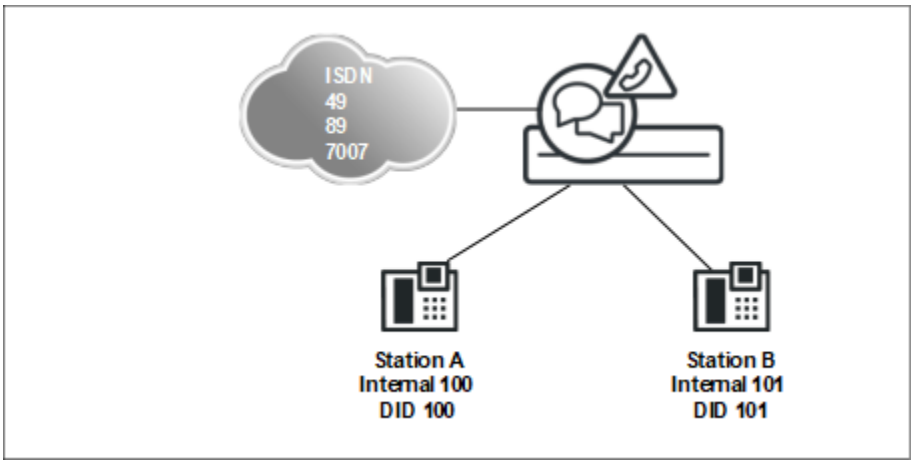


	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

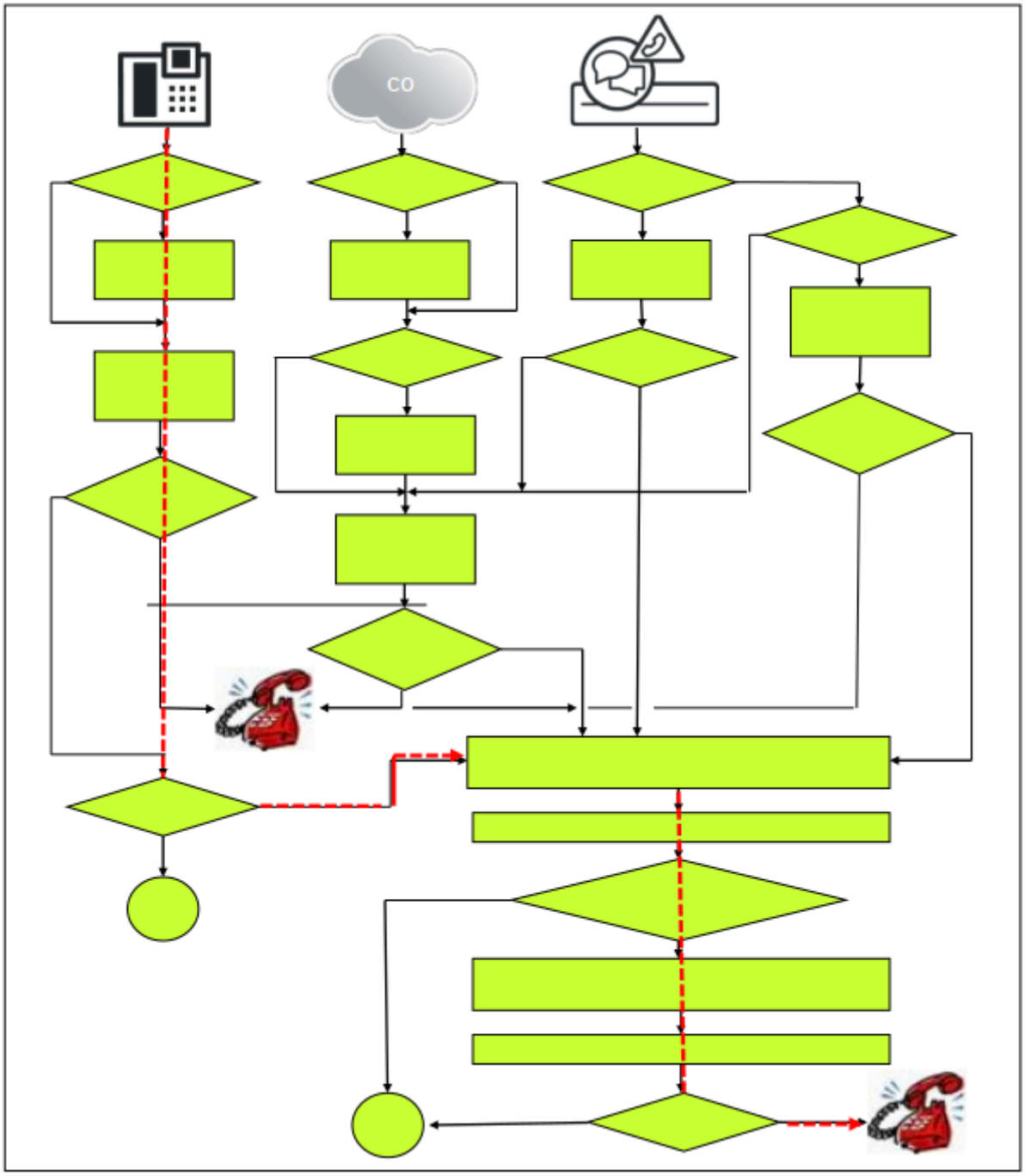
15.3.4.2 Abonné A appelle abonnés B à l'aide d'un numéro public

Configuration

Correspondances du "numéro de site" (Gateway Location)

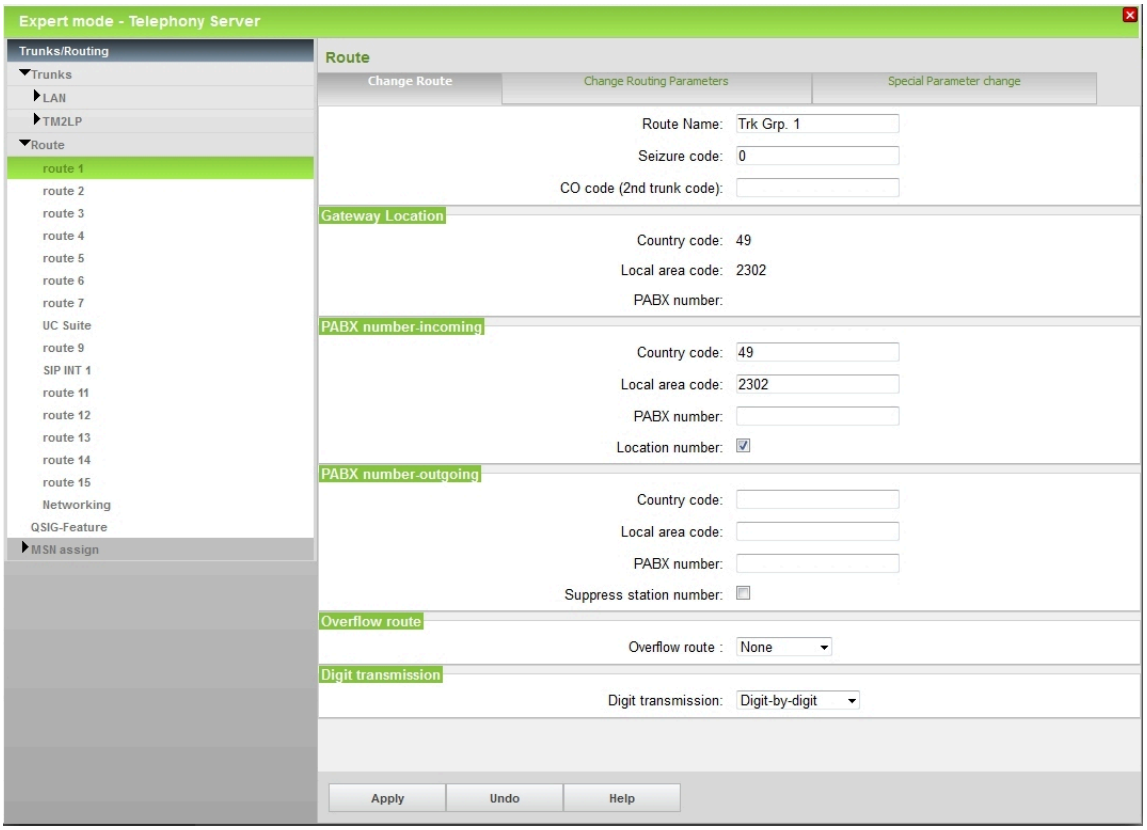


L'appel est acheminé de manière interne au système puisque le numéro de destination est un abonné SDA du propre système.



	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

Une fois que le numéro de destination est détaché à l'aide de Gateway Location, il est recherché, à l'aide du numéro détaché, une destination dans le plan de numérotation SDA.

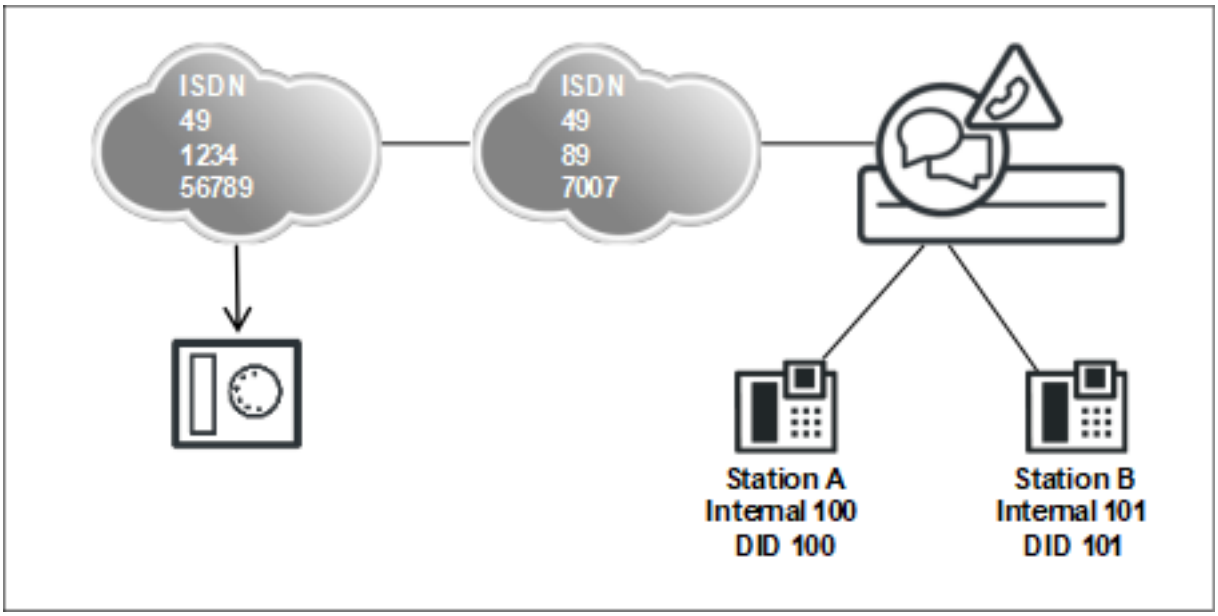


Le numéro de site (Gateway Location) est, lors de la numérotation, évalué à l'aide du numéro public. Si, dans les parties pertinentes, le numéro composé est conforme à ce numéro, la table SDA est évaluée et, en cas de concordance, la destination interne correspondante est appelée (pas de prise de ligne). Lorsque le place le flag Location Numer, les données de site sont automatiquement reprises des données de faisceau correspondantes (PABX-Number incoming) et n'ont pas besoin d'être modifiées dans les scénarios par défaut.

Dans les tables SDA, seuls des numéros valides, correspondant à ce système, peuvent être inscrits car sinon il peut se produire des effets de recouvrement avec des numéros du réseau public. Dans certains cas, il est appelé une destination interne, identifiée par une SDA non valide, alors que l'on souhaite effectuer un appel vers une destination externe, via une ligne.

Les modifications du flag "numéro de site" ont dans certains cas une influence sur les entrées LCR par défaut prédéfinies. Il faut s'assurer que la prise de ligne par défaut continue à fonctionner après modification du numéro de site. Cela est important en cas de sélection de numéros publics.

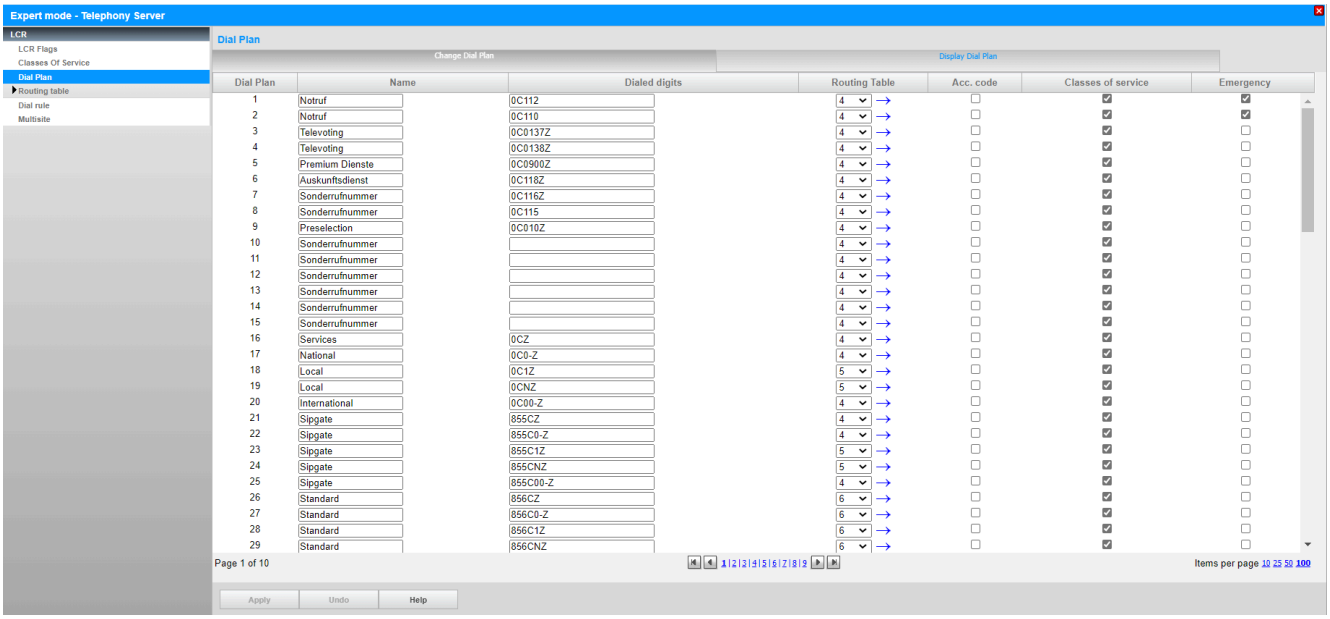
15.3.4.3 Abonnés A appelle abonné externe via le réseau



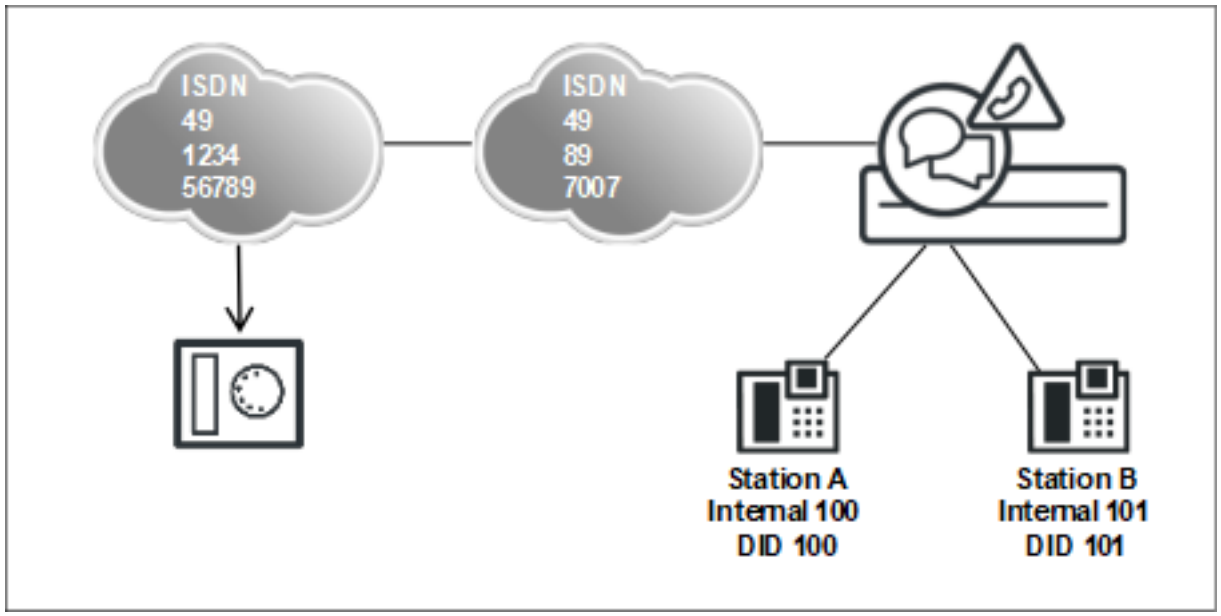
L'appel est acheminé par LCR étant donné que la destination n'est pas dans le propre système de communication.

En plus des données du scénario précédent ""Abonné A appelle abonnés B à l'aide d'un numéro public", il faut disposer dans LCR d'une entrée de plan de numérotation adaptée pour assurer la prise de ligne (par ex. "0CZ").

La table de routage LCR et le plan de numérotation doivent être organisés en conséquence.

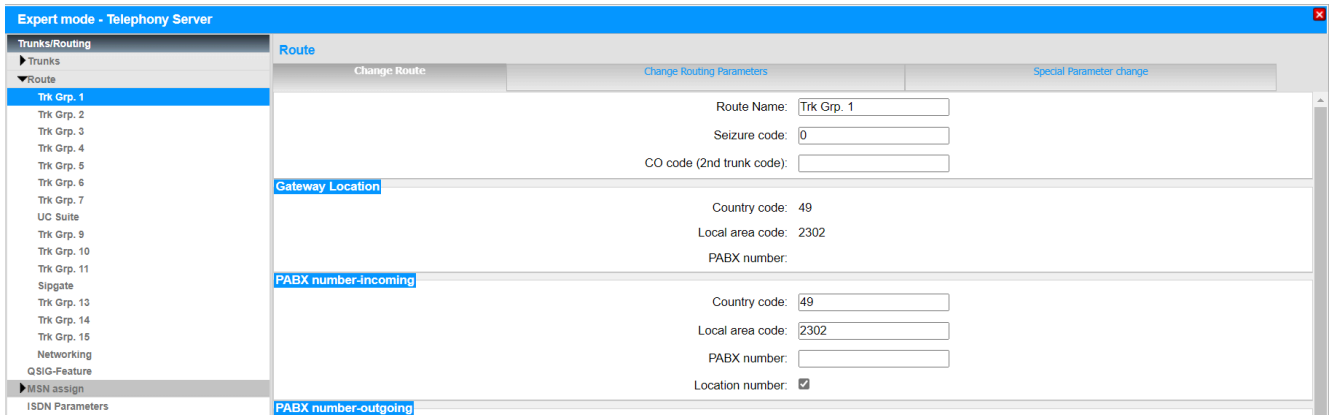


15.3.4.4 Réseau RNIS appelle abonné A



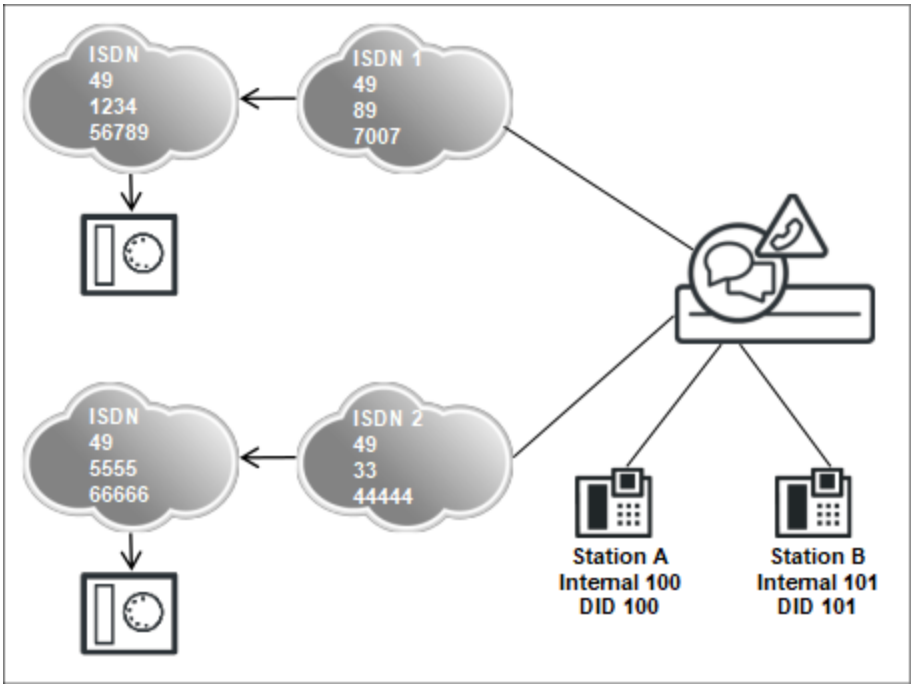
Dans un appel entrant via ligne RNIS, le numéro de destination est détaché à partir des données de configuration du numéro de l'installation entrant (PABX number incoming) du faisceau. Avec la partie restante du numéro de destination (SDA), il est recherché une destination dans le plan de numérotation SDA.

Les paramètres du site de la passerelle ou l'indicateur **Numéro de site** ne jouent aucun rôle dans ce scénario.

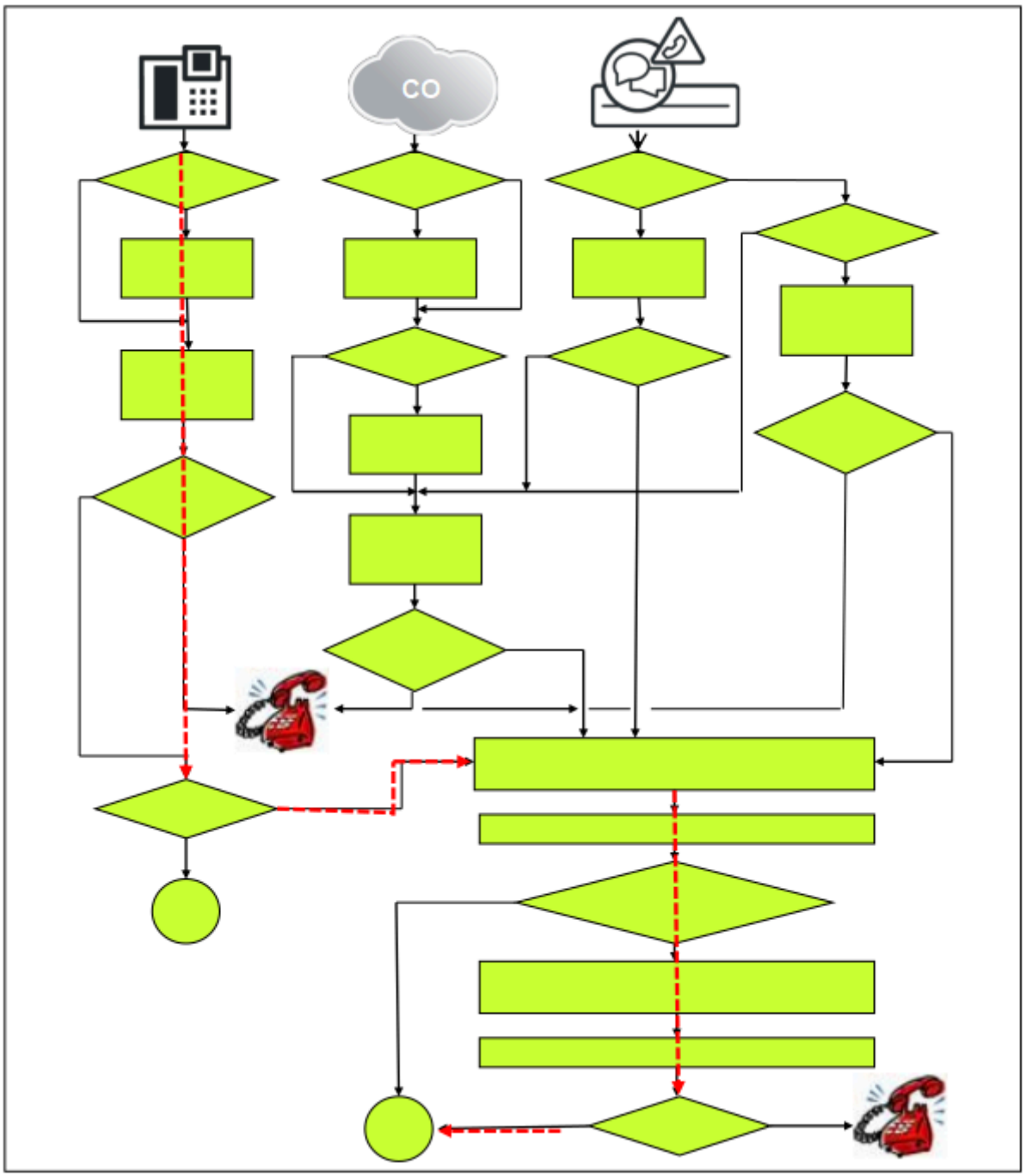


15.3.4.5 Configurations spéciales

Configurations spéciales
et conséquences : 2 lignes réseau



L'abonné A appelle l'abo externe via la connexion réseau 1 ou 2



Exemple :

- Un client souhaite utiliser une connexion standard RNIS 1. Celle-ci est paramétrée comme numéro de site.
- En plus, une seconde connexion RNIS 2 est utilisée pour les applications particulières.

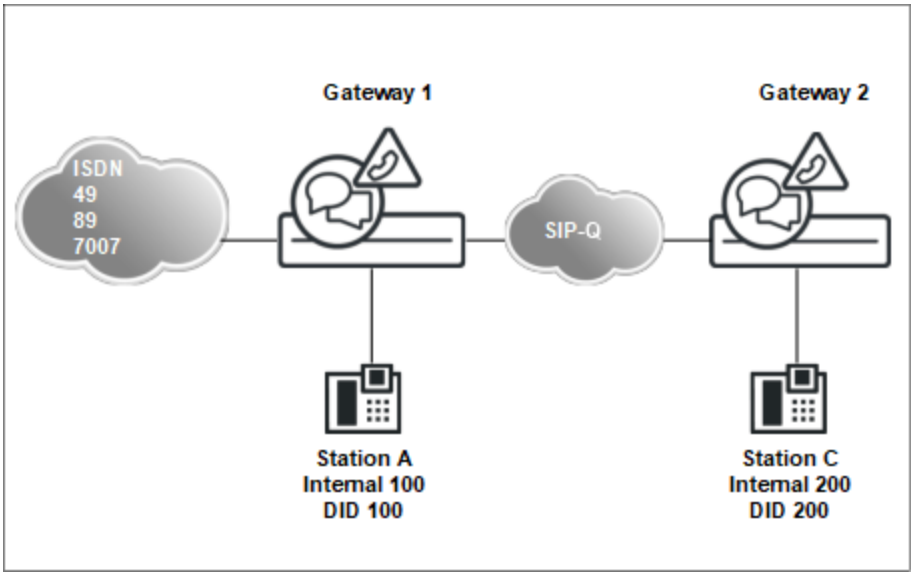
Remarques ou Restrictions :

- Une SEULE ligne réseau (RNIS 1 = site du système) est supportée de manière intégrale, c.-à-d. qu'il n'est pas possible de paramétrer une configuration multiclient (système multisociétés) avec des connexions réseau possédant les mêmes droits.

- La connexion réseau RNIS 2 supplémentaire peut servir aux appels de base (entrant/sortant).
- Dans les scénarios de commutation comples, il n'est pas toujours possible de garantir une représentation correcte du numéro.
- En cas de connexion d'applications, seule le numéro de site est supporté, de même que la sélection de destinations internes avec numéro public.
- La configuration relative au faisceau et à LCR est effectuée comme indiqué dans les exemples précédents.

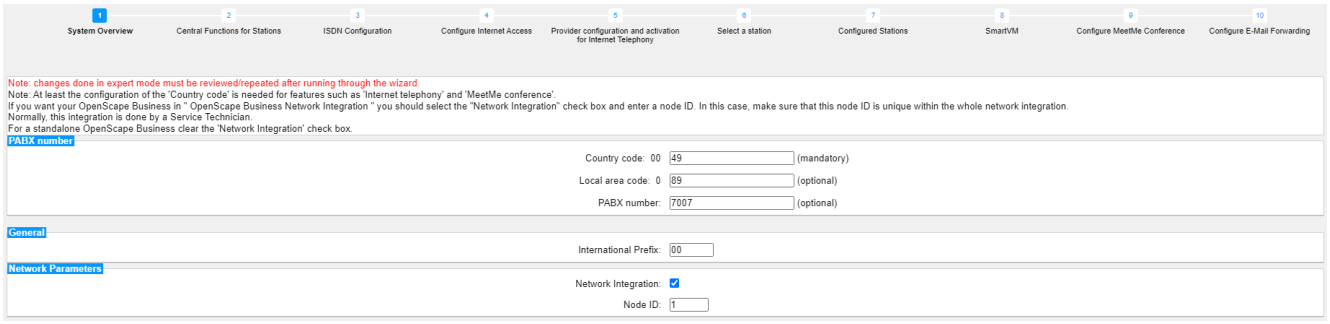
15.3.4.6 Abonné A appelle abonné C via numéro d'appel interne

Système de communication en réseau en tant que sous-installation (sans ligne réseau)



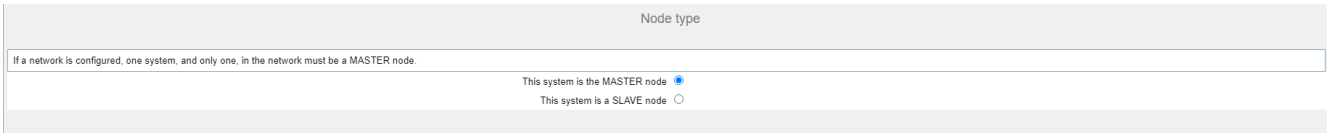
Conditions des systèmes indépendants avant mise en réseau :

- Les deux systèmes de communication ont des adresses IP univoques et sont intégrés dans le réseau IP du client.
- Les deux systèmes de communication peuvent être gérés dans le réseau client avec WBM.
- Dans l'installation de base, il existe un ID de nœud univoque par système de communication pour la mise en réseau (par ex. Système 1 = ID de nœud 1 et système 2 = ID de nœud 2).
- Définition de la numérotation dans l'installation de base des systèmes 1 et 2 : la numérotation des systèmes indépendants (standalone) doit tenir compte de la numérotation fermée de l'interconnexion de réseaux future.
- Cet exemple est basé sur l'hypothèse qu'une numérotation fermée (obligatoire lors de l'utilisation de UC Suite !) est utilisée, configuration à l'aide d'assistant de mise en réseau. Dans une numérotation ouverte (possible avec UC Smart) l'assistant réseau n'est pas utilisé. Il ne l'est pas non plus lors de l'association OpenScape Voice et OpenScape 4000.



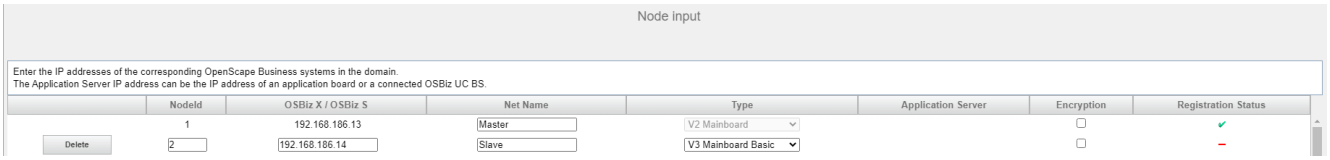
Démarrage de l'assistant réseau dans le système 1. Ce système (ce nœud) est déclaré en tant que maître). Le maître assure différentes fonctions centrales dans l'interconnexion de réseaux (par ex. administration, gestion des licences dans la procédure de licence centrale, CSP sur l'ensemble du réseau).

S'il y a un OpenScape Business S dans l'interconnexion de réseaux, il doit être de préférence désigné comme maître (bande passante, performances).



Les adresses IP sont inscrites par nœud de manière à ce que les systèmes soient indépendants à l'issue de l'administration. Dans **Type** figurent les systèmes OpenScape Business.

Ce dialogue doit aussi être effectué pour le nœud 2 (Esclave).



Une fois la configuration terminée, les deux systèmes (nœuds) synchronisent leurs numéros d'appel et inscrivent les numéros d'appel de l'autre noeud dans la table CAR.

Avec la création des tables CAR, la téléphonie sur l'ensemble du réseau avec les numéros internes est possible. UC Suite est également démarré sur l'ensemble du réseau. Les autres opérations de mise en service complète du réseau figurent dans les autres scénarios.

Le contrôle des entrées CAR est possible avec **Mode Expert** > **Passerelle vocale** > **Mise en réseau** > **Routage**.

Vous trouvez l'aperçu sur la synchronisation automatique dans l'interconnexion des réseaux dans WBM (État Sync).

Les autres nœuds de réseau peuvent maintenant être administrés en accès direct dans la barre de navigation, dans l'option de menu **Mise en réseau**.

15.3.4.7 Abonné A appelle abonné C via numéro public d'une interconnexion de réseaux

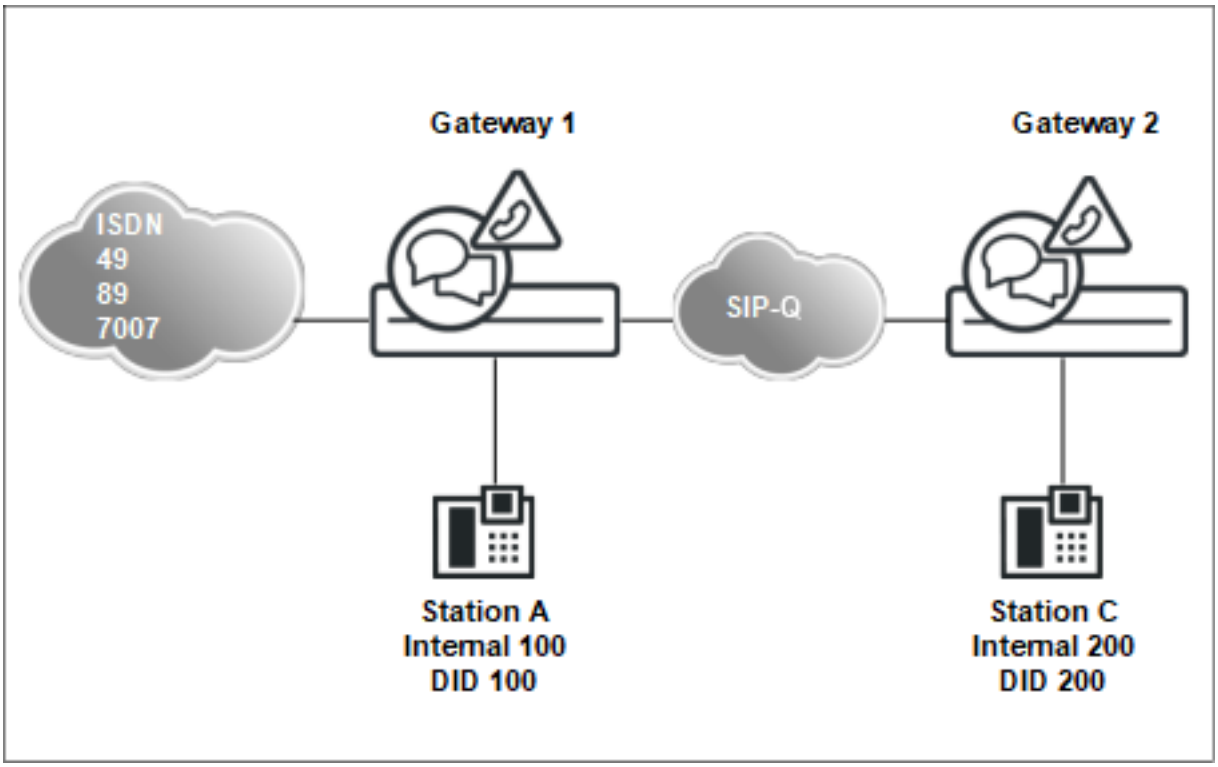
Système de communication en réseau comme sous-installation

Configuration du noeud 1, configuration dans LCR avec passerelle dédiée

Configuration du noeud 2, définition du faisceau "Mise en réseau"

Configuration du noeud 2, définition du numéro de site sur "ligne réseau dummy".

Configuration du nœud 2, configuration dans le LCR avec passerelle dédiée



Particularités de ce scénario

- Le système 1 reconnaît que le numéro de destination ne fait pas partie de son propre système. La recherche est donc effectuée dans LCR. La passerelle dédiée dans le LCR du système 1 doit être utilisée pour l'adressage direct de l'ID de nœud du système 2. Le numéro de destination n'est pas un numéro interne du réseau (il serait alors dans la table CAR), mais un numéro public que l'abonné peut composer en trois longueurs différentes :

  long = 00049897007nnn

  moyen = 00897007nnn

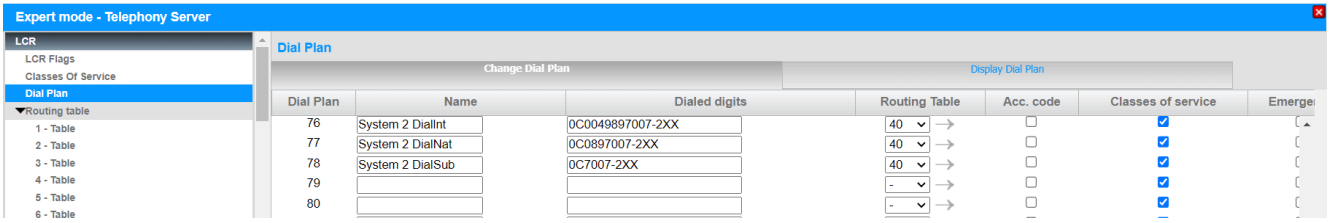
  court = 07007nnn

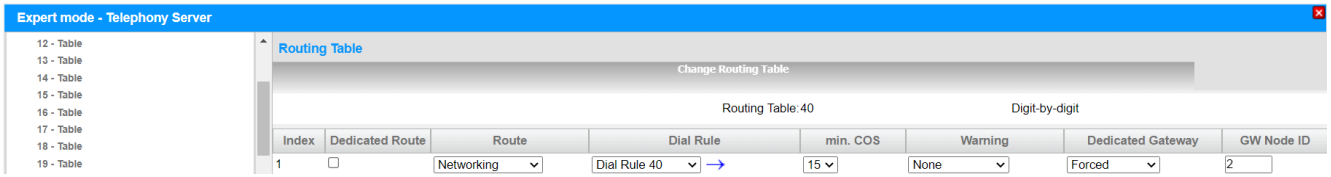
  L'exemple part de l'hypothèse que tous les numéros de sélection directe à l'arrivée 2xx sont des abonnés du système 2.

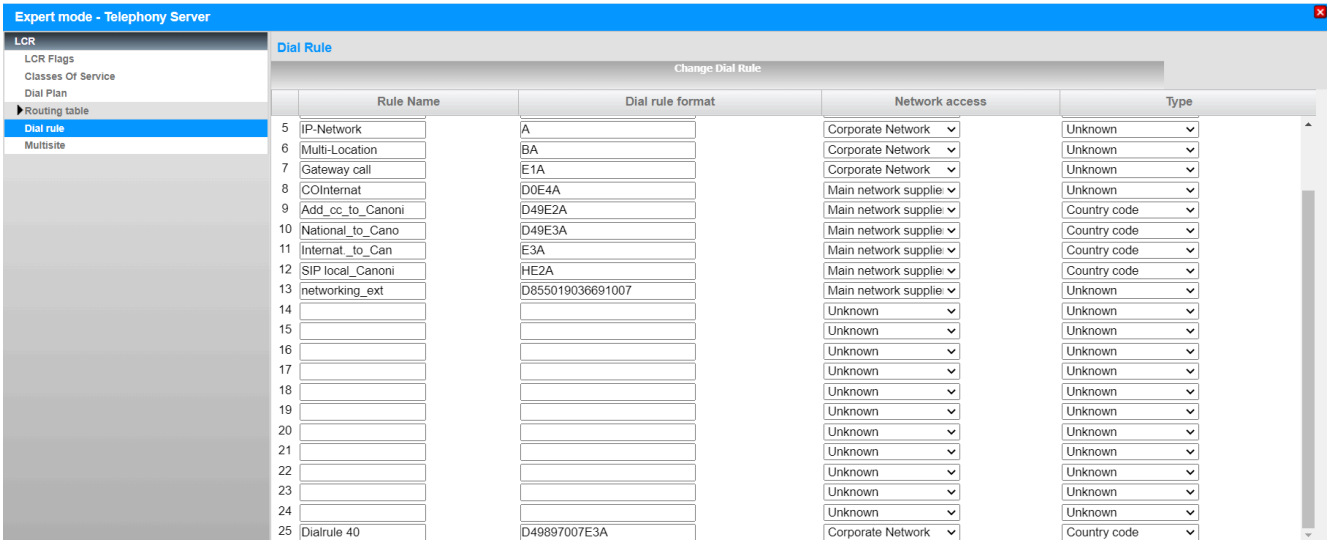
  Remarque : Les entrées du plan de numérotation doivent être configurées de manière suffisamment précise pour que TOUS les numéros trouvés fassent vraiment partie du sous-noeud (interconnexion de réseaux). En fonction des spécificités du plan de numérotation, cela peut

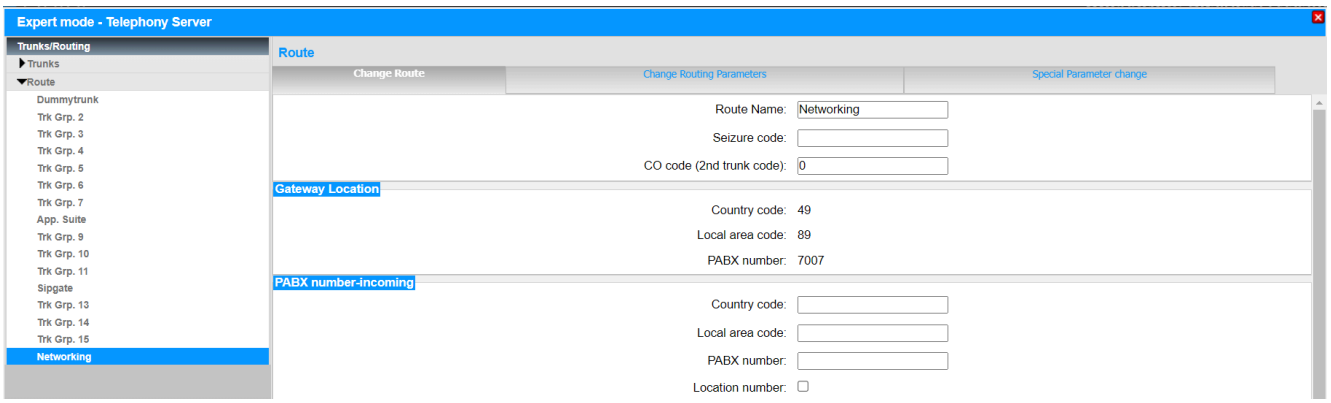
nécessiter un nombre plus grand d'entrées, par ex. en cas de raccordement réseau divisé ou de configuration MSN.

- On inscrit dans le noeud 2 un numéro de site au moyen de la "Ligne réseau dummy" avec les données de site du noeud 1 (passerelle) de manière à ce que le numéro de destination puisse être détaché lors de la numérotation publique avant la recherche d'une destination interne dans le noeud 2.

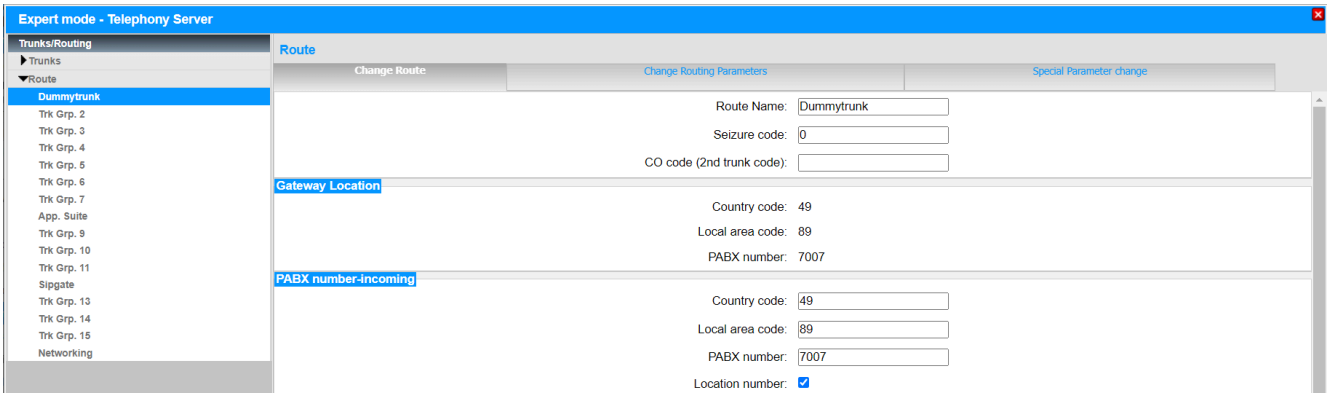








Dans l'onglet **Modifier les paramètres de routage**, définissez le type de faisceau sur **PABX**.



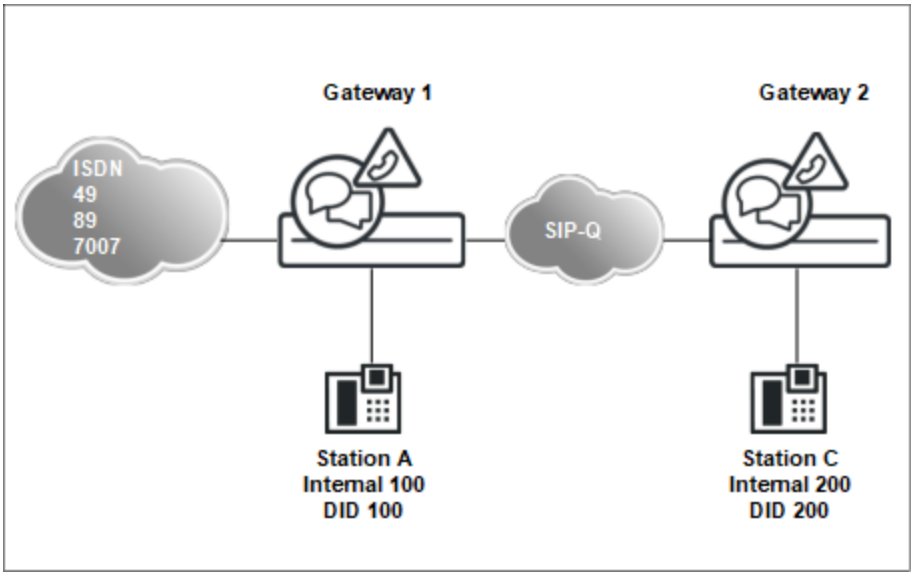
Dans l'onglet **Modifier les paramètres de routage**, définissez le type de faisceau sur **CO**.

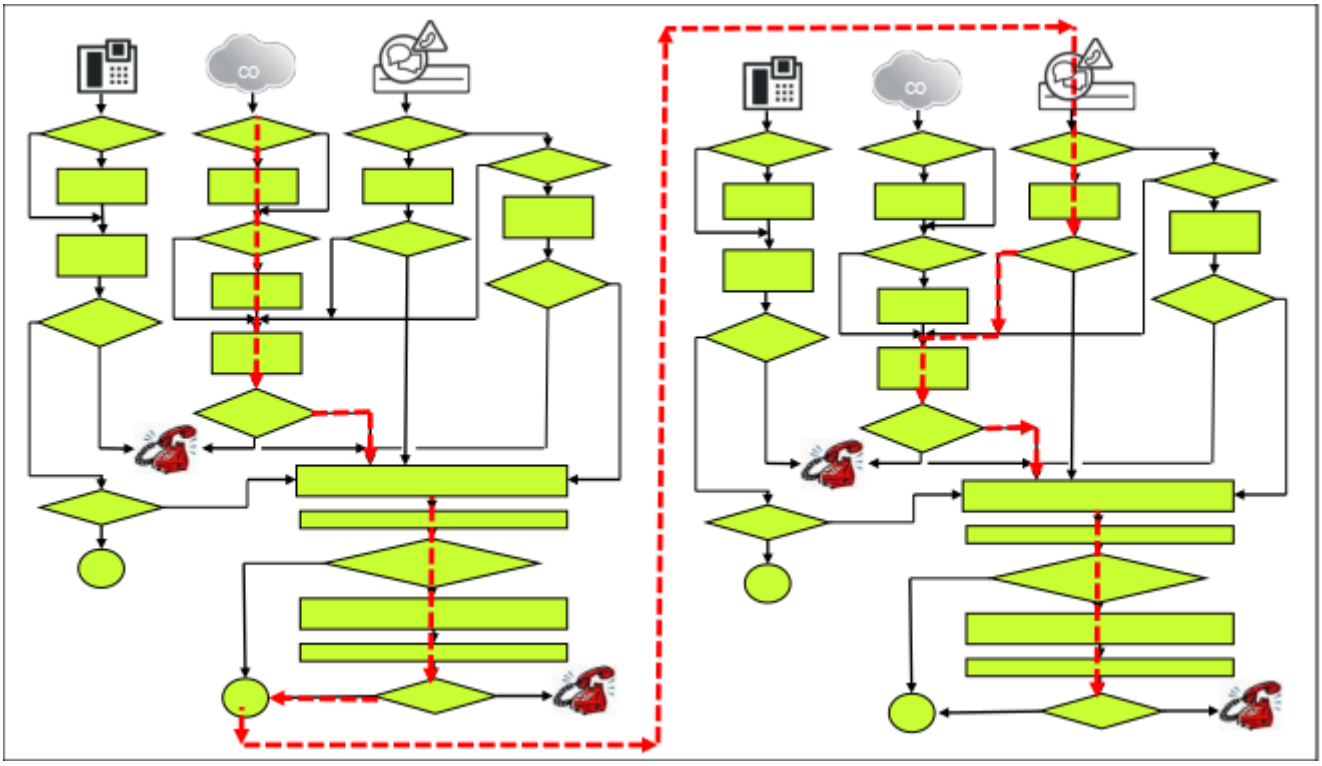
Dans le noeud 2, tous les numéros de téléphone publics, qui ne font pas partie du propre noeud, sont acheminés vers le noeud 1 (sélection par défaut, par ex. 0CZ)

15.3.4.8 RNIS appelle abonnés C

Système en réseau comme sous-installation

Particularités de cette configuration





Exemple : appel entrant avec numéro de destination avec TON = abonné

- Paramétrage du noeud 1 comme indiqué dans le précédent scénario.

  Dans les deux cas, l'adressage du noeud 2 est réalisé avec le numéro de téléphone public, indépendamment du fait que l'origine de la connexion se situe au noeud 1 (abonné du système 1) ou dans le réseau public.

  Conseil : Les entrées du plan de numérotation doivent être configurées de manière suffisamment précise pour que TOUS les numéros trouvés fassent vraiment partie du sous-noeud (interconnexion de réseaux). En fonction des spécificités du plan de numérotation, cela peut nécessiter un nombre plus grand d'entrées, par ex. en cas de raccordement réseau divisé ou de configuration MSN.

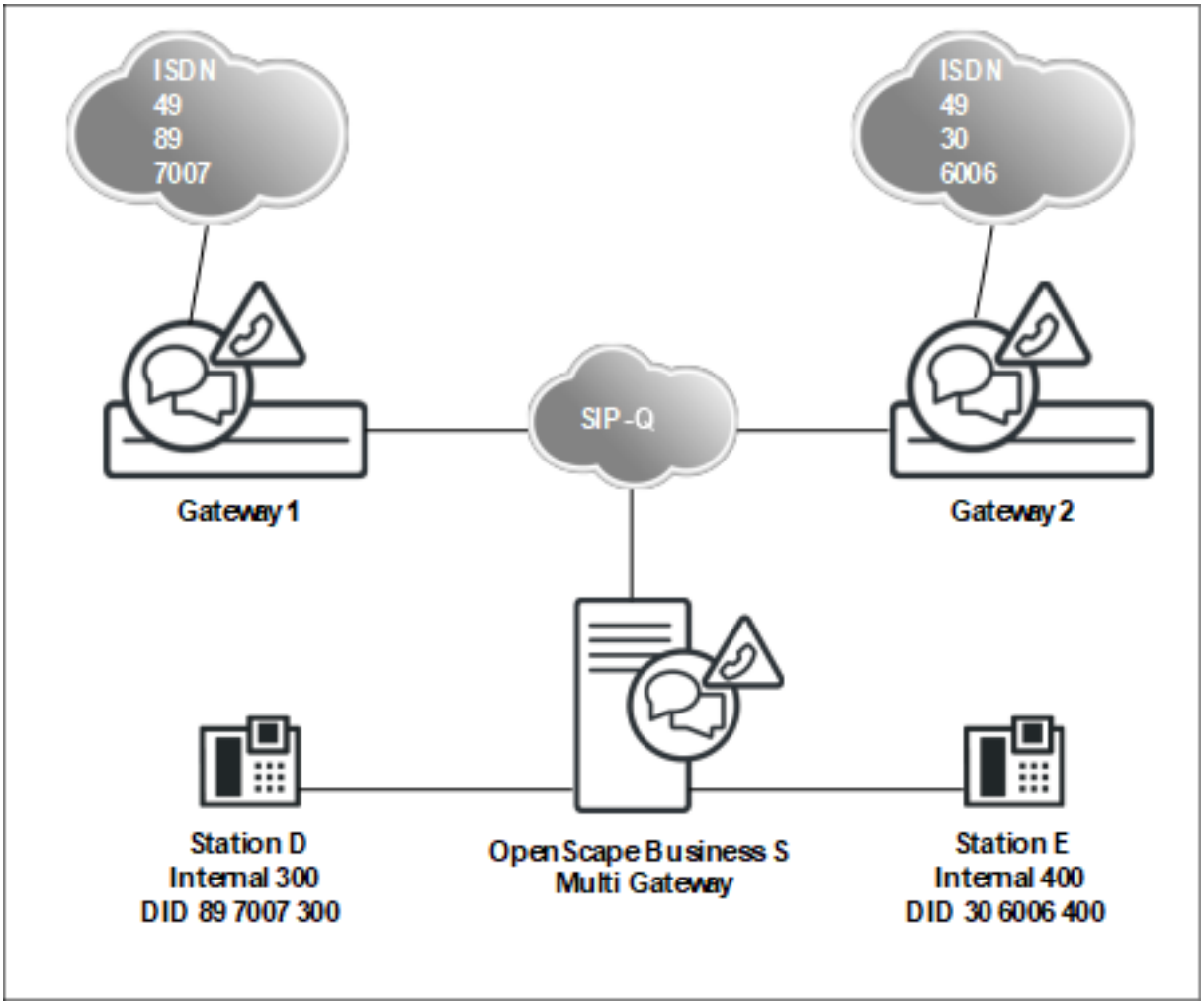
- Paramétrage du noeud 2 comme indiqué dans le précédent scénario.

15.3.4.9 Passerelle 1 résau RNIS appelle abonné D

Système en réseau dans une configuration multi-passerelle

Configuration

Configuration de la multi-passerelle, OpenScape Business S

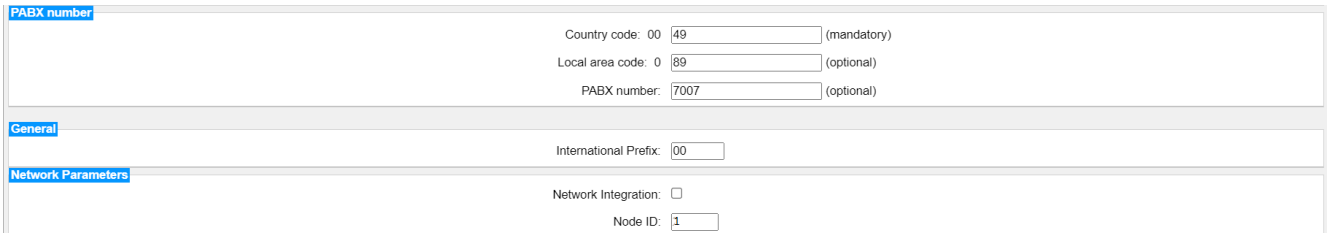


Exemple: Appel entrant avec numéro de destination où TON = abonné

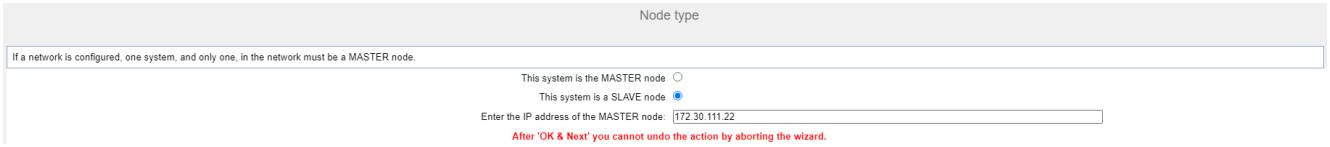
Particularités de ce scénario :

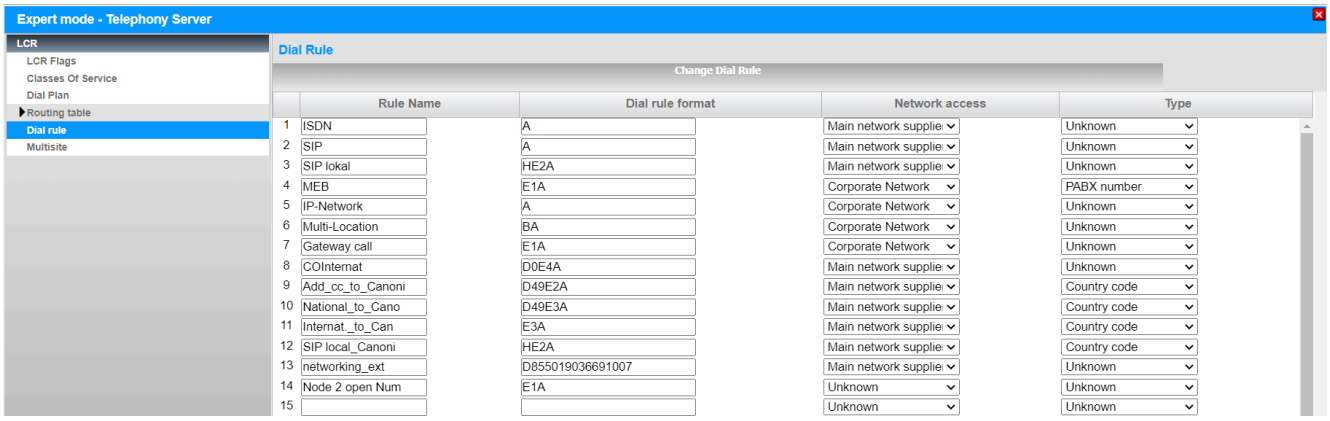
- La passerelle 1 est normalement paramétrée comme dans le scénario précédent (Passerelle 1) c.-à-d. qu'il est tout d'abord réalisé l'installation de base puis l'assistant de mise en réseau intervient. Différence essentielle : les passerelles sont paramétrés comme Esclave, OpenScape Business S comme Maître (Performance, Bande passante, Procédure de licence).
- Dans cet exemple, seules les différences essentielles par rapport au précédent scénario sont mentionnées.

Installation de base de Passerelle 1



Assistant mise en réseau pour Passerelle 1





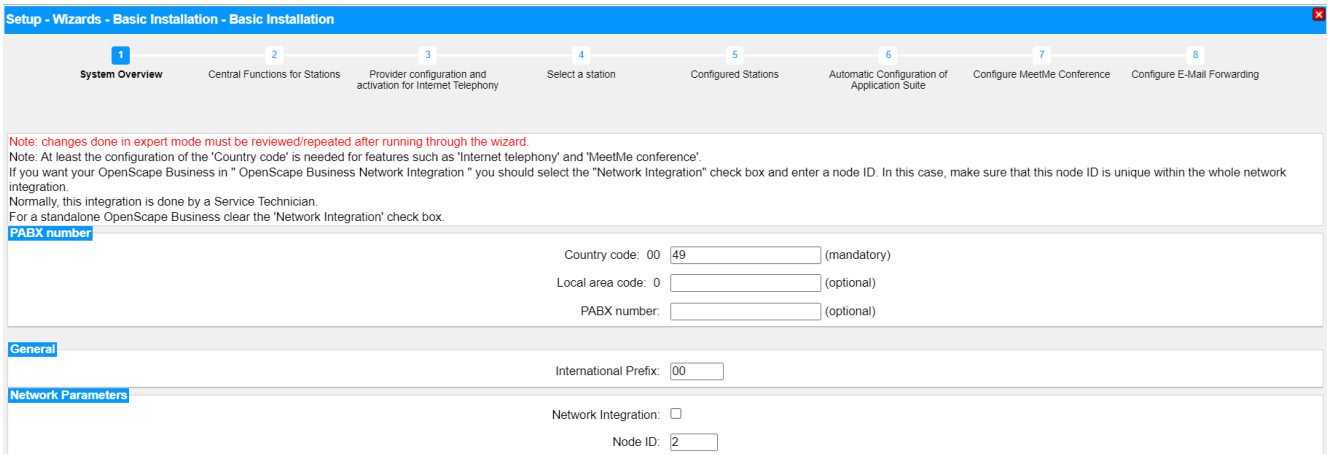
Dans OpenScape Business S, le numéro de destination est déjà inscrit au "format national" comme SDA.

"BA" (Broaden ALL) n'a de signification que dans une passerelle.

"BA" est uniquement nécessaire lorsque le numéro de destination d'origine TON unknow a été reçu, c.-à-d. qu'il contient seulement "SDA court" = partie poste.

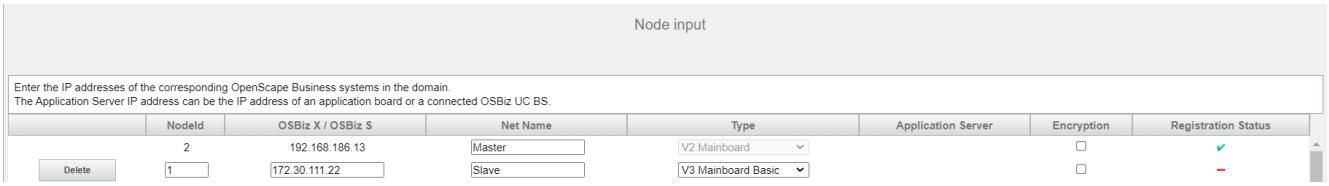
- Il est tout d'abord réalisé l'installation de base, puis l'asssistant de mise en réseau intervient.
- Pour chaque abonné de OpenScape Business S il est paramétré :
  - Numéro interne au format court (par ex. 300)
  - Numéro SDA au format national (par ex. 89 7007 300)
  - ID de noeud passerelle correspondant

Installation de base de OpenScape Business S, Multi-passerelle



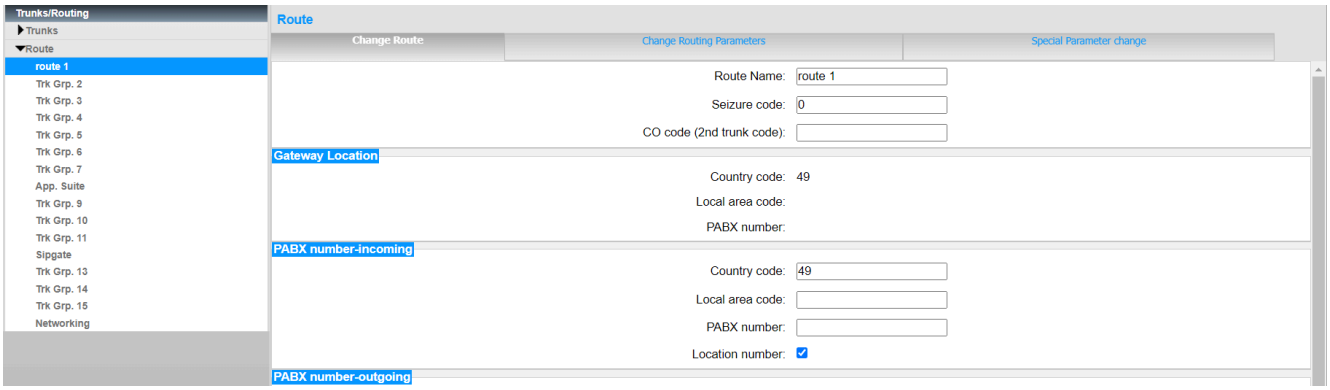
Conseil : Dans les données d'installation, n'inscrire que l'indicatif du pays, le reste du numéro global figure dans l'entrée SDA de l'abonné.

Assistant de mise en réseau de OpenScape Business S, Multi-passerelle



Dans la configuration du réseau, sélectionnez Multi passerelle.

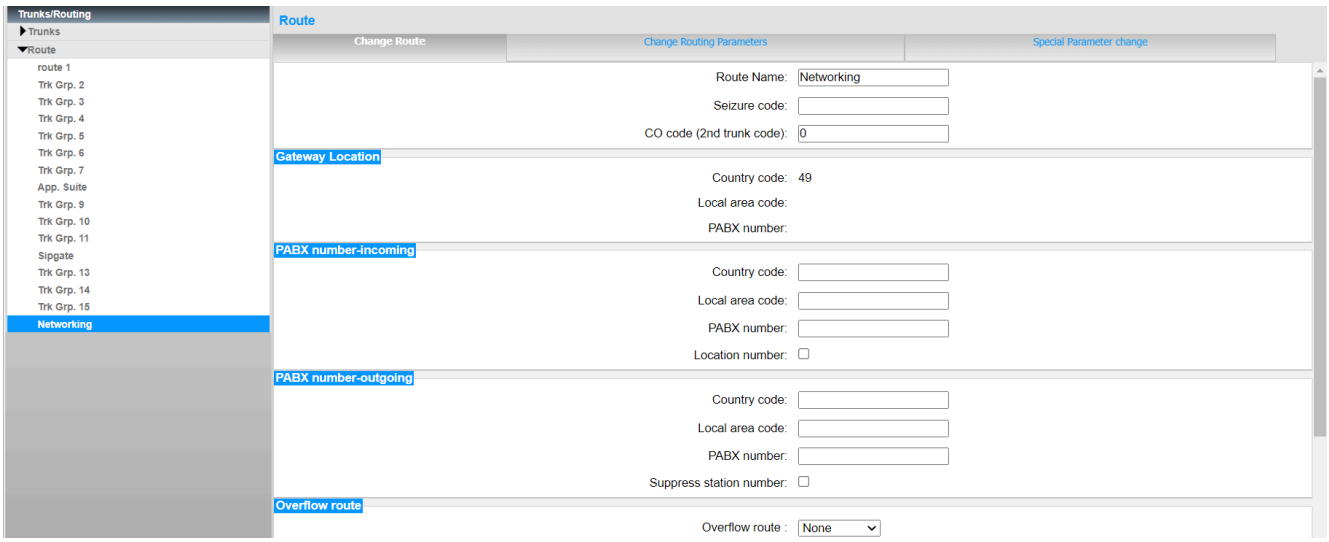
Faisceaux de OpenScape Business S, Multi-passerelle



L'indicatif du pays a déjà été inscrit dans l'assistant.

Paramètres de routage : Type de faisceau CO (réseau)

Ce faisceau reçoit le type "Réseau".



Paramètres de routage: Type de numéro outgoing=National, type de faisceau PABX

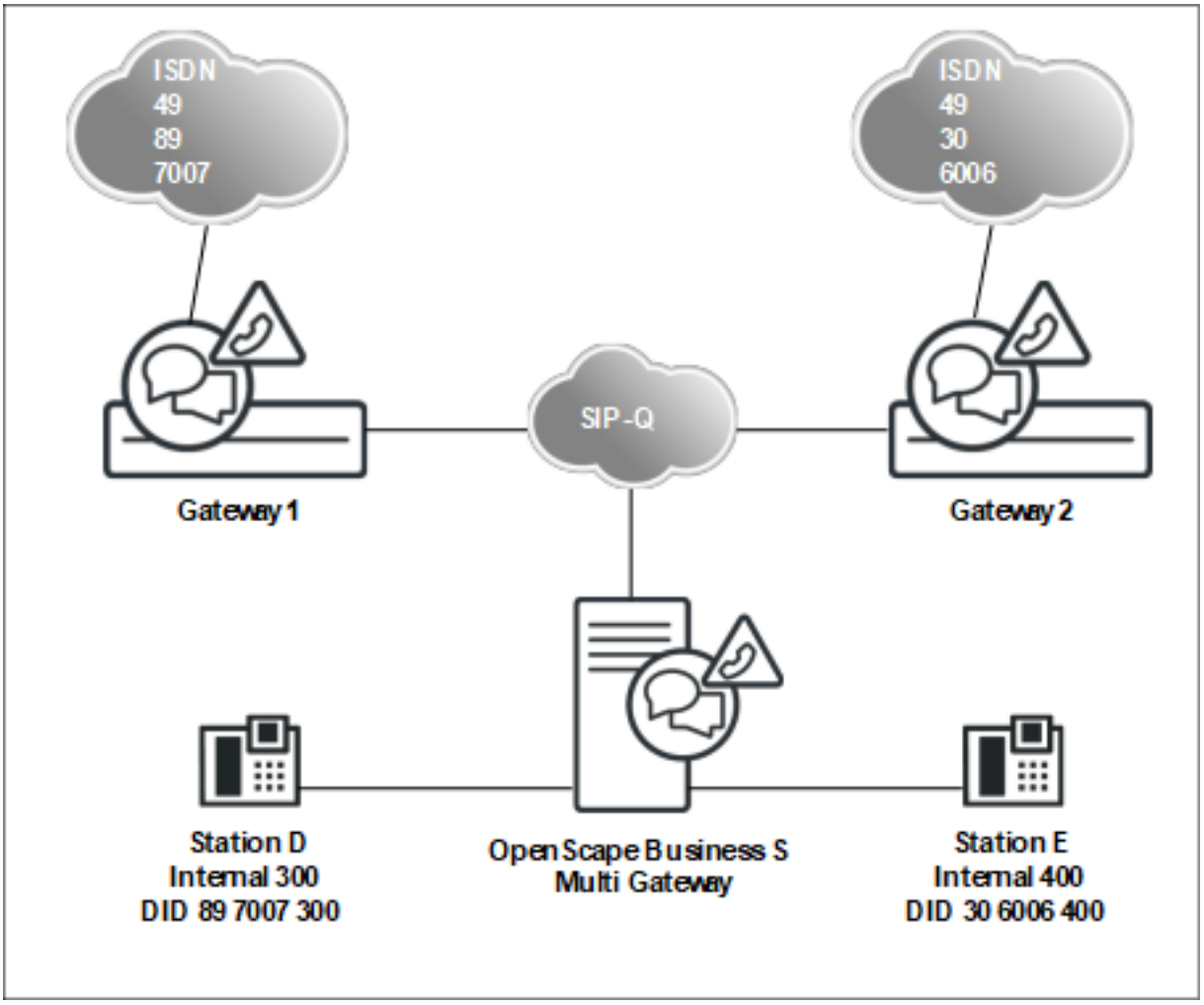
Ce faisceau reçoit le type "PABX", et le champ "N° et type, sortant" doit être configuré avec l'**indicatif du réseau local**.

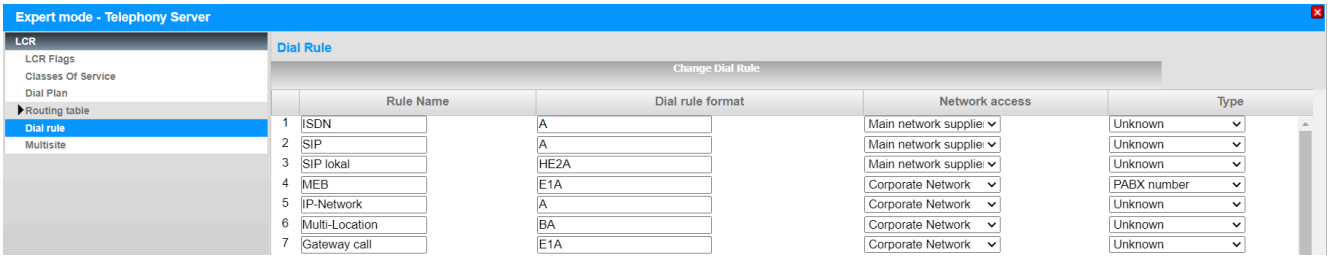
15.3.4.10 Abonnés D appelle abonné externe via le réseau

Système en réseau dans une configuration multi-passerelle

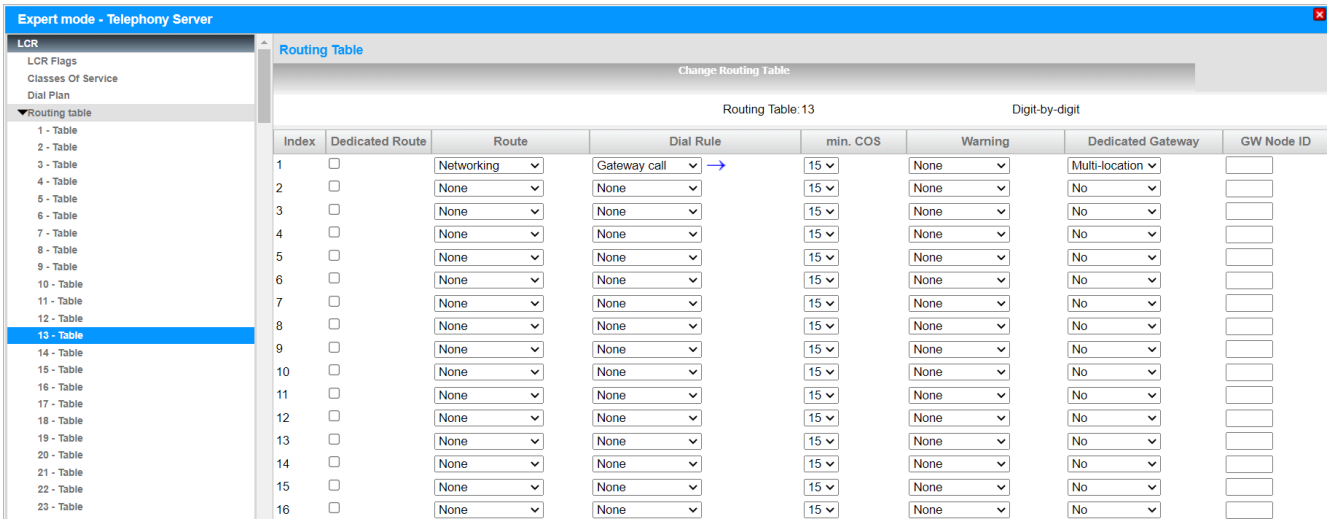
Configuration de OpenScape Business S, Multi-passerelle

Routage de OpenScape Business S, Multi-passerelle, vers les passerelles





	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



La configuration de la passerelle 1 est réalisée comme dans l'exemple précédent. C'est également le cas avec la passerelle 2.

15.4 Appels d'urgence

Le système de communication et les téléphones raccordés offrent diverses options pour émettre un appel d'urgence. Un administrateur peut configurer une hotline/ligne directe après temporisation ou encore un service d'appel d'urgence.

Si la période d'activation n'est pas encore démarrée ou si le système de communication est en Failover Period, les appels d'urgence peuvent toujours être effectués à partir des deux premiers téléphones actifs.

Conditions

Le centre de traitement des appels d'urgence est joint en composant l'indicatif réseau (par ex. 0) et le numéro d'appel d'urgence (par ex. 112). A partir des applications, il faut pour cette raison sélectionner le numéro d'urgence des appels d'urgence en faisant figurer au début l'indicatif réseau.

Déroulement par principe

Cas 1 : sélection de l'appel d'urgence via ligne RTC

Cas 2 : sélection de l'appel d'urgence via ITSP

Cas 3 : accord spécial avec ITSP ou fournisseurs RTC

Cas 4 : appels d'urgence en cas de Mobile Logon (IP-Mobility)

Les appels d'urgence d'un abonné du système de communication sont lancés par la sélection de l'indicatif réseau et du n° d'appel d'urgence. Le n° d'appel d'urgence est fourni par le système de communication au fournisseur (RTC ou ITSP).

L'appel d'urgence est placé dans le réseau local auquel est affecté le raccordement du système de communication. Remarque : tous les abonnés qui

ne se trouvent pas sur le site du système de communication (par ex. abonnés Mobility, utilisateurs CallMe (télétravailleurs) ou téléphones distants via WAN) devraient sélectionner l'appel d'urgence via un téléphone mobile ou un autre téléphone fixe afin de placer l'appel d'urgence dans le réseau local de leur site.

Pas tout les appels d'urgence supportés par les ITSP Dans ce cas, la configuration LCR doit veiller à ce que les appels d'urgence soient acheminés via le RTC.

Dans le cas où tous les abonnés du système de communication ne se tiennent pas sur un même site, mais sont tous affectés à un site sans RTC propre, il est possible, en accord avec le fournisseur, de définir une procédure individuelle de signalisation d'appel d'urgence. Par ex. : En fonction de l'ID de l'appelant, l'appel d'urgence peut être achemné par le fournisseur vers le réseau local convenu. Ces dispositions sont individuelles et ne sont soumises à aucune directive.

Mobile Logon (IP-Mobility) signifie que l'abonné change de téléphone et emporte avec lui le numéro.

Dans ce cas, les appels d'urgence fonctionnent tant que les téléphones sont inscrits sur les sites des passerelles. Tous les abonnés qui ne sont pas sur le site de la passerelle (par ex. abonnés Mobility, utilisateurs CallMe (télétravailleurs) ou téléphones distants via WAN) devraient sélectionner l'appel d'urgence via un téléphone mobile ou un autre téléphone fixe afin de placer l'appel d'urgence dans le réseau local de leur site.

Conseil : Pour les scénarios multi-passerelles où la fonctionnalité Mobile Logon est utilisée, des exigences particulières s'appliquent. La configuration correspondante est décrite dans le chapitre "Appels d'urgence en combinaison avec Mobile Logon".

15.4.1 Ligne directe après temporisation / Hotline

Il est possible d'activer la fonction Hotline pour chaque abonné. Il faut déterminer si, après décrochage du combiné, la liaison avec la destination de la hotline doit être établie immédiatement (Hotline) ou après un certain temps (Tempo).

Ligne directe après temporisation

Si, pendant la durée prédéfinie (temporisation du renvoi) l’abonné appuie sur une touche quelconque de chiffres, il n’y a **pas** d’établissement de la liaison avec la destination de la hotline.

La valeur de temporisation est configurée de manière centrale par l'administrateur et peut être activée/désactivée de manière individuelle pour chaque abonné.

Hotline

Lorsque la hotline est activée, l’abonné n’a **aucune** possibilité d’entrer un numéro. Il est possible de composer un numéro avant de décrocher le combiné. Après avoir décroché le combiné, l'abonné est toujours relié automatiquement à la destination de hotline interne ou externe définie préalablement.

Lorsqu'une destination de ligne directe est définie pour le renvoi d'appel ou le renvoi temporisé, l'appel de l'abonné est toujours renvoyé.

Informations spécifiques du système

L'administrateur a configuré 6 destinations de lignes directes et la durée de la temporisation (0-99 secondes) du renvoi sur ligne directe. Si l'administrateur entre la valeur 0 pour la temporisation du renvoi, la destination de la Hotline est aussitôt appelée.

Correspondances

Rubrique	Correspondance
Ne pas déranger	Si la fonction Ne pas déranger est activée pour la destination, l'appelant entend la tonalité d'occupation.

15.4.1.1 Comment configurer et modifier la destination de ligne directe (Hotline)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, allez à **Système** > **Renvoi/P.O/Hotline**.
4) Dans **Hotline**, vous pouvez inscrire 6 destinations différentes (**n° de destination**).
5) Cliquez sur **Appliquer** puis sur **OK**.

15.4.1.2 Comment modifier la temporisation du renvoi sur ligne directe

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Système**.
4) Cliquez sur **Renvoi/P.O/Hotline**.
5) Dans Hotline, vous pouvez modifiez la **durée de la temporisation**.
6) Cliquez sur **Appliquer** puis sur **OK**.

15.4.1.3 Comment configurer la temporisation ou la Hotline pour un abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés**.
4) Cliquez par ex. sur **Clients IP**.
5) Cliquez par ex. sur **Clients TFA**.
6) Sélectionnez l'abonné correspondant et dans le champ **Hotline**, sélectionnez **Tempo** ou **Hotline**.
7) Si vous avez paramétré Hotline, vous devez encore paramétrer dans le champ Hotline le **nombre de destinations hotline**.
8) Cliquez sur **Appliquer** puis sur **OK**.

15.4.2 Coupure de la ligne pour un appel d'urgence

En cas d'émission d'un appel d'urgence lorsque aucune ligne réseau n'est libre, le système déclenche une déconnexion forcée. La ligne libre est automatiquement affectée à l'abonné qui émet l'appel d'urgence.

La déconnexion fonctionne pour les lignes RNIS et ITSP.

Lorsque toutes les lignes sont occupées, les abonnés peuvent déclencher une libération de ligne automatique ou manuelle.

- Automatique : la fonctionnalité Acheminement (LCR) est active et il y a un numéro d'urgence enregistré dans LCR.
- Manuellement : la fonctionnalité "Libérer lignes" est toujours active pour le poste opérateur ; elle est exécutée à partir d'une touche ou d'un indicatif.

Informations spécifiques du système

L'administrateur peut configurer un nombre illimité de numéros d'appel d'urgence.

Pour qu'il soit possible d'effectuer une coupure automatique de ligne lorsque toutes les lignes sont occupées, le numéro d'urgence doit figurer dans le plan de numérotation de l'acheminement LCR et le drapeau Appel d’urgence *Mode Expert* doit être placé pour ce numéro.

15.4.2.1 Comment activer ou désactiver la libération de ligne pour les appels d'urgence

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Routage**.
3) Dans l'arborescence du menu, allez à **LCR** > **Plan de numérotation**.
4) Dans la fenêtre **Modifier le plan de numérotation** sélectionnez l'une des possibilités suivantes.
   - Si vous voulez activer la fonction, cochez la case **N° appel d'urgence** du numéro correspondant.
   - Si vous souhaitez désactiver la fonction, décochez la case **N° appel d'urgence** pour le numéro correspondant.
5) Cliquez sur **Appliquer** puis sur **OK**.

15.4.3 Uniquement pour les Etats-Unis, le Canada : Service d'appel d'urgence E911

Avec le service d'appel d'urgence étendu E911, outre le numéro d'appel, des informations relatives à la localisation géographique (adresse stockée) de l'appelant sont transmises à l'émission de l'appel d'urgence.

Il n'est pas nécessaire que l'appelant indique verbalement sa position géographique à la centrale de secours qui reçoit l'appel.

Aux Etats-Unis, cette fonction n'est activée que lorsque l'appelant compose le numéro d'appel d'urgence 911.

Pour le service d'appel d'urgence E911, l'administrateur doit associer un code d'emplacement LIN (Location Identification Number) à chaque abonné avec numéro SDA valide. Le code LIN attribué à des postes d'abonnés situés à proximité géographique doit être identique. Le centre de traitement des appels d'urgence dispose d'une base de données dans laquelle tous les codes LIN sont enregistrés et qui permet d'identifier le nom et l'adresse de l'appelant au moyen du code LIN transmis.

Correspondances

Sujet	Correspondance
CLIP	Pour les Etats-Unis, le code LIN est activé par défaut. Si le CLIP (Calling Line Identification Presentation) est activé pour les Etats-Unis, le code LIN est automatiquement désactivé.

15.4.3.1 Comment modifier le CLIP / LIN

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés**.
4) Cliquez par ex. sur **Clients IP**.
5) Cliquez sur l'onglet **Modifier l'abonné**.

6) Dans le champ **CLIP/Lin**, entrez le code d'emplacement LIN à 16 chiffres pour l'abonné correspondant.
7) Cliquez sur **Appliquer** puis sur **OK**.

15.4.4 Appels d'urgence en combinaison avec Mobile Logon

Si l'on utilise la fonctionnalité Mobile Logon dans une interconnexion de réseau multi-passerelle, l'emplacement physique peut être modifié en cas de changement de téléphone. C'est pourquoi, des mesures particulières sont nécessaires pour le routage des appels d'urgence.

Description de l'algorithme pour la sélection d'un appel d'urgence

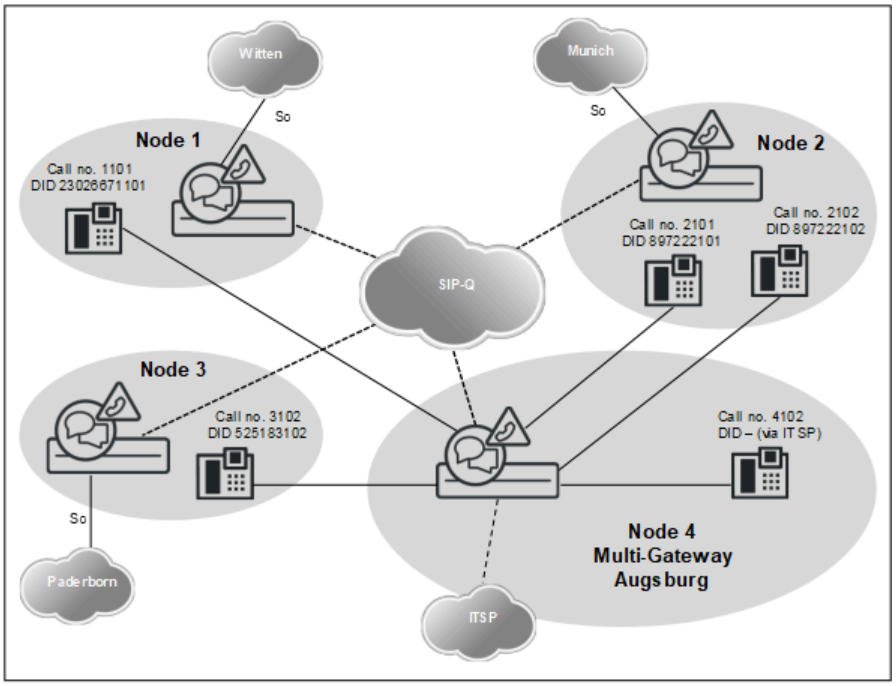
Lorsqu'un abonné compose un numéro d'urgence (identifiant dans LCR), l'algorithme contrôle si un numéro d'urgence a été configuré sur le téléphone. Celui-ci est ensuite utilisé pour créer un numéro d'appel dérivé, qui est utilisé dans l'interconnexion de réseau pour le routage de l'appel via la passerelle correcte.

Chaque numéro identifié comme n° d'appel d'urgence dans le plan de numérotation dispose d'une référence à une entrée dans la table de routage. Une classe de discrimination (classe de service, COS) inférieure doit être affectée à chaque entrée de la table de routage associée à un numéro d'urgence. Une classe de discrimination plus basse signifie que chaque abonné est autorisé à placer un numéro d'appel d'urgence.

15.4.4.1 Configuration du scénario d'appel d'urgence

La configuration du scénario d'appel d'urgence indique, pour une interconnexion de réseau multi-passerelle, les opérations à effectuer pour le paramétrage.

Traitement des numéros d'urgence



Mobile Logon n'est supporté qu'à l'intérieur d'un noeud, c.-à-d. que le changement de site - et donc les exigences particulières pour les appels d'urgence - ne s'appliquent qu'aux téléphones qui sont exploités sur des noeuds multi-passerelle (4). D'une manière générale, tous les téléphones concernés du noeud 4 sont connectés, mais se trouvent physiquement sur différents emplacements.

- Dans tous les téléphones concernés, il est nécessaire d'avoir une entrée pour l'appel d'urgence (partie raccordement du numéro d'appel canonique du noeud du site + indicatif de prise de ligne du faisceau d'appel d'urgence).
- L'entrée LCR (noeud_4local) dans le tableau suivant n'est nécessaire que si des téléphones sont physiquement présent sur le noeud 4 (multi-passerelle). Il est indiqué tout d'abord le numéro de site qui est ici incomplet (uniquement code du pays). La condition est de disposer d'un accès ITSP au noeud 4, qui supporte les appels d'urgence dans le réseau local.
- Lors de la sélection sur le téléphone, on parvient à une règle LCR identifiée par un appel d'urgence (par ex. 0C11x).
- Le numéro d'appel d'urgence enregistré dans le téléphone (et transmis au système lors de la connexion) est comparé aux données d'emplacement du système (indicatif national, indicatif du réseau local, numéro de l'installation).

  Si différent, il est établi un numéro d'urgence "long" :

  – Supprimer le code d'accès : 0112 -> 112
  – Ajouter <Indicatif de prise de ligne LDAP><Préfixe international><Numéro d'urgence programmé> : par ex.112 -> 0 00 49897220 112
- Le numéro d'urgence "long" est acheminé par LCR conformément aux règles LCR spécifiques soit directement sur le réseau local, soit par une ligne interautomatique en direction du noeud partenaire et, de là, sur le réseau local.

Conseil : Comme il n'est pas entré dans le téléphone le numéro de site complet du noeud local, il faut inscrire une règle LCR adaptée pour l'appel d'urgence local sur site multi-passerelle.

Configuration des données de site pour noeud 4

Paramètres de faisceau

Noeud 4, Téléphones

Aperçu des entrées figurant dans le LCR pour le noeud 4, correspondant à un appel d'urgence

Noeud 4	Noeud passerelle
Site G. Pays	49
Site G. Réseau local	
Site G. Installation	
Préfixe international	00
Préfixe national	0
Indicatif de prise de ligne LDAP	0

Faisceau	N° type, sortant	Type RNR
Mise en réseau	National	Int/SDA

Faisceau Networking	
Indicatif réseau (2e AKZ)	0

Site Witten	
Call Number (numéro de téléphone)	1101
Emergency Number (N° appel d'urgence)	4923026670

Site München	
Call Number (numéro de téléphone)	2101
Emergency Number (N° appel d'urgence)	49897220

Site Paderborn	
Call Number (numéro de téléphone)	3102
Emergency Number (N° appel d'urgence)	49525180

Site Augsburg	
Call Number (numéro de téléphone)	4102

Site Augsburg	
Emergency Number (N° appel d'urgence)	490

Plan de numérotation			Table de routage			Règle de numérotation		
Nom	Chiffres composés	Service d'urgence	Faisceau	Passerelle dédiée	ID Passerelle	Règle de numérotation	Type	Type
Appel d'urgence [3]	0C112	X	Mise en réseau	Multi-passerelle	1	E1A	Corp. Réseau	Inconnu(e)
Appel d'urgence [3]	0C0110	X						
Réseau	0CZ							
Appel_d'urgence_après_1	0C00492302667-0-11X	X	Mise en réseau	Forcée	1	E3A	Corp. Réseau	Inconnu(e)
Appel_d'urgence_après_2	0C004989722-0-11X	X			2			
Appel_d'urgence_après_3	0C004952518-0-11X	X			3			
Appel d'urgence_4local [4]	0C0049-0-11X	X	ITSP	Non		E4A	Fournisseur réseau principal	Inconnu(e)

15.4.5 Service d'appel d'urgence E112 pour l'Europe

Avec le service d'appel d'urgence étendu E112, outre le numéro d'appel, des informations relatives à la localisation géographique (adresse stockée) de l'appelant sont transmises à l'émission de l'appel d'urgence.

L'information géographique est transmise dans un document XML normalisé. La définition du contenu de ce document dépend du pays et de l'ITSP. Donc, vous devez entrer uniquement le sous-ensemble requis de données que vous avez reçu de votre ITSP (par exemple, en Suisse, seul le champ NAM est utilisé).

La fonctionnalité est activée par la configuration des numéros d'urgence dans LCR et par la définition des informations de localisation appropriées.

15.4.5.1 Comment ajouter une urgence SIP à une station

Conditions préalables

Vous êtes connecté au WBM avec le profil **Expert**

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert** .
2) Dans l'arborescence de navigation, cliquez sur **Passerelle vocale** > **téléphonique** .
3) Dans l'arborescence du menu, cliquez sur **Paramètres d'urgence SIP** .

[3] Dans le cadre des règles ci-dessus, la situation d'appel d'urgence est reconnue dans cet exemple, mais il n'y a pas de routage. Pour le routage de l'appel d'urgence, on utilise le numéro d'appel d'urgence "long" dérivé.

[4] Comme les abonnés sont reliés physiquement au site multi-passerelle, il faut établir une règle LCR propre pour un accès à l'appel d'urgence local (via faisceau ITSP).

4) Dans l'onglet **Configuration générale** , choisissez le **mode de localisation** souhaité :

a) **Emplacement XML (RFC 4119 et RFC5139)** , sans paramètres supplémentaires.
Dans l'onglet **Ajouter un emplacement** , renseignez le paramètre **Nom de l'identifiant d'emplacement** (obligatoire) et le(s) paramètre(s) défini(s) pour les informations de localisation que vous avez reçues de votre fournisseur de services de télécommunications (par exemple, en Suisse, seul le champ NAM est utilisé).

b) **Numéro virtuel d'urgence (Belgique)**

Dans l'onglet **Configuration générale** , remplissez les **paramètres** .

Dans l'onglet **Ajouter un emplacement** , renseignez le **nom de l'emplacement** et les paramètres définis pour les informations de localisation par votre fournisseur de services de téléphonie sur IP (ITSP).

5) Cliquez sur **Appliquer** puis sur **OK** .

Un identifiant de localisation est automatiquement attribué à l'identifiant de localisation. **Urgence SIP** .

6) Dans l'arborescence de navigation, cliquez sur **Postes** > **téléphoniques** .

7) Dans l'arborescence du menu, cliquez sur **Stations** .

8) Cliquez sur **Clients IP** , par exemple.

9) Cliquez sur l'onglet **Modifier les stations** .

10) Saisissez l'identifiant de localisation correspondant dans le champ **Urgence SIP** .

11) Cliquez sur **Appliquer** puis sur **OK** .

15.5 Service de gestion des appels (Call Admission Control)

La fonctionnalité Service de gestion des appels (Call Admission Control CAC) permet de limiter la bande passante utilisée par le nombre des communications.

Le système de communication offre trois possibilités d'influence sur la bande passante nécessaire.

- Limitation du nombre de communications simultanées via ITSP
- Limitation du besoin en bande passante pour les communications passerelle
- Restriction du nombre de communications dans les scénarios de mise en réseau

15.5.1 Limitation du nombre de communications simultanées via ITSP

Le nombre maximum d'appels pouvant être effectués via un ITSP peut être limité en configurant la largeur de bande disponible en amont. En réduisant le nombre de ces appels (appels Internet), les besoins en bande passante peuvent être réduits davantage.

Les paramétrages nécessaires sont effectués dans les assistants **Réseau/ Internet** et **Téléphonie centrale**.

Le nombre d'appels possibles via un ITSP peut être consulté en **mode Expert** sous **Téléphonie** >**Voice Gateway** > **SIP Paramètres**.

Les appels Internet sont :

- Appels ITSP
- Appels Unify Phone
- appels myPortal for Teams
- Appels myPortal@work
- Appels Device@Home

Seuls les appels LAN myPortal@work et les appels WebRTC purs ne réservent pas de bande passante car la charge utile est directe.

15.5.2 Limitation du besoin en bande passante pour les communications passerelle

La configuration des codecs admissibles pour les communications passerelle permet d'influencer la bande passante.

Si l'on utilise uniquement des codecs à compression, les besoins en bande passante sont inférieurs. Si l'on utilise différents codecs, il est possible d'abaisser la priorisation des codecs sans compression de sorte que ceux-ci sont utilisés plus rarement.

Les paramètres correspondants sont définis dans **Mode Expert** sous **Téléphonie** > **Passerelle vocale** > **Changer les paramètres de codec**.

15.5.3 Restriction du nombre de communications dans les scénarios de mise en réseau

Le système de communication offre deux moyens pour contrôler la bande passante dans les scénarios de mise en réseau.

Restriction par le nombre de lignes vers d'autres noeuds de réseau

Limitation de la bande passante par sélection ciblée du codec

En affectant un nombre déterminé de lignes en direction d'autres noeuds de réseau, il est possible de définir une limite supérieure pour tous lescommunications simultanées possible à partir et vers ces noeuds.

La bande passante disponiblepeut être définie grâce à la configuration des codecs utilisés depuis le partenaire (adresse IP de destination) et vers celui-ci.

Les paramètres correspondants sont définis dans **Mode Expert** sous **Téléphonie** > **Passerelle vocale** > **Ajouter les paramètres de codec de destination**.

15.6 Système multisociétés

La capacité totale du système de communication peut, sur le plan de l'organisation, être divisée en six sous-installation au maximum. Cela permet par exemple à plusieurs entreprises d'utiliser en commun un système de communication.

La fonctionnalité Système multisociétés est réalisée en utilisant les fonctionnalités existantes. Cela signifie qu'il n'y a pas de configuration explicite des installations partielles.

La gestion des connexions autorisées et interdites entre les différents abonnés et ligne intervient par le biais des groupes de matrices de connexion.

Fonctionnalités dans le système multisociétés :

- Renvoi distinct
- Numéro de l'installation
- Liste des appelants
- Entrée en tiers
- DISA
- Appel interphone
- Enregistrement des données de taxation
- Destinations hotline
- Textes d'info, textes d'absence
- Communications internes
- Annuaire interne
- Impression KDS
- Renvoi de nuit
- Position de parcage
- Groupes de matrices de connexion
- Messagerie vocale
- Contrôle de la numérotation

Le système de communication peut être utilisé comme un système multisociétés et ainsi être utilisé par plusieurs sociétés. Le fonctionnement de toutes les fonctionnalités est conservé sans aucune modification pour tous les abonnés.

Font exception certaines ressources qui doivent réparties entres les sous-exploitants (sociétés). Celles-ci peuvent être affectées à un, plusieurs ou à tous les sous-exploitants. Les ressources à répartir sont les suivantes :

- Abonnés
- Faisceaux
- Poste opérateur
- Station de renvoi
- Equipement d'annonce, messagerie vocale
- Groupes de matrices de connexion
- Ouverture de porte
- Lignes DISA

A partir des groupes de restriction de trafic il est défini la capacité de liaison des sous-exploitants, les uns avec les autres.

Pour chaque zone partielle, il est possible de créer des destinations de hotline propres.

Correspondances

Sujet	Correspondances
GEZ	Il existe un seul système de taxation centralisé pour toutes les sous-zones.
Communications internes	Les communications internes entre abonnés de sous-zones "différentes" sont possibles à condition que la matrice de connexion VBZ l'autorise.

Sujet	Correspondances
LCR	La prise de ligne automatique n'est configurable que pour l'ensemble du système.
Impression KDS	L'impression de la base de données n'a lieu que pour le système tout entier.
Annuaire interne	Il est indiqué les noms de tous les abonnés et les numéros abrégés du système.
Commuter	Il n'est pas possible de commuter les lignes transférées par P.O.
Renvoi distinct	Renvoi distinct programmable uniquement pour l'ensemble du système.

15.6.1 Numérotation abrégée centralisée dans les systèmes multi-sociétés

La numérotation abrégée centralisée dans les systèmes multi-sociétés permet de sélectionner des numéros abrégés en fonction des groupes de matrices de connexion. Pour cela, à l'aide de la WBM, il est possible d'affecter une plage de numéros abrégés aux groupes de matrices de connexion correspondants.

Correspondances

Sujet	Correspondances
Numéros de téléphone ext.	Les numéros abrégés ne peuvent comporter que des numéros de téléphone externes.
	Le numéro externe doit être indiqué avec le préfixe faisceau ou de prise de ligne.
Noms des destinations de numérotation abrégée	A chaque destination de numérotation abrégée peut être affecté un nom.
Poste de portier	Le poste de portier ne peut pas appeler une destination de numérotation abrégée.
Groupes de restriction de trafic	Il est impossible d'affecter plusieurs plages de numéros abrégés à un groupe VBZ.

16 Préposés

OpenScape Business propose des fonctions d'assistance pour chaque cas d'utilisation (par exemple, des standards automatiques, des standards téléphoniques et sur PC).

Aperçu des intervenants disponibles

	Peut être utilisé pour	Matériel	Licence
Répondants automatiques			
Répondeur automatique d'entreprise (UC Smart)	UC Smart	OpenScape Business X OpenScape Business S	Requis
Répondeur automatique d'entreprise (UC Suite)	Suite UC	OpenScape Business S	Requis
Préposés téléphoniques			
Préposé OpenStage			
Préposés utilisant un ordinateur			
mon assistant	Suite UC	OpenScape Business S	Requis

16.1 Standard automatique

Le standard automatique constitue, avec la messagerie vocale, un service automatique intégré de transmission et une mémoire de messages, par exemple pour le siège de la société. Le standard automatique diffuse aux appelants un message d'accueil. Durant ou après cette annonce, l'appelant peut, de manière automatique ou en entrant des chiffres, être transféré vers un poste ou vers une boîte de messagerie.

Pour cela, différentes fonctions sont disponibles ; elles permettent une commutation individuelle à l'aide d'annonces, par ex. "Appuyez sur 1 pour le service technique, sur 2 pour le service commercial". L'appelant est automatiquement relié aux collaborateurs du service commercial ou du SAV une fois qu'il a entré le chiffre souhaité.

Le Company AutoAttendant (standard automatique de l'entreprise) n'est pas affecté à un numéro de téléphone interne, mais à une instance centrale. Il est donc possible d'affecter à un poste plusieurs Company AutoAttendants ou boîtes vocales. Il est ainsi possible pour l'utilisateur d'effectuer individuellement un renvoi vers le Company AutoAttendant correspondant. En fonction du renvoi, il est diffusé à l'appelant l'annonce de la boîte vocale personnelle ou l'annonce centrale de la société. Grâce au Company AutoAttendant, il est également possible de diffuser des annonces individuelles par poste, indépendamment de la boîte vocale personnelle.

Aperçu des fonctions

- Renvoi après annonce, vers une direction configurée
- Annonce en fonction de l'état - selon l'état du poste (libre ou occupé), il est possible de diffuser différentes annonces.

- Annonces différentes Jour/Nuit (commutation manuelle ou automatique)
- Gestion centrale du calendrier avec le renvoi de nuit automatique
- Post-sélection d'un numéro quelconque jusqu'à la longueur configurée (désactivable)
- N° abrégé (=appel direct depuis l'extérieur) vers des destinations configurées (numéro ou boîte vocale au choix)

  Au total, 4 liste avec au total 10 destinations et une destination séparée sont possibles. La liste active est définie par le message d'accueil sélectionné.
- Post-sélection d'un numéro quelconque jusqu'à la longueur configurée. La fonction de post-sélection peut être désactivée afin d'éviter les fraudes à la taxation.
- Standard automatique multiple

  Les boîtes vocales du standard automatique peuvent être configurées en tant que destinations de la numérotation abrégée (manuel 1 à 4, Jour/Nuit). Cela permet un chaînage de boîtes de messagerie.

  Le Company AutoAttendant se comporte comme dans un renvoi d'appel, la communication passe d'une boîte vocale à la suivante, en chaîne, avec diffusion de toujours la même annonce. Au total, jusqu'à 100 boîtes vocales Standard automatique sont disponibles.
- Numérotation rapide

  Les annonces peuvent être désactivées pour assurer une commutation rapide.
- Annonce avant réponse avec signalisation en parallèle (sans numéro abrégé)

  Si le message d'accueil est diffusé à l'appelant, l'appel est signalé en même temps à l'abonné de manière acoustique (et optique). Lorsque l'abonné décroche, l'annonce est interrompue et l'abonné est relié à l'appelant. Si l'abonné ne décroche pas, l'annonce est diffusée en boucle jusqu'à ce que l'abonné décroche ou effectue un renvoi à l'aide de la Gestion des appels.
- Reconnaissance de la tonalité occupé
- Renvois des fax (reconnaissance automatique de la tonalité fax) vers une destination fax préconfigurée.
- Retour d'appel

  Dans un retour d'appel (sauf pour un appel fax), l'appelant est renvoyé vers la boîte vocale correspondante s'il y en a et si l'enregistrement des messages est activé.

Remarque : Pour assurer un retour automatique au P.O. grâce au système de messagerie vocale, il est nécessaire d'inscrire le numéro du P.O en interne (par défaut 9, Etats-Unis 0).

Remarque : L'administration (TUI) d'une boîte vocale de standard automatique ne peut être effectuée qu'à partir d'un téléphone. C'est pourquoi, le mot de passe pour de la boîte vocale du standard automatique AutoAttendant-Mailbox doit être obligatoirement différent du la boîte vocale personnelle du téléphone !

Exemples d'application

- Exemple 1 : **Annonces indépendantes des services d'intervention ou d'urgence**

  En dehors des horaires de travail, transfert vers le standard automatique (par ex. à l'aide du renvoi de nuit). Le standard automatique effectue sur demande la liaison avec le technicien SAV en service ou propose de déposer un message dans une boîte vocale centrale. Dans ce cas, une annonce conduit au renvoi vers les différents numéros de mobile des technicien SAV.
- Exemple 2 : **Différents services du dimanche pour les cabinets médicaux**

  La nécessité d'indiquer le service du dimanche sur le répondeur ou de changer la cassette du répondeur est supprimée. Le client définit autant de standards automatiques (AutoAttendant) qu'il a d'adjoints. Les standards automatiques sont indiqués une fois et activés en fin de semaine avec un renvoi (renvoi de nuit) vers le standard automatique concerné. C'est ici l'inverse : plusieurs annonces différentes conduisent à la même boîte vocale.

16.1.1 Company AutoAttendant (UC Smart)

Le Company AutoAttendant (UC Smart) est le standard automatique de la solution de communications unifiées UC Smart. Il peut être utilisé comme standard automatique personnel et comme standard automatique central.
La première configuration est réalisé par le WBM, ensuite la commande et la configuration peuvent se faire par le téléphone.

Company AutoAttendant (UC Smart) peut être exploité en deux modes :

- **Standard automatique personnel**

  Le standard automatique personnel est affecté à un abonné ou à un groupe et réagit au numéro de téléphone de l'abonné ou du groupe d'origine appelé, qui est à l'origine du renvoi (par ex. `12345678-100`).

  Le standard automatique personnel est joint via le groupement "Messagerie vocale" (numéro par défaut : 351). L'exploitation est réalisée via les ports SmartVM (ports EVM) de type "Phonemail" qui doivent être tous affectés à ce groupement.

  L'exploitation en parallèle avec UC Suite est impossible.
- **Standard automatique central**

  Le standard automatique central est utilisé comme P.O. central et réagit à son propre numéro de téléphone (par ex.`12345678-0`). Le comportement est le même que l'appel soit envoyé directement au standard automatique ou qu'un renvoi ait été effectué.

  Le standard automatique central est joint via un ou plusieurs groupements propres (numéro par défaut : 352). L'exploitation est réalisée via les ports SmartVM (ports EVM) de type "Standard" qui doivent être affectés à un ou plusieurs groupements (100 maxi.).

  Par défaut, un Company Auto Attendant (index de groupe 3) est configuré avec 2 ports SmartVM. Les noms et types de ports peuvent être modifiés

avec l'assistant **Téléphonie centrale** > **SmartVM** (voir également Comment configurer la boîte vocale (SmartVM)).

La liste des numéros abrégés et le chargement de message d'accueil peuvent être modifiés avec l'assistant **Téléphonie** > **Connexions** > **SmartVM** (voir Comment charger, sauvegarder et effacer des messages d'accueils). De la même manière d'autres (99 maxi.) standards automatiques d'entreprise (UC Smart) peuvent être paramétrés et activés.

L'exploitation en parallèle avec UC Suite est possible.

Le standard automatique d'entreprise (UC Smart) est soumis à une licence (licence de standard automatique d'entreprise). S'il n'y a pas de licence, les "Règles" du Company AutoAttendant sont ignorées, les appels sont envoyés au poste central de renvoi.

16.1.1.1 Comment configurer un standard automatique d'entreprise créé

Dans l'exemple, il faut créer pour la journée une annonce avant réponse avec possibilité d'enregistrement (par ex. boîte vocale 100). La nuit, directement après l'annonce correspondante, il est effectué un renvoi distinct vers la boîte Nuit avec possibilité de réception (également boîte vocale 100).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

UC Smart est activé.

Par défaut, après l'annonce en service Jour et Nuit, il est effectué un retour au poste de renvoi.

Par défaut la fonction Speeddial et la post-sélection ne sont pas activés.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Connexion**.
3) Dans l'arborescence du menu, cliquez sur **Connexion** > **SmartVM**.
4) Dans l'arborescence du menu, cliquez sur **Standard automatique**.
5) Dans la ligne du standard automatique souhaité (par ex. `352`) décochez **Renvoi après annonce** afin de pouvoir entrer la numérotation abrégée durant le message d'accueil.
6) Cochez la case **Pas de surnumérotation**. Donc, seule l'entrée de numéros abrégés est possible (impossible d'entrer un numéro de téléphone interne).
7) Cliquez sur **Appliquer** puis sur **OK**.
8) Dans l'arborescence du menu, cliquez sur **Standard automatique** et ensuite sur l'entrée du standard automatique souhaité (Par ex. `352`).
9) Cliquez sur l'onglet **Modifier Destination numérotation abrégée/Renvoi distinct (Jour)**.
10) Dans la ligne **Numéro abrégé 0**, sélectionnez à partir de la liste déroulante **Sélectionner** l'abonné du poste de renvoi (par ex. abonné 100) et dans la liste déroulante **Type** l'entrée **Boîte de messagerie**.
11) Dans la ligne **Renvoi distinct**, sélectionnez à partir de la liste déroulante **Sélectionner** l'abonné du poste de renvoi (par ex. abonnés 100).

12) Cliquez sur **Appliquer** puis sur **OK**.
13) Cliquez sur l'onglet **Modifier Destination numérotation abrégée/Renvoi distinct (Nuit)**.
14) Dans la ligne **Renvoi distinct**, sélectionnez à partir de la liste déroulante **Sélectionner** l'abonné du poste de renvoi (par ex. abonné 100) et dans la liste déroulante **Type** l'entrée **Boîte de messagerie**.
15) Cliquez sur **Appliquer** puis sur **OK**.
16) Dans l'arborescence du menu, cliquez sur **SmartVM**.
17) Afin d'éviter un double message d'accueil avec la boîte de messagerie de renvoi distinct, sélectionnez dans la ligne de l'emplacement de renvoi (par ex. abonnés 100), à partir de la liste déroulante **Message d'accueil** l'entrée **Néant**. Directement après le message d'accueil du standard automatique d'entreprise, il est alors diffusé le signal d'enregistrement.
18) Le message d'accueil du standard automatique d'entreprise peut être modifié à l'aide d'un téléphone ou par le **Mode Expert** > **Maintenance** > **SmartVM** (voir Configuration de la boîte vocale (SmartVM)).

16.1.1.2 Comment créer un nouveau standard automatique d'entreprise

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

UC Smart est activé.

Licences nécessaires

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.

2) Configurez tout d'abord le groupement

a) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Appels entrants**.

b) Cliquez sur **Appels entrants** > **Groupes/Groupement** dans l'arborescence du menu.

c) Cliquez sur l'onglet **Ajouter un groupe**.

d) Dans le champ **Numéro de téléphone**, entrez le numéro du nouveau standard automatique (par ex. `353`).

e) Dans le champ **Numéro SDA**, entrez le numéro SDA du nouveau standard automatique (par ex. `353`).

: Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

---

f) Dans le champ **Nom**, entrez le nom du nouveau standard automatique (par ex. `Standard automatique 353`).

g) Dans la liste déroulante **Type d'abonné**, sélectionnez l'entrée **groupement cyclique**.

h) Dans la zone **Membre groupe**, dans la liste déroulante Numéros de téléphone, sélectionnez le port de standard automatique souhaité (par ex. **745 SmartVM 7**).

i) Cliquez sur **Appliquer** puis sur **OK**.

j) Pour ajouter un autre port de standard automatique au groupement, cliquez dans l'arborescence du menu sous **Groupes/Groupement** sur le standard automatique souhaité et ensuite sur l'onglet **Ajouter un membre**. Dans **Numéro de téléphone**, sélectionnez un autre port de standard automatique (par ex. **746 SmartVM 8**).

k) Cliquez sur **Appliquer** puis sur **OK**.

3) Configurez la boîte de messagerie du standard automatique :

a) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Connexions**.

b) Dans l'arborescence du menu, cliquez sur **Connexions** > **SmartVM**.

c) Dans l'arborescence du menu, cliquez sur **Standard automatique**.

d) Si nécessaire, cochez les deux cases dans la ligne du standard automatique souhaité (par ex. `353`) :

Renvoi après annonce : si activé, l'appelant durant le message d'accueil, entrer un numéro de numérotation abrégée afin d'établir un aiguillage.

Pas de surnumérotation : si activé, seuls des numéros abrégés peuvent être entrés, mais aucun numéro interne.

e) Cliquez sur **Appliquer** puis sur **OK**.

f) Dans l'arborescence du menu, cliquez sur **SmartVM**.

g) Cliquez sur

h) Dans l'onglet **Modifier boîtes de messageries SmartVM**, ligne du standard automatique souhaité, dans **Message d'accueil**, sélectionnez le message d'accueil souhaité.

i) Dans la ligne du standard automatique souhaité, cochez **Standard automatique**.

j) Cliquez sur **Appliquer** puis sur **OK**.

4) Configurez les possibilités de commutation (par ex. « 0 » pour connecter et « 1 » pour une annonce) :

a) Dans l'arborescence de menu, cliquez sur ***SmartVM** puis sur **AutoAttendant**.

b) Dans l'arborescence du menu, cliquez sur **Standard automatique** et ensuite sur l'entrée du standard automatique souhaité (par ex. 352).

c) Cliquez sur l'onglet **Modifier Destination numérotation abrégée/ Renvoi distinct (Jour).**

d) Dans la ligne **N° abrégé 0**, sous **numéro de téléphone** indiquez le numéro de téléphone à connecter et sélectionnez dans la liste déroulante **Type** l'entrée **Numéro de téléphone**.

e) Dans la ligne **Numéro 1**, sélectionnez à partir de la liste déroulante **Sélectionner** l'abonné du poste de renvoi (par ex. abonné 100) et dans la liste déroulante **Type** l'entrée **Boîte de messagerie**.

f) Dans la ligne **Renvoi distinct**, sélectionnez à partir de la liste déroulante **Sélectionner** le standard automatique d'entreprise (Company AutoAttendant) (par ex. 353).

g) Cliquez sur **Appliquer** puis sur **OK**.

h) Si le flag **Pas de surnumérotation** est désactivé, il est possible, durant le message d'accueil, de sélectionner aussi des numéros internes. Pour limiter les fraudes, il convient de contrôler ou limiter la **Limitation de la longueur des numéros** afin qu'il soit impossible d'appeler des numéros externes (voir **Mode Expert** > **Serveur de téléphonie** > **SmartVM** > **Modifier les paramètres SmartVM**).

16.1.2 Company AutoAttendant (UC Suite)

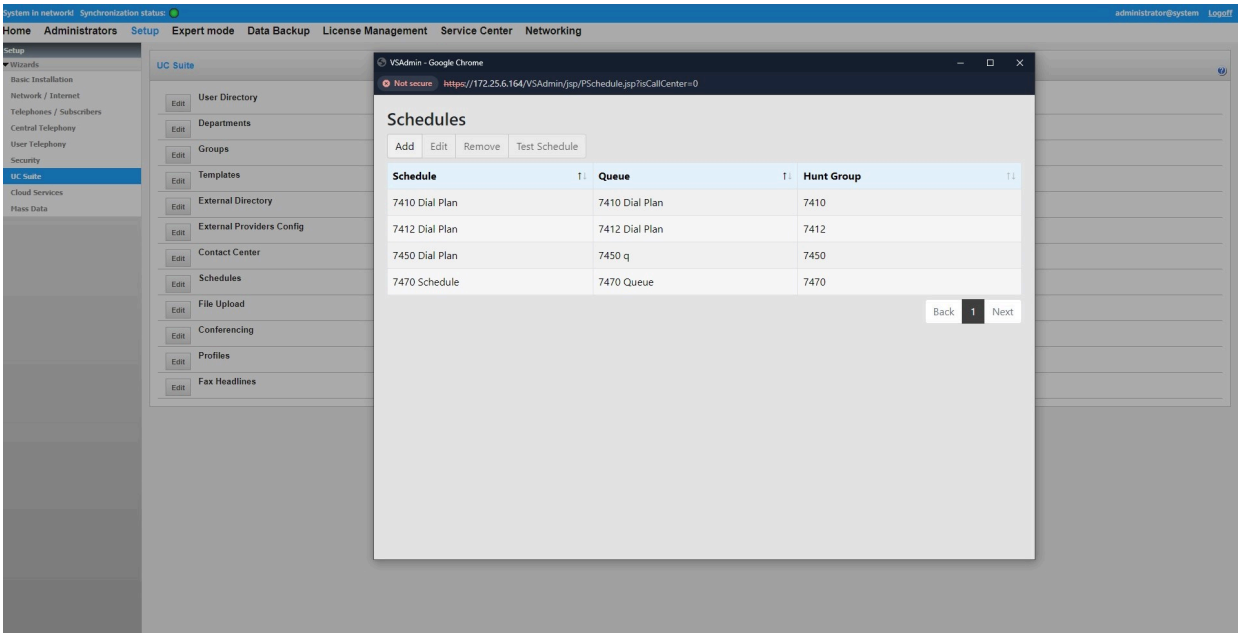
Le Company AutoAttendant central (UC Suite) est un poste opérateur qui ne peut être configuré que par l'administrateur. Afin de faciliter l'installation et la configuration, on dispose de cinq modèles qui peuvent être adaptés par l'administrateur.

L'administrateur est en mesure de configurer en fonction des règles le Company AutoAttendant (UC Suite) avec l'aide des calendriers. Les calendriers offrent des possibilités de sélection étendues, par ex. par nom.

16.1.2.1 Calendriers

Ce calendrier et les règles y figurant (Call Control Vector CCV) définissent comment les appels entrants doivent être traités selon les jours et selon les périodes de temps.

Il est par exemple possible de définir, pour les jours ouvrés, une règle pour l'équipe du matin (de 6h00 à 14h00), une pour l'équipe de midi (14h00 à 22h00) et une pour l'équipe de nuit (22h00 à 06h00). Il est possible de définir une règle de fin de semaine pour le week-end. Dans chacune de ces règles, il est par exemple possible d'indiquer si une annonce doit être diffusée ou non et/ou la destination de renvoi des appels.



Un calendrier doit comporter au moins une règle (Call Control Vector CCV). Pour la période de validité d'un calendrier, les règles déterminent la manière dont les appels entrants sont gérés. Les règles s'appliquent uniquement aux appels et non aux fax et e-mails.

Les règles sont créées à l'aide de l'éditeur de règles graphique (Éditeur de CCV) en associant des objets CCV prédéfinis ; une fois terminées, elles peuvent être enregistrées sous un nom.

Les règles enregistrées peuvent être attribuées à un ou plusieurs calendriers en tant que règle par défaut (CCV par défaut) ou exception (Exception-CCV). L'ouverture, la modification et le nouvel enregistrement à l'aide de l'éditeur de règles sont possibles à tout moment.

Si une règle par défaut (CCV par défaut) a été affectée à un calendrier, ce calendrier peut être enregistré sous un nom librement définissable. Un calendrier avec une règle par défaut s'applique, après affectation à une file d'attente, 24 h sur 24 et 365 jours par an. Si à certains moments (pause, weekend, jours fériés, congés, etc.) d'autres règles s'appliquent, celles-ci peuvent être programmées dans le calendrier correspondant en tant que règles exceptionnelles (Exceptions-CCV). Il est ainsi possible de définir par exemple comment les appels entrants sont traités durant la période de congés. Les calendriers de congés sont prioritaires par rapport à d'autres calendriers et règles.

Éditeur de règles (éditeur de CCV)

L'éditeur de règles permet de définir des règles à partir des objets CCV prédéfinis. La disposition des objets CCV et leurs propriétés déterminent la manière dont les appels entrants sont traités.

Remarque : Une règle a une limite supérieure de 500 objets CCV.

Les objets CCV prédéfinis suivants sont disponibles.

Conseil : Pour tous les objets CCV indiqués s'appliquent les deux caractéristiques générales suivantes.

Description : possibilité de décrire l'objet CCV, par exemple l'annonce d'accueil.

Exécuter après la sélection : entrée du/des chiffre(s) nécessaires sans espace, virgule ou autre caractère. L'indication se rapporte à l'objet CCV précédent. Si 9 a été indiqué dans Chiffres acceptés, il faut aussi que 9 figure ici.

- **Lire le message**

  Provoque la diffusion de l'annonce sélectionnée. Il est possible de sélectionner un fichier audio figurant dans UC Suite. De plus, il est possible d'importer un nouveau fichier audio dans UC Suite ou d'enregistrer une nouvelle annonce puis de l'importer comme fichier audio dans UC Suite.

  La lecture de l'annonce provoque l'occupation d'un canal Media Stream Channel.

  Propriétés :

  – **Nom du fichier** : sélection d'une annonce (fichier audio au format wav)
  – **Touches Interrompre** : touche ou raccourci clavier permettant à l'appelant d'interrompre la diffusion de l'annonce.
  – **Gestionnaire de fichiers** : ce bouton permet directement de charger un fichier audio au format wav ou de créer un nouveau fichier voix avec l'enregistreur.
- **Déconnecter l'appelant**

  Provoque la coupure de la communication.

  Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.
- **Aller à CCV**

  Crée une boucle avec un autre objet CCV.

  Propriétés :

  – **CCV cible** : Sélection de l'objet CCV

- **Exécuter après la sélection**

  Provoque l'exécution du ou des objets CCV suivants en fonction des chiffres indiqués (action selon chiffres indiqués).

  Propriétés :

  – **Nom du fichier** : sélection d'une ou plusieurs annonces (fichier audio au format wav)
  – **Playlist** : Liste de diffusion des annonces sélectionnées (fichier audio au format wav) dans l'ordre de diffusion
  – **Délai Sélection de chiffre dépassé** : durée, en secondes, pendant laquelle le système de communication attend la saisie des chiffres.

    Si l'entrée de tous les chiffres n'a pas lieu dans le délai indiqué, le message (annonce) est de nouveau diffusé.
  – **Lien vers** : liste des chiffres avec destination.

    Les chiffres et destinations peuvent être ajoutés, traités et supprimés.
  – **Gestionnaire de fichiers** : ce bouton permet directement de charger un fichier audio au format wav ou de créer un nouveau fichier voix avec l'enregistreur.

  Le contenu de la playlist est affiché dans l'éditeur de règle à l'aide d'une infobulle lorsque l'on se positionne avec le pointeur de la souris sur l'objet CCV.
- **Transfert simple**

  Cette fonction dépend du paramètre **Standard automatique normal SST** (WBM, **Mode Expert** : **Applications** > **OpenScape Business UC Suite** > **Serveur** > **Paramètres généraux**) :

  – **Standard automatique normal SST** activé (paramètre standard, pas pour les États-Unis) : provoque le transfert de l'appel, indépendamment du fait que la destination est libre, occupée ou non disponible.

    Conseil : Pour un abonné avec Rejet des appels en instance, l'appel n'est transmis que lorsque l'abonné de destination est libre. Il ne se produit pas d'avertissement sur occupation.
  – **Standard automatique normal SST** désactivé (paramètre standard, uniquement pour les États-Unis) : provoque le transfert de l'appel, lorsque la destination est libre.

    Si la destination est occupée et que le rejet des appels en instance est désactivé, ou bien si la destination n'est pas disponible, il est diffusé une annonce à l'appelant. L'appelant peut choisir de laisser un message

sur la boîte vocale de l'abonné ou de composer le numéro d'une autre destination.

Si la destination est occupée et que le rejet des appels en instance est activé, il n'y a pas de transmission de l'appel.

Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

Propriétés :

– **Poste cible** : indication du numéro d'appel interne ou du numéro SDA externe, avec numéro de ligne réseau. Les espaces, les virgules ou autres caractères ne sont pas autorisés.

Le numéro de téléphone du poste cible est indiqué dans l'objet CCV.

Remarque : Après un transfert simple, le système déconnecte l'appel après avoir fait retentir la sonnerie durant 5 minutes.

- **Enregistrer dans la boîte vocale**

  Lance un appel vers la boîte vocale souhaitée d'un abonné ou vers un groupe Boîte vocale

  Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

  Propriétés :

  – **Boîte vocale Utilisateur** : indiquer le numéro de la messagerie vocale d'un utilisateur ou d'un groupe de messagerie vocale

  Le numéro d'appel et le nom de la boîte vocale ou le groupe Boîte vocale sont affichés dans l'éditeur de règle à l'aide d'une infobulle lorsque l'on se positionne avec le pointeur de la souris sur l'objet CCV.

- **Transfert supervisé**

  Provoque le transfert de l'appel vers une destination interne. Durant le transfert, l'appelant entend la musique d'attente (Music On Hold MoH de la UC Suite).

  À la différence du transfert en une étape vers l'objet CCV, il faut ici ajouter deux autres objets CCV. Il faut définir la manière dont le système de communication doit se comporter lorsque la destination est occupée ou en cas de non-réponse. Normalement, une annonce est diffusée à l'appelant dans ces cas.

  Propriétés :

  – **Poste cible** : indication du numéro de téléphone interne.

    Seuls sont supportés des numéros de téléphone internes du propre nœud. Le renvoi vers des destinations externes, des abonnés virtuels, d'autres standards automatiques (AutoAttendant), UCD (y compris le

Centre de contacts), ainsi que les destinations externes CallMe n'est pas autorisé ! Pour ces scénarios, utiliser la SST (transfert pas à pas).

– **Délai de sonnerie dépassé (s)** : durée, en secondes, pendant laquelle il faut décrocher l'appel.

  Si l'appel n'est pas décroché dans le délai imparti, il est renvoyé vers le système de communication et l'objet CCV suivant est utilisé.

  Conseil : La durée indiquée ici doit être inférieure à la durée paramétrée pour le renvoi temporisé (paramètre par défaut pour le renvoi temporisé = 15 secondes). Voir Comment configurer le transfert d'appel.

– **Annuler l'appel en cas de renvoi des appels adressés au destinataire** : Option (uniquement pour un numéro interne.)

  Lorsque cette option est activée, la destination d'appel est contrôlée. Si un renvoi temporisé ou un renvoi d'appel a été programmé pour la destination d'appel, l'appel est renvoyé vers le système de communication et l'objet CCV suivant est utilisé.

– **Contrôler l'état de présence lorsque vous transférez un appel** : Option

  Si l'option est activée, il est effectué un contrôle de l'état Présence de la destination d'appel. Si l'état Présence est différent de Bureau, l'appel est renvoyé vers le système de communication et l'objet CCV suivant est utilisé.

  Remarque : Si un appel entrant provient d'un numéro supprimé/inconnu et que l'appel est automatiquement pris en charge par le standard automatique UC Suite et transféré par la fonction superviseur, le numéro de l'appelant affiché devient le numéro de UC Suite.

- **Numérotation par nom**

  L'appelant est invité à entrer les trois premières lettres du nom de l'abonné demandé à l'aide du clavier de numérotation.

  S'il existe un abonné dont le nom commence par la lettre entrée, une connexion est établie.

  S'il existe plusieurs abonnés dont le nom commence par la lettre entrée, les noms de ces abonnés sont indiqués à l'appelant (10 abonnés maxi.). Si l'abonné n'a pas enregistré d'annonce du nom, il est diffusé à la place le numéro de téléphone. Après sélection de l'abonné souhaité, une connexion est créée.

  Si aucun abonné ne comprend les lettres de début entrées, l'appelant reçoit un message correspondant.

  Conseil : Les touches du clavier de numérotation réagissent au premier appui. Chaque appui permet de contrôler s'il existe des noms de famille d'abonné correspondant aux lettres correspondant à la touche.

  Exemple: dans le répertoire interne, il existe les cinq noms de famille suivants commençant par t, u et v : Taylor, Taler, Ullrich, Vasquez et Volterra. Pour établir une connexion avec

l’abonné Taylor, il faut appuyer sur les touches suivantes : 8 2 9

Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

Propriétés :

– **Méthode** : sélection de **Transférer au poste** ou **Enregistrer dans la messagerie vocale**.

  Selon la méthode sélectionnée, il est établi une liaison avec l'abonné souhaité ou avec sa boîte vocale. Dans ce cas, seuls les abonnés internes dont le nom et le prénom figurent dans le répertoire interne bénéficient d'une assistance.

- **Composer par poste**

  L'appelant est invité à composer le numéro de l'abonné demandé à l'aide du clavier de numérotation.

  Si l'appelant sélectionne le numéro d'un abonné virtuel, il est invité à entrer un autre numéro d'appel. Ensuite, une liaison est établie. Si l'abonné demandé ne répond pas, sa boîte vocale prend l'appel.

  Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

  Propriétés :

  – **Méthode** : sélection de **Transférer au poste** ou **Enregistrer dans la messagerie vocale**.

    Selon la méthode sélectionnée, il est établi une liaison avec l'abonné souhaité ou avec sa boîte vocale. Notez que seuls les abonnés internes du réseau dont le numéro de téléphone figure dans le répertoire interne bénéficient d'une assistance.

- **Régler langue**

  Provoque le choix de la langue pour l'annonce par défaut sur la base du numéro de l'appelant. Remarque : seules les annonces par défaut (annonces système) et non pas les annonces personnelles sont prises en considération.

  Il est possible de définir par exemple que, pour un numéro avec indicatif national + 49, il sera diffusé une annonce en allemand et que, pour un numéro avec indicatif national +33, il sera diffusé une annonce en allemand.

  Propriétés :

  – **Langue par défaut** : liste déroulante de sélection d’une langue.

    La langue choisie ici est utilisée pour tous les numéros de téléphone pour lesquels il n'a pas été défini de langue.
  – **Motif** : indication du numéro de téléphone, auquel une langue déterminée doit être affectée.

    Il est possible d'utiliser les jokers ci-après. * = nombre quelconque, ? = chiffre quelconque.
  – **Langue** : liste déroulante permettant de choisir la langue qui doit être affectée au numéro de téléphone correspondant (**Modèle**).

  Il est possible d'affecter un nombre non limité de numéros d'appel différents à une langue (**Modèle**).

- **Routage CLI**

  Provoque le renvoi d'un appel en direction d'un ou plusieurs objets CCV successifs à l'aide du numéro de l'appelant.

  Il est possible, par exemple, de définir que, pour un numéro avec indicatif national +49, il sera tout d'abord diffusé une annonce en allemand (objet CCV **Lire le message**) puis que l'appel sera ensuite renvoyé vers un téléphone interne (objet CCV **Transfert simple**). L'indicatif local peut également être utilisé (par exemple 089 pour Munich).

  Dans le contexte de UC Suite et CLI Routing, les utilisateurs doivent considérer des scénarios spécifiques, tels que les appels entrants de MS Teams Native SIP Trunk. Si vous avez l'intention d'envoyer vers OpenScape Business les numéros des appelants au format canonique, y compris l'indicatif de pays, vous devez établir des règles de routage CLI supplémentaires.

  Par exemple, si les appelants de MS Teams ont des numéros au format +49777555XXXX, et que 777555 est la partie commune de ces numéros, les utilisateurs doivent créer des règles de routage CLI pertinentes qui intègrent cette partie commune (777555).

  Propriétés :

  – **Standard** : liste déroulante pour sélection de l'objet CCV.

    L'objet CCV sélectionné ici est utilisé pour tous les numéros de téléphone, même pour ceux où aucune destination spécifique n'a été définie.
  – **Motif** : indication du numéro de téléphone, auquel un objet CCV déterminé doit être affecté en tant que destination.

    Il est possible d'utiliser les jokers ci-après. * = nombre quelconque, ? = chiffre quelconque.
  – **Description**

    Indication d'une explication.

    Pour le **Modèle** +49 (=Indicatif national Allemagne), il est possible, par exemple, d'indiquer Allemagne.

    Le texte indiqué ici est affiché dans l'éditeur de règles.
  – **Destination** : liste déroulante permettant de choisir l'objet CCV auquel il est attribué comme destination au numéro de téléphone correspondant (**Modèle**).

  Un objet CCV peut affecter un nombre non limité de numéros d'appel différents (**Modèle**) en tant que destinations.
- **Branche sur variable**

  Provoque le renvoi d'un appel en direction d'un ou plusieurs objets CCV successifs sur la base d'une condition.

  Il est possible de définir par exemple que les appelants vont entendre une annonce (Veuillez rappeler ultérieurement...) dès que plus de 20 appels figurent dans une file d'attente.

  Propriétés :

  – **Variable** : sélection d'**Appels** ou **Agents disponibles**.

    Selon la variable sélectionnée, la condition est le nombre des appels en attente dans une file d'attente ou le nombre des agents disponibles (y

compris les agents en durée de post-traitement) d'une file d'attente. Dans la liste déroulante correspondante, la condition (**inférieur à**, **supérieur à**, **inférieur ou égal à**, **supérieur ou égal à**, **égal à**) doit être sélectionnée et la valeur de comparaison doit être entrée dans le champ de saisie correspondant.

– **Branche Vrai** : liste déroulante pour la sélection de l'objet CCV qui doit être utilisé comme destination si la condition est remplie.
– **Branche Faux** : liste déroulante pour la sélection de l'objet CCV qui doit être utilisé comme destination si la condition n'est pas remplie.

Le nombre des agents disponibles dans une file d'attente est influencé par les modifications suivantes de l'état des agents :

– Connexion d'un agent dans la file d'attente à l'aide de « Connexion/ Login » : --> +1
– Déconnexion d'un agent de la file d'attente à l'aide de « Déconnexion/ Logout » : --> -1
– Agent à l'état "En pause" :-->-1
– Agent à l'état "Disponible après pause" :--> +1

Le nombre des agents disponibles dans une file d'attente **n'est pas** influencé par les modifications suivantes de l'état des agents :

– Agent à l'état « En Sonnerie »
– Agent à l'état « En communication »
– Agent à l'état « Post-traitement »
– Agent à l'état « Appel manqué »
– Agent à l'état « En Dépassement »

16.1.2.1.1 Comment ajouter une exception dans CCV

Si à certains moments (pause, week-end, jours fériés, congés, etc.) d'autres règles s'appliquent, celles-ci peuvent être programmées dans le calendrier correspondant en tant que règles exceptionnelles (Exceptions CCV). Il est ainsi possible de définir par exemple comment les appels entrants sont traités durant la période de congés. Les calendriers de congés sont prioritaires par rapport à d'autres calendriers et règles.

Étape par étape

1) Naviguez vers le **Mode expert > Applications > OpenScape Business UC Suite**.
2) Cliquez sur **Calendriers**, sélectionnez l'un des calendriers disponibles et cliquez sur **Modifier**.

   Vous pouvez cliquer sur **Ajouter** pour créer un nouveau calendrier.
3) Cliquez sur **Ajouter** dans la zone **Exceptions**.
4) Remplissez le champ **Description**, si vous le souhaitez.

5) Sélectionnez le type d'exception parmi les options disponibles :
   - **À l'intérieur de la plage Heure** : sélectionnez une heure, un jour et une périodicité spécifiques pour l'exception
   - **À l'intérieur de la plage Date Heure** : sélectionnez une date, une heure, un jour et une périodicité spécifiques pour l'exception
   - **Calendrier de congés** : sélectionnez une date de congés spécifique pour l'exception
   - **Récurrence annuelle** : indiquez si l'exception doit se répéter chaque année
6) Cliquez sur **Sauvegarder**.

16.1.2.2 Modèles

Les templates ci-après sont des modèles prédéfinis normalisés pour le Company AutoAttendant (UC Suite), ils peuvent être modifiés à loisr et adaptés aux besoins spécifiques.

Modèle 1 - 7410 CCV: Appel avec commutation (sans messagerie vocale)

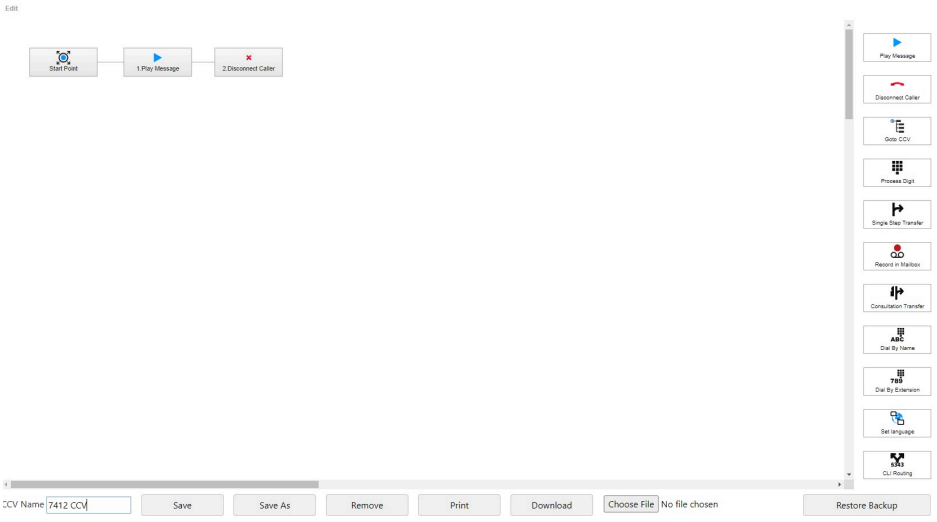
Il est diffusé une annonce à l'appelant. Ensuite, il lui est demandé d'appuyer sur une touche (chiffre) et il est transféré vers un abonné. Si l'appelant n'appuie sur aucune touche, il est transféré au poste de renvoi (par défaut 100).

Modèle 2 - 7411 CCV: Communication d'interphone avant la réponse

Il est diffusé une annonce à l'appelant. Ensuite, une commutation a lieu vers le poste de renvoi 100.

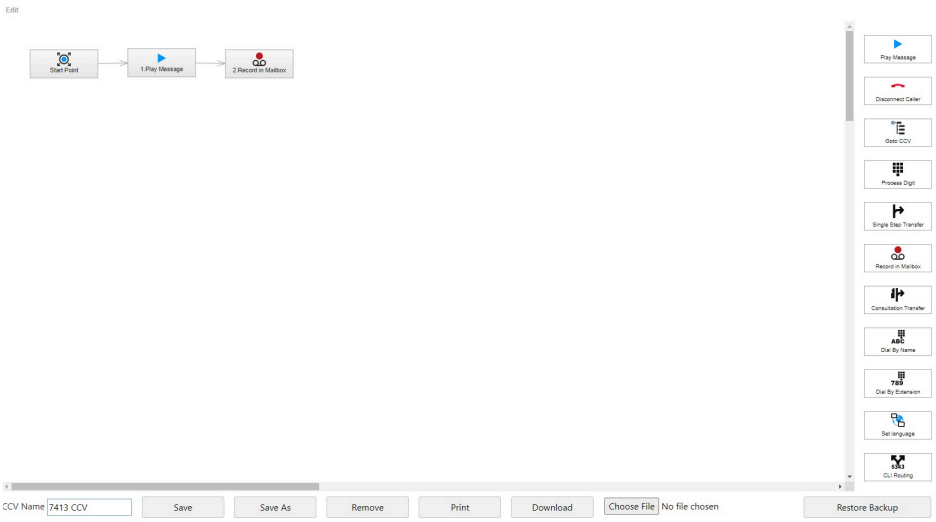
Modèle 3 - 7412 CCV: Appeler en dehors des heures de bureau

Lors de la réception d'un appel en dehors des horaires de travail, il est diffusé une annonce à l'appelant. Ensuite, la connexion est coupée.



Modèle 4 - 7413 CCV: Appeler en dehors des heures de bureau grâce au renvoi d'appel vers la messagerie vocale

Lors de la réception d'un appel en dehors des horaires de travail, il est diffusé une annonce à l'appelant. Ensuite, il lui est demandé de procéder à un enregistrement dans une boîte vocale et il peut laisser un message.



16.2 Préposé OpenStage

Les fonctions d'assistant peuvent être assurées à l'aide d'un téléphone OpenStage spécialement configuré. L'opérateur OpenStage est également un poste d'interception.

Disposition des clés

OpenStage Attendant est la destination de tous les appels entrants non-DID et des appels pour lesquels aucun utilisateur n'a pu être joint (appels interceptés) via les critères d'attribution des appels. L'opérateur achemine ensuite ces appels vers la destination appropriée.

Les téléphones OpenStage suivants peuvent servir d'opérateur :

- OpenStage 30
- OpenStage 40
- OpenStage 60
- OpenStage 80

Sur les téléphones OpenStage configurés comme consoles d'opérateur, les touches de fonction programmables sont attribuées comme suit :

- Service de nuit
- Annuaire (annuaire téléphonique)
- Appels en attente
- Outrepasser
- Prise
- Externe 1
- Externe 2 (non compatible avec OpenStage 40)
- Clé vide non attribuée (non compatible avec OpenStage 40)

16.3 mon assistant

Un large éventail de fonctions d'assistant est à votre disposition via mon assistant. Les abonnés peuvent être facilement gérés ici via des boutons utilisateur. De plus, les fonctions de messagerie (messagerie vocale, fax, messagerie instantanée, SMS et courriels) sont disponibles via le Centre de messagerie.

Fonctions principales de l'agent de service

Un maximum de 20 assistants peuvent être connectés par système de communication (par nœud). La configuration maximale du réseau est égale aux capacités totales des systèmes de communication en réseau. La présence et le statut téléphonique sont affichés pour tous les abonnés du réseau. Le centre de messagerie de mon assistant affiche les abonnés de son propre système de communication.

- Gérer les appels en attente ou acceptés
- Les données de l'appel en cours sont affichées.
- Les appels en attente sont affichés.
- Liste des appelants
- Journal des appels ouverts, programmés, internes, externes, répondus, manqués et sortants
- application d'annuaire (répertoire téléphonique)
  - LDAP (par exemple, ODS)
  - Répertoire personnel / Contacts Outlook
  - Répertoire interne, pour toutes les stations interconnectées du réseau.
- État du champ lumineux occupé de tous les abonnés internes du système ainsi que de toutes les stations du réseau
  - Statut du téléphone : Libre, Occupé, Appel reçu, Transfert d'appel, Ne pas déranger
  - Statut de présence (Bureau, Appelez-moi, Réunion, Malade, Pause, Absent du bureau, Vacances, Déjeuner, Rentré à la maison (à l'échelle du réseau)

  Remarque : Le statut de présence « malade » peut ne pas être disponible, selon les paramètres système définis par l'administrateur.
- Vous avez le choix entre trois styles d'interface.
- Un maximum de 20 assistants peuvent être connectés par système de communication (jusqu'à 20 licences par OpenScape Business X5/X8 et OpenScape Business S). L'octroi de la licence à mon assistant se fait via le WBM.

Exigences techniques (voir les informations commerciales pour plus de détails)

- PC Windows standard
- Microsoft Windows 10 / 8.1 / 8 / 7 (versions 32 bits et 64 bits possibles)
- Microsoft Windows Vista (32 bits)
- Utilisation possible du serveur de terminal

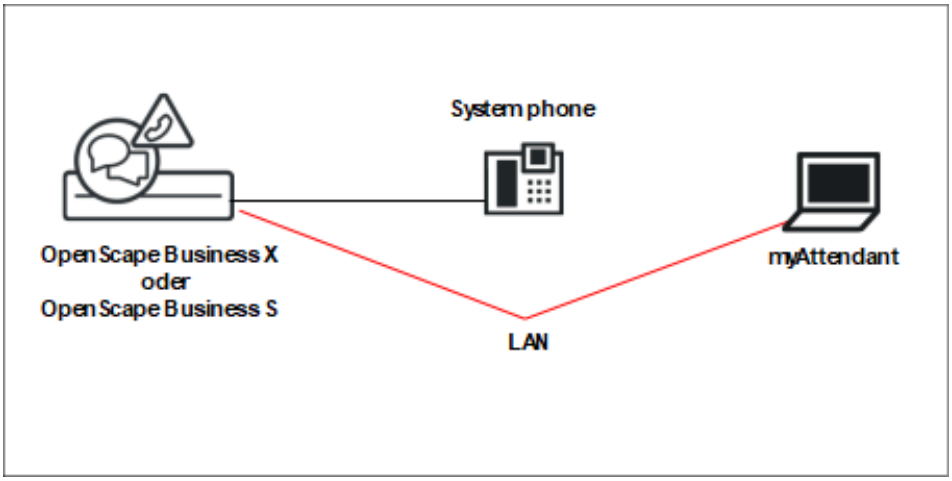
Logiciels supplémentaires

- Oracle Java 8 ou supérieur ou, alternativement, OpenJDK 8 (voir **Logiciel** > **du centre de services**)

Téléphones compatibles

- Openstage 40/60/80 HFA
- Téléphone de bureau OpenScape IP 35G/55G HFA
- Téléphone de bureau OpenScape IP 35G Eco HFA
- Téléphone de bureau OpenScape CP 100/200/205/400/600/600E/700/700X HFA
- Téléphone de bureau OpenScape CP 110/210/410/710 HFA
- Téléphones SIP compatibles avec la norme RFC 3725, par exemple : 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

Installation simple et rapide ; les premières étapes de l'installation sont envoyées à l'utilisateur par le système (si son adresse électronique a été configurée).



16.3.1 Gestion des abonnés

Pour la gestion des abonnés dans myAttendant, on dispose des boutons utilisateur, du répertoire interne, du répertoire externe et du répertoire personnel.

Boutons utilisateur

Les boutons utilisateur se trouvent dans l'onglet **Par défaut** et font partie de la page principale de myAttendant.

Dans un onglet des boutons utilisateur, 100 boutons utilisateur sont disponibles par défaut. Vous pouvez modifier le nombre de boutons utilisateur par défaut par onglet à chaque fois que vous le souhaitez.

Par défaut, les boutons utilisateur sont triés par ordre alphabétique selon le nom de famille.

Il est possible de créer plusieurs onglets pour les boutons utilisateur ; vous pouvez choisir librement le nom de ces boutons utilisateur.

Il est possible d'affecter aux boutons utilisateur des abonnés internes et externes, ainsi que des contacts personnels (utilisateurs).

16.3.2 Centre de messages

Dans **Centre de messagerie** de myAttendant, les messages voix, fax et instantanés ainsi que les SMS et e-mails sont consignés et gérés.

Les messages peuvent être gérés pour d'autres abonnés. Ils doivent pour cela bénéficier d'une autorisation.

Dans la liste des abonnés, tous les abonnés du système de communication sont listés avec leur état Présence/Absence. En haut figure votre propre état, avec l'aperçu des messages ouvert. Les autres abonnés suivent dans l'ordre alphabétique.

En fonction de la sélection opérée dans la liste des messages, il est affiché sous forme de tableau, des informations sur les messages ; celles-ci peuvent ensuite être sélectionnées pour modification.

Les types de messages peuvent être gérés comme indiqué ci-après.

- Les **messages vocaux** peuvent être écoutés, effacés, renvoyés,
- Les **messages LAN** peuvent être lus, modifié et supprimés,
- Les **messages Fax** peuvent être renvoyés.

Messages LAN

Les messages LAN ne peuvent être créés que par les utilisateurs de myAttendant. Ils servent de "tableau noir" pour l'abonné qui peut prendre des notes (sur les différents abonnés). Ces messages peuvent être consultés, modifiés ou effacés ; ils ne peuvent pas être envoyés à d'autres abonnés.

16.3.3 Scénario 1 : Comment paramétrer myAttendant sur un système OpenScape Business unique

Conditions préalables

La licence pour myAttendant est disponible

RNIS avec licence valide

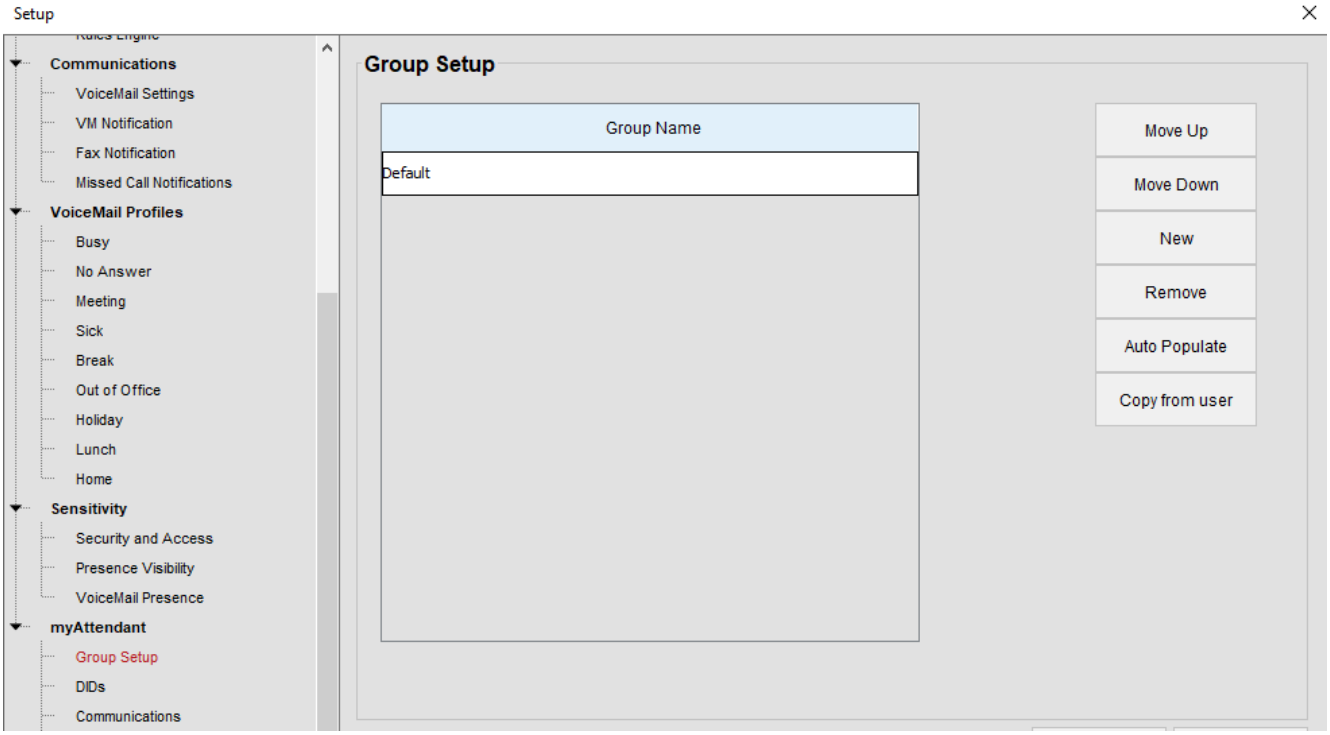
Serveur d'application ou Carte d'application disponible

UC Suite est activé à l'aide de l'assistant d'installation de base

Étape par étape

1) Configurer le téléphone du poste opérateur à l'aide de WBM
2) Sous **Abonnés**>**Clients IP**>**Clients système**>**Abonnés**>**Modifier les indicateurs abonné**, désactiver **Rejet des appels en instance** en **mode Expert**.
3) Sous **Serveur de téléphonie**>**Configuration de base**>**Téléphone> Renvoi distinct**>**P.O.**>**Hotline**, activez la fonctionnalité **Avertissement immédiat pour les appels du P.O** en **mode Expert**.

4) Contrôlez ou modifiez les critères de renvoi et les numéros du P.O. (définir les options de renvoi et les numéros du poste opérateur).
5) Procédure de licence de myAttendant
6) Après connexion au système de communication, il est possible de remplir automatiquement le BLF. Vous pouvez effectuer cette configuration dans myAttendant, sous **Configuration > myAttendant > Paramétrage de groupe**.



16.3.4 Scénario 2 : Comment paramétrer deux myAttendants ou plus sur un système OpenScape Business unique

Le scénario 2 s'appuie sur le scénario 1 et il est paramétré en supplément.

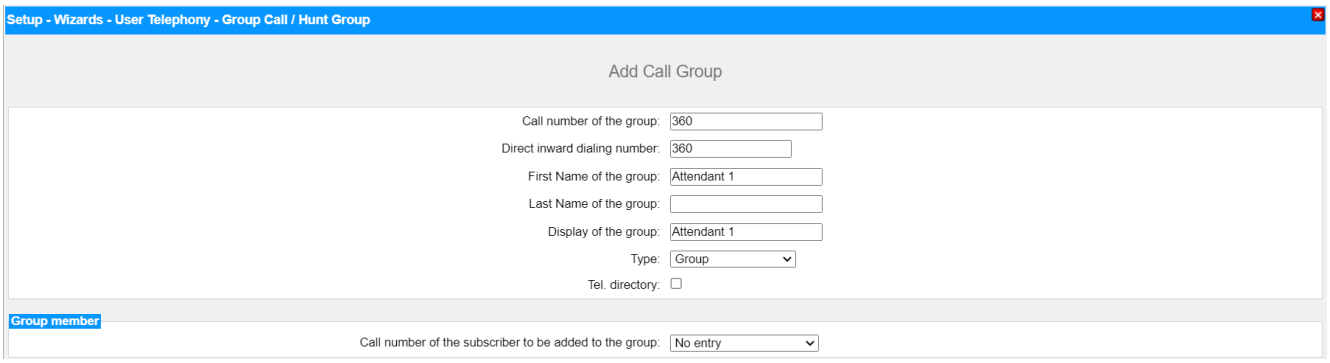
Conditions préalables

Licences suffisantes pour myAttendant

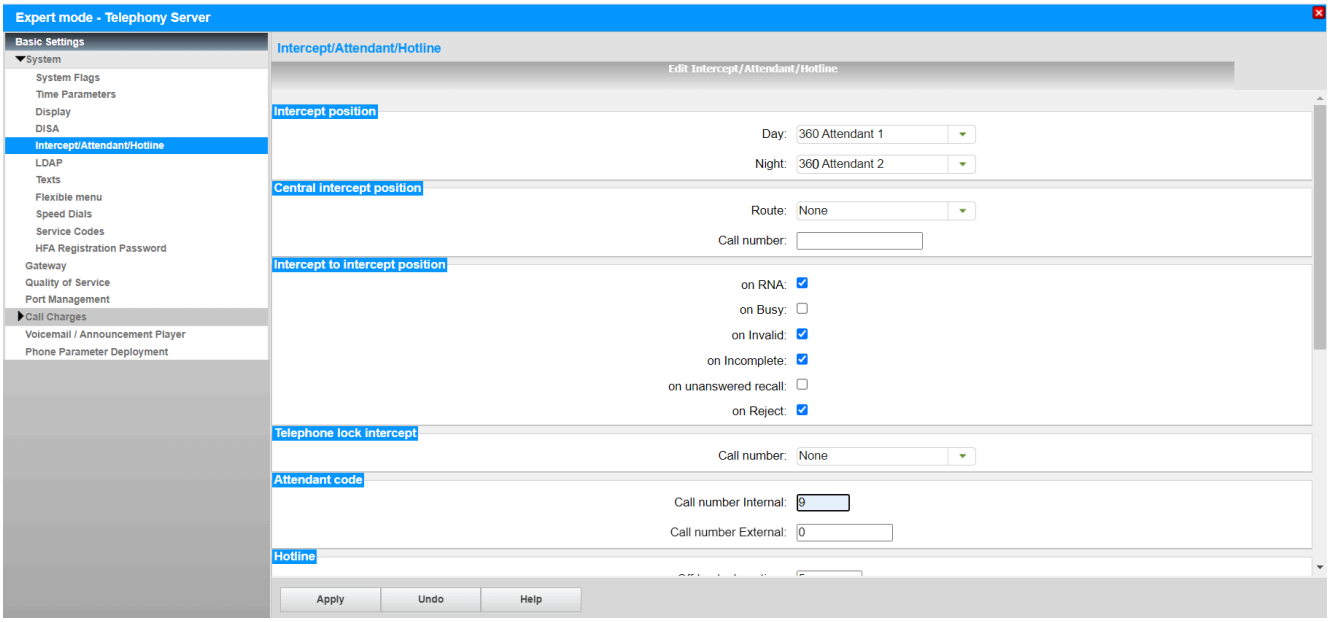
RNIS avec licence valide

Étape par étape

1) Configurez un groupe (composé uniquement de postes opérateur) dans la WBM, sous **Configuration** > **Téléphonie utilisateurs** > **Appel de groupe/ Groupe de recherche** > **Ajouter**.



2) Sélectionnez ce groupe lors de la configuration des téléphones de poste opérateur OpenStage.



16.3.5 Scénario 3 : Comment configurer un réseau OpenScape Business avec un myAttendant central

Le scénario 3 s'appuie sur le scénario 1 et 2 et il est paramétré en supplément. Le nœud 1 est associé au nœud 2. Le poste opérateur central se trouve sur le nœud 2.

Conditions préalables

Nombre de licences suffisant pour myAttendant

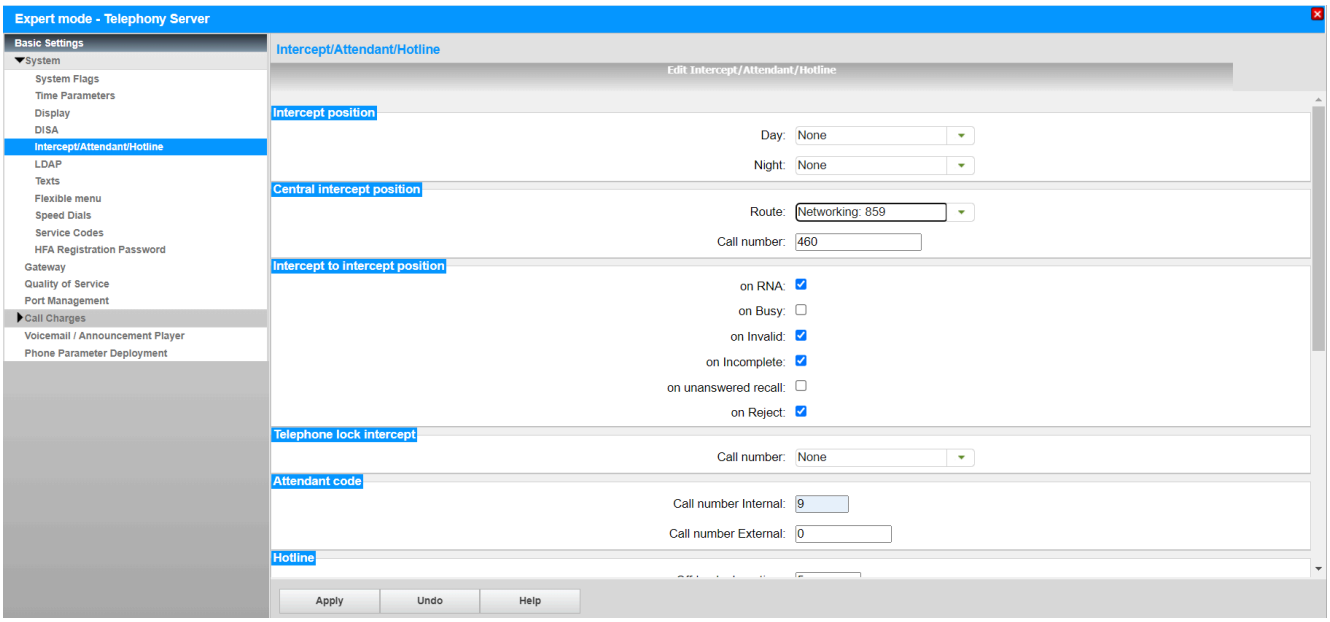
Des licences pour la mise en réseau sont disponibles

RNIS avec licence valide

LCR est paramétré

Étape par étape

1) Établissez un poste de renvoi central sur le nœud 1. Le poste de renvoi central doit être créé dans un nœud où AUCUN poste opérateur n'a été configuré.



2) Configurez le poste opérateur pour le système 2 (comme décrit au scénario 2).
3) Installez myAttendant avec les données utilisateur du noeud 2.

16.4 Poste de renvoi

Afin qu'aucun appel ne se perde, le système de communication permet de renvoyer vers un poste de renvoi distinct (à définir) les appels externes qui ne peuvent pas être affectés à un abonné ou qui ne reçoivent pas de réponse. En tant qu'administrateur, vous pouvez configurer les critères de renvoi.

Le poste de renvoi peut être un abonné un groupe d'abonnés ou un dispositif d'annonces :

- Poste de renvoi (Poste opérateur)
- Abonnés
- Groupe de recherche
- Appel de groupe
- Equipement d'annonces externe

Un groupe UCD ne doit pas être sélectionné comme poste de renvoi.

Si un poste de renvoi distinct est configuré, les appels sont alors renvoyés vers ce poste de renvoi. Si aucun poste de renvoi n'est configuré, les appels renvoyés sont adressés au premier abonné IP.

Si un abonné interne est paramétré comme poste de renvoi, il lui est automatiquement affecté la configuration des touches standard. De plus, il est possible d'autoriser le poste de renvoi pour la fonctionnalité "Entrée en tiers".

En tant qu'administrateur, vous pouvez affecter au poste de renvoi, interne et externe, un numéro de poste (2 positions) permettant d'y accéder directement.

Un renvoi s'applique pour l'ensemble du système, c'est-à-dire de façon identique pour tous les abonnés sur les systèmes multi-sociétés. Voir aussi "Poste de renvoi central dans l'interconnexion de réseaux" au chapitre Mise en réseau.

Critères de renvoi

Avec les critères de renvoi, vous définissez en tant qu'administrateur dans quelles situations le renvoi doit avoir lieu. Les états de renvoi suivants sont possibles.

- Sur non réponse

  L'appel se conforme aux indications figurant dans la gestion des appels (par ex. un renvoi temporisé configuré). Si aucun abonné ne prend l'appel, celui-ci est transmis au poste de renvoi.
- Renvoi sur occupation lorsque plus aucun renvoi temporisé n'est possible

  Tout d'abord, le système vérifie si une tonalité d'avertissement doit être envoyée ou non. S'il n'est pas possible d'envoyer une tonalité d'avertissement, l'appel se conforme aux indications figurant dans Call Management (par exemple un renvoi temporisé d'appel configuré). Si aucun abonné ne prend l'appel, celui-ci est transmis au poste de renvoi. Le renvoi distinct sur occupation se rapporte uniquement au premier appel, et non pas aux connexions commutées ou sortantes. Le retour d'appel d'un abonné externe n'est pas immédiatement rejeté chez l'abonné de destination occupé, mais une tonalité d'avertissement est générée.
- Sur fausse numérotation

  Si le numéro appelé n'est pas configuré ou n'est pas actif.
- Si numérotation incomplète

  Si le numéro appelé est trop court. S'il existe un poste central de renvoi distinct, aucune numérotation incomplète n'est évaluée.
- Retour en cas de non-réponse

  Si un renvoi avant réponse est effectué et demeure sans réponse et si le retour d'appel vers la destination d'origine n'est pas non plus répondu, le système effectue alors un renvoi distinct, une fois écoulée la temporisation réglée.
- Sur Rejet

  Si l'appel a été refusé par un abonné interne, l'appel se conforme aux indications de Call Management (par ex. un renvoi temporisé d'appel configuré). Si aucun abonné ne prend l'appel, celui-ci est transmis au poste de renvoi.
- En cas d'absence de numéro de téléphone

  Comme pour une fausse numérotation.
- En cas de transfert d'appel avec chaînage

  Si un appel renvoyé rencontre une nouveau renvoi lorsqu'il arrive à la destination du premier renvoi et que le nombre des chaînages possibles est dépassé, il est alors effectué un renvoi distinct. Le nombre des chaînages possibles est fonction dans inscriptions dans le renvoi temporisé. Au maximum trois chaînages sont autorisés.

- En cas de code de verrouillage

  Lorsqu'un abonné compose un préfixe faisceau sur un téléphone où le code de verrouillage est activé, un renvoi a lieu. L'administrateur définit pour ce cas une destination de renvoi séparée.
- En cas d'annonce (uniquement avec UC Suite)

  Lorsqu'un abonné compose le numéro du P.O. (2 positions) alors qu'il est en train d'entendre une annonce de la boîte vocale ou du standard automatique, un renvoi a lieu. L'administrateur définit pour ce cas une destination de renvoi séparée.

Correspondances

Rubrique	Correspondance
Appels de données	Les appels de données sont coupés au lieu d'être rejetés.
Groupe de recherche	A partir d'un groupe de recherche, il n'est pas réalisé de renvoi distinct ; l'appel est réacheminé au premier abonné du groupe de recherche et reste donc à l'intérieur du groupe de recherche.
Configuration des touches par défaut	La programmation des touches par défaut comprend également la touche **Affichage du Nb d'appels**. Celle-ci ne peut être attribuée qu'à 6 terminaux. Lorsque la limite est atteinte, aucune autre fonction de touche par défaut n'est attribuée. Les fonctions de touches par défaut attribuées ne sont pas retirées lorsque l'appareil n'est plus défini comme poste de renvoi.
Lignes S_0	Pour les lignes S_0, une analyse n'est effectuée que si aucun poste de renvoi Jour/Nuit n'est configuré.
Renvoi de nuit	Pour pouvoir atteindre la même destination depuis les lignes SDA et les lignes réseau analogiques lorsque le service de nuit est activé, l'entrée du numéro de poste de nuit dans Renvoi distinct > P.O. doit être identique au **N° Nuit** dans **l'acheminement Ligne**.

16.4.1 Comment configurer le poste de renvoi et les critères de renvoi

A l'aide de l'assistant **Poste opérateur**, vous pouvez configurer les numéros pour le poste de renvoi ainsi que les critères de renvoi.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Avancé**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs** .
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Poste opérateur**.

4) Dans **Poste opérateur** et **Numéro du P.O** (2 positions) indiquez les numéros de téléphone souhaités pour le poste de renvoi.
5) Dans la zone **Critères de renvoi**, définissez les valeurs souhaitées.
6) Cliquez sur **OK&Suivant** puis sur **Quitter**.

16.4.2 Comment configurer le poste de renvoi distinct central

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configuration de base** > **Système** > **Renvoi/P.O/Hotline**.
4) Dans la zone **Poste de renvoi central**, sélectionner l'entrée souhaitée dans la liste déroulante **Faisceau**.
5) Dans la plage **Poste de renvoi central**, indiqué le **Numéro de téléphone** souhaité pour **Jour** et **Nuit**.
6) Cliquez sur **Appliquer** puis sur **OK**.

16.4.3 Comment configurer le renvoi en cas de code de verrouillage

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configuration de base** > **Système** > **Renvoi/P.O/Hotline**.
4) Dans la zone **Renvoi en cas de code de verrouillage** dans la liste déroulante **Numéro de téléphone**, sélectionnez l'entrée souhaitée.
5) Cliquez sur **Appliquer** puis sur **OK**.

16.4.4 Comment configurer le renvoi en cas d'annonce

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Dans l'arborescence du menu, cliquez sur **Serveur**.
4) Cliquez sur l'onglet **Paramètres généraux**.
5) Dans la fenêtre **Numéro du poste de renvoi**, entrez le numéro de poste de renvoi dans le champ **Numéro de destination**.
6) Cliquez sur **Enregistrer** et fermez la fenêtre.

17 Centre de contacts multimédia

Le centre d'appels est une solution hautement performante pour la distribution et le traitement optimaux des appels, fax et e-mails entrants. La distribution intelligente, en fonction des compétences, est la garantie que l'appelant, indépendamment du moyen de contact utilisé, est mis en contact avec l'agent le mieux qualifié du centre d'appels. Grâce à l'application myAgent, tous les agents du centre d'appels disposent de fonctions confortables pour le traitement et le post-traitement des appels, fax et e-mails. Pour l'évaluation de l'exploitation du centre d'appels, myReports fournit de nombreux modèles de rapport.

Le centre d'appels multimédia est entièrement intégré au logiciel UC Suite. Toutes les composantes logicielles nécessaires sont comprises. Les fonctions du centre d'appel elles-mêmes sont validés dans le cadre d'une licence.

Le centre d'appels utilise les ressources du système de communication comme les files d'attente pour les appels entrants et les fonctions Unified Communications pour l'enregistrement et la diffusion des annonces.

La composante logicielle centrale du centre d'appels gère toutes les fonctions de routage pour les appels, fax, e-mails entrants ; elle gère également les PC postes de travail et les affichages muraux raccordés par un LAN.

L'application myAgent est installée sur les postes de travail (PC) des agents. Il est également possible d'installer (option) l'application myReports pour générer et envoyer des rapports. Le logiciel nécessaire peut être cherché directement dans la zone de téléchargement du système de communication et installé sur le PC client.

Au moyen de la WBM, il est procédé à la configuration des fonctions de base du Centre d'appels, des calendriers et règles de distribution ainsi que des agents. Le paramétrage pour l'exploitation au quotidien du centre d'appels, par exemple l'affectation des agents aux files d'attente, peut aussi être directement effectué à l'aide de myAgent.

Si le centre d'appels n'est pas disponible en raison de problèmes (défaillance, connexion manquante ou similaire), il est possible de réaliser une solution de repli avec la fonction UCD du système de communication. Les règles de distribution pour les cas d'urgence doivent être prises en compte lors de la configuration des groupes UCD dans le cadre de la première configuration du centre d'appels.

Conseil : Pour avoir des informations sur UC Suite et les fonctions Unified-Communications, consultez le chapitre UC Suite.

17.1 Centre d'appels Clients

L'application myAgent fournit à tous les agents du centre d'appels des fonctions confortables pour le traitement et le post-traitement des appels, fax et e-mails. L'application myReports permet d'établir des rapports sur les appels, files d'attente, agents, performances, niveaux de service et codes de post-traitement du centre de contacts. Plus de 100 modèles de rapport prédéfinis sont disponibles.

17.1.1 myAgent

Grâce à myAgent, tous les agents disposent de fonctions confortables pour le traitement et le post-traitement des appels, fax et e-mails.

myAgent offre les fonctionnalités suivantes :

- Traitement de
  - Effectuer des appels
  - Fax
  - E-mails
- Fonction de rappel pour les agents
- Affichage et modification de l'état de l'agent
- Affichage et modification de l'état de présence des abonnés internes du système de communication
- Représentation des files d'attente en temps réel
- Enregistrement des appels, si activé dans le système de communication
- Messagerie instantanée
- Demande d'assistance par
  - Surveillance d'appel (diffère selon le pays)
  - Entrée en tiers dans les appels
  - Messagerie instantanée
- Intégration de l'annuaire interne, de l'annuaire externe, du répertoire hors ligne externe (LDAP) et des contacts Outlook pour les recherches par nom
- Création de rapports sur la base de modèles de rapport prédéfinis

En fonction du niveau d'autorisation attribué, l'agent dispose de fonctions standard (Agent) ou de fonctions étendues (Superviseur ou Administrateur) dans myAgent (voir Fonctions soumises à autorisation pour les agents).

L'affectation des agents aux files d'attente est effectuée à l'aide de l'application myAgent. Cette affectation ne peut être effectuée que par un agent avec classe de discrimination Superviseur ou Administrateur. Dans ce cas, il est possible d'affecter aux agents les propriétés suivantes (Affectation des agents) qui ont une influence sur la distribution des appels, fax et e-mails dans une file d'attente.

- **Agent primaire** ou **Agent de débordement**

  Des appels sont répartis de manière égale entre les agents primaires. Un agent de débordement ne reçoit un appel que si les appels dépassent un certain nombre ou si un appel a dépassé un certain temps d'attente.
- **Activer le rappel d'agent**

  Le rappel d'agent permet à un appelant en file d'attente de laisser un message vocal aux agents. Dès qu'un agent compétent est disponible, il reçoit un appel, entend le message vocal de l'appelant et peut le rappeler.
- **Niveau de compétence**

  Le niveau de compétence détermine la répartition des appels entre les agents dans une file d'attente ; les agents disposant du niveau de compétence le plus élevé sont privilégiés lors de la distribution des appels. Lorsque tous les agents ont le même niveau de compétence, l'appel est envoyé à l'agent libre depuis le plus longtemps.

- **Post-traitement**

  Le post-traitement permet aux agents de terminer les éventuelles tâches à traiter, par exemple d'ordre administratif, après la fin d'un appel, avant qu'un nouvel appel ne leur soit adressé.
- **Débordement après x appels dans la file d'attente**

  Les appels au-delà de ce nombre maximum sont envoyés à un agent de débordement.
- **Débordement après x secondes**

  Les appels qui dépassent ce temps d'attente sont envoyés à un agent de débordement.

Le domaine **Liste des affectations d'agent** indique aux agents de niveau d'autorisation Superviseur ou Administrateur l'affectation des agents aux files d'attente. Les agents de niveau d'autorisation Agent ne voient que les files d'attente auxquelles ils sont affectés.

17.1.2 Prérequis pour myAgent

Pour utiliser myAgent, le PC client de l'abonné doit être équipé de la configuration matérielle et logicielle appropriée.

Conseil : Vous devez impérativement tenir compte des remarques figurant dans le fichier `ReadMe first` se trouvant dans répertoire de stockage des fichiers d'installation.

Téléphones

myAgent peut être utilisé en combinaison avec les téléphones suivants :

- OpenStage HFA
- Téléphone de bureau OpenScape IP 35G/55G HFA
- Téléphone de bureau OpenScape IP 35G Eco HFA
- Téléphone de bureau OpenScape CP 100/200/205/400/600/600E/700/700X HFA
- Téléphone de bureau OpenScape CP 110/210/410/710 HFA
- OpenStage T
- OpenScape Édition Personnelle HFA

Les appareils plus anciens (tels que optiPoint 410/420/500 et Gigaset M2/SL3/S4/SL4/S5) sont pris en charge. Les appareils Optiset E ne peuvent pas être utilisés. myAgent ne peut pas être utilisé avec les stations SIP, les stations Mobility, les stations virtuelles, les groupes ou les stations MULAP. Vous trouverez des informations détaillées sur les téléphones testés et mis sur le marché dans l'avis de mise sur le marché.

Systèmes d'exploitation

myAgent peut être utilisé en combinaison avec les systèmes d'exploitation suivants :

- Microsoft Windows 10 / 8.1 / 8 / 7 (versions 32 bits et 64 bits possibles)
- Microsoft Windows Vista (32 bits)

Conseil : Le système d'exploitation utilisé requiert toujours la dernière version de toutes les mises à jour disponibles (Service Packs et correctifs).

La prise en charge de myReports pour Microsoft Windows XP et Microsoft Windows Server 2003 prendra fin en même temps que la fin du support de ces produits par Microsoft. Le produit continuera d'être pris en charge, mais ne sera plus testé en détail.

Logiciels supplémentaires

- Oracle Java 8 ou supérieur ou, alternativement, OpenJDK 8 (voir **Logiciel** > **du centre de services**)
- Adobe Reader 9 ou version ultérieure (pour les rapports au format PDF)

Configuration matérielle minimale requise

- Processeur 2 GHz
- RAM : 2 GO
- Réseau local 100 Mbps
- Résolution d'écran XGA (1024 x 768), myPortal pour Outlook : résolution d'écran SVGA (800 x 600)

Serveur Terminal Microsoft, serveur Citrix XenApp

myAgent peut être utilisé dans les environnements Microsoft Terminal Server et Citrix Server sous les conditions préalables suivantes :

Conseil : Les environnements Terminal Server et Citrix Server, y compris les services hébergés et les environnements virtuels, sont sous la responsabilité du client.

Conseil : Les environnements serveur Citrix peuvent décoder correctement certains caractères régionaux (par exemple, les trémas allemands).

Systèmes d'exploitation :

- Microsoft Windows Server 2015 (32 bits / 64 bits) en tant que serveur Terminal Server Microsoft
- Microsoft Windows Server 2012 (32 bits / 64 bits) en tant que serveur Terminal Server Microsoft
- Microsoft Windows Server 2008 R2 (64 bits) en tant que serveur Terminal Server Microsoft
- Microsoft Windows Server 2008 R2 (64 bits) avec Citrix XenApp 6.5 Server (mode bureau)

La prise en charge de myAgent pour Microsoft Windows XP et Microsoft Windows Server 2003 prendra fin en même temps que la fin du support de ces produits par Microsoft. Le produit continuera d'être pris en charge, mais ne sera plus testé en détail.

Configuration matérielle requise : Le nombre de clients installables dépend des performances du serveur et de la quantité de mémoire disponible. Si le serveur

est également utilisé pour d'autres applications, leurs besoins en mémoire doivent également être pris en compte.

Vous trouverez plus d'informations sur la configuration de Citrix XenApp Server à l'adresse suivante :

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

Fichiers d'installation

Les options suivantes sont disponibles pour fournir les fichiers d'installation aux utilisateurs :

- L'administrateur télécharge les fichiers d'installation depuis le **Centre de services** et les met à la disposition des utilisateurs via un lecteur réseau, par exemple.

Vous devez tenir compte des remarques figurant dans le fichier `ReadMe first`, se trouvant dans répertoire de stockage des fichiers d'installation.

Conseil : La distribution automatique du fichier MSI via un service de déploiement avec Microsoft Windows Server n'est pas prise en charge.

17.1.3 myReports

Les agents de niveau Superviseur ou Administrateur peuvent, à l'aide de myReports, établir des rapports sur les agents et leurs activités, sur les appels, les files d'attente, les performances, les niveaux de service et les codes de post-traitement.

myReports offre les fonctionnalités suivantes :

- Plus de 100 modèles de rapports prédéfinis et classés par domaines (groupes de rapports) pour la création de rapports.
- Calendriers pour générer les rapports selon une programmation temporelle
- Envoi immédiat ou temporisé des rapports par e-mail
- Exportation des rapports à gestion temporelle
- Formats de sortie pour l'aperçu de rapport, l'envoi d'e-mails et l'exportation de rapports : Excel, PDF et Word
- Aperçu du rapport pour contrôler le format souhaité du rapport à créer.

Fonctions de l'utilisateur

myReports possède sa propre gestion des utilisateurs qui règle l'accès aux fonctions de myReports à l'aide de rôles d'utilisateur. Il est fait la distinction entre l'utilisateur myReports (utilisateur par défaut) et l'administrateur myReports.

Votre fonction d'utilisateur actuelle est définie lors de votre connexion à myReports.

Les différences entre les fonctions de l'utilisateur sont indiquées dans le tableau ci-après.

myReports : Opération	Fonction de l'utilisateur	
	myReports Utilisateur	myReports Administrateur
Rapports		
Aperçu Rapport	X	X
Envoyer immédiatement un rapport par e-mail	X	X
Ajouter un modèle de rapport	X	X
Effacer les modèles de rapport ajoutés	X	X
Définir un nouveau modèle de rapport		X
Actualiser les modèles de rapport prédéfinis		X
Calendriers		
Ajouter un calendrier	X	X
Afficher les détails d'un calendrier	X	X
Modifier le calendrier	X	X
Supprimer le calendrier	X	X
Configuration		
Changer la langue de l'interface utilisateur	X	X
Modifier la couleur de l'interface utilisateur	X	X
Configurer un modèle de courrier électronique	X[5]	X
Modifier l'adresse du serveur	X	X
Modifier le mot de passe Administrateur		X
Configurer les préfixes pour les numéros de téléphone externes		X
Activer/Désactiver la protection des données		X
Comment configurer l'emplacement d'enregistrement pour l'exportation des rapports à gestion temporelle		X
Paramétrer la langue		X[6]
Paramétrer la langue par défaut		X[6]

[5] Pour la configuration du modèle de courrier électronique, il est nécessaire d'entrer le mot de passe de l'administrateur

17.1.3.1 Comment réinitialiser le mot de passe pour l'Administrateur myReports

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**.
4) Cliquez sur **Maintenance**.
5) Cliquez sur **Réinitialiser le mot de passe** dans la zone **Rapports**.

Étapes suivantes

Informez le ou les administrateur(s) myReports de la réinitialisation du mot de passe de l'administrateur au mot de passe par défaut dans `Rapports`.

17.1.4 Conditions nécessaires pour myReports

Afin d'utiliser myReports, le PC client de l'abonné doit présenter des configurations de matériel et de logiciel adaptées.

Conseil : Assurez-vous de consulter les remarques figurant dans le fichier `ReadMe first`, qui se trouve dans le répertoire de stockage des fichiers d'installation.

Systèmes d'exploitation

myReports peut être utilisé en combinaison avec les systèmes d'exploitation suivants :

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bits ou 64 bits)
- Microsoft Windows Vista (32 bits)

Conseil : Le système d'exploitation utilisé a toujours besoin de la version la plus actuelle de toutes les mises à jour disponibles (Service Packs et Patches).

L'assistance pour myReports pour Microsoft Windows XP et Microsoft Windows Server 2003 se termine au même moment que l'arrêt de l'assistance par Microsoft. Le produit continue à bénéficier d'une assistance, mais il n'est plus testé de manière détaillée.

---

[6] Pour être en mesure de paramétrer la langue ainsi que la langue par défaut, il faut être inscrit en tant que Administrateur myReports avec un mot de passe.

Logiciels supplémentaires

- Oracle Java 8 ou version ultérieure, ou bien OpenJDK 8 (voir **Centre de service** > **Logiciel**)
- Adobe Reader 9 ou version ultérieure (pour les rapports au format PDF)
- Microsoft Excel 16 / 2013 / 2010 (pour les rapports au format Excel)
- Microsoft Word 16 / 2013 / 2010 (pour les rapports au format Word)

Configuration minimale requise du matériel

- CPU 2 GHz
- RAM : 2 Go
- LAN 100 Mbit/s (LAN 1 Gbit/s recommandé)
- Résolution écran XGA (1024x768), myPortal for Outlook : SVGA (800x600)

PC multi-utilisateurs

Pour les PC multi-utilisateurs fonctionnant sous Microsoft Windows 7 ou Microsoft Windows Vista, chaque utilisateur local peut utiliser myReports avec ses paramètres personnels si le premier utilisateur local les a installés en utilisant les droits d'administration locale. Seul le premier utilisateur local disposant de droits d'administration locaux est en mesure d'effectuer les mises à jour avec AutoUpdate.

Microsoft Terminal Server, Citrix XenApp Server

Les conditions suivantes doivent être respectées pour pouvoir utiliser myReports dans les environnements Microsoft Terminal Server et Citrix Server :

Conseil : Les environnements Terminal Server et Citrix Server, y compris les services hébergés et les environnements virtuels, relèvent de la responsabilité du client.

Conseil : Il peut arriver que les environnements du serveur Citrix ne décodent pas correctement certains caractères régionaux (par ex. inflexions en allemand).

Systèmes d'exploitation :

- Microsoft Windows Server 2015 (32 bits / 64 bits) come Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bits / 64 bits) come Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bits) comme Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bits) avec Citrix XenApp 6.5 Server (Desktop Mode)

Conditions matérielles : le nombre des clients pouvant être installés est fonction des performances du serveur et de la mémoire de travail disponible. Lorsque d'autres applications sont utilisées sur le serveur, il faut tenir compte de leurs besoins en mémoire de travail.

Vous trouverez des informations supplémentaires sur la configuration dans Citrix XenApp Server dans :

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

Fichiers d'installation

Pour la fourniture des fichiers d'installation aux utilisateurs, les possibilités suivantes sont disponibles.

- L’administrateur télécharge les fichiers d’installation à partir du **Centre de service** et les fournit aux utilisateurs, par ex. sur un lecteur réseau.

Vous devez tenir compte des remarques figurant dans le fichier `ReadMe first`, se trouvant dans répertoire de stockage des fichiers d'installation.

Conseil : La distribution automatique du fichier MSI via un service de déploiement avec Microsoft Windows Server n’est pas prise en charge.

17.1.5 Remarques sur l'utilisation simultanée de myAgent et des clients UC Suite

Lorsque myAgent et d'autres clients UC Suite sont utilisés simultanément via un seul compte utilisateur UC Suite, la possibilité d'interactions mutuelles ne peut être exclue.

Dans cette section, le terme myPortal est utilisé de manière générique pour désigner myPortal pour ordinateur, myPortal pour Outlook et myPortal @work.

Exemples d'interactions mutuelles :

- Modifier le statut de présence via myPortal

  Ces exemples s'appliquent au paramètre **de messagerie vocale** par défaut pour toutes les destinations de transfert d'appel.

  – myAgent : L’agent est connecté.

  myPortal : La réinitialisation automatique du statut de présence à Office est désactivée.

  Modifier le statut de présence via myPortal entraîne la déconnexion immédiate de l'agent de la ou des files d'attente. Une fois que l'agent

se déconnecte via myAgent, son statut de présence dans myPortal est réinitialisé à **Bureau** .

Un changement de statut de l'agent via myAgent (par exemple, passage à **Pause**) est enregistré par myPortal, mais cela ne s'applique pas à **Connexion** , **Déconnexion** et **Temps de travail** .

– myAgent : L’agent est connecté.

myPortal : La réinitialisation automatique du statut de présence à « Office » est activée.

Si l'agent modifie son statut via myAgent en **« Pause »** , il sera automatiquement de nouveau disponible une fois la pause terminée.

Un changement de statut de présence via myPortal à **« Pause** » entraîne la déconnexion immédiate de l’agent de la ou des files d’attente.

– myAgent : L’agent est connecté.

Un changement de statut de présence via myPortal en mode « **Ne pas déranger »** entraîne la déconnexion immédiate de l'agent de la ou des files d'attente.

- Appels sortants via monPortail

  Le statut de présence de l'abonné est visible via myAgent.

  Les appels apparaissent uniquement dans le journal de myPortal. Aucun transfert vers les statistiques du centre de contact n'est effectué, car il ne s'agit pas d'appels provenant du centre de contact.
- Appels entrants au numéro de poste de l'agent

  Le statut de présence de l'abonné est visible via myAgent.

  Les appels apparaissent uniquement dans le journal de myPortal. Aucun transfert vers les statistiques du centre de contact n'est effectué, car il ne s'agit pas d'appels provenant du centre de contact.
- Enregistrement d'un appel

  L'enregistrement des appels via myPortal n'est pas enregistré par myAgent. myAgent propose cette fonction même si l'enregistrement d'un appel est déjà en cours via myPortal.

17.2 Agents

Les agents qui font partie d'une file d'attente (abonnés) constituent un groupe de travail qui peut être utilisé par exemple pour les hotlines techniques ou dans la réception des commandes. Les appels, fax et e-mails entrants sont répartis de manière équitable entre les agents disponibles d'une file d'attente.

Pour utiliser comme agent un abonné du système de communication, il faut que cet abonné soit configuré comme agent. Les droits des agents sont définis en sélectionnant le niveau d'autorisation (Agent, Superviseur ou Administrateur). Un agent avec le niveau d'autorisation Superviseur ou Administrateur dispose d'autorisations élargies (voir Fonctions soumises à autorisation pour les agents).

Un agent peut être défini comme un agent disponible de manière durable. L'agent demeure ensuite disponible pour les appels, fax et e-mails, même s'il n'a pas répondu à un appel, un fax ou un e-mail.

17.2.1 Fonctions soumises à autorisation pour les agents

Lors de la configuration d'un abonné comme agent, les droits de l'agent sont définis par le choix du niveau de discrimination (agent, superviseur ou administrateur. Un agent ayant le niveau d'autorisation Superviseur ou Administrateur dispose d'autorisations élargies.

Les différences entre les niveaux sont indiquées dans le tableau ci-après.

myAgent :	**Niveau d'autorisation (classe de service)**		
Opération	**Agent**	**Superviseur**	**Administrateur**
Affecter un agent à une file d'attente	–	X	X
Déplacer l'agent vers une autre file d'attente	–	X	X
Supprimer l'agent d'une file d'attente	–	X	X
Modifier l'état d'un agent	–	X	X
Afficher/masquer la liste de liaison agent	Files d'attente assignées	Toutes les files d'attente	Toutes les files d'attente
Modifier l'affectation de l'agent	–	X	X
Afficher la liste des appels en direct	Files d'attente assignées	Toutes les files d'attente	Toutes les files d'attente
Placer myAgent automatiquement au premier plan en cas d'alarme	–	X	X
Activer la tonalité d'alarme	–	X	X
Afficher le panneau mural	Files d'attente assignées	Toutes les files d'attente	Toutes les files d'attente
Afficher le graphique Niveau de service	Files d'attente assignées	Toutes les files d'attente	Toutes les files d'attente
Afficher le graphique Temps moyens	Files d'attente assignées	Toutes les files d'attente	Toutes les files d'attente
Déplacer un appel vers la première position d'une file d'attente	–	X	X
Enregistrer un appel	Appel actuel	Tous les appels	Tous les appels
Enregistrer sous forme de fichier WAV l'enregistrement d'un appel ou l'envoyer par e-mail sous forme de fichier WAV.	–	X	X
Enregistrer un fax en tant que fichier au format TIFF ou l'envoyer par e-mail	–	X	X
Enregistrer un e-mail sous la forme d'un fichier EML ou l'envoyer par e-mail sous la forme d'un fichier EML	–	X	X
Surveillance d'appel (diffère selon le pays)	–	X	X

myAgent : Opération	Niveau d’autorisation (classe de service)		
	Agent	**Superviseur**	**Administrateur**
Entrée en tiers dans un appel	–	X	X
Répondre à une demande d’assistance	–	X	X
Créer un rapport	–	X	X
Ouvrir WBM	–	X	X

17.2.2 Agents préférés

Il est possible d'affecter un ou plusieurs agents préférés d'une file d'attente à chaque appelant (par exemple à chaque client qui appelle). Dans ce cas, le système de communication essaie tout d'abord de transférer à un agent préférentiel l'appelant et les demandes de rappel de cet appelant. Lorsque plusieurs agents préférés ont été définis, il est possible de fixer une priorité (ordre) pour l'affectation des agents préférés.

Si aucun des agents préférés n'est disponible, l'appel est transféré à un agent disponible quelconque.

17.2.3 Agent figurant dans plusieurs files d'attente

Un agent peut être affecté à plusieurs files d'attente avec différents niveaux de compétence. Il faut indiquer si l'agent doit avoir le rôle d'agent primaire ou celui d'agent de débordement.

17.2.4 Pauses du Centre de contacts

Pour permettre à chaque agent d'utiliser des pauses spécifiques, il est possible de définir des pauses du centre de contacts de différentes durées (par exemple pause Déjeuner, pause Cigarette). Les pauses du centre de contacts sont disponibles pour l'ensemble du système et peuvent, en cas de nécessité, être sélectionnées par un agent à l'aide de myAgent.

17.2.5 Connexion/Déconnexion d'agent via téléphone

La connexion/déconnexion au centre de contacts est également prise en charge par téléphone sans avoir à se servir de myAgent pour utiliser les fonctions du centre de contacts. Si un agent a été connecté par téléphone, seuls les appels vocaux peuvent être traités. Les fenêtres contextuelles et l'entrée de code de post-traitement ne sont pas prises en charge dans ce cas. Cela s'applique également si myAgent est actif et que l'agent se connecte au centre de contacts à l'aide du téléphone. La fonctionnalité complète de myAgent peut être récupérée si l'agent se déconnecte via le téléphone, puis se connecte via myAgent.

Conditions et contraintes

- Les fonctions du centre de contacts OpenScape Business par téléphone ne fonctionnent que pour les agents pour lesquels une licence myAgent est attribuée dans OpenScape Business
- Toutes les fonctions ne sont prises en charge que sur les téléphones qui sont validés pour une utilisation avec le centre de contacts OpenScape Business
- Dans le cas où la connexion par téléphone a réussi et que le client myAgent associé n'est pas actif, seuls les appels vocaux sont routés vers l'agent
- Dans le cas où la connexion par téléphone a réussi et que le client myAgent associé est actif, les e-mails / fax et les rappels ne sont pas présentés à l'agent s'il ouvre une session par téléphone. Dans ce cas, les écrans contextuels et le post-traitement fonctionnent comme d'habitude, mais seuls les appels vocaux seront fournis à l'agent. Pour obtenir une fonctionnalité complète, l'agent doit d'abord se déconnecter via le mode téléphone et se connecter ensuite via myAgent

Connexion au centre de contacts par téléphone

Lorsque les agents se connectent par téléphone au centre de contacts OpenScape Business, indépendamment de myAgent client, et que le centre de contacts est actif :

- Les fonctions UCD pour la connexion sont utilisées sur le téléphone
- Les fonctions de connexion peuvent être exécutées soit à l'aide du code de fonctionnalité soit à l'aide d'une touche programmée
- L'agent est connecté à toutes les files d'attente auxquelles il est affecté dans la configuration du centre de contacts
- L'affichage du téléphone indique à l'agent l'état de la connexion
- Seules les informations de file d'attente UCD (par exemple les informations sur les appels en file d'attente) sont affichées sur demande

L'agent peut utiliser les fonctions suivantes :

- Connexion/Déconnexion (avec ID agent UCD)
- Post-traitement
- Disponible/Non disponible
- Affichage des appels dans la file d'attente UCD à laquelle l'ID des agents UCD a été attribué

Remarque : Renvoi de nuit UCD ne doit pas être utilisé par l'agent.

Remarque : L'indicateur de disponibilité permanente de myAgent fonctionne avec la connexion par téléphone. Ceci signifie que, si un agent est connecté avec son téléphone et un appel est manqué, cet agent reste disponible pour l'appel suivant. C'est le même comportement qu'avec le client myAgent.

En cas de défaillance du centre de contacts pendant l'ouverture de session de l'agent, l'agent reste connecté en UCD et les appels vocaux sont acheminés conformément au routage UCD. Dans le cas où cet agent n'était pas connecté, il peut se connecter à UCD par téléphone.

Déconnexion du centre de contacts par téléphone

Lorsque les agents se déconnectent par téléphone du centre de contacts OpenScape Business, indépendamment de myAgent client, et que le centre de contacts est actif :

- Les fonctions UCD pour la déconnexion sont utilisées sur le téléphone
- Les fonctions de déconnexion peuvent être exécutées soit à l'aide du code de fonctionnalité soit à l'aide d'une touche programmée
- L'agent est déconnecté de toutes les files d'attente auxquelles il est affecté dans la configuration du centre de contacts
- L'affichage du téléphone indique à l'agent l'état de la déconnexion
- Aucune autre information Centre de contacts / UCD (par exemple, informations sur les appels en file d'attente) n'est affichée

Définir l'agent disponible / non disponible par téléphone

Lorsqu'un agent définit par téléphone son état (disponible/indisponible pour le routage des contacts du centre de contacts OpenScape Business), indépendamment de myAgent client, et que le centre de contacts est actif :

- L'affichage du téléphone indique à l'agent l'état de la connexion
- Si myAgent n'est pas actif, seuls les appels vocaux sont routés par l'agent

Paramétrer/réinitialiser le travail après appel (Post-traitement) via téléphone

Lorsqu'un agent place par téléphone son état sur "Travailler après appel", indépendamment de myAgent client, et que le centre de contacts est actif, il n'est envoyé aucun appel à l'agent jusqu'à la fin du délai de post-traitement spécifique de l'agent qui est configuré dans le centre de contacts OpenScape Business ou jusqu'à ce que l'agent ait réinitialisé le post-traitement par téléphone.

Mappage état

Le changement d'état de l'agent par téléphone est affecté comme indiqué ci-après par rapport à la situation de l'agent de myAgent :

Equipement téléphonique			myAgent			
Code de fonctionnal	**Code de fonctionnal**	**Description**	Texte d'affichage du téléphone	**Etat**	**Texte supplémentair**	Remarque
*401	ID agent UCD	UCD - Intégration agents	Disponible	Disponible	-	L'agent est défini comme disponible dans toutes les files d'attente affectées
#401	–	UCD - Retrait agent	Non disponible	Non disponible	-	L'agent est défini comme non disponible à partir de toutes les files d'attente affectées

Equipement téléphonique			myAgent			
Code de fonctionnal	**Code de fonctionnal**	**Description**	Texte d'affichage du téléphone	**Etat**	**Texte supplémentair**	Remarque
*402	–	UCD - Agent disponible	Disponible	-	-	Disponible (fin du temps de travail)
#402	–	UCD - Agent indisponible	Non disponible	Post-traitement	Décompte à partir de 999,999 secondes	-
*403	–	UCD Activer post-traitement	Post-traitement	Post-traitement	Décompte du temps de travail configuré	Le temps de travail doit être terminé avant qu'il ne soit possible de recommencer. Il n'y pas de cumul du temps de travail comme dans myAgent. Une fois que le temps de travail est écoulé, l'agent est automatiquement remplacé à l'état disponible.
#403	–	UCD Désactiver post-traitement	Disponible	Disponible	-	-
*404	destination du renvoi de nuit	UCD Activer renvoi de nuit	–	N'est pas supporté	-	Le renvoi de nuit UCD ne doit pas être utilisé
#404	–	UCD Désactiver renvoi de nuit	–	N'est pas supporté	-	Le renvoi de nuit UCD ne doit pas être utilisé

Equipement téléphonique			myAgent			
Code de fonctionnal	**Code de fonctionnal**	**Description**	Texte d'affichage du téléphone	**Etat**	**Texte supplémentair**	Remarque
*405	–	UCD Interroger file d'attente	-	-	-	Seule la file d'attente à laquelle l'ID de l'agent UCD a été affecté est affichée, indépendamment du fait que l'agent est affecté à plusieurs files d'attente dans le centre de contacts

17.3 Files d'attente et calendriers

Les files d'attente constituent la base du centre de contacts. Les appels, les fax et les e-mails destinés à une file d'attente sont gérés en fonction du niveau de compétences des agents, de la priorité et du temps d'attente. Il est possible de diffuser des annonces aux appelants qui se trouvent en attente. Le calendrier définit la manière dont les appels entrants doivent être traités certains jours et à certaines heures.

17.3.1 Files d'attente

En général, la distribution des appels se passe de telle sorte qu'un appel entrant, un fax ou un e-mail est transféré vers la file d'attente de l'abonné (agent) du groupe dont la dernière communication remonte le plus loin. Il est également possible de définir d'autres règles de distribution (par exemple à l'aide des niveaux de compétence des agents). Si tous les agents sont occupés, les appels arrivants sont placés en attente puis répartis ensuite en fonction de leur priorité et de leur temps d'attente en direction des agents qui se libèrent.

A partir des calendriers et des règles y figurant (= CCV, Call Control Vector), il est possible de définir comment un appel en file d'attente doit être traité à une heure définie ou lors d'un jour défini. Les règles définissent par exemple l'annonce diffusée à l'appelant ou la destination de renvoi de l'appel.

Les fax, e-mail et rappels d'agent sont directement affectés aux files d'attente, indépendamment des calendriers.

Lors de l'affectation des agents aux files d'attente, il est possible d'affecter différentes caractéristiques aux agents (affectation des agents) qui ont une influence sur la distribution des appels dans une file d'attente (par exemple agent primaire ou agent de débordement, niveau de compétence). Il est possible d'affecter les agents aux files d'attente

- à l'aide de la WBM par un administrateur de profil **Advanced**.
- à l'aide de l'application myAgent par un agent de niveau Superviseur ou Administrateur.

Si un agent est affecté à plusieurs files d'attente, il est possible de déterminer si les appels pour une file d'attente doivent être envoyés à cet agent avec une priorité supérieure à celle des appels pour les autres files d'attente.

Pour les files d'attente, il est possible de définir les paramètres essentiels suivants à l'aide de la WBM.

- Activer, désactiver, effacer les files d'attente

  Avertissement : après effacement d'une file d'attente, il n'est pas possible d'établir des rapports sur les périodes de temps passées. Il est préférable de désactiver les files d'attente qui ne sont plus nécessaires.
- Configurer les alarmes de files d'attente

  Les possibilités suivantes sont offertes :

  – Nombre des alarmes en file d'attente (nombre seuil d'alarmes) : Lorsque le nombre indiqué ici d'appels en attente dans la file d'attente est dépassé, l'icône de la file d'attente passe du vert à l'orange pour les agents. Les agents de niveau de discrimination Superviseur ou Administrateur peuvent décider d'être avertis par une tonalité d'alarme ou de faire apparaître automatiquement myAgent au premier plan.
  – Durée de l'alarme dans le file d'attente (durée seuil de l'alarme) : si le temps d'attente d'un appel dans la file d'attente indiqué ici est dépassé, l'entrée correspondante de la liste des appels au centre de contacts devient rouge pour les agents.. Les agents de niveau de discrimination Superviseur ou Administrateur peuvent décider d'être avertis par une tonalité d'alarme ou de faire apparaître automatiquement myAgent au premier plan.
- Définir le délai d'expiration appels manqués, fax et e-mails

  Si un appel, un fax ou un e-mail n'est pas pris par un agent à l'issue de l'intervalle de temps indiqué ici, l'appel, le fax ou l'e-mail est transmis à l'agent libre suivant.
- Définir le seuil pour les appels abandonnés

  A partir du temps indiqué, il est décidé si l'appel abandonné doit être intégré ou non dans les statistiques (dans les reports). Sont consignés dans les statistiques les appels qui sont abandonnés une fois écoulé le temps indiqué.
- Configurer la profondeur de la file d'attente

  Contrôle du nombre maximal d'appels actifs et en attente dans une file d'attente spécifique. Le centre de contacts indique au système que le seuil défini de la taille de la file d'attente est atteint. En conséquence, le système rejette chaque nouvel appel pour la file d'attente appropriée avant que l'appel ne soit connecté au système, jusqu'à ce que le nombre d'appels soit inférieur au seuil.

  La taille maximale de la file d'attente est déterminée par les paramètres suivants :

  – Nombre maximum de positions en attente à l'intérieur de la file d'attente. (WLS = taille de la boucle d'attente)
  – Nombre maximal d'appels actifs et en attente de la file d'attente (taille de la profondeur de file d'attente).

- Paramétrer les pilotes pour les messages Fax entrants

  Si des numéros ont été configurés, ceux-ci peuvent être sélectionnés pour les messages Fax entrants. Les messages Fax envoyés à ces numéros sont placés dans la file d'attente et traités comme des appels entrants.
- Paramétrer le service pour les e-mails entrants

  Il est possible de paramétrer plusieurs adresses e-mail pour une file d'attente. Les e-mails envoyés à cette adresse sont placés dans la file d'attente et traités comme des appels entrants.
- Paramétrer l'adresse électronique de l'expéditeur

  Adresse e-mail de la file d'attente qui est affichée chez le destinataire lors de l'envoi d'un e-mail par un agent.
- Activer l'acheminement intelligent des appels

  Un appel entrant est renvoyé à l'agent qui a été connecté en dernier à l'appelant. Il faut pour cela qu'aucun agent préféré n'ait été défini pour cet appelant.

17.3.2 Planifications

Pour chaque file d'attente, il est déterminé, à partir d'un calendrier et des règles y figurant (Call Control Vector CCV), comment les appels entrants doivent être traités selon les jours et selon les périodes de temps.

Il est par exemple possible de définir, pour les jours ouvrés, une règle pour l’équipe du matin (de 6h00 à 14h00), une pour l’équipe de midi (14h00 à 22h00) et une pour l’équipe de nuit (22h00 à 06h00). Il est possible de définir une règle de fin de semaine pour le week-end. Dans chacune de ces règles, il est par exemple possible d'indiquer si une annonce doit être diffusée ou non et/ou la destination de renvoi des appels.

Les calendriers sont l'élément essentiel dans la configuration du centre d'appels. S'il n'est pas défini au moins un calendrier, il n'est pas possible de terminer avec succès la configuration d'un centre d'appels. Il faut affecter au moins un calendrier à chaque file d'attente. Il peut toujours s'agir du même calendrier.

Un calendrier doit comporter au moins une règle (Call Control Vector CCV). Pour la période de validité d'un calendrier, les règles déterminent la gestion des appels entrants dans une file d'attente. Les règles s'appliquent uniquement aux appels et non aux fax et e-mails.

Les règles sont créées à l’aide de l’éditeur de règles graphique (Éditeur de CCV) en associant des objets CCV prédéfinis ; une fois terminées, elles peuvent être enregistrées sous un nom.

Les règles enregistrées peuvent être attribuées à un ou plusieurs calendriers en tant que règle par défaut (CCV par défaut) ou exception (Exception-CCV). L'ouverture, la modification et le nouvel enregistrement à l'aide de l'éditeur de règles sont possibles à tout moment.

Si une règle par défaut (CCV par défaut) a été affectée à un calendrier, ce calendrier peut être enregistré sous un nom librement définissable. Un calendrier avec une règle par défaut s'applique, après affectation à une file d'attente, 24 h sur 24 et 365 jours par an. Si à certains moments (pause, week-end, jours fériés, congés, etc.) d’autres règles s’appliquent, celles-ci peuvent être programmées dans le calendrier correspondant en tant que règles

exceptionnelles (Exceptions-CCV). Il est ainsi possible de définir par exemple comment les appels entrants sont traités durant la période de congés. Les calendriers de congés sont prioritaires par rapport à d'autres calendriers et règles d'une file d'attente.

Éditeur de règles (éditeur de CCV)

L'éditeur de règles permet de définir des règles à partir des objets CCV prédéfinis. La disposition des objets CCV et leurs propriétés déterminent la manière dont les appels entrants sont traités.

Remarque : Une règle a une limite supérieure de 500 objets CCV.

Les objets CCV prédéfinis suivants sont disponibles.

Conseil : Pour tous les objets CCV indiqués s'appliquent les deux caractéristiques générales suivantes.

Description : possibilité de décrire l'objet CCV, par exemple l'annonce d'accueil.

Exécuter après la sélection : entrée du/des chiffre(s) nécessaires sans espace, virgule ou autre caractère. L'indication se rapporte à l'objet CCV précédent. Si 9 a été indiqué dans Chiffres acceptés, il faut aussi que 9 figure ici.

- **Lire le message**

  Provoque la diffusion de l'annonce sélectionnée. Il est possible de sélectionner un fichier audio figurant dans UC Suite. De plus, il est possible d'importer un nouveau fichier audio dans UC Suite ou d'enregistrer une nouvelle annonce puis de l'importer comme fichier audio dans UC Suite.

  La lecture de l'annonce provoque l'occupation d'un canal Media Stream Channel.

  Propriétés :

  – **Nom de fichier** : sélection d'une annonce (fichier audio au format wav)
  – **Touches Interrompre** : touche ou raccourci clavier permettant à l'appelant d'interrompre la diffusion de l'annonce.
  – **Gestionnaire de fichiers** : ce bouton permet directement de charger un fichier audio au format wav ou de créer un nouveau fichier voix avec l'enregistreur.
- **Musique d'attente**

  Lance la musique d'attente (Music on Hold MOH du système de communication) pour les appelants extérieurs, pendant une durée réglable

  Propriétés :

  – **Valeur temporelle** : durée, en secondes, pendant laquelle la musique d'attente est diffusée.
- **Déconnecter l'appelant**

  Provoque la coupure de la communication.

  Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

- **Informer l'appelant de sa position dans la file**

  Informe l'appelant sur sa position actuelle en file d'attente.
- **Temps d’attente estimé**

  Informe l’appelant sur son temps d’attente estimé.

  Le temps d’attente estimé est calculé à partir des données suivantes :

  1) Temps moyen historique en file d’attente pour toutes les files d’attente
  2) Temps moyen historique en file d’attente pour cette file d’attente
  3) Durée de communication moyenne historique pour cette file d’attente
- **Aller à CCV**

  Crée une boucle avec un autre objet CCV.

  Propriétés :

  – **CCV cible** : Sélection de l’objet CCV
- **Enregistrer le rappel**

  Permet à un appelant en file d'attente d'activer un rappel d'agent (enregistrement d'un message Voix). Le rappel d'agent prend la place de l'appelant dans la file d'attente. Le rappel d’agent figurant dans la liste des appels au centre d’appels est présenté aux agents disposant de la propriété **Activer le rappel d’agent**.

  Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

  Propriétés :

  – **Type** : sélection de **Rappel simple** ou **Rappel extensif**.

    À la différence d'un rappel simple, l'appelant dispose, dans un rappel extensif, de possibilités et d'informations supplémentaires (confirmation ou modification du numéro de téléphone servant pour le rappel, confirmation du message Voix).
  – **Longueur maximale du message** : temps en secondes disponible pour que l’appelant enregistre le message Voix.

- **Exécuter après la sélection**

  Provoque l'exécution du ou des objets CCV suivants en fonction des chiffres indiqués (action selon chiffres indiqués).

  Propriétés :

  – **Nom de fichier** : sélection d'une ou plusieurs annonces (fichier audio au format wav)
  – **Liste de diffusion** : Liste de diffusion des annonces sélectionnées (fichier audio au format wav) dans l'ordre de diffusion
  – **Délai pour les chiffres** : durée, en secondes, pendant laquelle le système de communication attend la saisie des chiffres.

    Si l'entrée de tous les chiffres n'a pas lieu dans le délai indiqué, le message (annonce) est de nouveau diffusé.
  – **Lien vers** : liste des chiffres avec destination.

    Les chiffres et destinations peuvent être ajoutés, traités et supprimés.
  – **Gestionnaire de fichiers** : ce bouton permet directement de charger un fichier audio au format wav ou de créer un nouveau fichier voix avec l'enregistreur.

  Le contenu de la playlist est affiché dans l'éditeur de règle à l'aide d'une infobulle lorsque l'on se positionne avec le pointeur de la souris sur l'objet CCV.
- **Transfert simple**

  Cette fonction dépend du paramètre **Standard automatique normal SST** (WBM, **Mode Expert** : **Applications** > **OpenScape Business UC Suite** > **Server** > **General Settings**) :

  – **Console opérateur SST normale** activée (paramètre par défaut ; pas pour les États-Unis) : provoque le transfert de l'appel, que la destination soit libre, occupée ou indisponible.

    Conseil : Pour un abonné avec Rejet des appels en instance, l'appel n'est transmis que lorsque l'abonné de destination est libre. Il ne se produit pas d'avertissement sur occupation.
  – **SST de la console opérateur normale** désactivé (paramètre par défaut, uniquement pour les États-Unis) : provoque le transfert de l'appel si la destination est gratuite.

    Si la destination est occupée et que le rejet des appels en instance est désactivé, ou bien si la destination n'est pas disponible, il est diffusé une annonce à l'appelant. L'appelant peut choisir de laisser un message

sur la boîte vocale de l'abonné ou de composer le numéro d'une autre destination.

Si la destination est occupée et que le rejet des appels en instance est activé, il n'y a pas de transmission de l'appel.

Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

Propriétés :

– **Poste cible** : indication du numéro d'appel interne ou du numéro SDA externe, avec numéro de ligne réseau. Les espaces, les virgules ou autres caractères ne sont pas autorisés.

Le numéro de téléphone du poste cible est indiqué dans l'objet CCV.

Remarque : Après un transfert simple, le système déconnecte l'appel après avoir fait retentir la sonnerie durant 5 minutes.

- **Transférer dans la file d'attente**

  Provoque le transfert de l'appel vers une file d'attente

  Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

  Propriétés :

  – **File d'attente** : Sélection de la file d'attente
- **Enregistrer dans la boîte vocale**

  Lance un appel vers la boîte vocale souhaitée d'un abonné ou vers un groupe Boîte vocale

  Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

  Propriétés :

  – **Boîte vocale Utilisateur** : indiquer le numéro de la messagerie vocale d'un utilisateur ou d'un groupe de messagerie vocale

  Le numéro d'appel et le nom de la boîte vocale ou le groupe Boîte vocale sont affichés dans l'éditeur de règle à l'aide d'une infobulle lorsque l'on se positionne avec le pointeur de la souris sur l'objet CCV.
- **Transfert supervisé (également appelé transfert filtré)**

  Provoque le transfert de l'appel vers une destination interne. Durant le transfert, l'appelant entend la musique d'attente (Music On Hold MoH de la UC Suite).

  À la différence du transfert en une étape vers l'objet CCV, il faut ajouter ici deux autres objets CCV. Il faut définir la manière dont le système de communication doit se comporter lorsque la destination est occupée ou en cas de non-réponse. Normalement, une annonce est diffusée à l'appelant dans ces cas.

  Propriétés :

  – **Poste cible** : indication du numéro de téléphone interne.

    Seuls sont supportés des numéros de téléphone internes du propre nœud. Le renvoi vers des destinations externes, des postes virtuels, des

AutoAttendants supplémentaires, des utilisateurs Mobility, ainsi que vers des destinations CallMe externes, n'est pas autorisé !

Pour ces scénarios, il convient d'utiliser le SST (transfert en une seule étape). Pour transférer un appel vers un autre UCD faisant partie de Centre de contacts, il convient d'utiliser l'objet CCV **Transfert vers la file d'attente**.

– **Délai de sonnerie** : durée, en secondes, pendant laquelle il faut décrocher l'appel.

Si l'appel n'est pas décroché dans le délai imparti, il est renvoyé vers le système de communication et l'objet CCV suivant est utilisé.

Conseil : La durée indiquée ici doit être inférieure à la durée paramétrée pour le renvoi temporisé (paramètre par défaut pour le renvoi temporisé = 15 secondes). Voir Comment configurer le transfert d'appel.

– **Retrait de l'appel si l'appareil de destination est renvoyé / dévié** : option (applicable uniquement pour le numéro d'appel interne.)

Lorsque cette option est activée, la destination d'appel est contrôlée. Si un renvoi temporisé ou un renvoi d'appel a été programmé pour la destination d'appel, l'appel est renvoyé vers le système de communication et l'objet CCV suivant est utilisé.

– **Contrôler l'état de présence lorsque vous transférez un appel** : Option

Si l'option est activée, il est effectué un contrôle de l'état Présence de la destination d'appel. Si l'état Présence est différent de Bureau, l'appel est renvoyé vers le système de communication et l'objet CCV suivant est utilisé.

- **Numérotation par nom**

L'appelant est invité à entrer les trois premières lettres du nom de l'abonné demandé à l'aide du clavier de numérotation.

S'il existe un abonné dont le nom commence par la lettre entrée, une connexion est établie.

S'il existe plusieurs abonnés dont le nom commence par la lettre entrée, les noms de ces abonnés sont indiqués à l'appelant (10 abonnés maxi.). Si l'abonné n'a pas enregistré d'annonce du nom, il est diffusé à la place le numéro de téléphone. Après sélection de l'abonné souhaité, une connexion est créée.

Si aucun abonné ne comprend les lettres de début entrées, l'appelant reçoit un message correspondant.

Conseil : Les touches du clavier de numérotation réagissent au premier appui. Chaque appui permet de contrôler s'il existe des noms de famille d'abonné correspondant aux lettres correspondant à la touche.

dans le répertoire interne, il existe les cinq noms de famille suivants commençant par t, u et v : Pour établir une

connexion avec l’abonné Taylor, il faut appuyer sur les touches suivantes :

Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

Propriétés :

– **Méthode** : sélection de **Transférer au poste** ou **Enregistrer dans la boîte vocale**.

  Selon la méthode sélectionnée, il est établi une liaison avec l'abonné souhaité ou avec sa boîte vocale. Dans ce cas, seuls les abonnés internes dont le nom et le prénom figurent dans le répertoire interne bénéficient d'une assistance.

- **Composer par poste**

  L'appelant est invité à composer le numéro de l'abonné demandé à l'aide du clavier de numérotation.

  Si l'appelant sélectionne le numéro d'un abonné virtuel, il est invité à entrer un autre numéro d'appel. Ensuite, une liaison est établie. Si l'abonné demandé ne répond pas, sa boîte vocale prend l'appel.

  Après cet objet CCV, il n'est pas possible d'ajouter d'autres objets CCV.

  Propriétés :

  – **Méthode** : sélection de **Transférer au poste** ou **Enregistrer dans la boîte vocale**.

    Selon la méthode sélectionnée, il est établi une liaison avec l'abonné souhaité ou avec sa boîte vocale. Notez que seuls les abonnés internes du réseau dont le numéro de téléphone figure dans le répertoire interne bénéficient d'une assistance.

- **Régler langue**

  Provoque le choix de la langue pour l'annonce par défaut sur la base du numéro de l'appelant. Remarque : seules les annonces par défaut (annonces système) et non pas les annonces personnelles sont prises en considération.

  Il est possible de définir par exemple que, pour un numéro avec indicatif national + 49, il sera diffusé une annonce en allemand et que, pour un numéro avec indicatif national +33, il sera diffusé une annonce en allemand.

  Propriétés :

  – **Langue par défaut** : liste déroulante pour sélectionner une langue.

    La langue choisie ici est utilisée pour tous les numéros de téléphone pour lesquels il n'a pas été défini de langue.
  – **Modèle** : spécifie les numéros d'appel auxquels une langue particulière doit être affectée.

    Il est possible d'utiliser les jokers ci-après. * = nombre quelconque, ?
  – **Langue** : liste déroulante pour sélectionner la langue à affecter aux numéros d'appel pertinents (correspondant au **Modèle**).

  Il est possible d'affecter un nombre non limité de numéros d'appel différents à une langue (**Modèle**).

- **Routage CLI**

  Provoque le renvoi d'un appel en direction d'un ou plusieurs objets CCV successifs à l'aide du numéro de l'appelant.

  Il est possible, par exemple, de définir que, pour un numéro avec indicatif national +49, il sera tout d'abord diffusé une annonce en allemand (objet CCV **Lire le message**) puis que l'appel sera ensuite renvoyé vers un téléphone interne (objet CCV **Transfert simple**). L'indicatif local peut également être utilisé (par exemple 089 pour Munich).

  Dans le contexte de UC Suite et CLI Routing, les utilisateurs doivent considérer des scénarios spécifiques, tels que les appels entrants de MS Teams Native SIP Trunk. Si vous avez l'intention d'envoyer vers OpenScape Business les numéros des appelants au format canonique, y compris l'indicatif de pays, vous devez établir des règles de routage CLI supplémentaires.

  Par exemple, si les appelants de MS Teams ont des numéros au format +49777555XXXX, et que 777555 est la partie commune de ces numéros, les utilisateurs doivent créer des règles de routage CLI pertinentes qui intègrent cette partie commune (777555).

  Propriétés :

  – **Standard** : liste déroulante pour sélectionner l'objet CCV.

    L'objet CCV sélectionné ici est utilisé pour tous les numéros de téléphone, même pour ceux où aucune destination spécifique n'a été définie.
  – **Modèle** : indication du numéro de téléphone, auquel un objet CCV déterminé doit être affecté en tant que destination.

    Il est possible d'utiliser les jokers ci-après. * = nombre quelconque, ?
  – **Description**

    Indication d'une explication.

    Pour le **Modèle** +49 (=Indicatif national Allemagne), il est possible, par exemple, d'indiquer Allemagne.

    Le texte indiqué ici est affiché dans l'éditeur de règles.
  – **Cible** : liste déroulante permettant de choisir l'objet CCV auquel il est attribué comme destination au numéro de téléphone correspondant (**Modèle**).

  Un objet CCV peut affecter un nombre non limité de numéros d'appel différents (**Modèle**) en tant que destinations.
- **Branche sur variable**

  Provoque le renvoi d'un appel en direction d'un ou plusieurs objets CCV successifs sur la base d'une condition.

  Il est possible de définir par exemple que les appelants vont entendre une annonce (Veuillez rappeler ultérieurement...) dès que plus de 20 appels figurent dans une file d'attente.

  Propriétés :

  – **Variable** : sélection d'**Appels** ou **Agents disponibles**.

    Selon la variable sélectionnée, la condition est le nombre des appels en attente dans une file d'attente ou le nombre des agents disponibles (y compris les agents en durée de post-traitement) d'une file d'attente. Dans

la liste déroulante correspondante, la condition (**inférieur à**, **supérieur à**, **inférieur ou égal à**, **supérieur ou égal à**, **égal à**) doit être sélectionnée et la valeur de comparaison doit être entrée dans le champ de saisie correspondant.

– **Branche Vrai** : liste déroulante pour la sélection de l'objet CCV qui doit être utilisé comme destination si la condition est remplie.
– **Branche Faux** : liste déroulante pour la sélection de l'objet CCV qui doit être utilisé comme destination si la condition n'est pas remplie.

Le nombre des agents disponibles dans une file d'attente est influencé par les modifications suivantes de l'état des agents :

– Connexion d'un agent dans la file d'attente à l'aide de « Connexion/ Login » :
– Déconnexion d'un agent de la file d'attente à l'aide de « Déconnexion/ Logout » :
– Agent à l'état "En pause" : --> -1
– Agent à l'état "Disponible après pause" : --> +1

Le nombre des agents disponibles dans une file d'attente **n'est pas** influencé par les modifications suivantes de l'état des agents :

– Agent à l'état « En Sonnerie »
– Agent à l'état « En communication »
– Agent à l'état « Post-traitement »
– Agent à l'état « Appel manqué »
– Agent à l'état « En Dépassement »

• **Données branchement**

Provoque le renvoi d'un appel en direction d'un ou plusieurs objets CCV successifs sur la base d'une condition.

Il est possible de définir par exemple que les appelants vont entendre une annonce (Veuillez rappeler ultérieurement...) dès que plus de 20 appels figurent dans une file d'attente.

Propriétés :

– **Variable** : Sélection des **données LDAP2 (pager)**.

L'interrogation à distance des données est effectuée via LDAP, soit directement vers une base de données compatible LDAP ou indirectement via le service de répertoire (ODS) vers une base de données SQL / ODBC. Les résultats des requêtes sont assignés via le champ LDAP UC Suite faisant l'objet d'un mappage avec les critères appropriés du centre de contacts. Dans la liste déroulante correspondante, la condition (**inférieur à**, **supérieur à**, **inférieur ou égal à**, **supérieur ou égal à**, **égal à**) doit être sélectionnée et la valeur de comparaison doit être entrée dans le champ de saisie correspondant. Il est nécessaire d'affecter les mots clés « pager » et « info ».

– **Expiration** : durée en secondes avant une expiration.
– **Branche Expiration** : liste déroulante pour la sélection de l'objet CCV qui doit être utilisé comme destination en cas d'expiration.
– **Branche Vrai** : liste déroulante pour la sélection de l'objet CCV qui doit être utilisé comme destination si la condition est remplie.
– **Branche Faux** : liste déroulante pour la sélection de l'objet CCV qui doit être utilisé comme destination si la condition n'est pas remplie.
– **Description** : Indication d'une explication.

17.3.3 Post-traitement

En fonction du code de post-traitement, les appels entrants peuvent être affectés à certaines rubriques (commande, réclamation, service clientèle, etc.). L'affectation est effectuée par un agent après avoir terminé l'appel (pendant le temps de travail) en saisissant le motif de clôture approprié à l'aide de myAgent.

Il est possible de définir les codes de post-traitement individuellement pour chaque file d'attente.

Il est fait la distinction entre les aspects suivants.

- Post-traitement simple

  Pour les files d'attente en mode "Post-traitement simple", il est possible de définir un ou plusieurs codes de post-traitement.

  Exemple: Les deux motifs de post-traitement « problème matériel » et « problème logiciel » ont été définis pour une file d'attente. Chaque appel se voit attribuer l'un de ces motifs de post-traitement par un agent pendant le temps de travail. Il est ainsi possible d'établir un rapport avec l'aperçu de tous les appels concernant le sujet Problème matériel.

- Post-traitement multiple

  Pour les files d'attente en mode "Post-traitement multiple", il est possible de définir un ou plusieurs codes de post-traitement et de les regrouper en groupes et sous-groupes.

  Sous chaque groupe ou sous-groupe (le cas échéant), au moins un élément doit également être configuré pour permettre à l'agent de post-traitement d’un appel. Le post-traitement d'un appel n'est pas possible si un groupe ou un sous-groupe est vide. Ceci ne s'applique qu'aux files d'attente pour lesquelles la configuration « Post-traitement multiple » est activée.

  Exemple: Un groupe Matériel avec les motifs de post-traitement telles que la carte mère et l’alimentation et un groupe Logiciel avec les motifs de post-traitement tel que le système d'exploitation et les pilotes ont été définis pour une file d'attente. Chaque appel se voit attribuer l'un de ces motifs de post-traitement par un agent pendant le temps de travail. Il est ainsi possible d'établir un rapport avec un aperçu sur tous les appels liés à des problèmes matériels ou encore avec un aperçu de tous les appels concernant les problèmes Matériel relatifs à la carte mère.

17.3.4 Niveau de service

Le niveau de service donne des indications sur la qualité de réponse d'une file d'attente. Cela est possible en comparant le temps d'attente dans une file d'attente aux valeurs de consigne qui peuvent être attribuées individuellement pour chaque file.

Les valeurs de consigne pour le degré de service (Grade of Service, GoS) peuvent être définies librement dans une file d'attente en liaison avec le temps d'attente de l'appelant. Pour chaque appel à une file d'attente correspondante, le niveau de service est déterminé à la fin de l'appel et il est consigné dans la base de données. Les agents de profil "Superviseur" ou "Administrateur" peuvent effectuer une évaluation du degré de service à l'aide de l'application myAgent.

17.3.5 Affichage mural (Wallboard)

Il est possible d'afficher les détails de la file d'attente à partir de myAgent. L'affichage des détails de la file d'attente comprend un tableau avec des informations statistiques sur les files d'attente, en temps réel pour la période actuelle de 24 heures. L'affichage peut être effectué par exemple sur un grand écran LCD ou bien à l'aide d'un projecteur (wallboard).

Un agent avec le niveau d'autorisation Agent reçoit des informations sur les files d'attentes auxquelles il est affecté. Un agent avec le niveau d'autorisation Superviseur ou Administrateur reçoit des informations sur toutes les files d'attente.

Pour l'affichage mural, il convient de paramétrer un utilisateur séparé. Il faut pour cela une licence d'abonné (utilisateur IP ou utilisateur TDM) et une licence myAgent.

17.3.6 Rappel d'agent

Si un appelant trouve que le temps d'attente dans la file d'attente est trop long et si le calendrier correspondant contient l'objet CCV **Enregistrer le rappel**, l'appelant peut laisser une demande de rappel. Cette demande de rappel conserve la position d'origine de l'appelant dans la file d'attente et elle est communiqué à l'agent sous la forme d'un message vocal. Après écoute du message voix, l'agent peut rappeler l'appelant via une fenêtre surgissante.

S'il a été défini un agent préféré pour un appelant, le système tente tout d'abord de transmettre les demandes de rappel de cet appelant à l'agent préféré. Si l'agent préféré n'est disponible, la demande de rappel est transférée à un agent disponible quelconque.

17.4 Suivi VIP

Dans chaque file d'attente, il est possible de déterminer de manière individuelle si certains appelants ou si les appelants correspondant à des modèles de numéros paramétrables doivent être traités de manière préférentielle et donc être adressés plus rapidement à un agent libre.

Si tous les agents d'une file d'attente sont occupé, les appelants VIP sont connecté de manière préférentielle au prochain agent devenu libre.

17.4.1 Priorités des appelants VIP

A partir des priorités des appelants VIP, il est possible de définir individuellement pour chaque file d'attente si les appelants figurant dans la liste d'appels VIP (par ex. les clients) doivent ou non être traités prioritairement.

Les valeurs de priorité des appelants VIP peuvent être définies librement dans une file d'attente en liaison avec le temps d'attente de l'appelant Cela permet

de définir le degré de priorisation des appelants VIP par rapport aux appelants normaux.

Si un appelant VIP active le rappel d'agent (réception d'un message Voix avec demande de rappel), le rappel d'agent figure dans la file d'attente à la place de l'appelant VIP. Dans ce cas, la priorité des appelants VIP n'est pas reprise.

Les appelants VIP doivent être consignés dans la liste d'appels VIP (voir Liste d'appels VIP).

17.4.2 Liste d'appels VIP

Les appelants déjà consignés dans le système de communication (répertoire externe) peuvent être intégrés dans la liste d'appels VIP. Il peut être effectué une sélection multiple ou bien on peut utiliser la fonction "**Sélectionner tout**". De plus, il est possible d'entrer des modèles de numéros d'appel. Les modèles de numéro se composent d'une séquence de chiffres définie et d'un joker (wildcard). Ainsi, tous les collaborateurs d'une entreprise peuvent être par exemple intégrés dans la liste d'appels VIP.

Pour chaque file d'attente, il est possible de définir, avec la priorités des appelants VIP, si

- les appelants figurant dans la liste d'appels VIP et
- les appelants correspondant au modèle de numéro d'appel contenu dans la liste d'appels VIP doivent être traités prioritairement.

Il n'est pas possible d'entrer des modèles de numéro d'appel au format canonique. L'utilisation de signes d'abréviation pour les préfixes de pays (par ex. +49 à la place de 0049) n'est pas possible. Les modèles de numéro d'appel doivent toujours être indiqués sans indicatif réseau.

Exemples pour modèle de numéro :

- 089 7577* (089 = Indicatif local Munich, 7577 = Numéro de l'installation d'une entreprise, * = joker pour un nombre quelconque). L'inscription de ce modèle de numéro dans la liste d'appels VIP permet à tous les appelants de Munich, dont le numéro commence par 7577, d'être traités prioritairement.
- 0039* (0039 = Indicatif national Italie, * = joker pour un nombre quelconque). L'inscription de ce modèle de numéro dans la liste d'appels VIP permet à tous les appelants d'Italie d'être traités prioritairement.

Les caractères suivants peuvent servir de joker (wildcard) dans un modèles de numéro d'appel :

- * = joker pour un nombre quelconque
- ? = joker pour un chiffre quelconque

17.5 Solution de repli (solution Fallback)

Si le centre de contacts n'est pas disponible suite à un problème (défaillance générale, pas de liaison ou circonstance similaire), il se produit un passage automatique sur la fonctionnalité "Uniform Call Distribution UCD" du système de communication. Cette fonctionnalité sert donc de solution de repli pour le centre de contacts.

En cas de défaillance du centre d'appels, les appels entrants sont affectés conformément à la solution de repli. La distribution de fax et d'e-mails n'est pas possible.

Selon les exigences, il est possible de configurer l'une des solutions de repli indiquées ci-après.

Solution de repli par défaut

Dans ce cas, la solution de repli est basée sur les ID UCD (ID d'agents) des agents.

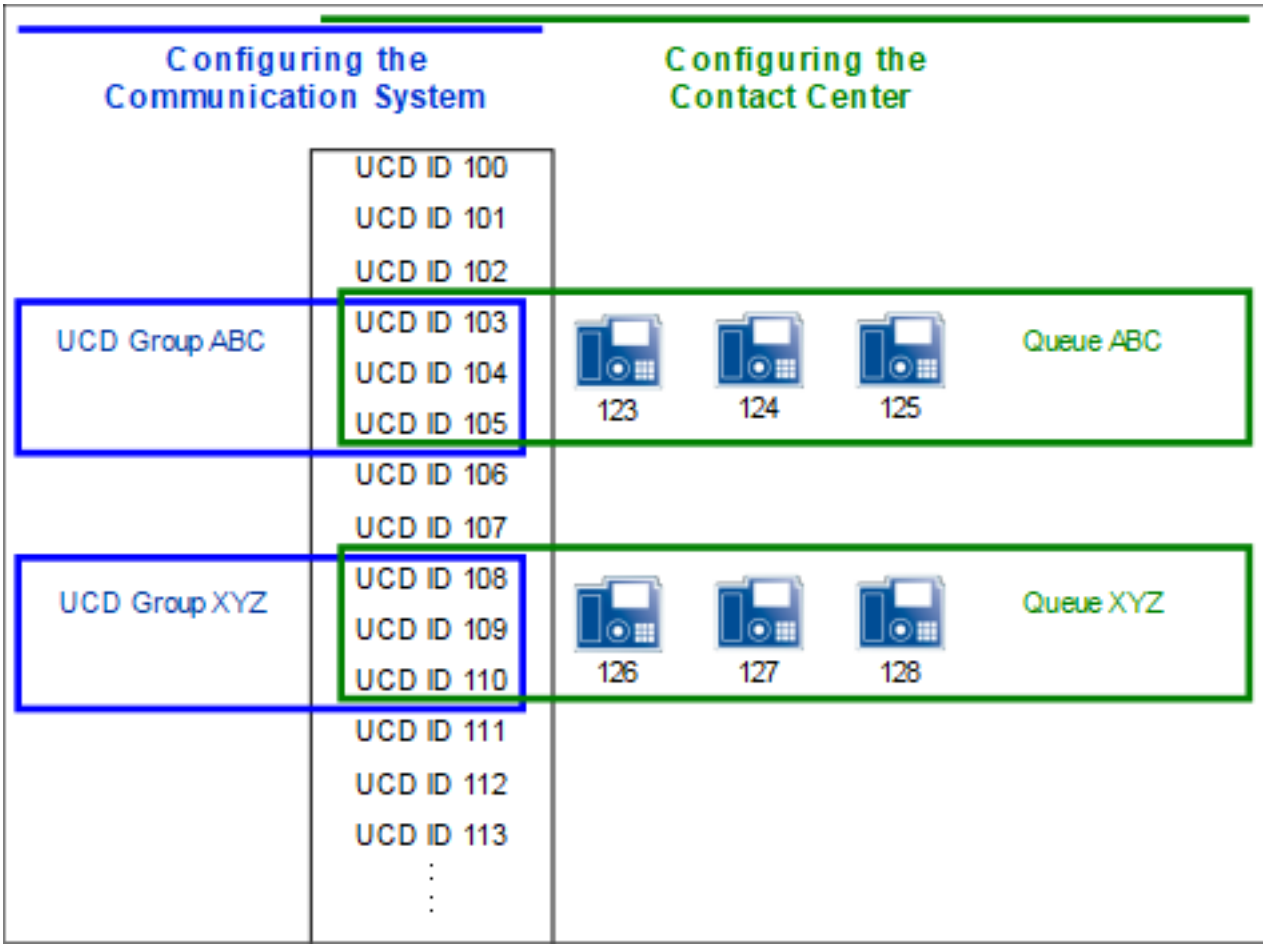
- Il est attribué aux groupes UCD du système de communication des agents, à l'aide des ID UCD. L'UCD-ID détermine dans quel groupe UCD l'agent sera affecté en cas de défaillance du centre d'appels.

Pour que la solution de reprise par défaut fonctionne correctement, il faut affecter à chaque file d'attente les agents de centre d'appels avec ID UCD qui ont été eux-mêmes affectés aux groupes UCD correspondants.

En cas de défaillance du centre d'appels, les appels entrants sont affectés aux agents inscrits via les différents groupes UCD.

Exemple:

- Les groupes UCD ABC sont affectés aux ID UCD 103, 104 et 105. Les groupes UCD XYZ ont été affectés aux ID UCD 108, 109 et 110.
- Les abonnés 123, 124 et 125 sont configurés en tant qu’agents avec les ID UCD 103, 104 et 105. Les abonnés 126, 127 et 128 sont configurés en tant qu’agents avec les ID UCD 108, 109 et 110.
- Lors de l'affectation des agents aux files d'attente, les abonnés 123, 124 et 125 doivent être affectés à la file d'attente ABC et les abonnés 126, 127 et 128 à la file d'attente XYZ.



Solution de repli de base

Dans ce cas, tous les agents du centre d'appels sont affectés uniquement au groupe UCD Sauvegarde à l'aide de leurs ID UCD. L'affectation des agents correspondants permet d'utiliser aussi ces ID UCD dans les files d'attente du centre d'appels. Cela garantit que, lors d'une défaillance du centre d'appels, les agents ne doivent pas établir une nouvelle connexion manuelle sur leur téléphone, à l'aide d'un autre ID. Ce groupe UCD de sauvegarde sert de destination de renvoi temporisé à tous les groupes UCD (files d'attente) du système de communication.

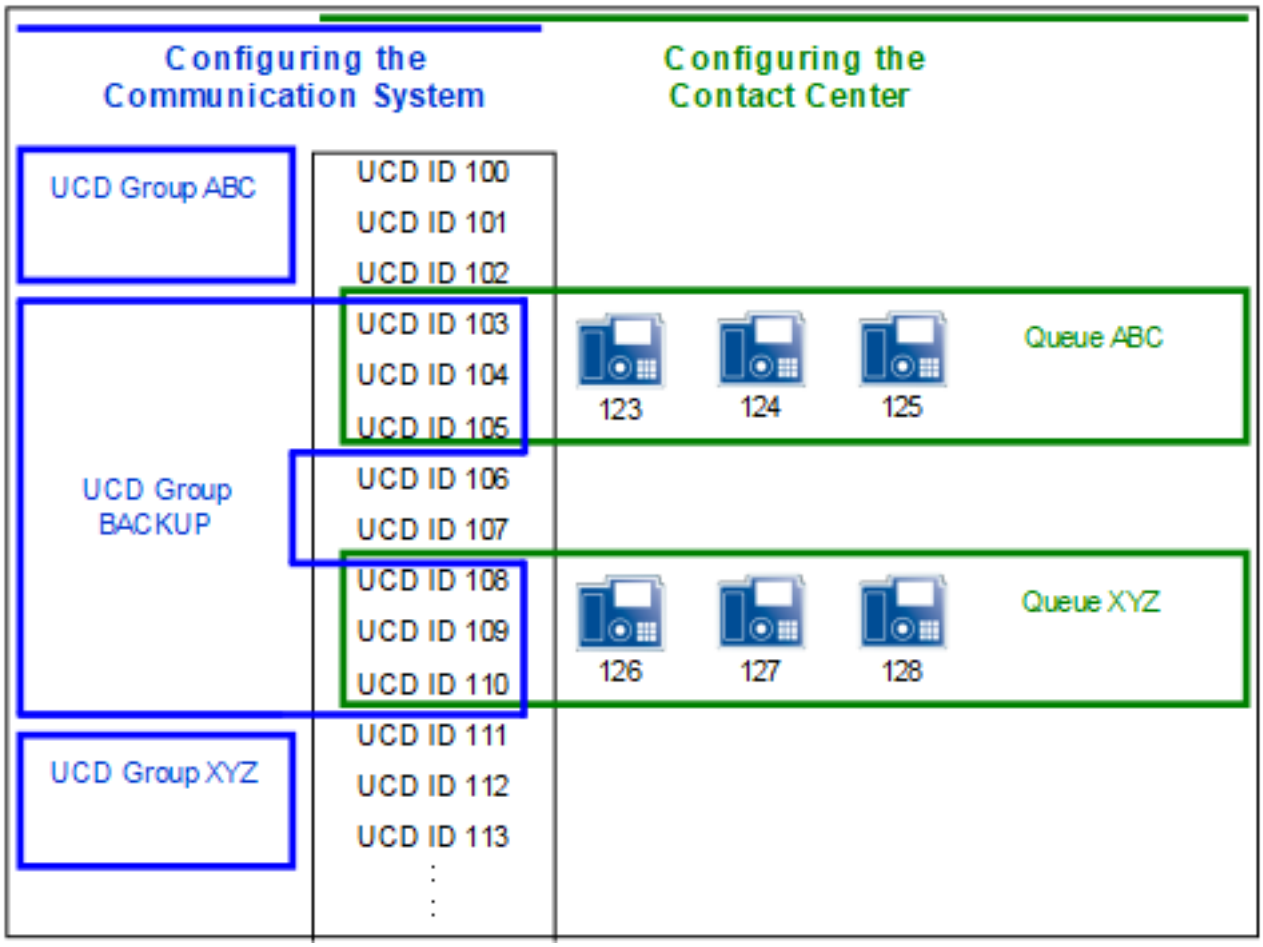
Remarque : Le groupe UCD de sauvegarde configuré doit également être configuré en tant que groupe dans le centre d'appels. C'est seulement ainsi que l'on peut garantir la surveillance de ce groupe aussi.

En cas de défaillance du centre d'appels, les appels entrants sont alors répartis entre tous les agents du groupe UCD de sauvegarde.

Exemple:

- Il n'a été attribué aucun ID UCD aux groupes UCD ABC et XYZ. Il est affecté au groupe UCD SAUVEGARDE les ID UCD 103 à 105 et 108 à 110.

- Les abonnés 123, 124 et 125 sont configurés en tant qu'agents avec les ID UCD 103, 104 et 105. Les abonnés 126, 127 et 128 sont configurés en tant qu'agents avec les ID UCD 108, 109 et 110.
- Lors de l'affectation des agents aux files d'attente, les abonnés 123, 124 et 125 sont affectés à la file d'attente ABC et les abonnés 126, 127 et 128 à la file d'attente XYZ.



Solution de repli spécifique à un client

Dans ce cas, la configuration du centre d'appels, spécifique du client, est reproduite dans plusieurs groupes UCD.

En cas de défaillance du centre de contacts, on parvient ainsi à un comportement similaire pour la solution de repli.

Pour plus d'informations sur la configuration de la distribution des appels à l'aide de la fonctionnalité de distribution uniforme des appels (UCD) du système de communication, voir UCD (Uniform Call Distribution).

Un avantage essentiel de la solution de repli spécifique client est la reproduction exacte du centre de contacts dans la solution de repli.

Le désavantage de la solution de repli spécifique client est l'importance de la configuration nécessaire. De plus, toutes les modifications apportées à la configuration du centre d'appels doivent aussi être effectuées sur la solution de repli afin de garantir un comportement similaire en matière de distribution des appels.

L'avantage essentiel de la solution de repli par défaut et de base est sa configuration simple.

17.6 Configuration de base du centre d'appels

Lors de la configuration du centre d'appels, il faut tout d'abord définir les groupes UCD. Les files d'attente du Centre d'appels sont des groupes de travail basés sur les groupes UCD du système de communication. Ensuite, il est possible d'effectuer la configuration du centre d'appels (calendriers, files d'attente, etc.).

Avant de configurer le centre d'appels, il faut déterminer avec le client le déroulement de la distribution des appels en mode normal et en mode de secours.

Conseil : La configuration du centre d'appels ne doit intervenir qu'une fois la configuration du système de communication et de la suite UC est entièrement achevée.

Si des modifications sont apportées à la configuration des groupes UCD, il faut ensuite redémarrer la UC Suite à l'aide du Centre de service du WBM.

Les licences suivantes sont la condition de l'utilisation d'un centre d'appels :

- Un nombre correspondant de licences pour les agents (myAgent)
- Centre d'appels-Licence Fax (pour la réception et l'envoi de fax), si nécessaire
- Centre d'appels-Licence e-mail (pour la réception et l'envoi d'e-mails), si nécessaire

17.6.1 Exemple de configuration d'un centre d'appels

Un exemple illustre le principe de fonctionnement du centre d'appels avec OpenScape Business. La structure et la configuration de cet exemple sont basées sur un scénario client fictif, avec les fonctions standard du Centre de contacts.

Exemple de scénario pour un centre d'appels

La société XYZ gère un centre d'appels avec les numéros de téléphone suivants (files d'attente) :

- Numéro de téléphone 440 pour Service
- Numéro de téléphone 444 pour Sales
- Numéro de téléphone 456 pour les appels gratuits (Hotline). Les appelants entendent une annonce et peuvent ensuite, en composant les numéros correspondants joindre la fonction Service ou la fonction Ventes.

Le centre d'appels comprend six collaborateurs (agents), trois sont affectés à Services et trois à Sales.

Les files d'attente des secteurs Service et Sales doivent être joignables directement durant les heures d'ouverture de 09h00 à 17h00. Les deux files d'attente disposent d'une boîte Fax et d'une adresse e-mail.

Si tous les agents sont en communication ou non disponible, l'appelant doit en être informé et il doit entendre une musique d'attente. Si aucun agent n'est libre au bout d'un certain temps, l'appelant peut formuler une demande de rappel et contacter le poste opérateur en composant un chiffre spécifié. Si aucun chiffre n'est sélectionné, l'appelant doit être automatiquement remplacé dans la file d'attente.

En dehors des heures d'ouverture, il doit être diffusé une annonce permettant un enregistrement avec demande de rappel (rappel d'agent).

Remarque : La lecture d'annonces est uniquement possible via des lignes. Pour lire l'annonce, l'appel doit provenir d'une ligne ou l'appel doit être suivi par le Centre de contacts OpenScape.

Durant la pause déjeuner de 12h00 à 13h00, il doit être diffusé pour les files d'attente de Service et Sales une annonce qui donne la possibilité d'effectuer un enregistrement avec demande de rappel.

Solution de repli (Fallback) à l'aide du groupe UCD de sauvegarde : si le centre d'appels n'est pas disponible en raison de problèmes (défaillance, connexion en panne ou similaire), il faut se commuter immédiatement sur la fonctionnalité "Uniform Call Distribution UCD" du système de communication . Pour cela, tous les agents du centre d'appels doivent être affectés à un seul groupe UCD de sauvegarde. Ce groupe UCD de sauvegarde doit être paramétré comme destination de renvoi temporisé pour tous les groupes UCD du système de communication. En cas de défaillance du centre d'appels, les appels entrants sont répartis entre les agents du groupe UCD de sauvegarde.

Configuration de l'exemple de scénario

Les activités suivantes doivent être réalisées pour le scénario pris en exemple :

- Configuration des groupes UCD

  Les files d'attente du Centre de contacts sont des groupes de travail basés sur les groupes UCD du système de communication. Avant la configuration du centre d'appels à proprement parler, il faut définir les groupes UCD.

  Pour le centre d'appels de la société XYZ pris comme exemple, il faut configurer trois groupes UCD (Service, Sales, Hotline).
- Configuration de la solution de repli (Fallback)

  Dans l'exemple donné, il faut configurer un groupe UCD Sauvegarde et le définir en tant que destination de renvoi temporisé de tous les groupes UCD du système de communication .
- Configuration des abonnés en tant qu'agents

  Dans l'exemple donné, il faut configurer six abonnés comme agents.
- Enregistrer des annonces individuelles

  Dans l'exemple donné, il faut enregistrer différentes annonces. Il existe par exemple des annonces pour le cas où tous les agents sont indisponibles ou pour informer l'appelant des options possibles **Effectuer une action après la sélection**).
- Charger des annonces individuelles

  Dans l'exemple donné, les annonces enregistrées doivent être chargées dans le système de communication.

- Définition des calendriers

  Pour chaque période de temps du calendrier, il est utilisé une règle (Call Control Vector CCV) pour définir comme les appels entrants seront traités certains jours et à certaines heures.

  Dans l'exemple donné, il faut un calendrier (calendrier par défaut XYZ) avec une règle pour les périodes de temps en dehors des heures d'ouverture et des exceptions pour les heures d'ouverture et la pause du déjeuner. De plus, il faut définir un second calendrier (Standard Schedule Hotline) avec une règle pour les appels gratuits (Hotline).

Calendrier	Règle (CCV)	
Calendrier par défaut XYZ	Out Of The Office	Périodes en dehors des heures d'ouverture
	Open	Heures d'ouverture 08h00 à 11h59 = Open1
		Heures d'ouverture 13h00 à 17h00 = Open2
	Déjeuner	Déjeuner 12h00 à 12h59
Standard Schedule Hotline	Hotline	24 heures

- Ajouter trois files d'attente

  Dans l'exemple donné, il faut configurer une file d'attente pour Service et pour Sales. Il faut configurer une autre file d'attente (Hotline) pour les appels gratuits.
- Affecter les agents aux files d'attente

  Dans l'exemple donné, il faut affecter trois agents à la file d'attente Service et trois agents à la file d'attente Sales.

Vous trouverez des informations sur la configuration de toutes les fonctions de centre de contacts dans Marche à suivre pour la configuration .

17.6.1.1 Comment configurer les groupes UCD dans le centre de contacts qui sert d'exemple

A l'aide de l'assistant **UCD** vous configurez dans le centre de contacts de la société XYZ pris comme exemple trois groupes UCD (Service, Sales, Hotline) en leur donnant comme numéros de téléphone 440, 444 et 456.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **UCD**. Le système affiche la liste de tous les groupes UCD possibles.

4) Pour configurer un groupe UCD, cliquez dans la ligne du groupe UCD souhaité sur **Modifier**.
5) Dans le champ **Numéro d'appel**, entrez le numéro `440` du groupe UCD Service.
6) Dans le champ **Numéro SDA**, entrez le numéro SDA `440`du groupe UCD Service.
7) Dans le champ **Nom**, entrez le nom `Service`.
8) Cliquez sur **OK&Suivant**. La fenêtre **Affectation des agents UCD** s'affiche.
9) Cliquez sur **OK&Suivant** puisque n'est pas possible d'attribuer un ID UCD au groupe UCD Service.

   Etant donné qu'il faut paramétrer pour le centre de contacts exemple de la société XYZ une solution de repli à l'aide d'un groupe UCD de sauvegarde, il ne faut affecter aucun ID UCD aux trois groupes UCD Service, Sales et Hotline.
10) Cliquez sur **OK&Suivant**. La fenêtre **Modifier Annonce/débordement** s'affiche.
11) Cliquez sur **OK** car les paramètres affichés pour la configuration du groupe UCD ne sont pas valides.
12) Répétez les étapes 4 à 11 pour le groupe UCD Sales avec numéro de téléphone 444 et pour le groupe UCD Hotline avec numéro de téléphone 456.
13) Cliquez sur **OK & Suivant** puis sur **Quitter**.

17.6.1.2 Comment configurer une solution de repli (fallback) dans l'exemple donné de centre de contacts

À l'aide de l'assistant Distribution d'appels, vous configurez le groupe **UCD** de sauvegarde avec numéro de téléphone 400 pour le centre de contacts de la société XYZ de notre exemple. Dans l'exemple donné, les agents UCD 101 à 106 sont utilisés. De plus, vous définissez le groupe de sauvegarde UCD comme destination de renvoi de tous les groupes UCD du centre de contacts exemple de la société XYZ.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Le groupe de sauvegarde UCD avec le numéro d'appel 400 doit être configuré dans les files d'attente du centre de contacts de la UC Suite.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **UCD**. Le système affiche la liste de tous les groupes UCD possibles.
4) Pour configurer un groupe UCD, cliquez dans la ligne du groupe UCD souhaité sur **Modifier**.
5) Dans le champ **Numéro d'appel**, entrez le numéro `400` du groupe UCD Sauvegarde.

6) Dans le champ `Numéro SDA`, entrez le numéro SDA **400** du groupe UCD Sauvegarde.
7) Dans le champ **Nom**, entrez le nom `Sauvegarde`.
8) Cliquez sur **OK & Suivant**. La fenêtre **Affectation des agents UCD** s'affiche.
9) Sélectionnez les ID d'agents UCD souhaités dans la **Sélection** et affectez-les au groupe UCD Sauvegarde en cliquant sur **Ajouter**.
10) Cliquez sur **OK & Suivant**. La fenêtre **Affecter les utilisateurs** s'affiche.
11) Attribuez à tous les ID des agents UCD les abonnés souhaités.
12) Cliquez sur **OK & Suivant**. La fenêtre **Modifier Annonce/débordement** s'affiche.
13) Cliquez sur **OK** car les paramètres affichés pour la configuration du groupe UCD Sauvegarde ne sont pas valides.
14) Pour configurer la sauvegarde du nouveau groupe UCD Sauvegarde en tant que destination du renvoi temporisé du groupe UCD Service, cliquez dans la ligne du groupe UCD Service sur **Modifier**.
15) Cliquez autant de fois que nécessaire sur **OK & Suivant** pour afficher la fenêtre **Modifier Annonce/débordement**.
16) Dans la liste déroulante **Destination du débordement** sélectionnez le groupe UCD Sauvegarde avec numéro de téléphone 400 comme destination de renvoi temporisé.
17) Cliquez sur **OK**.
18) Répétez les étapes 14 à 17 pour configurer le nouveau groupe UCD Sauvegarde en tant que destination du renvoi des groupes UCD Sales et Hotline.
19) Cliquez sur **OK & Suivant** puis sur **Terminer**.

17.6.1.3 Comment configurer les abonnés en tant qu'agents du centre de contacts dans l'exemple présenté

A l'aide de l'assistant **Répertoire utilisateur** configurez les abonnés comme agents pour le centre de contacts de la société XYZ, prix comme exemple. Dans l'exemple donné, les abonnés des numéros 101 à 106 sont configurés comme agents. Les abonnés avec numéros de téléphone 101 et 104 reçoivent le niveau d'autorisation **Superviseur**, les autres abonnés le niveau d'autorisation **Agent**.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**.
4) Sélectionnez l'abonné correspondant au **Poste** 101 et cliquez sur **Modifier**.
5) Dans l'arborescence du menu, cliquez sur **Données personnelles** > **Niveau utilisateur**.

6) Cochez la case **Agent durablement disponible**. L'agent demeure ensuite disponible pour les appels, fax et e-mails, même s'il n'a pas répondu à un appel, un fax ou un e-mail.
7) Dans la liste déroulante **Niveau**, sélectionnez le niveau d'autorisation **Superviseur**.
8) Cliquez sur **Sauvegarder**.
9) Répétez les étapes 4 à 8 pour configurer comme agents les abonnés des numéros de téléphone 102 à 106.

17.6.1.4 Comment enregistrer les annonces pour le centre d'appels exemple

À l'aide de l'assistant **Enregistreur**, vous pouvez enregistrer des annonces pour le centre d'appels exemple de la société XYZ. Il faut entre autres prévoir une annonce pour le cas où tous les agents sont injoignables.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Chargement du fichier**.
4) Activez le champ d'option **Enregistreur**.
5) Dans la liste déroulante **Abonné**, sélectionnez le numéro du téléphone qui servira à effectuer l'enregistrement.
6) Cliquez sur **Appeler**. Le numéro sélectionné est appelé.
7) Décrochez le combiné et indiquez dans **Nom de fichier** un nom pour votre annonce.
8) Cliquez sur **Enregistrer** pour démarrer l'enregistrement de l'annonce.
9) Cliquez sur **Arrêter** dès que vous avez fini de formuler l'annonce.
10) Si vous souhaitez écouter votre nouvelle annonce, cliquez sur **Lire**.
11) Cliquez sur **Fermer** pour enregistrer l'annonce.

Conseil :

Une fois que l'annonce a été enregistrée et sauvegardé, elle ne peut plus être effacée. L'utilisation du même nom de fichier peut provoquer l'écrasement d'une annonce déjà enregistrée. Exemple : l'enregistrement du fichier audio `announcement1.wav` écrase le fichier `announcement1.wav` précédent.

---

12) Répétez les étapes 3 à 10 pour enregistrer d'autres annonces pour le centre d'appels exemple de la société XYZ.

17.6.1.5 Comment charger les annonces pour le centre d'appels exemple

A l'aide de l'assistant **Chargement du fichier**, vous pouvez charger les annonces destinées au centre d'appels exemple de la société XYZ.

Conditions préalables

Un fichier audio au format .wav, avec les caractéristiques suivantes, est disponible : mono, échantillonnage 8 kHz, format de l'échantillon 16 bits, longueur de trame 2.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Chargement du fichier**.
4) Cliquez sur l'onglet **Gestionnaire de fichiers audio**.
5) Sélectionnez **Poste opérateur auto** dans la liste déroulante **Destination de téléchargement**.
6) Sélectionnez le champ d'option **Téléchargeur** et cliquez sur **Choisir un fichier**, puis allez à l'endroit où le fichier audio est enregistré et cliquez sur **Ouvrir**.
7) Cliquez sur **Charger**.

Conseil :

Après le chargement du fichier, il n'est plus possible d'effacer le fichier audio. L'utilisation du même nom de fichier peut provoquer l'écrasement d'un fichier audio déjà chargé. Exemple : le chargement du fichier audio `announcement1.wav` écrase le fichier `announcement1.wav` précédent.

---

8) Répétez les étapes 4 à 7 pour charger d'autres annonces pour le centre d'appels exemple de la société XYZ.

17.6.1.6 Comment ajouter le calendrier standard XYZ au centre d'appels de l'exemple

A l'aide de l'assistant **Centre de contacts**, définissez le calendrier avec les règles pour les pauses et les heures d'ouverture, dans notre exemple pour le centre de contacts de la société XYZ. Pour cela, il faut définir un calendrier (calendrier XYZ par défaut) pour le heures en dehors des horaires d'ouverture (Out Of The Office) et les exceptions pour les horaires de travail (08h00 à 11h59 = Open1, 13h00 à 17h00 = Open2) et le déjeuner (12h00 à 12h59 = pause déjeuner.

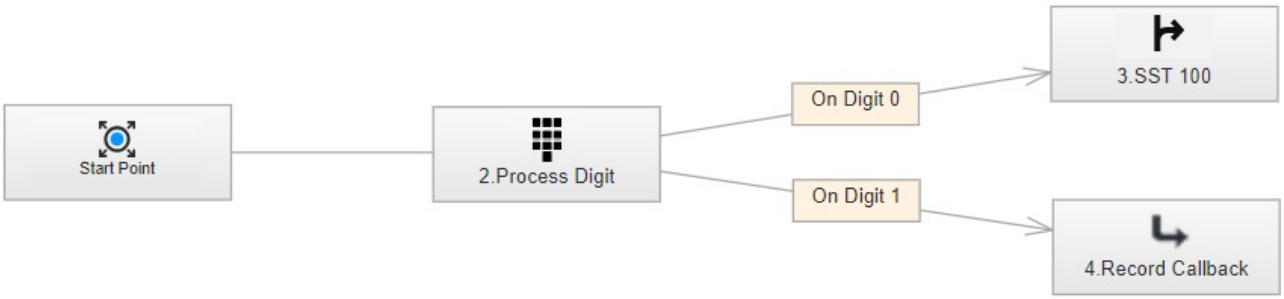
Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Calendrier**. Tous les calendriers disponibles sont affichés.
5) Cliquez sur **Ajouter**.

6) Cliquez sur **Ajouter** dans la zone **Calendrier**.
7) Définissez la règle présentée pour les périodes en dehors des heures d'ouverture.



Dans la liste des outils CCV, cliquez sur l'un des objets CCV de la règle représentée et déplacez-le dans l'éditeur de règle. Entrez les caractéristiques indiquées ci-après dans la fenêtre de l'objet CCV qui s'ouvre et validez en cliquant sur **Enregistrer**. Répétez l'opération pour tous les autres objets CCV. Associez les objets CCV en cliquant avec le bouton droit de la souris sur le premier des deux objets CCV à relier. Dans le menu déroulant, sélectionnez à l'aide de **Lien vers** le second des deux objets CCV à relier. Répétez l'opération pour tous les autres objets CCV à connecter.

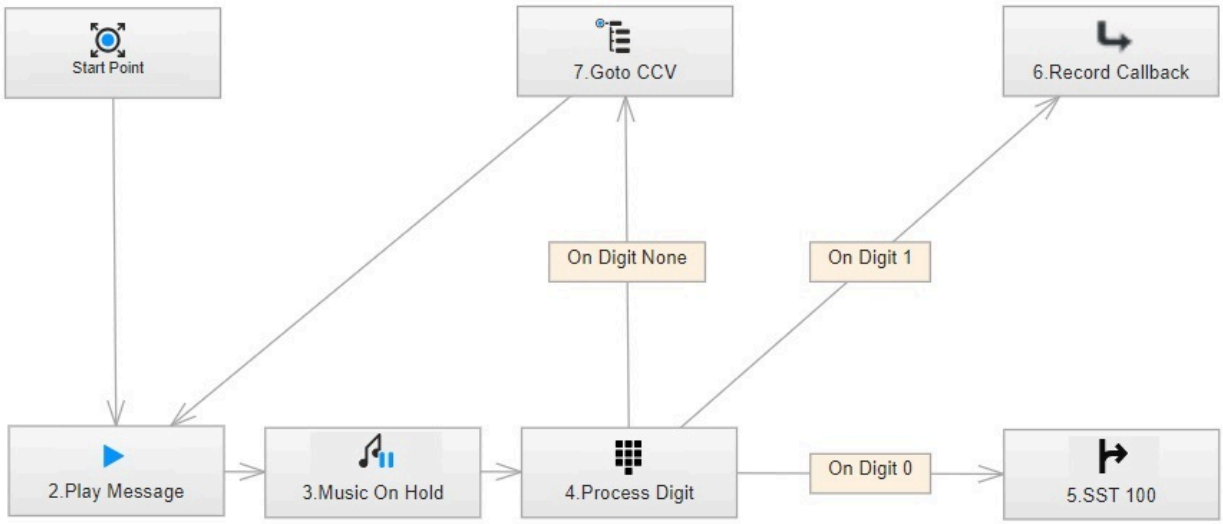
Propriétés	Valeur
1er Objets CCV : **Exécuter la sélection**	
Playlist	Fichier audio au format wav
Délai Sélection de chiffre dépassé	5
Description	Communication d'interphone : « Appuyez sur le chiffre 0 pour ... ; Appuyez sur le chiffre 1 pour ...
Chiffres 2-5. Objets CCV : **Transfert simple**	
Poste cible	100
Description	Allez au Poste opérateur
Exécuter après la sélection	0
3ème Objets CCV : **Enregistrer le rappel**	
Type	Rappel extensif
Longueur maxi. du message	20
Description	Demande de rappel (rappel d'agent)
Exécuter après la sélection	1

Cliquez sur **Sauvegarder ...**. Entrez `En déplacement` comme **nom CCV** de la règle, puis cliquez sur **Enregistrer**. Si la nouvelle règle est incorrecte, aucun enregistrement n'est possible. Le ou les objets CCV incorrects sont

signalés en rouge dans l'éditeur de règles. Fermez la fenêtre qui confirme l'enregistrement de la règle.

Dans la liste déroulante **CCV par défaut** sélectionnez la règle `En déplacement`.

8) Dans le champ **Nom du calendrier**, entrez le nom `Calendrier standard XYZ`.
9) Cliquez sur **Sauvegarder**.
10) Cliquez sur **Ajouter** dans la zone **Calendrier**.
11) Définissez la règle présentée pour les horaires de travail.



Dans la liste des outils CCV, cliquez sur l'un des objets CCV de la règle représentée et déplacez-le dans l'éditeur de règle. Entrez les caractéristiques indiquées ci-après dans la fenêtre de l'objet CCV qui s'ouvre et validez en cliquant sur **Enregistrer**. Répétez l'opération pour tous les autres objets CCV. Associez les objets CCV en cliquant avec le bouton droit de la souris sur le premier des deux objets CCV à relier. Dans le menu déroulant, sélectionnez à l'aide de **Lien vers** le second des deux objets CCV à relier. Répétez l'opération pour tous les autres objets CCV à connecter.

Propriétés		Valeur
1er Objets CCV : **Lire le message**		
	Nom du fichier	Fichier audio au format wav
	Touches Interrompre	5
	Description	Annonce : agents non disponibles
Chiffres 2-5. Objets CCV : **Musique d'attente**		
	Valeur horaire	30
	Description	Musique d'attente durant 30 secondes
3ème. Objets CCV : **Exécuter la sélection**		
	Playlist	Fichier audio au format wav

Propriétés		Valeur
	Délai Sélection de chiffre dépassé	5
	Description	Communication d'interphone : « Appuyez sur le chiffre 0 pour ... ; Appuyez sur le chiffre 1 pour ...
4ème. Objet CCV **Transfert simple**		
	Poste cible	100
	Description	Allez au Poste opérateur
	Exécuter après la sélection	0
5ème. Objets CCV : **Enregistrer le rappel**		
	Type	Rappel extensif
	Longueur maxi. du message	20
	Description	Demande de rappel (rappel d'agent)
	Exécuter après la sélection	1
Chiffres 6-7. Objets CCV : **Aller à CCV**		
	CCV cible	1. Lire le message
	Description	Retour à l'annonce

Cliquez sur **Sauvegarder ...**. Entrez `Open` comme **de CCV** pour la nouvelle règle, puis cliquez sur **Enregistrer**. Fermez la fenêtre qui confirme l'enregistrement de la règle.

Dans la liste déroulante, sélectionnez la règle `Open` pour l'exception Open1.

12) Dans la zone **Exceptions**, cliquez sur **Ajouter** pour définir la première exception pour les heures ouvrables.

13) Entrez **Open1** dans le champ `Description`.

14) Définissez la période durant laquelle doit s'appliquer l'exception Open1 :

Activez le bouton radio **Dans la plage horaire**. Sélectionnez **08:00** comme heure de début dans la liste `Heure de début` et **11:59** comme heure de fin dans la liste `Heure de fin` pour définir la période quotidienne.

Dans la fenêtre **Sélectionner jours** indiquez les jours de la semaine où la règle doit s'appliquer. Pour finir, cliquez sur **Sauvegarder**.

15) Dans la zone **Exceptions**, cliquez sur **Ajouter** pour définir la seconde exception pour les heures ouvrables.

16) Entrez `Open2` dans le champ **Description**.

17) Dans la liste déroulante, sélectionnez la règle `Open` pour l'exception Open2.

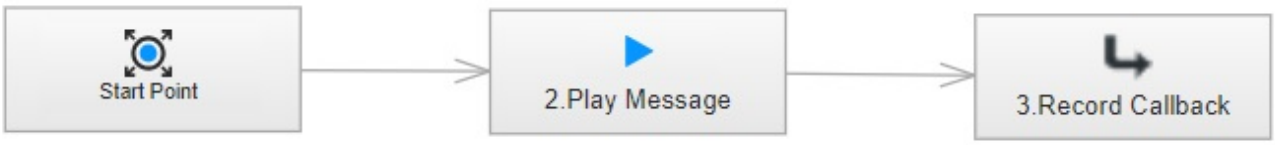
18) Définissez la période durant laquelle doit s'appliquer l'exception Open2 :

Sélectionnez l'option **Dans la plage horaire** dans la liste déroulante **Type**. Sélectionnez **13:00** comme heure de début dans la liste `Heure de`

`début` et **17:00** comme heure de fin dans la liste `Heure de fin` pour définir la période quotidienne.

Dans la fenêtre **Sélectionner jours** indiquez les jours de la semaine où la règle doit s'appliquer. Pour finir, cliquez sur **Sauvegarder**.

19) Définissez la règle présentée pour la pause de midi.



Dans la liste des outils CCV, cliquez sur l'un des objets CCV de la règle représentée et déplacez-le dans l'éditeur de règle. Entrez les caractéristiques indiquées ci-après dans la fenêtre de l'objet CCV qui s'ouvre et validez en cliquant sur **Enregistrer**. Répétez l'opération pour tous les autres objets CCV. Associez les objets CCV en cliquant avec le bouton droit de la souris sur le premier des deux objets CCV à relier. Dans le menu déroulant, sélectionnez à l'aide de **Lien vers** le second des deux objets CCV à relier. Répétez l'opération pour tous les autres objets CCV à connecter.

Propriétés	Valeur
1er Objets CCV : **Lire le message**	
Nom du fichier	Fichier audio au format wav
Touches Interrompre	Sélectionner Service
Description	Annonce : agents non disponibles
2Ème Objet CCV : **Enregistrer le rappel**	
Type	Rappel extensif
Longueur maxi. du message	20
Description	Demande de rappel (rappel d'agent)
Exécuter après la sélection	1

Cliquez sur **Sauvegarder ...**. Entrez `Pause déjeuner` comme **nom CCV** de la règle. Fermez la fenêtre qui confirme l'enregistrement de la règle.

Dans la liste déroulante, sélectionnez la règle Pause déjeuner pour l'exception `Pause déjeuner`.

20) Dans la fenêtre **Exceptions** cliquez sur **Ajouter** pour définir l'exception de la pause déjeuner.

21) Entrez **Pause déjeuner** dans le champ `Description`.

22) Définissez les heures où doit s'appliquer la pause déjeuner :

Sélectionnez l'option **Dans la plage horaire** dans la liste déroulante **Type**. Sélectionnez `12:00` comme l'heure de début dans la liste **Heure de début** et `12:59` comme l'heure de fin dans la liste **Heure de fin** pour définir la période quotidienne.

Dans la fenêtre **Sélectionner jours** indiquez les jours de la semaine où la règle doit s'appliquer. Pour finir, cliquez sur **Sauvegarder**.

23) Si vous souhaitez savoir quelle règle (CCV) du calendrier est activée à un moment quelconque, cliquez sur **Tester le calendrier**. Dans la liste déroulante **Date**, sélectionnez le jour souhaité et dans la liste de sélection **Heure**, sélectionnez l'heure souhaitée. Cliquez sur **Tester le calendrier**. Ensuite, le système indique la règle (CCV) activée ce jour-là et à cette heure-là. Cliquez sur **Fermer** pour fermer la fenêtre **Tester le calendrier**.
24) Cliquez sur **Sauvegarder**.
25) Fermez la fenêtre.

17.6.1.7 Comment ajouter le calendrier Schedule Hotline par défaut dans le centre de contacts de l'exemple

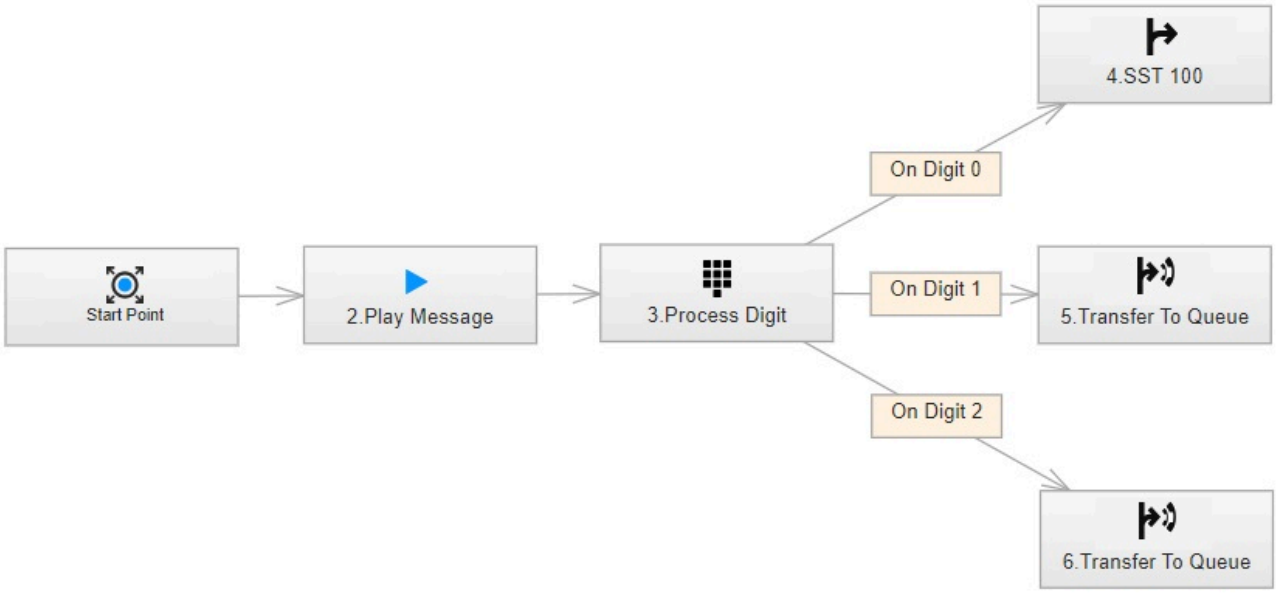
A l'aide de l'assistant Centre de contacts définissez le calendrier avec une règle pour les appels gratuits (Hotline) dans le **centre de contacts** de la société XYZ, prise en exemple.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Calendrier**. Tous les calendriers disponibles sont affichés.
5) Cliquez sur **Ajouter**.
6) Cliquez sur **Ajouter** dans la zone **Calendrier**.
7) Définissez la règle présentée pour les appels gratuits (Hotline).



Dans la liste des outils CCV, cliquez sur l'un des objets CCV de la règle représentée et déplacez-le dans l'éditeur de règle. Entrez les

caractéristiques indiquées ci-après dans la fenêtre de l'objet CCV qui s'ouvre et validez en cliquant sur **Enregistrer**. Répétez l'opération pour tous les autres objets CCV. Associez les objets CCV en cliquant avec le bouton droit de la souris sur le premier des deux objets CCV à relier. Dans le menu déroulant, sélectionnez à l'aide de **Lien vers** le second des deux objets CCV à relier. Répétez l'opération pour tous les autres objets CCV à connecter.

Propriétés	Valeur
1er Objets CCV : **Lire le message**	
Nom du fichier	Fichier audio au format wav
Touches Interrompre	5
Description	Communication d'interphone : Message d'accueil
Chiffres 2-5. Objets CCV : **Exécuter la sélection**	
Playlist	Fichier audio au format wav
Délai Sélection de chiffre dépassé	5
Description	Communication d'interphone : « Appuyez sur le chiffre 0 pour ... ; Appuyez sur le chiffre 1 pour ...
3ème. Objets CCV : **Transfert simple**	
Poste cible	100
Description	Allez au Poste opérateur
Exécuter après la sélection	0
4ème. Objet CCV **Transférer dans la file d'attente**	
File d'attente	440
Description	Allez à la file d'attente Service
Exécuter après la sélection	1
5ème. Objet CCV **Transférer dans la file d'attente**	
File d'attente	444
Description	Allez à la file d'attente Sales
Exécuter après la sélection	2

Cliquez sur **Sauvegarder ...**. Entrez `Hotline` comme **nom de CCV** pour la règle, puis cliquez sur **Enregistrer**. Si la nouvelle règle est incorrecte, aucun enregistrement n'est possible. Le ou les objets CCV incorrects sont signalés en rouge dans l'éditeur de règles. Fermez la fenêtre qui confirme l'enregistrement de la règle.

Sélectionnez la règle **Hotline** dans la liste déroulante `CCV par défaut`.

8) Entrez le nom du `Calendrier standard Hotline` dans le champ **Nom du calendrier**.
9) Cliquez sur **Enregistrer calendrier**.

17.6.1.8 Comment ajouter des files d'attente pour le centre de contact d'exemple

Cet exemple vous montre comment utiliser l'assistant **Centre de contacts** pour configurer des files d'attente pour l'exemple de centre de contacts de la société XYZ. Dans cet exemple, une file d'attente doit être configurée pour le service après-vente (avec le numéro de poste 440) et une autre pour le service commercial (avec le numéro de poste 444). Une autre file d'attente (Hotline, poste numéro 456) doit être configurée pour les appels gratuits.

Conditions préalables

Les groupes UCD **Service**, **Ventes** et **Hotline** pour l'exemple de centre de contact ont été configurés.

Les horaires **Standard Schedule XYZ** et **Standard Schedule Hotline** ont déjà été créés pour l'exemple de centre de contact.

Au moins un compte de messagerie est disponible pour la réception des courriels.

L'envoi de courriels a été configuré dans le système de communication.

Vous êtes connecté au WBM avec le profil **Avancé** .

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration** .
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'assistant **du centre de contact** .
4) Cliquez sur **File d'attente**.
5) Cliquez sur **Ajouter** .
6) Cliquez sur l'onglet **Paramètres généraux**.
7) Saisissez le nom `Service` dans le champ **Nom de file d'attente**.
8) Dans la liste déroulante **File d'attente active**, sélectionnez l'élément **Actif**.
9) Entrez le numéro **440** dans le champ `Groupement`.
10) Dans la liste déroulante **Commutateur téléphonique**, sélectionnez l'élément **CSP**.
11) Sélectionnez l'élément **Standard Schedule XYZ** dans la liste déroulante **Calendrier**.
12) Dans le champ **Nombre d'alarmes de file d'attente**, entrez la valeur `20`, par exemple.

    Si plus de 20 appels sont en attente dans la file d'attente, le symbole de la file d'attente sur le poste de l'agent passe du vert à l'orange.
13) Dans le champ **Temps d'alarme de file d'attente**, entrez la valeur `300`, par exemple.

    Dès que le temps d'attente pour un appel en file d'attente dépasse 300 secondes, l'élément correspondant dans la liste des appels du centre de contact pour les agents passe au rouge.
14) Dans le champ **Délai d'appel manqué**, entrez la valeur `100`, par exemple, afin que tout appel non répondu dans les 100 secondes soit renvoyé au prochain agent libre.
15) Entrez un numéro dans le champ **Seuil d'appel abandonné**, par exemple, `120`. Cela permet d'inclure dans les statistiques (d'un rapport) les appels abandonnés après 120 secondes.

16) Cochez la case **Screen Pop Enabled**. Une fenêtre contextuelle permettant d'afficher et de saisir les données client apparaîtra alors lors de la réception d'appels entrants dans myAgent.
17) Activez l'option **No Wrapup**.
18) Sélectionnez l'élément **Statique** dans la liste déroulante du **mode de profondeur de la file d'attente**.
19) Entrez un nombre dans le champ **Taille de la profondeur de la file d'attente**, par exemple `5`.
20) Cliquez sur l'onglet **Pilotes de file d'attente**.
21) Dans la liste déroulante **Pilotes de fax entrants**, sélectionnez l'option ou les options appropriées du ou des pilotes souhaités (numéro (s) de téléphone) afin que les fax soient mis en file d'attente.

    Les fax envoyés à ces numéros de téléphone seront alors ajoutés à la file d'attente et traités comme des appels entrants.
22) Sélectionnez l'une des options suivantes dans la zone **Service de messagerie entrante** afin que les e-mails soient placés dans la file d'attente :

    - Si vous souhaitez configurer une nouvelle adresse e-mail, cliquez sur **Ajouter**. La fenêtre **Ajouter** s'affiche.

      Sélectionnez la méthode d'authentification de votre serveur de messagerie dans la liste déroulante **Méthode d'authentification**. Vous pouvez choisir entre **Basic**, **OAuth 2.0 EWS** et **OAuth 2.0 Graph**.

      Entrez la désignation du serveur de messagerie à utiliser pour récupérer les e-mails dans le champ **Serveur** (par exemple, `pop3.web.de`).

      Entrez le numéro de port du serveur de messagerie dans le champ **Port** (par exemple, `110`, le numéro de port par défaut pour POP3).

      Si la méthode d'authentification sélectionnée est **Basic**, entrez les données d'accès au serveur de messagerie dans les champs **Nom d'utilisateur** et **Mot de passe**.

      Si la méthode d'authentification sélectionnée est **OAuth 2.0**, entrez le nom d'utilisateur pour accéder au serveur de messagerie dans les champs **Nom d'utilisateur**, **ID de locataire**, **ID d'application** et **Secret client**. L'ID du locataire, l'ID de l'application et le secret client correspondent à l'application enregistrée dans Azure AD pour les files d'attente de messagerie. Vous pouvez les obtenir auprès de votre administrateur Azure AD. Saisissez le périmètre de l'application dans le champ **Périmètre** (valeur par défaut : https://outlook.office365.com/.default).

      Indiquez si les courriels doivent être envoyés via une connexion SSL (Secure Socket Layer). Si vous souhaitez utiliser une connexion SSL, cochez la case **Utiliser la connexion SSL**. (Notez que le numéro de port du serveur de messagerie peut être modifié en conséquence. Le numéro de port par défaut pour POP3 via SSL = 995). Si vous ne souhaitez pas utiliser une connexion SSL, désactivez la case à cocher **Utiliser la connexion SSL**.

      Cliquez sur **Enregistrer** . La nouvelle adresse e-mail apparaîtra alors dans la zone **Service de messagerie entrante**.

- Si vous souhaitez modifier une adresse e-mail existante, marquez l'adresse e-mail souhaitée et cliquez sur **Modifier**. La fenêtre **Modifier** s'affiche.

  Modifiez les paramètres requis, puis cliquez sur **Sauvegarder**.
- Si vous souhaitez supprimer une adresse e-mail existante, marquez l'adresse e-mail souhaitée et cliquez sur **Supprimer l'e-mail**.

23) Cliquez sur l'onglet **Divers**.

24) Dans le champ **Adresse e-mail de retour**, saisissez l'adresse e-mail qui doit être affichée en tant qu'adresse de l'expéditeur (pour le destinataire) lorsqu'un e-mail est envoyé par un agent.

25) Si vous activez la case à cocher **Routage intelligent des Appels**, les appels entrants sont automatiquement renvoyés à l'agent avec lequel l'appelant a été connecté pour la dernière fois.

26) Cliquez sur **Enregistrer** .

27) Répétez les étapes 5 à 23 pour configurer la file d'attente des ventes. Répétez les étapes 5 à 17 et l'étape 23 pour configurer la file d'attente Hotline.

17.6.1.9 Comment affecter les agents aux files d'attente du centre d'appels exemple

À l'aide de l'assistant **Centre d'appels**, affectez les agents aux files d'attente pour l'exemple de centre d'appels de la société XYZ. Dans l'exemple donné, nous affectons trois agents à la file d'attente Service et trois agents à la file d'attente Sales.

Conditions préalables

Dans l'exemple de centre d'appels présenté, les files d'attente **Service** et **Ventes** ont été créées.

Dans le centre d'appels qui sert d'exemple, six agents ont été configurés.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.

3) Pour lancer l'assistant **Centre d'appels**, cliquez sur **Modifier**.

4) Cliquez sur **Liaisons de file d'attente**. Les files d'attente **Service** et **Ventes** s'affichent.

5) Sélectionnez la file d'attente à laquelle vous souhaitez affecter un agent, puis cliquez sur **Modifier**. Tous les agents déjà affectés à une file d'attente s'affichent.

6) Sélectionnez le premier agent de la file d'attente **Service** dans le tableau, puis cliquez sur **Modifier**. La fenêtre **Modifier** s'affiche.

7) Sélectionnez l'une des options suivantes :
   - Si l'agent doit recevoir des appels sans tenir compte de la charge de la file d'attente **Service**, sélectionnez **Agent primaire** dans la liste déroulante **Type**.
   - Si l'agent doit recevoir des appels uniquement en cas de débordement de la file d'attente **Service**, sélectionnez **Agent de débordement** dans la liste déroulante **Type**.
8) Si vous avez sélectionné **Agent de débordement** :
   a) Dans le champ **Débordement après (secondes)**, indiquez l'intervalle de temps à l'issue duquel les appels entrants d'un agent doivent être transférés en cas de débordement.
   b) Dans le champ **Débordement après appels dans file d'attente**, indiquez le nombre maximum d'appels. Un agent de débordement reçoit les appels qui se situent au-delà de ce nombre maximum.
9) Dans le champ **Niveau de compétence** de l'agent, indiquez un pourcentage.

   Le niveau de compétence vous permet de gérer la répartition des appels entre les agents dans la file d'attente **Service**. Les agent de niveau de compétence plus élevé sont utilisés de préférence lors de la distribution des appels. Lorsque tous les agents ont le même niveau de compétence, l'appel est envoyé à l'agent libre depuis le plus longtemps.
10) Sélectionnez l'une des options suivantes :
    - Si l'agent doit recevoir des demandes de rappel sous la forme de messages Voix, cochez la case **Activer le rappel d'agent**.
    - Lorsque l'agent ne doit pas recevoir de demande de rappel, décochez la case **Activer le rappel d'agent**.
11) Dans le champ **Post-traitement**, saisissez la durée de post-traitement automatique en secondes pour l'agent figurant dans la file d'attente **Service**.
12) Cliquez sur **OK**.
13) Répétez les étapes 5 à 12 pour affecter tous les agents aux files d'attente de l'exemple de centre d'appels.

17.6.2 Marche à suivre pour la configuration

Vous avez ici un aperçu des opérations à effectuer lors de la configuration du centre d'appels.

- Configuration des groupes UCD

  Les files d'attente du Centre de contacts sont des groupes de travail basés sur les groupes UCD du système de communication. Avant la configuration du centre d'appels à proprement parler, il faut définir les groupes UCD.
- Configuration d'une solution de reprise (Fallback)

  Si le centre de contacts n'est pas disponible suite à un problème (défaillance générale, pas de liaison ou circonstance similaire), il se produit un passage automatique sur la fonctionnalité "Uniform Call Distribution UCD" du système de communication. Cette fonctionnalité sert donc de solution de repli pour le centre d'appels (voir Solution de repli (solution Fallback)).
- Configuration des abonnés en tant qu'agents
- Enregistrer des annonces individuelles pour le centre d'appels

- Charger des annonces individuelles pour le centre d'appels

  Remarque : La lecture d'annonces est uniquement possible via des lignes. Pour lire l'annonce, l'appel doit provenir d'une ligne ou l'appel doit être suivi par le Centre de contacts OpenScape.

- Ajouter des calendriers
- Ajouter des files d'attente
- Définir les valeurs de consigne pour le niveau de service
- Définir les priorités des appelants VIP
- Modifier la liste d'appels VIP
- Définir les agents préférés
- Ajouter des pauses du centre d'appels
- Ajouter des codes de post-traitement
- Affectation des agents aux files d'attente

17.6.2.1 Comment configurer les groupes UCD pour le centre de contacts

A l'aide de l'assistant **UCD** vous pouvez configurer des groupes UCD pour le centre de contacts.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **UCD**. Le système affiche la liste de tous les groupes UCD possibles.
4) Pour configurer un groupe UCD, cliquez dans la ligne du groupe UCD souhaité sur **Modifier**.
5) Dans le champ **Numéro**, entrez le numéro du groupe UCD.
6) Dans le champ **Numéro SDA**, entrez le numéro SDA du groupe UCD.
7) Dans le champ **Nom** entrez le nom du groupe UCD.
8) Cliquez sur **OK&Suivant**. La fenêtre **Affectation des agents UCD** s'affiche.
9) Sélectionnez les ID d'agents UCD souhaités dans la **sélection** et affectez-les au groupe UCD en cliquant sur **Ajouter**.
10) Cliquez sur **OK&Suite**. La fenêtre **Affecter les utilisateurs** s'affiche.
11) Attribuez à tous les ID des agents UCD les abonnés souhaités.
12) Cliquez sur **OK&Suite**. La fenêtre **Modifier Annonce/débordement** s'affiche.
13) Cliquez sur **OK** car les paramètres affichés pour la configuration du groupe UCD ne sont pas valides.
14) Si vous souhaitez configurer d'autres groupes UCD pour le centre de contacts, répétez les étapes 4 à 11.
15) Cliquez sur **OK&Suivant** puis sur **Terminer**.

17.6.2.2 Comment configurer un abonné en tant qu'agent

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**.
4) Sélectionnez l'abonné souhaité dans le répertoire des utilisateurs et cliquez sur **Modifier**.
5) Dans l'arborescence du menu, cliquez sur **Données personnelles** > **Niveau utilisateur**.
6) Sélectionnez une des possibilités suivantes :

   Si l'agent doit être disponible de manière durable, coche la case **Agent disponible de manière durable**. L'agent demeure ensuite disponible pour les appels, fax et e-mails, même s'il n'a pas répondu à un appel, un fax ou un e-mail.

   Si l'agent ne doit pas être durablement disponible, décochez la case **Agent disponible de manière durable**. L'agent est désigné par l'état non disponible s'il n'a pas répondu à un appel, un fax ou un e-mail.
7) Dans la liste déroulante **Niveau**, sélectionnez le niveau d'autorisation.
8) Cliquez sur **Sauvegarder**.
9) Si vous souhaitez configurer un autre abonné comme agent, répétez l'étape 4 à l'étape 8.

17.6.2.3 Comment enregistrer une annonce individuelle pour le centre d'appels

À l'aide de l'assistant **Enregistreur**, vous pouvez enregistrer des annonces personnalisées pour le centre d'appels.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Chargement du fichier**.
4) Activez le champ d'option **Enregistreur**.
5) Dans la liste déroulante **Abonné**, sélectionnez le numéro du téléphone qui servira à effectuer l'enregistrement.
6) Cliquez sur **Appeler**. Le numéro sélectionné est appelé.
7) Décrochez le combiné et indiquez dans **Nom de fichier** un nom pour votre annonce.
8) Cliquez sur **Enregistrer** pour démarrer l'enregistrement de l'annonce.
9) Cliquez sur **Arrêter** dès que vous avez fini de formuler l'annonce.
10) Si vous souhaitez écouter votre nouvelle annonce, cliquez sur **Lire**.

11) Cliquez sur **Fermer** pour enregistrer l'annonce.

Conseil :

Une fois que l'annonce a été enregistrée et sauvegardé, elle ne peut plus être effacée. L'utilisation du même nom de fichier peut provoquer l'écrasement d'une annonce déjà enregistrée. Exemple : l'enregistrement du fichier audio `announcement1.wav` écrase le fichier `announcement1.wav` précédent.

17.6.2.4 Comment charger une annonce individuelle pour le centre d'appels

À l'aide de l'assistant **Chargement du fichier**, vous pouvez charger des annonces individuelles pour le centre d'appels.

Conditions préalables

Un fichier audio au format .wav, avec les caractéristiques suivantes, est disponible : mono, échantillonnage 8 kHz, format de l'échantillon 16 bits, longueur de trame 2.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Chargement du fichier**.
4) Cliquez sur l'onglet **Gestionnaire de fichiers audio**.
5) Sélectionnez **Poste opérateur auto** dans la liste déroulante **Destination de téléchargement**.
6) Sélectionnez le champ d'option **Téléchargeur** et cliquez sur **Choisir un fichier**, puis allez à l'endroit où le fichier audio est enregistré et cliquez sur **Ouvrir**.
7) Cliquez sur **Charger**.

Conseil : Après le chargement du fichier, il n'est plus possible d'effacer le fichier audio. L'utilisation du même nom de fichier peut provoquer l'écrasement d'un fichier audio déjà chargé. Exemple : le chargement du fichier audio `announcement1.wav` écrase le fichier `announcement1.wav` précédent.

17.6.2.5 Comment ajouter un calendrier

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Calendrier**. Tous les calendriers disponibles sont affichés.
5) Cliquez sur **Ajouter**.
6) Pour la sélection de la règle (CCV), choisissez l'une des possibilités suivantes.

   - Si vous voulez adresser au calendrier une règle déjà définie, sélectionnez la règle souhaitée dans la liste déroulante **CCV par défaut**.
   - Si vous souhaitez affecter une nouvelle règle qui n'a pas encore été définie au calendrier, cliquez sur **Modifier** dans la zone **Calendrier** et procédez comme suit :

     Dans la liste des outils CCV, cliquez sur l'objet CCV souhaité et faites-le glisser dans l'éditeur de règles. Entrez les caractéristiques souhaitées dans la fenêtre de l'objet CCV qui s'affiche et cliquez sur **Enregistrer**. Si nécessaire, faites glisser d'autres objets dans l'éditeur de règles et définissez leurs caractéristiques. Pour relier deux objets CCV, cliquez avec le bouton droit de la souris sur le premier des objets CCV à relier. Dans le menu déroulant, sélectionnez à l'aide de **Lien vers** le second des deux objets CCV à relier.

     Si vous souhaitez effacer un objet CCV de l'éditeur de règles, cliquez à l'aide du bouton droit de la souris sur l'objet CCV concerné et sélectionnez **Supprimer** dans le menu déroulant.

     Cliquez sur **Sauvegarder ...**. Entrez un nom pour la nouvelle règle puis cliquez sur **Enregistrer**. Fermez la fenêtre qui confirme l'enregistrement de la règle. Si la nouvelle règle est incorrecte, aucun enregistrement n'est possible. Le ou les objets CCV incorrects sont signalés en rouge dans l'éditeur de règles.

     Dans la liste déroulante **CCV par défaut**, sélectionnez la nouvelle règle que vous venez d'enregistrer.
   - Si vous voulez affecter au calendrier une nouvelle règle, basée sur une règle déjà définie, procédez comme indiqué ci-après.

     Dans la liste déroulante **CCV par défaut**, sélectionnez la règle souhaitée et cliquez sur **Modifier**. La règle est affichée dans l'éditeur de règles. Modifiez les règles.

     Dans la liste des outils CCV, cliquez sur l'objet CCV souhaité et faites-le glisser dans l'éditeur de règles. Entrez les caractéristiques souhaitées dans la fenêtre de l'objet CCV qui s'affiche et cliquez sur **Enregistrer**. Si nécessaire, faites glisser d'autres objets dans l'éditeur de règles et définissez leurs caractéristiques. Pour relier deux objets CCV, cliquez avec le bouton droit de la souris sur le premier des objets CCV à relier. Dans le menu déroulant, sélectionnez à l'aide de **Lien vers** le second des deux objets CCV à relier.

     Cliquez sur **Sauvegarder ...**. Entrez un **nom CCV** pour la nouvelle règle puis cliquez sur **Enregistrer**. Fermez la fenêtre qui confirme l'enregistrement de la règle. Si la nouvelle règle est incorrecte, aucun

enregistrement n'est possible. Le ou les objets CCV incorrects sont signalés en rouge dans l'éditeur de règles.

Dans la liste déroulante **CCV par défaut**, sélectionnez la nouvelle règle que vous venez d'enregistrer.

7) Si vous souhaitez imprimer la règle ou l'envoyer par e-mail, vous pouvez l'enregistrer sous forme de fichier PDF. Pour ce faire, cliquez sur **Imprimer**. La fenêtre **Imprimer** s'affiche.

Indiquez le nom du fichier et sélectionnez le répertoire où le fichier doit être enregistré. Cliquez sur **Sauvegarder**.

8) Dans le champ **Nom du calendrier** entrez le nom du nouveau groupe d'appel collectif.

9) Cliquez sur **Sauvegarder**.

10) Si vous voulez affecter une autre règle (CCV) à une période de temps définie à l'intérieur du calendrier, cliquez dans la zone de fenêtre **Exceptions** sur **Ajouter**. Ensuite, les champs de cette exception s'affichent.

11) Entrez le nom de la règle dans le champ **Description**.

12) Pour la sélection de la règle (CCV), choisissez l'une des possibilités suivantes.

- Si vous voulez affecter à cette période du calendrier une règle déjà définie, sélectionnez la règle souhaitée pour cette exception dans la liste déroulante.
- Si vous voulez affecter à cette période du calendrier une règle nouvelle, non encore définie, procédez comme indiqué ci-après.

  Cliquez sur **Ajouter** dans la zone **Calendrier**.

  Dans la liste des outils CCV, cliquez sur l'objet CCV souhaité et faites-le glisser dans l'éditeur de règles. Entrez les caractéristiques souhaitées dans la fenêtre de l'objet CCV qui s'affiche et cliquez sur **Enregistrer**. Si nécessaire, faites glisser d'autres objets dans l'éditeur de règles et définissez leurs caractéristiques. Pour relier deux objets CCV, cliquez avec le bouton droit de la souris sur le premier des objets CCV à relier. Dans le menu déroulant, sélectionnez à l'aide de **Lien vers** le second des deux objets CCV à relier.

  Si vous souhaitez effacer un objet CCV de l'éditeur de règles, cliquez à l'aide du bouton droit de la souris sur l'objet CCV concerné et sélectionnez **Supprimer** dans le menu déroulant.

  Cliquez sur **Sauvegarder ...**. Entrez un nom pour la nouvelle règle puis cliquez sur **Enregistrer**. Fermez la fenêtre qui confirme l'enregistrement de la règle. Si la nouvelle règle est incorrecte, aucun enregistrement n'est possible. Le ou les objets CCV incorrects sont signalés en rouge dans l'éditeur de règles.

  Dans la liste déroulante, sélectionnez pour cette exception la nouvelle règle qui vient d'être enregistrée.

- Si vous voulez affecter à la période du calendrier une nouvelle règle, basée sur une règle déjà définie, procédez comme indiqué ci-après.

  Dans la liste déroulante, sélectionnez pour cette exception la règle souhaitée et cliquez sur **Modifier**. La règle est affichée dans l'éditeur de règles. Modifiez les règles.

  Dans la liste des outils CCV, cliquez sur l'objet CCV souhaité et faites-le glisser dans l'éditeur de règles. Entrez les caractéristiques souhaitées dans la fenêtre de l'objet CCV qui s'affiche et cliquez sur **Enregistrer**. Si nécessaire, faites glisser d'autres objets dans l'éditeur de règles et définissez leurs caractéristiques. Pour relier deux objets CCV, cliquez avec le bouton droit de la souris sur le premier des objets CCV à relier. Dans le menu déroulant, sélectionnez à l'aide de **Lien vers** le second des deux objets CCV à relier.

  Cliquez sur **Sauvegarder ...**. Entrez un nom pour la nouvelle règle puis cliquez sur **Enregistrer**. Fermez la fenêtre qui confirme l'enregistrement de la règle. Si la nouvelle règle est incorrecte, aucun enregistrement n'est possible. Le ou les objets CCV incorrects sont signalés en rouge dans l'éditeur de règles.

  Dans la liste déroulante, sélectionnez pour cette exception la nouvelle règle qui vient d'être enregistrée.

13) Sélectionnez l'une des possibilités suivantes afin de déterminer à quel moment l'exception doit s'appliquer.

- Si l'exception doit s'appliquer à une période illimitée tout au long de l'année, sélectionnez l'option **Dans l'intervalle de temps** dans la liste déroulante **Type**. Entrez le début et la fin de la période de la journée dans les listes de sélection **Heure de début** et **Heure de fin**.

  Sélectionnez les jours de la semaine pour lesquels l'exception doit être appliquée. Pour finir, cliquez sur **Sauvegarder**.
- Si l'exception doit s'appliquer pendant une période limitée au cours de l'année, sélectionnez l'option **Dans l'intervalle de temps** dans la liste déroulante **Type**. Entrez la date de début de la période dans le champ **Date de début** et la date de fin dans le champ **Date de fin** pour l'année (format : jj.mm.aaaa). Entrez l'heure exacte de la date de début et de la date de fin dans les listes de sélection **Heure de début** et **Heure de fin**. L'exception s'appliquera entre la date/heure de début et la date/heure de fin de la période couverte.

  Sélectionnez les jours de la semaine pour lesquels l'exception doit être appliquée. Pour finir, cliquez sur **Sauvegarder**.
- Si l'exception doit s'appliquer aux jours fériés, sélectionnez les **calendriers des jours fériés** dans la liste déroulante **Type**. Entrez la date de début de la période de congés dans le champ **Date de début** et la date de fin dans le champ **Date de fin**. Entrez le début de la période de la journée dans la liste de sélection **Heure de début** et la fin de la période dans la liste de sélection **Heure de fin**.

  Conseil : Les calendriers de congés sont prioritaires par rapport à d'autres calendriers et règles d'une file d'attente.
- Si l'exception doit s'appliquer chaque année, sélectionnez **Récurrence annuelle** dans la liste déroulante **Type**. Saisissez les dates de début

et de fin de la récurrence annuelle dans les champs **Date de début** et **Date de fin**, respectivement. Sélectionnez les heures de début et de fin de la récurrence annuelle dans les zones de liste **Heure de début** et **Heure de fin**, respectivement.

14) Cliquez sur **Sauvegarder**.

15) Répétez les étapes 10 à 14 si vous souhaitez définir d'autres exceptions pour certaines périodes de temps.

16) Si vous souhaitez savoir quelle règle (CCV) du calendrier est activée à un moment quelconque, cliquez sur **Tester le calendrier**. Dans la liste déroulante **Date**, sélectionnez le jour souhaité et dans la liste de sélection **Heure**, sélectionnez l'heure souhaitée. Cliquez sur **Tester le calendrier**. Ensuite, le système indique la règle (CCV) activée ce jour-là et à cette heure-là. Cliquez sur **Fermer** pour fermer la fenêtre **Tester le calendrier**.

17) Si vous souhaitez assigner cette programmation à une ou plusieurs files d'attente, cochez la ou les cases correspondant à la ou aux files d'attente souhaitées dans la zone **Files d'attente**.

Remarque : Une file d'attente sélectionnée ne peut être affectée qu'à un seul calendrier, mais plusieurs files d'attente différentes peuvent être affectées à un calendrier sélectionné.

---

18) Fermez la fenêtre.

17.6.2.6 Comment modifier le calendrier

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Calendrier**. Tous les calendriers disponibles sont affichés.
5) Sélectionnez le calendrier à modifier et cliquez sur **Modifier**.
6) Modifiez les paramètres souhaités pour la CCV par défaut.
   - Si vous voulez affecter une règle (CCV) différente de celles figurant dans la liste déroulante **CCV par défaut**, sélectionnez la règle souhaitée dans la liste déroulante **CCV par défaut**.
   - Si vous souhaitez modifier la règle (CCV) figurant dans la liste **CCV par défaut**, cliquez sur **Modifier** dans la zone **Calendrier**. La règle est affichée dans l'éditeur de règles. Modifiez les règles. Cliquez sur **Sauvegarder ...**. Entrez un nom pour la nouvelle règle puis cliquez sur **Enregistrer**. Fermez la fenêtre qui confirme l'enregistrement de la règle.

     Dans la liste déroulante **CCV par défaut**, sélectionnez la nouvelle règle que vous venez d'enregistrer.
7) Cliquez sur **Sauvegarder**.

8) Modifiez les paramètres souhaités dans la zone **Exceptions** :

- Si vous souhaitez affecter une autre règle (CCV) à une période spécifique du calendrier, cliquez sur **Ajouter** dans la zone **Exception**. Dans la liste déroulante de cette exception, sélectionnez la règle souhaitée. A l'aide des champs d'option et listes déroulantes, sélectionnez la période de temps durant laquelle cette exception doit s'appliquer. Entrez le nom de la règle dans le champ **Description**. Cliquez sur **Sauvegarder**.
- Si vous souhaitez modifier cette exception ou l'une des exceptions affichées, cliquez sur **Modifier** sous la zone **Exception** après avoir sélectionné l'exception souhaitée, puis utilisez les boutons radio, les listes déroulantes et les champs pour spécifier quand cette exception doit s'appliquer et sur quelle règle (CCV). En outre, vous pouvez cliquer sur **Modifier CCV** sous la zone **Exception** pour modifier la règle associée (CCV). La règle est affichée dans l'éditeur de règles. Modifiez les règles. Cliquez sur **Sauvegarder ...**. Entrez un nom pour la nouvelle règle puis cliquez sur **Enregistrer**. Fermez la fenêtre qui confirme l'enregistrement de la règle.

  Dans la liste déroulante, sélectionnez la nouvelle règle qui vient d'être enregistrée. A l'aide des champs d'option et listes déroulantes, sélectionnez la période de temps durant laquelle cette règle (CCV) doit s'appliquer. Cliquez sur l'icône verte Enregistrer.
- Si vous souhaitez supprimer cette exception ou l'une des exceptions affichées, cliquez sur le bouton **Supprimer** après la sélection de l'exception souhaitée.

9) Si vous souhaitez savoir quelle règle (CCV) du calendrier est activée à un moment quelconque, cliquez sur **Tester le calendrier**. Dans la liste déroulante **Date**, sélectionnez le jour souhaité et dans la liste de sélection **Heure**, sélectionnez l'heure souhaitée. Cliquez sur **Tester le calendrier**. Ensuite, le système indique la règle (CCV) activée ce jour-là et à cette heure-là. Cliquez sur **Fermer** pour fermer la fenêtre **Tester le calendrier**.

10) Si vous souhaitez assigner cette programmation à une ou plusieurs files d'attente, cochez la ou les cases correspondant à la ou aux files d'attente souhaitées dans la zone **Files d'attente**.

Remarque : Une file d'attente sélectionnée ne peut être affectée qu'à un seul calendrier, mais plusieurs files d'attente différentes peuvent être affectées à un calendrier sélectionné.

---

11) Fermez la fenêtre.

17.6.2.7 Comment effacer un calendrier

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.

3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.

4) Cliquez sur **Calendrier**. Tous les calendriers disponibles sont affichés.
5) Marquez le calendrier souhaité et cliquez sur **Supprimer**.

Conseil : Il est impossible de supprimer un calendrier tant qu'il est affecté à une file d'attente. Avant d'effacer, il faut supprimer l'affectation du calendrier à la (aux) file(s) d'attente.

17.6.2.8 Comment enregistrer une règle (CCV) en tant que fichier PDF

L'assistant **Centre d'appels** vous permet d'enregistrer des règles (CCV) sous la forme de fichier PDF. Le fichier PDF peut ensuite être imprimé ou envoyé par e-mail.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Centre d'appels**.
4) Cliquez sur **Calendrier**. Tous les calendriers disponibles sont affichés.
5) Sélectionnez le calendrier qui contient la règle souhaitée et cliquez sur **Modifier**.
6) Dans la liste déroulante, sélectionnez la règle souhaitée et cliquez sur **Modifier**. La règle est affichée dans l'éditeur de règles.
7) Cliquez sur **Imprimer**. La fenêtre Enregistrer s'affiche.
8) Indiquez le nom du fichier et sélectionnez le répertoire où le fichier doit être enregistré.
9) Cliquez sur **Enregistrer**.
10) Fermez la fenêtre et confirmez la fermeture avec **Oui**.

17.6.2.9 Comment télécharger une règle (CCV) en tant que fichier de sauvegarde

L'assistant **Centre d'appels** vous permet de télécharger les règles (CCV) sous la forme de fichier de sauvegarde.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Centre d'appels**.
4) Cliquez sur **Calendrier**. Tous les calendriers disponibles sont affichés.

5) Sélectionnez le calendrier qui contient la règle souhaitée et cliquez sur **Modifier**.
6) Dans la liste déroulante **CCV**, sélectionnez la règle souhaitée et cliquez sur **Modifier** dans la zone **Calendrier**. La règle est affichée dans l'éditeur de règles.
7) Cliquez sur **Télécharger**.

La règle souhaitée (CCV) est à présent téléchargée en tant que fichier de sauvegarde.

17.6.2.10 Comment charger une règle téléchargée (CCV) dans un format de fichier de sauvegarde

L'assistant **Centre d'appels** vous permet de charger des règles (CCV) téléchargées précédemment dans un format de fichier de sauvegarde.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Télécharger une règle (CCV) dans un format de fichier de sauvegarde.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Centre d'appels**.
4) Cliquez sur **Calendrier**. Tous les calendriers disponibles sont affichés.
5) Sélectionnez le calendrier qui contient la règle souhaitée et cliquez sur **Modifier**.
6) Dans la liste déroulante **CCV**, sélectionnez la règle souhaitée et cliquez sur **Modifier** dans la zone **Calendrier**. La règle est affichée dans l'éditeur de règles.
7) Cliquez sur **Choisir un fichier**, allez à l'emplacement de stockage du fichier de sauvegarde de la règle souhaitée, puis cliquez sur **Ouvrir**.

   Si vous choisissez un fichier qui n'est pas dans un format de sauvegarde, une erreur se produira.
8) Cliquez sur **Restaurer la sauvegarde**.

La règle souhaitée (CCV) est maintenant chargée dans le système.

17.6.2.11 Comment ajouter un calendrier

Conditions préalables

Au moins un groupe UCD a été configuré.

Au moins un poste a été mis en place.

Au moins un compte de messagerie est disponible pour recevoir des e-mails (si les e-mails doivent être mis en file d'attente).

L'envoi d'e-mails a été configuré dans le système de communication (si des e-mails doivent être envoyés par des agents de la file d'attente).

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Pour lancer l'assistant **Centre d'appels**, cliquez sur **Modifier**.
4) Cliquez sur Visibilité de la **file d'attente**.
5) Cliquez sur **Ajouter**.
6) Cliquez sur l'onglet **Paramètres**.
7) Saisissez le nom de la file d'attente dans le champ **Nom de la file d'attente**.

   Recommandation : utilisez le nom de l'un de vos groupes UCD configurés.

   Conseil : Pour vous assurer que le nom de la file d'attente est entièrement affiché dans un rapport, vous devez sélectionner des désignations courtes et éviter les concaténations. Exemple : Groupe de ventes intérieures 1 (pas : Groupe de ventes intérieures 1)

8) Sélectionnez l'une des options suivantes pour l'état de la file d'attente :
   - Si vous souhaitez activer la nouvelle file d'attente, sélectionnez l'élément **Actif** dans la liste déroulante **File d'attente active**.
   - Si vous souhaitez désactiver la nouvelle file d'attente, sélectionnez l'élément **Inactif** dans la liste déroulante **File d'attente active**.

     La désactivation d'une file d'attente entraîne l'activation de la solution de repli via le groupe UCD associé. Si aucun agent pour le groupe UCD n'est connecté, et si aucune autre destination de renvoi d'appel n'a été saisie pour le groupe UCD, les appelants entendront le signal occupé.
9) Entrez le numéro d'appel d'un groupe UCD que vous avez configuré lors de la configuration Basic du centre de contact dans le champ **Groupement**.
10) Sélectionnez l'élément **CSP** dans la liste déroulante **Commutateur téléphonique**.
11) Dans la liste déroulante **Calendrier**, sélectionnez le calendrier souhaité.
12) Entrez la valeur de seuil d'alarme dans le champ **Nombre d'alarmes de file d'attente**.

    Lorsque le nombre indiqué ici d'appels en attente dans la file d'attente est dépassé, l'icône de la file d'attente passe du vert à l'orange pour les agents.
13) Entrez la valeur de seuil d'alarme en secondes dans le champ **Temps d'alarme de file d'attente**.

    Si le temps d'attente d'un appel dans la file d'attente indiqué ici est dépassé, l'entrée correspondante de la liste des appels au centre de contacts devient rouge.
14) Entrez le temps en secondes après lequel un appel sans réponse doit être renvoyé au prochain agent libre dans le champ **Délai d'appel manqué**.

15) Entrez le temps en secondes qui détermine si un appel abandonné doit ou non être inclus dans les statistiques (c'est-à-dire dans un rapport) dans le champ **Seuil d'appel abandonné**.

    Sont consignés dans les statistiques les appels qui sont abandonnés une fois écoulé le temps indiqué.

16) Sélectionnez l'une des options suivantes pour l'affichage des pops d'écran dans l'application myAgent :

    Conseil : Les fenêtres surgissantes sont nécessaires pour recevoir et exécuter les rappels automatiques et pour recevoir des fax et des e-mails.

    - Si vous souhaitez qu'une fenêtre surgissante d'affichage et de saisie des données client apparaisse dans myAgent lors des appels entrants, cochez la case **Screen Pop Enabled**.
    - Si vous ne souhaitez pas qu'une fenêtre surgissante apparaisse dans myAgent lors des appels entrants, désactivez la case à cocher **Screen Pop Enabled**.

17) Pour le focus d'entrée, sélectionnez l'une des possibilités suivantes :

    Pour les files d'attente avec mode récapitulatif, les agents peuvent affecter leurs appels à des catégories spécifiques (commandes, réclamations, service, etc.) à l'aide de codes récapitulatifs.

    - Si vous souhaitez configurer une file d'attente avec le mode de récapitulation Récapitulation simple, sélectionnez l'option **Récapitulation simple**.
    - Si vous souhaitez configurer une file d'attente avec le mode de récapitulation Récapitulation multiple, sélectionnez l'option **Récapitulation multiple**.
    - Si vous souhaitez configurer une file d'attente sans mode de récapitulation, sélectionnez l'option **Pas de récapitulation**.

18) Si vous souhaitez modifier la priorité de la file d'attente, cliquez sur **Priorités**.

    Cliquez sur les points rouges dans la zone **Priorité de la file d'attente dans le temps** et faites-les glisser vers les positions souhaitées. L'axe horizontal indique le temps d'attente dans la file d'attente et l'axe vertical indique la priorité de la file d'attente sélectionnée par rapport aux autres files d'attente. Si un agent est affecté à plusieurs files d'attente, il est possible de déterminer si les appels pour une file d'attente doivent être envoyés à cet agent avec une priorité supérieure à celle des appels pour les autres files d'attente.

    Faites glisser les barres de défilement dans la zone **Priorités du type d'appel** vers la position souhaitée. Cela définit la priorité des types d'appels dans la file d'attente sélectionnée. Des priorités plus élevées sont attribuées en déplaçant les barres de défilement progressivement vers la droite.

    Conseil : Une priorité plus élevée doit être choisie pour les appels vocaux que pour les autres types d'appels. Sinon, les appelants en attente pourraient être remplacés par des rappels, des télécopies ou des courriels.

19) Pour le focus d'entrée, sélectionnez l'une des possibilités suivantes :

La profondeur de la file d'attente peut être définie pour chaque file d'attente individuellement dans la boîte de dialogue de configuration de la file d'attente

- Si le **mode de profondeur de file d'attente** est défini sur **Statique**, les paramètres **WLS** et **Taille de la profondeur de file d'attente** peuvent être configurés.
- Si le **mode de profondeur de file d'attente** est défini sur **Néant**, le paramètre **WLS** peut néanmoins être configuré et affecte également la configuration UCD, mais le paramètre **Taille de la profondeur de file d'attente** ne peut pas être défini.

20) Saisissez la valeur Waiting Loop Size dans le champ **WLS**. La valeur **WLS**, qui correspond au nombre d'Appels vocaux en attente de connexion à un agent, affecte directement la configuration du paramètre Appels en file d'attente du groupe UCD attribué.

21) Si le **mode de profondeur de file d'attente** est défini sur **Statique**, saisissez la quantité de la profondeur de file d'attente dans le champ **Taille de la profondeur de file d'attente**. Le récapitulatif de la taille de la boucle de file d'attente (WLS) et les appels sur l'agent.

22) Cliquez sur l'onglet **Pilotes de file d'attente**.

23) Si des télécopies doivent être mises en file d'attente, sélectionnez l'option ou les options appropriées du ou des pilotes souhaités (numéro/s de téléphone) dans la zone **Pilotes de télécopie entrante**.

Les messages Fax envoyés à ces numéros sont placés dans la file d'attente et traités comme des appels entrants.

24) Sélectionnez l'une des options suivantes dans la zone **Service de messagerie entrante** afin que les e-mails soient placés dans la file d'attente :

- Si vous souhaitez configurer une nouvelle adresse e-mail, cliquez sur **Ajouter**. La fenêtre **Ajouter** s'affiche.

  Sélectionnez la méthode d'authentification de votre serveur de messagerie dans la liste déroulante **Méthode d'authentification**. Vous pouvez choisir entre **Basic**, **OAuth 2.0 EWS** et **OAuth 2.0 Graph**.

  Saisissez la désignation du serveur de messagerie à utiliser pour récupérer les e-mails dans le champ **Serveur** (par ex. : `pop3.web.de`).

  Saisissez le numéro de port du serveur de messagerie dans le champ **Port** (par ex. : `110`, numéro de port par défaut pour POP3).

  Si la méthode d'authentification sélectionnée est **Basic**, saisissez les données d'accès au serveur de messagerie dans les champs **Nom d'utilisateur** et **Mot de passe**.

  Si la méthode d'authentification sélectionnée est **OAuth 2.0**, saisissez le nom d'utilisateur pour accéder au serveur de messagerie dans les champs **Nom d'utilisateur**, **ID de locataire**, **ID d'application** et **Secret client**. ID du locataire, ID de l'application et Secret du client correspondant à l'application qui a été enregistrée dans Azure AD pour les files d'attente d'e-mails. Vous pouvez les obtenir auprès de votre administrateur Azure AD. Saisissez le périmètre de

l'application dans le champ **Périmètre** (valeur par défaut : https://outlook.office365.com/.default).

Indiquez si les e-mails doivent être envoyés via une connexion SSL (Secure Socket Layer). Si vous souhaitez utiliser une connexion SSL, cochez la case **Utiliser la connexion SSL**. (Notez que le numéro de port du serveur de messagerie peut alors être modifié. Le numéro de port par défaut pour POP3 via SSL = 995). Si vous ne souhaitez pas utiliser de connexion SSL, décochez la case **Utiliser la connexion SSL**.

Cliquez sur **Sauvegarder**. La nouvelle adresse e-mail apparaîtra alors dans la zone **Service de messagerie entrante**.

- Si vous souhaitez modifier une adresse e-mail existante, sélectionnez l'adresse e-mail souhaitée et cliquez sur **Modifier**. La fenêtre **Modifier** s'affiche.

  Modifiez les paramètres requis, puis cliquez sur **Sauvegarder**.
- Si vous souhaitez supprimer une adresse e-mail existante, sélectionnez l'adresse e-mail souhaitée et cliquez sur **Enlever**.

25) Cliquez sur l'onglet **Divers**.

26) Dans le champ **Adresse e-mail de retour**, saisissez l'adresse e-mail qui doit être affichée comme adresse de l'expéditeur (pour le destinataire) lorsqu'un e-mail est envoyé par un agent.

27) Sélectionnez l'une des options suivantes pour un acheminement intelligent des appels dans la file d'attente :

- Si les appels entrants doivent être automatiquement renvoyés à l'agent qui a été connecté en dernier avec l'appelant, activez la case à cocher **Rechercher le dernier client de l'agent si aucun agent préféré n'est trouvé**. Comme condition préalable, aucun agent privilégié ne doit avoir été défini pour l'appelant.
- Si les appels entrants ne doivent pas être automatiquement renvoyés à l'agent qui a été connecté en dernier avec l'appelant, désactivez la case à cocher **Rechercher le dernier client de l'agent si aucun agent préféré n'est trouvé**.

28) Cliquez sur **Sauvegarder**.

17.6.2.12 Comment modifier le calendrier

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.

3) Pour lancer l'assistant **Centre d'appels**, cliquez sur **Modifier**.

4) Cliquez sur **File d'attente**.

5) Marquez la file d'attente souhaitée et cliquez sur **Modifier**.

6) Cliquez sur l'onglet **Paramètres généraux**.

7) Modifiez les postes souhaités.

8) Sélectionnez l'une des options suivantes pour l'état de la file d'attente :

- Si vous souhaitez activer la file d'attente, sélectionnez l'élément **Actif** dans la liste déroulante **File d'attente active**.
- Si vous souhaitez désactiver la file d'attente, sélectionnez l'élément **Inactif** dans la liste déroulante **File d'attente active**.

  La désactivation d'une file d'attente entraîne l'activation de la solution de repli via le groupe UCD associé. Si aucun agent pour le groupe UCD n'est connecté, et si aucune autre destination de renvoi d'appel n'a été saisie pour le groupe UCD, les appelants entendront le signal occupé.

9) Sélectionnez l'une des options suivantes pour l'affichage des pops d'écran dans l'application myAgent :

Conseil : Les fenêtres surgissantes sont nécessaires pour recevoir et exécuter les rappels automatiques et pour recevoir des fax et des e-mails.

- Si vous souhaitez qu'une fenêtre surgissante d'affichage et de saisie des données client apparaisse dans myAgent lors des appels entrants, cochez la case **Screen Pop Enabled**.
- Si vous ne souhaitez pas qu'une fenêtre surgissante apparaisse dans myAgent lors des appels entrants, décochez la case **Screen Pop Enabled**.

10) Pour le focus d'entrée, sélectionnez l'une des possibilités suivantes :

Pour les files d'attente avec mode récapitulatif, les agents peuvent affecter leurs appels à des catégories spécifiques (commandes, réclamations, service, etc.) à l'aide de codes récapitulatifs.

- Si vous souhaitez définir le mode de récapitulation Récapitulation simple pour la file d'attente, sélectionnez l'option **Récapitulation simple**.
- Si vous souhaitez définir le mode de récapitulation Récapitulation multiple pour la file d'attente, sélectionnez l'option **Récapitulation multiple**.
- Si vous ne souhaitez pas définir de mode de récapitulation pour la file d'attente, sélectionnez l'option **Pas de récapitulation**.

11) Si vous souhaitez modifier la priorité de la file d'attente, cliquez sur **Priorités**.

Cliquez sur les points rouges dans la zone **Priorité de la file d'attente dans le temps** et faites-les glisser vers les positions souhaitées. L'axe horizontal indique le temps d'attente dans la file d'attente et l'axe vertical indique la priorité de la file d'attente sélectionnée par rapport aux autres files d'attente. Si un agent est affecté à plusieurs files d'attente, il est possible de déterminer si les appels pour une file d'attente doivent être envoyés à cet agent avec une priorité supérieure à celle des appels pour les autres files d'attente.

Faites glisser les barres de défilement dans la zone **Priorités du type d'appel** vers la position souhaitée. Cela définit la priorité des types d'appels dans la file d'attente sélectionnée. Des priorités plus élevées sont

attribuées en déplaçant les barres de défilement progressivement vers la droite.

Conseil : Une priorité plus élevée doit être choisie pour les appels vocaux que pour les autres types d'appels. Sinon, les appelants en attente pourraient être remplacés par des rappels, des télécopies ou des courriels.

---

12) Cliquez sur l'onglet **Pilotes de file d'attente**.

13) Sélectionnez les paramètres souhaités dans la zone **Pilotes de fax entrants** :

- Si des fax doivent être mis en file d'attente, cochez la ou les cases appropriées du ou des pilotes souhaités (numéro(s) de téléphone) dans la zone **Pilotes de fax entrants**.
- Si les fax ne doivent pas être mis en file d'attente, décochez la ou les cases **Pilotes de fax entrants**.

14) Sélectionnez les paramètres souhaités dans la zone **Service de messagerie entrante** :

- Si vous souhaitez configurer une nouvelle adresse e-mail, cliquez sur **Ajouter**. La fenêtre **Ajouter** s'affiche.

  Sélectionnez la méthode d'authentification de votre serveur de messagerie dans la liste déroulante **Méthode d'authentification**. Vous pouvez choisir entre **Basic**, **OAuth 2.0 EWS** et **OAuth 2.0 Graph**.

  Entrez la désignation du serveur de messagerie à utiliser pour récupérer les e-mails dans le champ **Serveur** (par exemple, `pop3.web.de`).

  Entrez le numéro de port du serveur de messagerie dans le champ **Port** (par exemple, `110`, le numéro de port par défaut pour POP3).

  Si la méthode d'authentification sélectionnée est **Basic**, entrez les données d'accès au serveur de messagerie dans les champs **Nom d'utilisateur** et **Mot de passe**.

  Si la méthode d'authentification sélectionnée est **OAuth 2.0**, entrez le nom d'utilisateur pour accéder au serveur de messagerie dans les champs **Nom d'utilisateur**, **ID de locataire**, **ID d'application** et **Secret client**. ID du locataire, ID de l'application et Secret du client correspondant à l'application qui a été enregistrée dans Azure AD pour les files d'attente d'e-mails. Vous pouvez les obtenir auprès de votre administrateur Azure AD. Saisissez le périmètre (scope) de l'application dans le champ **Périmètre** (valeur par défaut : https://outlook.office365.com/.default).

  Indiquez si les e-mails doivent être envoyés via une connexion SSL (Secure Socket Layer). Si vous souhaitez utiliser une connexion SSL, cochez la case **Utiliser la connexion SSL**. (Notez que le numéro de port du serveur de messagerie peut être modifié en conséquence.) Le numéro de port par défaut pour POP3 via SSL = 995). Si vous ne souhaitez pas utiliser une connexion SSL, désactivez la case à cocher **Utiliser la connexion SSL**.

  Cliquez sur **Sauvegarder**. La nouvelle adresse e-mail apparaîtra alors dans la zone **Service de messagerie entrante**.

- Si vous souhaitez modifier une adresse e-mail existante, marquez l'adresse e-mail souhaitée et cliquez sur **Modifier**. La fenêtre **Modifier** s'affiche.

  Modifiez les paramètres requis, puis cliquez sur **Sauvegarder**.
- Si vous souhaitez supprimer une adresse e-mail existante, marquez l'adresse e-mail souhaitée et cliquez sur **Supprimer**.

15) Cliquez sur l'onglet **Divers**.

16) Modifiez les postes souhaités.

17) Cliquez sur **Sauvegarder**.

17.6.2.13 Comment activer ou désactiver la file d'attente

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.

3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.

4) Cliquez sur **File d'attente**.

5) Cliquez sur **Modifier**.

6) Cliquez sur l'onglet **Paramètres généraux**.

7) Sélectionnez l'une des possibilités suivantes pour l'état de la file d'attente :

- Si vous souhaitez activer la file d'attente, sélectionnez dans la liste déroulante **File d'attente active** l'entrée **Active**.
- Si vous souhaitez désactiver la file d'attente, sélectionnez dans la liste déroulante **File d'attente active** l'entrée **Non active**.

  La désactivation d'une file d'attente conduit à l'activation de la solution de repli par le groupe UCD correspondant. Si aucun agent n'est inscrit dans le groupe UCD et qu'aucune autre destination de renvoi temporisé n'est inscrite pour le groupe UCD, les appelants entendent la tonalité Occupé.

8) Cliquez sur **Sauvegarder**.

17.6.2.14 Comment configurer dans les files d'attente les pilotes des messages fax entrants

Conditions préalables

Il existe au moins un numéro de fax pour la réception de fax.

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Abonnés**.

3) Dans l'arborescence du menu, cliquez sur **Abonnés** > **Application UC** > **Centre d'appels Fax**. Il s'affiche les numéros de port logiques prévus pour les boîtes Fax.
4) Dans l'arborescence du menu, cliquez sur le numéro de port souhaité.
5) Cliquez sur l'onglet **Modifier les paramètres de l'abonné**.
6) Dans le champ **Numéro**, indiquez le numéro du nouveau pilote pour les messages Fax entrants.
7) Dans le champ **Nom**, indiquez le nom du nouveau pilote pour les messages Fax entrants.
8) Dans le champ **N° SDA**, indiquez le numéro SDA du nouveau pilote pour les messages Fax entrants.
9) Cliquez sur **Appliquer** puis sur **OK**.

Le pilote pour messages Fax entrants peut maintenant être activé pour la file d'attente souhaitée.

17.6.2.15 Comment définir les valeurs de consigne pour le degré de service

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Niveau de service**.
5) Sélectionnez la file d'attente souhaitée et cliquez sur **Modifier**.
6) Placez les points rouge (cliquer-glisser) sur les positions souhaitées.

   L'axe horizontal correspond au temps d'attente dans la file d'attente en intervalles de 10 secondes, l'axe vertical correspond à la valeur de consigne du degré de service, en pourcentage.

   Vous précisez ainsi les valeurs de consigne pour la qualité de la commutation de la file d'attente. La comparaison entre les valeurs de consigne et les temps d'attente réels des utilisateurs permet d'obtenir des indications de qualité.
7) Cliquez sur **Sauvegarder**.

17.6.2.16 Comment définir les priorités des appelants VIP

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.

4) Cliquez sur **Priorités des appelants VIP**.
5) Sélectionnez la file d'attente souhaitée et cliquez sur **Modifier**.
6) Placez les points rouge (cliquer-glisser) sur les positions souhaitées.

   Vous définissez ainsi la priorité des appelants normaux par rapport aux appelants VIP.

   L'axe horizontal correspond au temps d'attente dans la file d'attente en intervalles de de 30 secondes, l'axe vertical correspond à la priorité des appels normaux qui ne sont pas dans la liste d'appels VIP.

   Vous pouvez par exemple placer les points rouges de manière à ce qu'une priorité de 100 pour cent soit atteinte au bout de 180 secondes. Dans ce cas, les appelants normaux ne sont traités à égalité par rapport aux appelants VIP qu'après un temps d'attente de 180 secondes. Les appels VIP entrants qui arrivent auparavant sont traités prioritairement dans la file d'attente.

   Variante : vous pouvez entrer les valeurs des différents intervalles individuels à droite à côté du diagramme.
7) Cliquez sur **Sauvegarder**.

17.6.2.17 Comment modifier la liste d'appels VIP

Conditions préalables

L'appelant prévu pour la liste des appels VIP figure dans le répertoire externe.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Liste d'appels VIP**.
5) Sélectionnez la file d'attente souhaitée et cliquez sur **Modifier**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez intégrer un appelant dans la liste d'appels VIP, cliquez sur **Ajouter** dans la zone supérieure de la fenêtre. Sélectionnez l'entrée souhaitée. Définissez la priorité de cet appelant VIP par rapport à d'autres appelants VIP en placez la barre de défilement de la partie inférieure de la fenêtre sur la position souhaitée. Plus vous êtes à droite et plus la priorité est élevée.
   - Si vous souhaitez intégrer un modèle de numéro d'appel dans la liste d'appels VIP, cliquez sur **Ajouter** dans la zone inférieure de la fenêtre. Dans le champ Modèle, indiquez le modèle de numéro d'appel souhaité (par exemple `089 7577*`). Définissez la priorité de tous les appelants VIP de ce modèle de numéro d'appel par rapport à d'autres appelants VIP en placez la barre de défilement sur la position souhaitée. Plus vous êtes à droite et plus la priorité est élevée.

     Il n'est pas possible d'entrer des modèles de numéro d'appel au format canonique. L'utilisation de signes d'abréviation pour les préfixes de pays

(par ex. +49 à la place de 0049) n'est pas possible. Les modèles de numéro d'appel doivent toujours être indiqués sans indicatif réseau.

Exemple pour un type de numéro : `089 7577*` (089 = Indicatif local Munich, 7577 = Numéro de l'installation zéro d'une entreprise, * = joker pour un chiffre quelconque). L'inscription de ce modèle de numéro dans la liste d'appels VIP permet à tous les appelants de Munich, dont le numéro commence par 7577, d'être traités prioritairement.

Les caractères suivants peuvent servir de joker (wildcard) dans un modèles de numéro d'appel :

– * = joker pour un nombre quelconque
– ? = joker pour un chiffre quelconque

- Si vous souhaitez modifier une entrée de la liste des appels VIP, sélectionnez l'entrée souhaitée et cliquez sur **Modifier**. Modifiez les paramètres souhaités.
- Si vous souhaitez supprimer une entrée de la liste des appels VIP, sélectionnez l'entrée souhaitée et cliquez sur **Supprimer**.

7) Cliquez sur **Sauvegarder**.

17.6.2.18 Comment définir les agents préférés

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Centre d'appels**.
4) Cliquez sur **Agents préférés**.
5) Sélectionnez la file d'attente souhaitée et cliquez sur **Modifier**.
6) Dans la zone **Clients**, sélectionnez l'appelant souhaité, qui correspond à la partie supérieure des deux tableaux.
7) Cliquez sur **Ajouter agent**.
8) Sélectionnez l'agent souhaité et cliquez sur **Enregistrer**.

Le nom de l'agent sélectionné s'affiche alors dans la zone **Agents préférés**.

9) Si vous souhaitez configurer un autre agent comme agent préféré, répétez les étapes 7 et 8.
10) Définissez la priorité des agents préférés lorsque plusieurs agents préférés ont été définis. Vous disposez des options suivantes :

- Si vous souhaitez attribuer une priorité supérieure, sélectionnez l'agent souhaité et, à l'aide du bouton **Vers le haut**, placez-le sur une position plus avancée dans la liste.
- Si vous souhaitez attribuer une priorité inférieure, sélectionnez l'agent souhaité et, à l'aide du bouton **Vers le bas**, placez-le sur une position moins avancée dans la liste.

17.6.2.19 Comment effacer des agents préférés

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Agents préférés**.
5) Sélectionnez la file d'attente souhaitée et cliquez sur **Modifier**.
6) Dans la zone **Agents préférés**, sélectionnez le ou les agents à supprimer.
7) Cliquez sur **Supprimer un agent**.

17.6.2.20 Comment ajouter une pause dans un centre d'appels

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Centre d'appels**.
4) Cliquez sur **Pauses du centre d'appels**.
5) Cliquez sur **Ajouter**.
6) Dans le champ **Nom**, entrez le nom de la pause du centre d'appels.
7) Dans le champ **Durée (Minutes)**, entrez la durée de la pause du centre d'appels en minutes.
8) Cochez la case **Active** afin d'activer la nouvelle pause de Centre d'appels pour l'ensemble du système.
9) Cliquez sur **Enregistrer**.
10) Si vous souhaitez ajouter une autre pause dans le centre d'appels, répétez les étapes 5 à 9.

17.6.2.21 Comment modifier la pause du centre de contacts

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Pauses du centre de contacts**.

5) Sélectionnez la pause souhaitée du centre de contacts et cliquez sur **Modifier**.
6) Modifiez les paramètres souhaités.
7) Sélectionnez une des possibilités suivantes :
   - Si la pause du centre d'appels doit être accessible aux agents, cochez la case **Actif**.
   - Si la pause du centre d'appels ne doit pas être accessible aux agents, décochez la case **Actif**.
8) Cliquez sur **Sauvegarder**.

17.6.2.22 Comment effacer une pause d'un centre d'appels

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Centre d'appels**.
4) Cliquez sur **Pauses du centre d'appels**.
5) Sélectionnez la pause souhaitée du centre d'appels et cliquez sur **Supprimer**.

17.6.2.23 Comment ajouter un code de post-traitement pour "Post-traitement simple"

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Codes de post-traitement de centre d'appels**. Sont affichées toutes les files d'attente pour lesquelles un code de post-traitement "Post-traitement simple" a été défini.
5) Cliquez sur **Ajouter**.
6) Dans la liste déroulante **File d'attente** sélectionnez la file d'attente à laquelle vous voulez ajouter un code de post-traitement.
7) Dans le champ **Description**, entrez la désignation du nouveau code de post-traitement.
8) Cliquez sur **Sauvegarder**.
9) Si vous souhaitez ajouter un autre code de post-traitement, répétez les étapes 5 à 8.

17.6.2.24 Comment modifier le code de post-traitement pour "Post-traitement simple"

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Codes de post-traitement de centre d'appels**. Sont affichées toutes les files d'attente pour lesquelles un code de post-traitement "Post-traitement simple" a été défini.
5) Sélectionnez l'entrée souhaitée et cliquez sur **Modifier**.
6) Si vous voulez affecter le code de post-traitement à une autre file d'attente, sélectionnez dans la liste déroulante **File d'attente** la nouvelle file d'attente.
7) Si vous souhaitez modifier la désignation du code de post-traitement, entrez la nouvelle désignation dans le champ **Description**.
8) Cliquez sur **Sauvegarder**.

17.6.2.25 Comment effacer un code de post-traitement pour "Post-traitement simple"

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Centre d'appels**.
4) Cliquez sur **Codes de post-traitement de centre d'appels**. Sont affichées toutes les files d'attente pour lesquelles un code de post-traitement "Post-traitement simple" a été défini.
5) Sélectionnez l'entrée souhaitée et cliquez sur **Supprimer**.

17.6.2.26 Comment ajouter un code de post-traitement pour "Post-traitement multiple"

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Code de multi-post-traitement**.

5) Dans la liste déroulante **File d'attente du centre de contacts**, sélectionnez la file d'attente souhaitée. Sont affichés les groupes et sous-groupes déjà définis pour cette file d'attente.

Remarque : Sous chaque groupe ou sous-groupe (le cas échéant), au moins un élément doit également être configuré pour permettre à l'agent de post-traitement d'un appel. Le post-traitement d'un appel n'est pas possible si un groupe ou un sous-groupe est vide.

---

6) Si vous souhaitez regrouper dans un groupe le nouveau code de post-traitement avec d'autres codes de post-traitement, sélectionnez l'une des possibilités suivantes.

- Si vous souhaitez affecter le nouveau code de post-traitement à un groupe ou sous-groupe existant, sélectionnez le groupe ou le sous-groupe souhaité et cliquez sur **Ajouter un élément**. Dans le champ Nouvel élément de post-traitement, entrez la désignation du **Nouveau élément de post-traitement** et cliquez sur **OK**.
- Si vous souhaitez affecter le nouveau code de post-traitement à un nouveau groupe, cliquez sur **Ajouter un groupe**. Dans le champ **Nom du groupe**, entrez la désignation du nouveau groupe et cliquez sur **OK**.

  Sélectionnez le nouveau groupe et cliquez sur **Ajouter un élément**. Dans le champ Nouvel élément de post-traitement, entrez la désignation du **Nouveau élément de post-traitement** et cliquez sur **OK**.
- Si vous souhaitez affecter le nouveau code de post-traitement à un nouveau sous-groupe, sélectionnez le groupe souhaité et cliquez sur **Ajouter un groupe**. Dans le champ **Nom du groupe**, entrez la désignation du nouveau sous-groupe et cliquez sur **OK**.

  Sélectionnez le nouveau sous-groupe et cliquez sur **Ajouter un élément**. Dans le champ Nouvel élément de post-traitement, entrez la désignation du **Nouveau élément de post-traitement** et cliquez sur **OK**.

7) Si vous souhaitez ajouter un autre motif de post-traitement, répétez les étapes 5 et 6.

17.6.2.27 Comment modifier le code de post-traitement pour "Post-traitement multiple"

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Code de multi-post-traitement**.
5) Dans la liste déroulante **File d'attente du centre de contacts**, sélectionnez la file d'attente souhaitée. Sont affichés les groupes et sous-groupes déjà définis pour cette file d'attente.
6) Sélectionnez le groupe ou le sous-groupe auquel est affecté le code de post-traitement à modifier. Tous les codes de post-traitement (éléments) affectés à ce groupe sont affichés.

7) Sélectionnez le code de post-traitement à modifier et cliquez sur **Renommer un élément**.
8) Dans le champ **Renommer le code de post-traitement**, entrez une nouvelle désignation pour le code de post-traitement et cliquez sur **OK**.
9) Si vous souhaitez modifier la désignation du groupe ou du sous-groupe, cliquez sur **Renommer le groupe**.
10) Dans le champ **Nom du groupe**, entrez une nouvelle désignation pour le groupe ou le sous-groupe et cliquez sur **OK**.

17.6.2.28 Comment effacer le code de post-traitement pour "Post-traitement multiple"

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Centre de contacts**.
4) Cliquez sur **Code de multi-post-traitement**.
5) Dans la liste déroulante **File d'attente du centre de contacts**, sélectionnez la file d'attente souhaitée. Sont affichés les groupes et sous-groupes déjà définis pour cette file d'attente.
6) Sélectionnez le groupe ou le sous-groupe auquel est affecté le code de post-traitement à effacer. Tous les codes de post-traitement (éléments) affectés à ce groupe sont affichés.
7) Sélectionnez le code de post-traitement à effacer et cliquez sur **Supprimer un élément**.
8) Si vous souhaitez effacer le groupe ou le sous-groupe, cliquez sur **Supprimer le groupe**.

17.6.2.29 Comment affecter un agent à une file d'attente

À l'aide de l'assistant **Centre d'appels**, vous pouvez affecter les agents à une ou plusieurs files d'attente.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Pour lancer l'assistant **Centre d'appels**, cliquez sur **Modifier**.
4) Cliquez sur **Liaisons de file d'attente**. Toutes les files d'attente disponibles s'affichent.
5) Sélectionnez la file d'attente où vous voulez affecter un agent et cliquez sur **Modifier**. Tous les agents déjà affectés à une file d'attente s'affichent.

6) Pour ajouter l'agent approprié à la file d'attente souhaitée, cliquez sur **Ajouter**. La fenêtre **Ajouter** s'affiche.
7) Sélectionnez l'une des options suivantes :
   - Si l'agent doit recevoir des appels sans tenir compte de la charge de la file d'attente, sélectionnez **Agent primaire** dans la liste déroulante **Type**.
   - Si l'agent doit recevoir des appels uniquement en cas de débordement de la file d'attente, sélectionnez **Agent de débordement** dans la liste déroulante **Type**.
8) Si vous avez sélectionné **Agent de débordement** :
   a) Dans le champ **Débordement après (secondes)**, indiquez l'intervalle de temps à l'issue duquel les appels entrants d'un agent doivent être transférés en cas de débordement.
   b) Dans le champ **Débordement après appels dans file d'attente**, indiquez le nombre maximum d'appels. Un agent de débordement reçoit les appels qui se situent au-delà de ce nombre maximum.
9) Dans le champ **Niveau de compétence** de l'agent, indiquez un pourcentage.

   En utilisant le niveau de compétences, vous gérez la répartition des appels en direction des agents, dans la file d'attente. Les agent de niveau de compétence plus élevé sont utilisés de préférence lors de la distribution des appels. Lorsque tous les agents ont le même niveau de compétence, l'appel est envoyé à l'agent libre depuis le plus longtemps.
10) Sélectionnez l'une des options suivantes :
   - Si l'agent doit recevoir des demandes de rappel sous la forme de messages Voix, cochez la case **Activer le rappel d'agent**.
   - Lorsque l'agent ne doit pas recevoir de demande de rappel, décochez la case **Activer le rappel d'agent**.
11) Dans le champ **Post-traitement**, saisissez la durée de post-traitement automatique en secondes pour l'agent figurant dans cette file d'attente.
12) Cliquez sur **Sauvegarder**.
13) Si vous voulez affecter d'autres agents aux files d'attente, répétez les étapes 5 à 12.

17.6.2.30 Comment supprimer un agent dans une file d'attente

À l'aide de l'assistant **Centre d'appels**, vous pouvez supprimer des agents d'une ou plusieurs files d'attente.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **UC Suite**.
3) Pour lancer l'assistant **Centre d'appels**, cliquez sur **Modifier**.
4) Cliquez sur **Liaisons de file d'attente**. Toutes les files d'attente disponibles s'affichent.

5) Sélectionnez la file d'attente d'où vous voulez supprimer un agent et cliquez sur **Modifier**. Tous les agents déjà affectés à une file d'attente s'affichent.
6) Sélectionnez l'agent souhaité et cliquez sur **Supprimer**.
7) Si vous souhaitez supprimer d'autres agents des files d'attente, répétez les étapes 5 et 6.

17.7 Remarques sur l'utilisation des centres d'appel

Vous disposez ici d'informations sur les particularités et les restrictions possibles dans l'exploitation du centre d'appels.

17.7.1 Restrictions lors de l'exploitation du centre d'appels

Certaines conditions s'appliquent à l'utilisation du centre d'appels. De plus, cela provoque des restrictions lors de l'utilisation des fonctionnalités système par les agents.

Conditions pour l'utilisation du centre d'appels

Les conditions suivantes pour l'utilisation du centre d'appels doivent être prises en compte :

- Lignes

  Le centre de contacts ne supporte aucune ligne réseau analogique (HKZ). Toutes les connexions externe du centre d'appels doivent avoir lieu via RNIS ou via téléphonie IP. Remarque : la connexion via la téléphonie IP est exclusivement possible à l'aide de fournisseurs de services de téléphonie sur Internet qui sont homologués.
- Mise en réseau

  Dans une mise en réseau, tous les agents doivent être connectés au système de communication où le centre d'appels est configuré.
- Téléphones d'agent

  Les agents peuvent utiliser tous les téléphones système (téléphones IP (HFA), par exemple OpenStage 40 ou $U_{P0/E}$, par exemple OpenStage 40 T) et les téléphones DECT. Remarque : seuls les téléphones DECT validés actuellement pour l'exploitation avec OpenScape Business Cordless peuvent être utilisés.

  L'utilisation de téléphones analogiques, RNIS et SIP est impossible.

  Les agents ne doivent pas être membres d'un groupe (appel de groupe, groupe de recherche) ou MULAP. Cette restriction s'applique aussi en liaison avec les fonctionnalités système utilisées avec MULAP : configuration Team (groupe Team), Chef/Secrétaire (groupe Top) et Mobility Entry".
- myAgent

  myAgent ne devrait pas être utilisé simultanément avec d'autres clients UC car la possibilité d'une influence réciproque de l'état Présence n'est pas exclue (voir Remarques sur l'utilisation simultanée de myAgent et des clients UC Suite). En mode de fonctionnement normal du centre d'appels, les agents utilisent exclusivement myAgent pour modifier leur état (Connexion, Déconnexion, Disponible etc.).

- Connexion des applications via l'interface CSTA

  Si les conditions suivantes sont respectées, la connexion des applications via l'interface CSTA es possible.

  – L'application ne doit pas créer de charge supplémentaire notable sur l'interface CSTA.

    En conséquence, le raccordements de solutions Unified Communications ou UCD, numéroteur CTI-Power-Dialer ou de solutions CTI avec de nombreux clients CTI individuels utilisés de manière intensive n'est pas autorisé.
  – L'application ne doit pas, via l'interface CSTA, gérer des téléphones d'agent ou créer des renvois d'appel pour les téléphones d'agent.

    En conséquence, la connexion d'applications CTI n'est pas autorisée pour les agents, les assistants règles ou les assistants personnels.

  La connexion de TAPI 120/170 est par principe validée. En ce qui concerne la charge du système de communication, il s'applique les mêmes conditions que pour la connexion d'autres application via l'interface CSTA. En liaison avec le centre de contacts, TAPI 120/170 doit de préférence être utilisé pour associer des systèmes CRM (Customer Relationship Management) / ERP (Enterprise Ressource Planning) dans la mesure où ils supportent TAPI.

Restrictions lors de l'utilisation de fonctionnalités système

Les fonctionnalités système indiquées ci-après ne sont pas disponibles pour les agents ou alors avec des restrictions. Ces fonctionnalités ne sont toutefois pas obligatoires pour les agents étant donné que l'affectation des appels est réalisée automatiquement par le centre d'appels. L'affectation est fonction des règles définies et de la disposition des agents.

- Fonctionnalités verrouillées

  L'activation des fonctionnalités système par myAgent et par le téléphone agent correspondant n'est pas supportée pour les agents disponibles du centre d'appels. Les agents peuvent activer les fonctionnalités système exclusivement à l'aide de myAgent.

  Les fonctionnalités système suivantes ne sont donc pas supportées en association avec myAgent :

  – Avertissement
  – Deuxième appel
  – Parcage
  – Appel de groupe
  – Ne pas déranger (pour agents connectés)
  – Entrée en tiers dans une communication d'agent (exception : agents disposant du niveau d'autorisation Superviseur ou Administrateur)
  – Fonctionnalités qui concernent le routage de l'appel et les communications actives

- Fonctionnalités avec conséquences sur le routage de l'appel

  Les fonctionnalités suivantes peuvent modifier l'acheminement des appels dans le centre d'appels ; elles ne doivent donc pas être exécutées par les agents.

  – Renvoi d'appel

    Si l'agent inscrit dans la file active un renvoi d'appel, il quitte la file.

    Le renvoi d'appel est désactivé dès que l'agent s'inscrit dans une file d'attente.
  – Ne pas déranger

    Si un agent connecté active Ne pas déranger à l'aide d'un client UC, il se produit une déconnexion.

    Ne pas déranger est désactivé dès que l'agent entre dans une file d'attente.
  – Relocate

    Le déménagement d'un téléphone modifie l'affectation logique des numéros de téléphone. La nouvelle affectation des numéros est transmise seulement après un restart (redémarrage) du centre d'appels.
  – Renvoi de nuit

    Lors de la configuration d'un renvoi de nuit dans le système de communication, il faut veiller à ce que la configuration des paramètres du centre d'appels (agents, files d'attente, etc.) soient identiques pour l'exploitation de jour et l'exploitation de nuit.
- Fonctionnalités avec conséquences sur les rapports

  L'exécution des fonctionnalités suivantes par un téléphone d'agent peut provoquer une falsification des rapports.

  – Interception d'appels du centre d'appels par de non agents
  – Transfert d'appel (par exemple à l'aide de la touche d'appel direct) des appels du centre d'appels vers de non agents
  – Conférence
  – Va-et-vient
  – Parcage

  Conseil : La fonctionnalité "Double appel" est neutre pour la représentation des appels du centre d'appels dans les rapports et elle peut être utilisée par les agents, indépendamment de la destination du double appel.
- Fonctions qui n'intéressent pas les agents

  Les fonctions suivantes n'ont pas d'importance puisque la fonctionnalité "Avertissement" est verrouillée pour les agents.

  – Poste opérateur
  – Destination de la hotline

17.8 Remarques sur l'utilisation des téléphones DECT

Les téléphones DECT peuvent être utilisés comme téléphones pour les agents de centres de contact. Toutefois, il convient de tenir compte des différences de procédure d'utilisation par rapport aux téléphones filaires.

Prérequis pour l'utilisation des téléphones DECT

- Seuls les téléphones DECT actuellement commercialisés pour fonctionner avec HiPath Cordless Office peuvent être utilisés.
- La zone dans laquelle se déplacent les agents du centre de contact doit offrir une couverture sans fil complète.
- Le nombre de stations de base doit être tel qu'il y ait suffisamment de canaux B disponibles pour les téléphones DECT des agents du centre de contact.
- Dans la mesure du possible, un agent de centre de contact ne devrait pas quitter la zone de couverture sans fil lorsqu'il est connecté à une file d'attente du centre de contact.

Différences dans le mode d'emploi par rapport aux téléphones filaires

- La connexion à une file d'attente du centre de contact n'est possible que via myAgent.
- Aucun message tel que **Disponible** ou **Pause**, par exemple, n'apparaît sur l'écran du téléphone DECT.
- Le contrôle d'un téléphone DECT via myAgent (par exemple, via la zone **Téléphonie** de la fenêtre principale de myAgent ou l'écran pop de l'appel entrant myAgent) n'est pas possible.
- Les appels entrants ne peuvent être acceptés que via le téléphone DECT.
- Les appels sortants doivent être initiés via le téléphone DECT.

Éléments à prendre en compte lors de l'utilisation de téléphones DECT :

- Temps de recherche

  Pour un appel entrant, le temps nécessaire pour trouver le téléphone DECT peut prendre plusieurs secondes (dans le pire des cas jusqu'à 20 secondes) avant qu'un appel ne soit signalé sur le téléphone DECT. Pendant la durée de la recherche, l'appelant entend la sonnerie.

  Le centre de contact considère ce temps comme « temps de prise en charge ». Le temps de prise en charge effectif par un agent de centre de contact comprend donc le temps de recherche et le temps d'alerte (c'est-à-dire le temps jusqu'à ce que l'appel soit pris en charge).

  Si un agent de centre de contact sort de la zone de couverture sans fil avec son téléphone DECT, cela peut entraîner des temps de recherche plus longs.
- Téléphone DECT introuvable

  Si un appel au centre de contact dépasse le délai prescrit pour qu'un agent prenne en charge l'appel (par exemple, parce que l'agent du centre de contact est hors de portée), l'agent est automatiquement déconnecté de la ou des files d'attente concernées. La reconnexion n'est possible que via myAgent.

17.9 Rapports

Sur la base des rapports, il est possible de déterminer l'état actuel du centre d'appels et d'analyser les forces et faiblesses des composantes correspondantes. Cela permet par exemple l'optimisation de la configuration du centre d'appels et une utilisation plus efficace des ressources du centre d'appels. Le centre d'appels fournit aux utilisateurs des rapports en temps réels ainsi que des historiques.

Rapports en temps réel

Les rapports en temps réel sont constamment actualisés. Ils fournissent des informations importantes, par ex. des indications sur la charge des agents, sur le niveau de service, sur les pourcentages d'interruption et sur la durée moyenne de traitement. Il est possible d'étudier pas à pas le déroulement du contact avec le client à partir des listes d'appelants constamment actualisées et qui peuvent être soumises à un tri. De plus, le contrôle des activités de tous les agents est possible. Ces informations peuvent par exemple servir lors de formations, de tâches de contrôle des contacts et d'opérations de suivi.

Les agents de niveau de discrimination Superviseur ou Administrateur peuvent être avertis acoustiquement ou visuellement en cas de dépassement de certaines grandeurs de mesure de fonctionnement définies. La détermination des valeurs seuil correspondantes est possible pour chaque file d'attente, individuellement.

Rapports historiques

Grâce à la sélection d'éléments de données et de paramètres de rapport spécifiques de l'utilisateur, il est possible de créer rapidement des historiques et de les présenter sous forme de graphiques ou de tableaux.

L'application myAgent permet d'utiliser plus de 20 modèles de rapport prédéfinis pour les rapports par défaut.

L'application myReports en option élargit les possibilités d'établir des historiques sur la bas de 100 modèles de rapport prédéfinis. l'établissement du rapport peut être programmé individuellement et les rapports établis peuvent être envoyés à des heures définies, dans des formats d'exportation courants, à des destinateurs d'e-mails définis ou bien être enregistrés à un emplacement de stockage configuré par l'administrateur myReports.

Conseil : Les rapports se basent sur l'historique des appels, enregistré dans le système de communication. La durée de conservation maximale de l'historique des appels est de 365 jours (paramètre par défaut). Un administrateur de profil **Expert** peut paramétrer pour l'ensemble du système la durée de conservation de l'historique des appels.

Exemple : la durée de conservation a été réglée sur 100 jours. Pour l'établissement des rapports, on peut donc se reporter à des données qui remontent au maximum à 100 jours.

Protection des données

Si l'administrateur myReports a activé la protection des données lors de la configuration de myReports, dans tous les rapports correspondants, les quatre dernière position des numéros d'appel (colonne CLI) sont remplacés par ****.

Si un abonné interne a identifié son numéro d'appel privé, numéro mobile, numéro externe 1 et/ou numéro externe 2 comme non visible, tous ces numéros d'appel ne sont pas affichés dans les rapports concernés.

17.9.1 Modèles de rapport prédéfinis

myReports fournit env. 100 modèles de rapport qui permettent d'établir des rapports.

Ces modèles correspondent aux domaines (groupes de rapports) suivants.

- **Activité Agent**
- **Agents**
- **CLI**
- **Historique des appels**
- **Appels**
- **Fax / E-mail**
- **Autres**
- **Performance**
- **Files d'attente**
- **Etat de présence de l'utilisateur**
- **Codes de post-traitement**

18 Mobilité

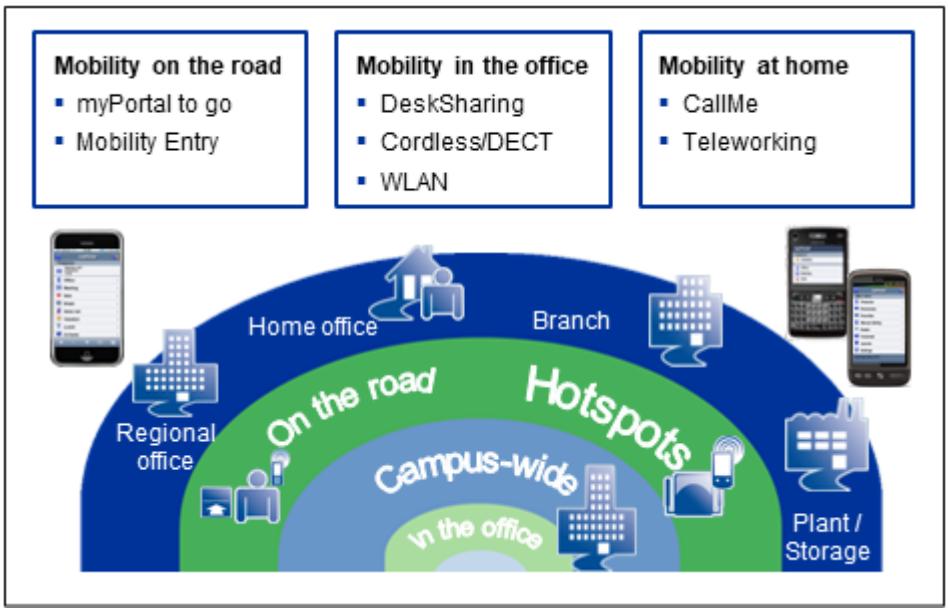
OpenScape offre des solutions de mobilité intégrées à toutes les entreprises. Cela comprend par ex. l'intégration de téléphones mobiles/SmartPhones, l'utilisation de téléphones sans fil/DECT et WLAN ou encore le DeskSharing et le télétravail. Mobility englobe la mobilité en déplacement, la mobilité au bureau et la mobilité à domicile.

Concepts associés

Abonnés à la page 378

18.1 Solutions mobilité intégrées

Les solutions mobilité intégrées dans le système de communication offrent des communications efficaces partout, sur les terminaux les plus divers.



18.2 Sur la route

La mobilité sur la route est obtenue grâce à l'intégration des téléphones mobiles via Mobility Entry. Le service One Number permet de joindre un abonné via un seul numéro de téléphone dans le monde entier. En outre, avec la téléphonie bimode, des économies supplémentaires peuvent être réalisées si l'abonné est à portée d'un WLAN.

La mobilité sur la route est la combinaison de :

- Téléphone de bureau et téléphone mobile (Mobility Entry)
  - Disponibilité sous un numéro (One Number Service)
  - Contrôle des fonctionnalités via les codes DTMF

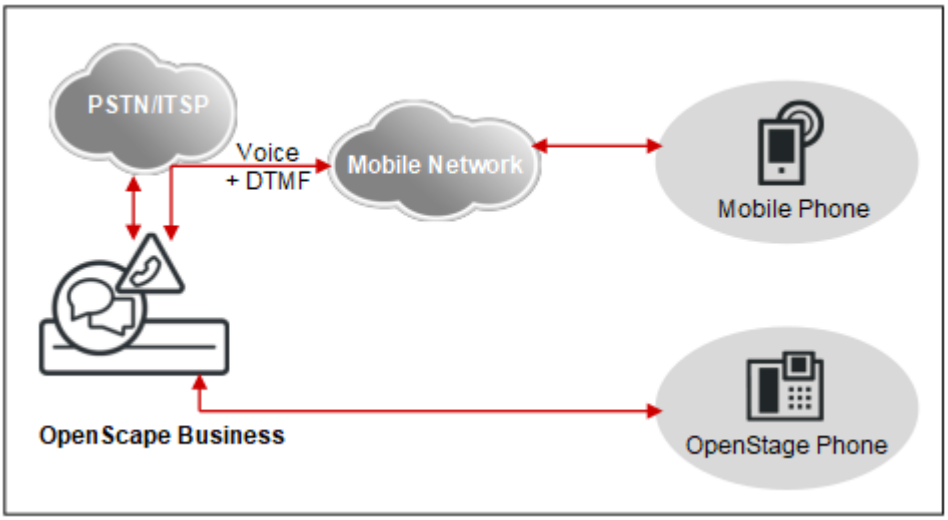
En plus de la combinaison du téléphone mobile et du téléphone de bureau, il est également possible de configurer un téléphone mobile seul (c'est-à-dire sans téléphone de bureau parallèle) à joindre sous un numéro de ligne fixe.

La fonctionnalité complète est obtenue avec les téléphones système (HFA). Les téléphones SIP peuvent être utilisés avec des restrictions.

18.2.1 Mobility Entry

Mobility Entry permet l'intégration des téléphones mobiles. Ainsi, l'abonné a accès à certaines fonctionnalités système via le téléphone mobile.

Mobility Entry permet la gestion des liaisons Voix via DTMF.



Mode de numérotation de Mobility Entry

Pour les communications sortantes, l'abonné de téléphonie mobile a le choix en plusieurs modes de numérotation.

Mobility Entry offre les modes de numérotation suivants :

- Callback
- Call through (transit via le système)

Si, lors d'un rappel, l'abonné de téléphonie mobile compose un numéro SDA spécial, l'appel est automatiquement coupé, avant l'établissement de la connexion ; un rappel (callback) est automatiquement effectué. Après le rappel, une nouvelle autorisation est nécessaire. L'abonné de téléphonie mobile peut effectuer des appels internes et externes via le système de communication et utiliser toutes les fonctionnalités Mobility.

Conditions nécessaires pour Callback :

- Le numéro externe du téléphone appelant est enregistré et configuré dans le système de communication. Si ce n'est pas le cas, l'appel est coupé et il n'y a pas de rappel.
- Le numéro SDA est configuré.
- Le numéro externe de l'abonné du téléphone mobile est transmis au système de communication (information CLIP).

Fonctions à l'état inactif

- Composer le numéro
- Programmer ou effacer le renvoi d'appel

- Comment activer ou désactiver NE PAS DERANGER
- Envoyer un message
- Réinitialiser tous les services
- Comment activer ou désactiver le refus de présentation de la ligne appelante (CLIR)

Fonctionnalités en cours de communication

- Double appel
- Va-et-vient
- Conférence
- Déconnexion et retour à l'abonné en attente
- Activer le rappel
- Permettre Suffixe MF

Pour la signalisation des fonctionnalités, il est utilisé des indicatifs système (par ex. *1 pour la programmation du renvoi d'appel).

Remarque : Pour les abonnés Mobility Entry, le flag abonné **Discrimination DISA** doit être activé.

Avec OpenScape Business X, on dispose au maximum de 16 Code Receiver DTMF, c.-à-d. que 16 abonnés au maximum (analogiques, Mobility, etc.) peuvent réserver simultanément un Code-Receiver DTMF. Les abonnés où le flag **Activation de la fonctionnalité basée DTMF** est placé se réservent respectivement un Code-Receiver pour la durée de la communication.

Dans OpenScape Business S, la gestion des fonctions s'effectue par codes DTMF lorsque les chiffres DTMF sont transmis selon RFC 2833. S'il est utilisé dans le réseau un Session Border Controller (SBC) externe, aucune identification DTMF n'est possible.

Remarque : L'entrée de mobilité doit uniquement être configurée sur les nœuds avec accès direct au réseau.

Concepts associés

One Number Service à la page 893
Postes de fonctionnalités d'entrée de mobilité à la page 890
Dépendances pour l'entrée en mobilité à la page 892

18.2.2 Postes de fonctionnalités d'entrée de mobilité

Le tableau suivant présente l'ensemble des fonctionnalités de Mobility Entry.

Fonctionnalité	Entrée Mobilité
Fonctions générales	
Contrat de téléphonie mobile avec option de données	non

Fonctionnalité	Entrée Mobilité
Signalisation d'appel parallèle sur téléphone système et téléphone mobile (jumelage)	oui
Transfert du numéro de l'appelant vers le téléphone mobile (si le réseau transmet des numéros de téléphone externes sous forme de CLIP ; CLIP sans filtrage)	oui
One Number Service (si le réseau transmet des numéros externes sous forme de CLIP, CLIP no Screening))	oui
Ne pas déranger /Désactiver le renvoi d'appel	oui
Suppression du numéro de terminal, activable/désactivable	oui
Identification automatique des terminaux enregistrés	oui
Fonctionnement sans le téléphone de bureau (comme un terminal virtuel)	oui
Peut être utilisé avec OpenScape Business S	oui
Statut de présence, Journal, boîte vocale	
Modifier l’état de présence	non
Consulter l’état de présence d’autres abonnés	non
Journal	non
Boîte vocale partagée ; peut également être vérifiée en déplacement	oui
Afficher la messagerie vocale reçue	non
Composer	
Accès aux contacts dans le téléphone mobile	oui
Accès aux contacts dans le système de communication	non
Favoris	non
Numérotation manuelle	oui
Répétition de la numérotation	non
Méthode de numérotation	Transf. app.
Terminer l'appel	
Consultation	oui
Va-et-vient	oui
Poste opérateur	oui
Conférences	oui
Rappel sur gratuit et occupé	oui

Fonctionnalité	Entrée Mobilité
Interception d'appel du téléphone mobile vers le téléphone système	oui
Indicateur d'occupation également pour les appels au téléphone mobile (avec service à un numéro)	oui

Concepts associés

Mobility Entry à la page 889

18.2.3 Dépendances pour l'entrée en mobilité

Mobility Entry dépend des fonctionnalités suivantes.

Dépendance	Entrée mobilité
Rappel de mobilité DID	Pour le mode de numérotation de rappel mobile, le numéro DID de rappel mobile doit être configuré.
numéro de téléphone de destination externe	La composition des numéros de téléphone de destination externes par l'abonné mobile est contrôlée par le système en raison de la configuration LCR. La numérotation peut donc être effectuée via le réseau fixe RNIS, le réseau fixe analogique ou via un fournisseur de services de téléphonie sur IP (ITSP).
Activer CLIP Sans dépistage	Vous ne pouvez pas afficher le numéro de l'appelant sur le terminal mobile à moins qu'il n'ait été fourni sans vérification par l'opérateur de réseau.
Clip d'abonné mobile	Le code CLIP de l'abonné mobile doit être transmis au système de communication. Ce service doit être mis à disposition par le fournisseur de réseau.
Administration LCR	Étant donné que certains fournisseurs de réseau (réseau fixe ou ITSP) n'acceptent pas les numéros de destination comportant un préfixe international distinct, le système doit supprimer ce préfixe de ces numéros de destination. Cela peut être réalisé dans le cadre du routage à moindre coût (LCR).
Canaux B / Connexions externes	Le nombre de canaux B dépend de la durée de la connexion ou du nombre de stations mobiles. Chaque appel externe entrant vers un abonné mobile nécessite deux canaux vocaux dans le système. Si le nombre de canaux vocaux disponibles est insuffisant, il se peut qu'il soit impossible de joindre un abonné mobile, et ce dernier pourrait ne pas être en mesure d'initier des appels avec le service de numéro unique.
Numéros d'urgence	Lorsqu'un utilisateur de téléphone mobile compose un numéro d'urgence via le système de communication, la localisation de son téléphone mobile ne peut pas être identifiée. Il est donc conseillé de composer directement un numéro d'urgence.
Composer les numéros de poste internes	Lors de la composition de numéros de téléphone internes au format international (par exemple, 0004989100) depuis le poste mobile, le numéro de localisation du système de communication doit être configuré. Sinon, les destinations internes sont acheminées via la plateforme d'échange, ce qui peut engendrer des coûts.
Maintenance de l'annuaire	-
Pare-feu	-
Connexion de données	-

Dépendance	Entrée mobilité
Connexions parallèles	-
Établissement de la connexion entre le système de communication et les stations mobiles via	Tous les types de lignes prenant en charge la transmission DTMF.

Concepts associés

Mobility Entry à la page 889

18.2.4 One Number Service

Grâce au One Number Service (ONS), le téléphone mobile devient un poste du réseau fixe. L'abonné est joignable dans le monde entier sous un numéro et il s'identifie désormais uniquement par son numéro fixe.

La configuration Team permet le One Number Service avec un numéro commun pour le bureau (téléphone système) et le téléphone mobile. L'appelant compose le numéro d'appel du téléphone système (réseau fixe). Les appels sortant du téléphone mobile sont signalés chez l'appelé sous le numéro du réseau fixe. Un autre avantage du One Number Service est l'affichage Occupé pour l'abonné mobile.

Concepts associés

Mobility Entry à la page 889

18.2.5 (Voir Téléphonie dual mode).

Les téléphones mobiles dual mode supportent les réseaux GSM/UMTS et les réseaux WLAN. L'enregistrement au système de communication est possible via un WLAN en tant que terminal SIP.

Si le téléphone mobile bimode se trouve dans la plage WLAN, il est automatiquement appelé terminal SIP. S'il est en dehors de la portée WLAN, le téléphone mobile bimode est appelé via GSM/UMTS (c'est-à-dire que la fonctionnalité de téléphone mobile intégré est disponible).

Le renvoi automatique vers le numéro de téléphone GSM ne fonctionne que si le terminal SIP associé est entré dans le système en tant que terminal de téléphone mobile (intégration du téléphone mobile). Cela signifie que si le terminal SIP est enregistré, il est appelé terminal SIP, et s'il n'est pas enregistré, il est appelé via le numéro de téléphone GSM attribué dans la configuration d'intégration du téléphone mobile. Le contrôle des appels se produit généralement au sein du client SIP à la place

Les appels dans les locaux de l'entreprise se font via le WLAN. Tant que les appels sont effectués via le WLAN, aucuns frais d'appel ne sont encourus sur le téléphone mobile. Le transfert et l'itinérance sont pris en charge dans la plage WLAN (si l'infrastructure LAN sans fil est conçue pour cela), mais pas du WLAN au GSM, et vice versa.

18.2.6 Configuration de l'entrée de mobilité

Mobility Entry est configuré avec l'assistant d'**intégration de téléphone mobile**.

L'assistant **d'intégration de téléphone mobile** permet à l'administrateur de :

- Configurer le service de numéro unique
- Mise en place d'un système d'accès pour les personnes à mobilité réduite
- Configurer les téléphones à double mode

L'intégration des téléphones GSM aux réseaux mobiles s'effectue via des stations virtuelles. Les fonctionnalités sont ainsi transférées à la station mobile. Chaque station disposant d'une licence correspondante (utilisateur mobile) peut se voir attribuer un maximum d'une station mobile.

Modes de fonctionnement des téléphones mobiles

Les modes de fonctionnement suivants sont implémentés pour les téléphones mobiles :

- **Mode GSM**

  Les appels vers le numéro d'appel mobile interne sont signalés par le téléphone mobile GSM.
- **Mode Wi-Fi**

  Si le téléphone mobile Wi-Fi est joignable via le réseau Wi-Fi, l'appel est effectué via le réseau Wi-Fi. Si le réseau Wi-Fi n'est pas disponible, l'appel est effectué via GSM.

Jumelage

Les appels sont signalés en parallèle sur le téléphone mobile et le téléphone fixe (double signal). Pour mettre en œuvre le jumelage, une configuration d'équipe doit être mise en place une fois la configuration de l' **intégration des téléphones mobiles** terminée. Pour ce faire, utilisez l'assistant **de configuration d'équipe** et sélectionnez d'abord le numéro de téléphone sous lequel la signalisation parallèle doit avoir lieu (par exemple, le téléphone système). Sur le téléphone du système, une touche Direct Station Select (DSS) vers les stations Mobility peut être programmée pour le transfert sans interruption des appels de téléphone mobile. La fonctionnalité complète est obtenue avec les téléphones système (HFA). Les téléphones SIP peuvent être utilisés, mais sont soumis à certaines restrictions, par exemple ils ne prennent pas en charge les touches MULAP.

Concepts associés

Configuration des équipes (Team) / groupes Team et fonctions Chef/ Secrétaire / groupes Top à l'aide des assistants à la page 662

Conditions nécessaires pour Application Launcher à la page 1127

18.2.6.1 Comment intégrer les téléphones mobiles GSM

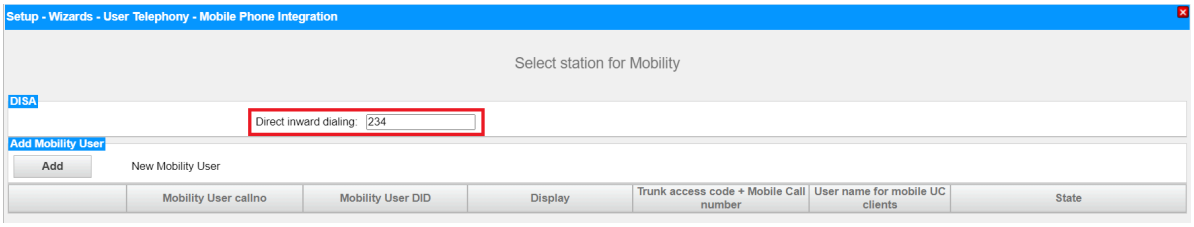
À l'aide de l'assistant **Intégration de téléphones mobiles**, vous intégrez les téléphones mobiles dans le système de communication.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Intégration de téléphones mobiles**. La fenêtre **Sélectionner un poste pour Mobility** s'affiche.
4) Dans **DISA**, sélectionnez le numéro **SDA** (ou entrez-le) qui permet aux abonnés mobiles d'accéder au système de communication.



Remarque : DISA est requis pour Mobility Entry (pour contrôler le système à l'aide de DTMF) et pour myPortal for Mobile (uniquement lors de l'utilisation de Call Through).

5) Cliquez sur **Ajouter** ou **Modifier** pour l'abonné dont vous souhaitez intégrer le téléphone mobile GSM dans le système de communication. La fenêtre **Affecter des utilisateurs Mobility** s'affiche.
6) Sélectionnez **Mode GSM** comme mode d'exploitation du téléphone portable.
7) Dans **Indicatif de prise réseau+Numéro de mobile**, indiquez le numéro de téléphone du téléphone mobile (par ex. 0016012345678).
8) Entrez le **numéro interne de l'abonné Mobility** (par ex. 777), un **nom interne quelconque** et le **numéro SDA**. Notez que le numéro d'appel interne ne doit pas avoir déjà été attribué.

: Si vous souhaitez utiliser le SDA DID 879, 890 ou 891, vous devez faire les réglages par l'intermédiaire de ManagerE et non pas via WBM.

9) Uniquement avec UC Smart : Affectez une Boîte Vocale au Terminal si nécessaire :
   a) Sélectionnez dans la liste déroulante **Type de boîte de messagerie UC Smart** si l'abonné doit recevoir une boîte de messagerie standard ou une boîte de messagerie de diffusion (AutoAttendant).
   b) Uniquement avec une boîte vocale standard : si un appelant peut laisser un message dans la boîte vocale, cochez la case **Enregistrement**.
   c) Dans la liste déroulante **Message d'accueil**, sélectionnez un message d'accueil.
   d) Si le mot de passe de la boîte vocale doit être rétabli, cochez la case **Réinitialisation mot de passe**.

> **Remarque :** La case à cocher **Réinitialisation du mot de passe** ne doit pas être cochée lors de la création d'une nouvelle boîte vocale. Elle permet de réinitialiser le mot de passe de la boîte vocale. Lors de la création d'une nouvelle boîte vocale, l'abonné doit de toute façon modifier le mot de passe initial lors de son premier accès à cette boîte vocale.

10) Cliquez sur **OK & Suivant**.
11) Cliquez sur **OK et suivant**, puis sur **Terminer**.

18.2.6.2 Comment intégrer des téléphones bimodes (GSM/WLAN) avec un client HFA ou SIP

L'assistant d'**intégration de téléphone mobile** peut être utilisé pour configurer un téléphone mobile en tant que téléphone bimode avec client système (client HFA) ou client SIP (mode WLAN).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

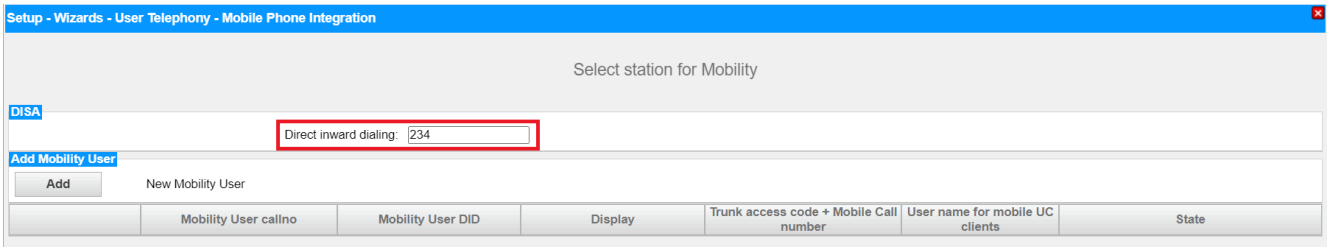
Le dispositif HFA ou le terminal SIP doit être configuré via le Web based Management (Web admin).

La licence d'utilisateur Mobilité a été attribuée à l'abonné.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Intégration de téléphones mobiles**. La fenêtre **Sélectionner un poste pour Mobility** s'affiche.

4) Dans **DISA**, sélectionnez le numéro **SDA** (ou entrez-le) qui permet aux abonnés mobiles d'accéder au système de communication.



Remarque : DISA est requis pour Mobility Entry (pour contrôler le système à l'aide de DTMF) et pour myPortal for Mobile (uniquement lors de l'utilisation de Call Through).

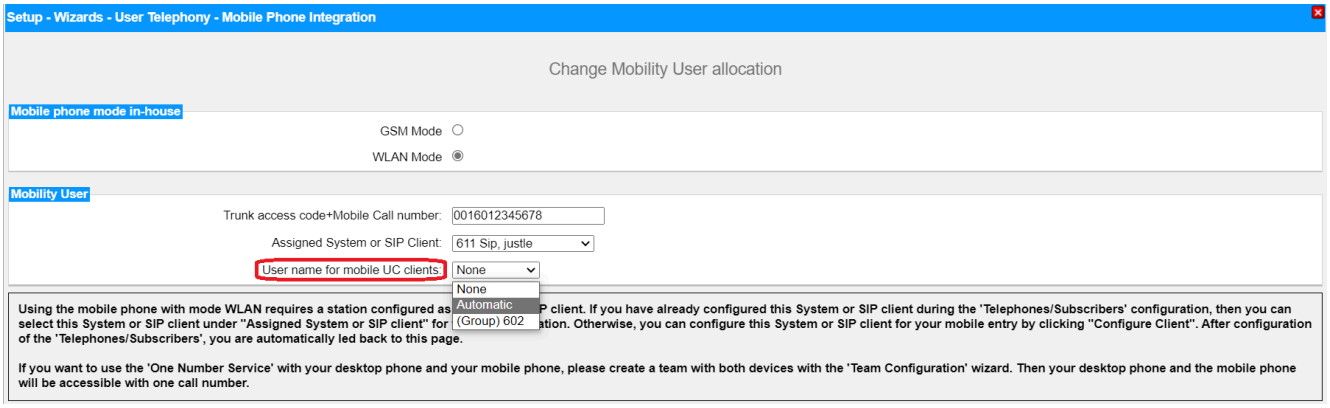
5) Cliquez sur **Ajouter** ou **Modifier** pour l'abonné dont vous souhaitez intégrer le téléphone mobile GSM dans le système de communication. La fenêtre **Affecter des utilisateurs Mobility** s'affiche.

6) Sélectionnez **Mode WLAN** comme mode d'exploitation du téléphone portable.

7) Dans **Indicatif de prise réseau+Numéro de mobile**, indiquez le numéro de téléphone du téléphone mobile (par ex. 0016012345678).

8) Sélectionnez **Système attribué ou Client SIP** dans la liste déroulante.

   Si le système attribué (poste HFA) ou le poste SIP n'est pas encore configuré, cliquez sur **Configurer le poste** et configurez un système ou un poste SIP. Après la configuration du système ou du terminal SIP, vous serez automatiquement renvoyé à cette page.



9) Cliquez sur **OK & Suivant**.

10) Cliquez sur **OK et suivant**, puis sur **Terminer**.

18.2.6.3 Comment activer l'interface Web pour les téléphones mobiles et les clients Web

Conditions préalables

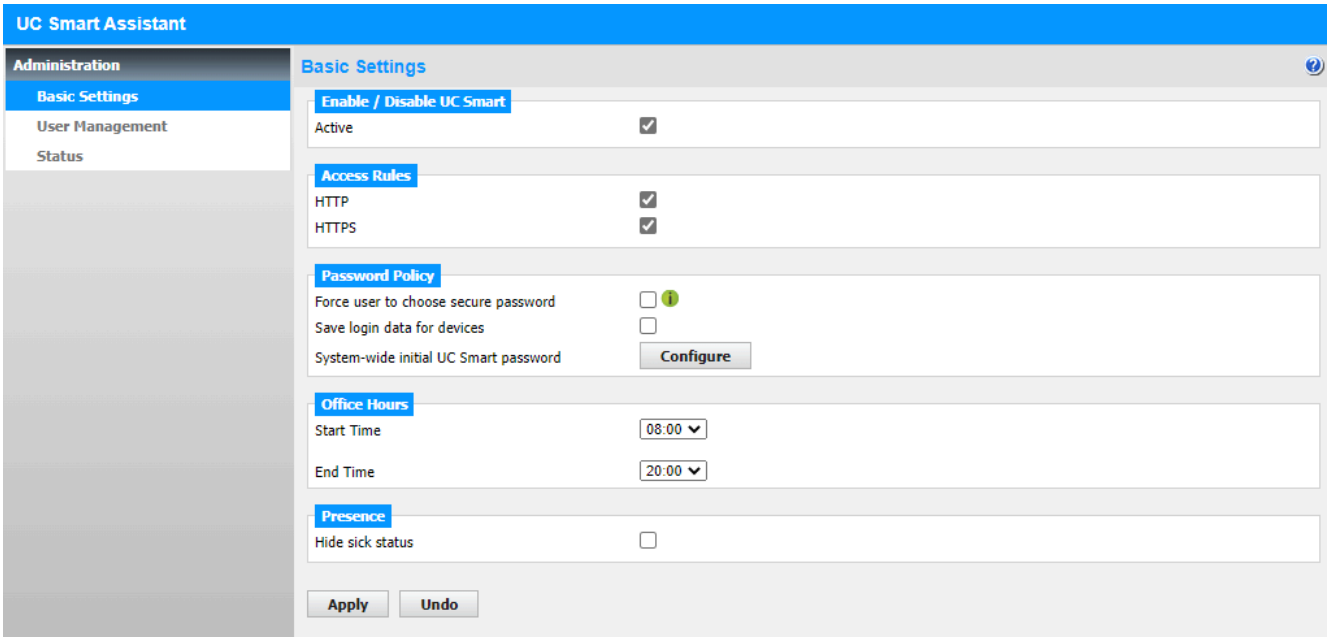
Vous êtes connecté au WBM avec le profil **Expert** .

Les services Web doivent être activés comme condition préalable pour les fonctionnalités suivantes :

- Intégration des téléphones mobiles
- Lanceur d'applications

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert** .
2) Si vous utilisez UC Smart, cliquez dans l'arborescence de navigation sur **Applications** > **UC Smart** > **Paramètres Basic**.
3) Assurez-vous que UC Smart est **actif**.
4) Si vous souhaitez activer les services Web pour téléphones mobiles, sélectionnez au moins une des options suivantes :
   - Si vous souhaitez activer les connexions cryptées, cochez la case **HTTPS**.
   - Si vous souhaitez activer les connexions non chiffrées, cochez la case **HTTP**.



5) Cliquez sur **Appliquer** puis sur **OK** .

18.2.6.4 Comment effacer l'intégration de téléphone mobile

L'Assistant **Intégration de téléphones mobiles** permet d'effacer l'intégration du téléphone mobile.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie utilisateurs**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Intégration de téléphones mobiles**. La fenêtre **Sélectionner un poste pour Mobility** s'affiche.
4) Cliquez sur **Modifier** de l'abonné que vous voulez effacer. La fenêtre **Affecter des utilisateurs Mobility** s'affiche.
5) Dans la fenêtre en bas cliquez sur **Effacer les données**.
6) Cliquez sur **OK&Suivant**.
7) Cliquez sur **OK&Suivant** puis sur **Terminer**.

18.3 Mobilité au bureau

La mobilité au bureau est réalisée grâce au DeskSharing, aux téléphones sans fil et aux téléphones WLAN. Avec le DeskSharing sont proposées, en liaison avec la mobilité IP (ouverture de session mobile et appel flexible), des fonctionnalités pour abonnés mobiles qui permettent d'utiliser le téléphone d'un poste de travail tiers comme son propre téléphone.

18.3.1 Desk Sharing

Avec le Desk Sharing, plusieurs abonnés peuvent partager un téléphone système et donc un téléphone IP (HFA).

Avec le Desk Sharing, les abonnés n'ont pas de lieu de travail fixe ni de téléphone de bureau fixe. Le Desk Sharing permet à plusieurs abonnés mobiles du système de communication de partager un poste de travail et/ou un téléphone. L'abonné se connecte simplement au téléphone du lieu de travail où il se trouve.

Après la connexion, le numéro de poste de l'abonné connecté est transféré sur le téléphone système utilisé. Le téléphone système utilisé n'est plus joignable sous son numéro de poste d'origine. Si l'abonné se connecte sur un autre téléphone système, son numéro de poste est transféré sur ce nouveau téléphone système. Lorsque l'utilisateur se déconnecte (Déconnexion), le téléphone système se reconnecte automatiquement avec son propre numéro non mobile.

L'une des étapes suivantes doit être effectuée sur le téléphone système pour activer la fonction :

- Saisir le code pour la "connexion mobile" + le numéro de la station mobile + le mot de passe/PIN facultatif

Lors de l'utilisation de téléphones ayant un nombre différent de touches de fonction, le transfert des configurations de touches peut être soumis à des restrictions.

Si le Desk Sharing doit être mis en œuvre pour les téléphones IP (HFA) dans des nœuds en réseau, un DLS (Service de déploiement) externe doit être installé. L'expertise requise à cet effet est supposée.

Les fonctions suivantes peuvent être utilisées pour le Desk Sharing :

- Appel par haut-parleur (radiomessagerie)

- Conférence
- Entrée en tiers
- Basculer/Connecter
- Parking
- Consultation
- Transférer
- Prise d'appel
- Ne pas déranger
- Renvoi d’appel
- Envoi d'un message (message en attente)
- Rappel auto
- Suppression du numéro de poste
- Groupe de sonnerie activé

Remarque : Pour chaque numéro de téléphone mobile, une licence Deskshare supplémentaire est nécessaire. Cette licence Deskshare doit être activée pour l'abonné et ce dernier doit être configuré comme **mobile**. En outre, la fonction de relocalisation doit être activée.

Un téléphone système utilisé pour le Desk Sharing ne nécessite pas nécessairement de licence. Cependant, si aucune licence n'est activée et qu'aucun abonné Desk Sharing n'est connecté, même les appels d'urgence ne seront pas possibles à partir de ce téléphone. Le téléphone système/l'abonné doit être configuré comme **Non-mobile**.

Si un téléphone système ne doit pas être utilisé pour le Desk Sharing, il doit être configuré comme **Non mobile et bloqué**.

Remarque : La fonction Desk Sharing ne doit pas être utilisée avec les deux premiers postes système actifs.

18.3.2 Solution sans fil intégrée

OpenScape Business Cordless est la solution sans fil intégrée permettant de faire fonctionner des téléphones sans fil (téléphones DECT) via le système de communication. Les fonctionnalités HFA d'OpenScape Business peuvent alors être utilisées avec les téléphones DECT connectés.

Dans la solution sans fil intégrée, les téléphones DECT sont des stations internes spécifiques au système, contrairement aux systèmes DECT séparés, qui sont connectés via des interfaces standard.

La connexion des stations de base OpenScape Business pour le fonctionnement des téléphones DECT peut être mise en œuvre via :

- Pour Unify OpenScape Business X1/X5 : connexions directes aux interfaces $U_{P0/E}$ de la carte mère du système de communication (DECT Light)
- Pour Unify OpenScape Business X5 : connexion aux interfaces $U_{P0/E}$ d'une carte SLU8N/SLU8NR (DECT Light)
- Pour Unify OpenScape Business X8 : connexion aux interfaces $U_{P0/E}$ d'un SLMUC (SLMU + CMAe)

La technologie radio sans fil correspond à la norme DECT (Digital Enhanced Cordless Telecommunications). L'ensemble de la zone radio administrée par le système est constitué de stations de base qui forment ensemble soit un réseau complet de cellules radio qui se chevauchent, soit des « îlots » radio individuels. La taille d'une cellule radio dépend des facteurs locaux/structurels.

Mode ECO

En mode ECO (mode économique), la puissance d'émission des téléphones DECT est soit réduite d'une valeur fixe (statique), soit chaque téléphone DECT ajuste sa puissance d'émission indépendamment de la force du signal reçu (adaptatif). Le mode ECO peut être activé au niveau du système de communication à l'échelle du système pour tous les équipements Dect (**Mode Expert** > **Téléphonie** > **Sans fil** > **À l'échelle du système**). Aucune configuration n'est requise sur les téléphones DECT. Un redémarrage manuel du système est nécessaire pour activer la fonctionnalité dans le cas d'OpenScape Business X1, X5.

- Réglage statique de la puissance d'émission

  Les téléphones DECT et la station de base réduisent la puissance d'émission à une valeur fixe définie.
- Ajustement adaptatif de la puissance d'émission

  Les téléphones DECT émettent à puissance normale ou réduite, en fonction de la force du champ de réception. Lors d'un transfert, le système passe d'abord à une puissance d'émission élevée, puis réduit cette puissance en fonction de la réception.

Téléphones DECT

La solution sans fil intégrée prend en charge les téléphones mobiles compatibles GAP de fabricants tiers. L'ensemble des services HFA ne peut cependant être utilisé qu'avec les téléphones DECT homologués.

Configuration

Pour une description de la configuration, voir Configuration de la solution sans fil intégrée.

Tableaux et stations de base

Les descriptions des cartes et des terminaux de base peuvent être trouvées dans la *documentation de service Unify OpenScape Business dans les chapitres Cartes et Terminal de base*.

18.3.2.1 Présentation du système

La connexion des stations de base Unify OpenScape Business pour Unify OpenScape Business X5 se fait soit directement aux interfaces $U_{P0/E}$ de la carte mère, soit aux interfaces UP0/E d'une carte SLU8N/SLU8NR installée (DECT Light). Avec OpenScape Business X8, les stations de base peuvent être connectées aux cartes sans fil SLMUC.

Connexions directes (DECT Light)

Les stations de base peuvent être connectées directement aux interfaces $U_{P0/E}$ de l'OCCM, OCCMB, OCCMA et OCCMR, OCCMBR, OCCMAR du système de

communication Unify OpenScape Business X5R ou aux interfaces UP0/E d'une carte SLU8N/SLU8NR8.

En utilisant la sous-carte CMAe sur les cartes mères, les fonctions de conversion ADPCM et d'annulation d'écho (48 canaux pour CMAe) sont mises à disposition. Jusqu'à quatre appels peuvent être effectués par station de base. Jusqu'à sept stations de base peuvent être connectées aux interfaces $U_{P0/E}$ des cartes mères OCCM, OCCMB, OCCMA et OCCMR, OCCMBR, OCCMAR.

Si aucun CMAe n'est installé, un maximum de deux appels peuvent être effectués par station de base. Dans ce cas, la conversion ADPCM est effectuée directement par la station de base DECT.

Remarque : Si CMAe n'est pas installé, aucune fonction de gestion d'écho n'est disponible.

Lors de la connexion de stations de base à une carte SLU8N/SLU8NR, les exigences de connectivité suivantes s'appliquent :

- Au total, un maximum de 15 stations de base (7 sur la carte mère et 8 autres sur une carte SLU8N/SLU8NR) peuvent être exploitées. Le nombre maximal de téléphones DECT connectables est de 64 avec un CMAe.
- Une seule carte SLU8N/SLU8NR peut être utilisée pour la connexion des stations de base.
- Seul le premier port du terminal de base peut être utilisé pour connecter le terminal de base à une interface $U_{P0/E}$ de la carte SLU8N/SLU8NR.
  Les ports 2 et 3 du terminal de base ne sont pas pris en charge pour la connexion à une autre interface $U_{P0/E}$.
- Les interfaces $U_{P0/E}$ de la carte SLU8N/SLU8NR peuvent être utilisées avec une combinaison mixte de terminaux de base et/ou de téléphones.

Connexion de planches sans fil

Le terminal de base BS5 peut être connecté aux interfaces $U_{P0/E}$ des cartes sans fil suivantes :

- SLMUC (SLMU + CMAe) avec Unify OpenScape Business X8 (voir le *chapitre SLMUC de la documentation de service*)

  La connexion des terminaux de base peut se faire via une, deux ou trois interfaces $U_{P0/E}$. Les 8 dernières interfaces d'un SLMUC ne peuvent être utilisées que comme 2e ou 3e interface UP0 de la station de base. La connexion supplémentaire des interfaces $U_{P0/E}$ augmente la capacité de trafic du terminal de base et donc le nombre de canaux Voix simultanément disponibles.

18.3.2.2 Capacité du système

Selon le système de communication, jusqu'à 64 stations de base peuvent être connectées et jusqu'à 250 équipements Dect peuvent être utilisés.

Le tableau suivant montre la configuration maximale possible de la solution sans fil intégrée.

Remarque : Les abonnés de base BS4 (S30807-U5491-X), BS3/1 (S30807-H5482-X), BS3/3 (S30807-H5485-X) et BS3/S (X30807-X5482-X100) sont progressivement retirées du marché et ne peuvent plus être commandées. Cependant, ils peuvent encore être connectés à OpenScape Business X1R. En cas de défaut, on utilisera les stations de base actuelles.

Remarque : Si aucun CMAe n'est installé, un maximum de deux appels peut être effectué par station de base. Dans ce cas, la conversion ADPCM est effectuée directement par la station de base DECT, mais l'annulation d'écho n'est pas directement prise en charge. Si l'annulation d'écho est nécessaire, une carte secondaire CMAe est requise.

OpenScape Business	Nombre maximum d'utilisateurs		Module d'horloge	Nombre max. de terminaux de base BS en cas de connexion via 1xU_{P0}	Ports/ Communications simultanées par BS	Nombre maximal de dispositifs enregistrés	Nombre maxi. de communications simultanées
	SLUN	SLMUC					
X1	-	-	-	7	1/2	16	14
	-	-	CMAe	7	1 - 4	16	16
X5 $U_{p0/E}$ embarqué (SLUC)	-	-	-	7	1/2	32	14
	-	-	CMAe	7	1 - 4	64	28
	1	-	CMAe	15	1 - 4	64	48
X8	-	4	CMAe	64	3/12	250 (128 par SLMUC)	192[7]

Remarque : La désignation SLUC dans le tableau fait référence aux interfaces UP0/ E de la carte mère. SLUN désigne généralement les cartes SLU8N ou SLU8NR.

18.3.2.3 Téléphones cordless/DECT

L'insertion du module SLC et l'entrée de l'identifiant système DECT permet de configurer 16 combinés. Les codes de combiné (PIN) sont attribués et les combinés peuvent être inscrits. Pour utiliser d'autres combinés, vous devez d'abord les valider.

Si un combiné est remplacé en service, il faut modifier le code PIN avant d'inscrire l'appareil de remplacement. En cas de remplacement, il faut par principe attribuer un nouveau PIN aux abonnés concernés dans le système de communication. Cela déconnecte automatiquement le combiné. En outre, il n'est plus possible de déclarer en fraude un combiné à l'aide de l'ancien PIN.

7 La valeur maximale par SLMUC est de 48. Selon l'emplacement des téléphones sans fil en cas d'itinérance, tous les appareils enregistrés (250) pourraient être actifs si 4 SLMUC sont disponibles.

18.3.2.4 Signification des résultats obtenus en testant le système radio

Important :

Les valeurs enregistrées avec un téléphone portable ne sont pas très précises et ne sont destinées qu'à des évaluations sommaires. De plus, des téléphones portables différents peuvent enregistrer des valeurs différentes dans des conditions ambiantes identiques. Si vous avez besoin de résultats plus précis, nous vous recommandons d'utiliser l'outil de service HicomnbspCordlessnbsp (HCS-DECT).

La figure suivante donne un exemple d'affichage des résultats de mesure pour un téléphone portable Gigaset avec un appel en cours :

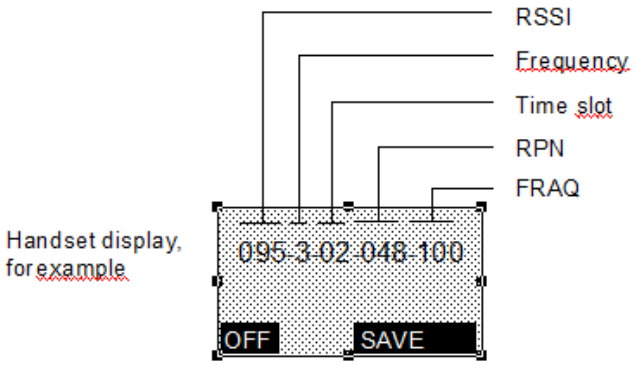


Illustration 7 : Résultat de mesure

Section	Description
RSSI (signa radio)	Force des signaux radio reçus de la station de base, normalisée à un maximum de 100. Si la valeur est <nbsp50, la connexion radio à la station de base n'est plus garantie. Une force acceptable est >nbsp50 (> -60 dBm).
Fréquence	Fréquence (0 – 9)
Intervalle de temps (emplacement)	Intervalle de temps (0 – 11) du canal de réception sur lequel la mesure est exécutée.

Section	Description
RPN (numéro de port)	**OpenScape Business X1/X3/X5/ X8** ID de station de base, par exemple, 048, numéro de port sur les modules SLC. Si le combiné passe sur une station de base/ cellule radio qui se chevauche, le numéro de port actuel (où le canal D de la station de base est configuré) s'affiche sur le combiné. Formule : A x 16 + B A = numéro de la carte SLC (1 - 127) ; 16 = facteur B = port de la carte SLC associée (où le canal D du terminal de base est configuré) Exemples : RPN = 1 x 16 + port 0 = 016 RPN = 2 x 16 + port 8 = 040. Le numéro de port (PRN) est affiché au format hexadécimal avec un H joint pour les combinés Gigaset S3 professionnel et Gigaset SL3 professionnel. La valeur hexadécimale est affichée sans le H joint, par ex.nbsp « -028- » dans le cas des combinés Gigaset S4 professionnel et OpenStage SL4 professionnel. Si la valeur 040 était affichée précédemment, la valeur 028H est maintenant affichée pour le combiné Gigaset S3/SL3 professionnel. La désignation hexadécimale est différenciée de façon unique avec le suffixe « H ». C'est également valable pour les équipements OpenScape DECT Phone S5/SL5 (le préfixe H n'est pas présent).
FRAQ (qualité d'image)	Satisfaisant entre 95 % et 100 % (90 % à 94 % pour de courtes périodes non critiques), mauvais lorsque < 95 %.

Pour plus d'informations sur le menu de mesure, voir : *OpenScape Sans fil Enterprise, Documents de service, chapitre : Test de la zone radio* et *Unify OpenScape Business X5/X8, Documents de service, chapitre : Vérifier la couverture radio.*

18.3.3 Configuration de la solution cordless intégrée

La configuration de la solution cordless intégrée comprend le réglage des stations de base et la connexion des téléphones DECT/mobiles au système de communication.

La configuration est réalisée à l'aide du mode Expert.

Les conditions telles que : étude, définition de la couverture, montage et câblage, mise en place du système et insertion des modules SLC ou CMA sont réunies (voir aussi Documentation maintenance). Les téléphones DECT sont chargés. L'identifiant système DECT est connu. Les informations sur les abonnés, numéros de téléphone et éventuellement leur attribution au module SLC sont disponibles.

Déroulement général de la configuration de la solution cordless intégrée

1) Entrer l'identifiant système DECT et configurer évent. d'autres paramètres Cordless
2) Configuration de la station de base cordless
3) Inscrire les téléphones DECT sur Cordless
4) Si nécessaire, ajouter d'autres téléphones DECT

Après la mise en service des téléphones DECT, le numéro d'appel, le nom et d'autres paramètres des abonnés DECT peuvent être modifiés à l'aide de la WBM, à l'aide de l'assistant **Terminaux/Abonnés**.

Identifiant système DECT

L'identification système DECT sert à différencier les différents systèmes DECT et ainsi à identifier les signaux radio. C'est seulement ainsi que la synchronisation des combinés inscrits sur le système est possible.

L'identifiant système DECT est une séquence de chiffres hexadécimale à 8 positions ; il est fourni lors de l'acquisition du système DECT. Il est valable pour l'ensemble du système (y compris en cas de service Clientèle).

L'identifiant système DECT comprend les chiffres suivants :

Chiffre	Signification
Chiffre 1.	E/ARC (Access Right Code)
2ème - 5ème chiffres	EIC (Equipment Installers Code)
6ème - 7ème chiffres	FPN (Fixed Part Number)
8ème chiffre	FPS (Fixed Part Subscriber)

18.3.3.1 Comment entrer l'identifiant système DECT et configurer d'autres paramètres cordless (données pour l'ensemble du système)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une station de base OpenScape Business est raccordée au système de communication.

L'identifiant système DECT à 8 positions fourni lors de la commande du système DECT est disponible.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Cordless**.
3) Dans l'arborescence du menu, cliquez sur **Cordless** > **Dans l'ensemble du système**.
4) Dans **Identifiant du système**, entrez l'identifiant DECT à 8 positions.
5) Ne modifiez les paramètres pour l'ensemble du système de **Traitement de l'écho** et **Mode ECO** que si cela est nécessaire. Vous trouverez des explications sur ces paramètres dans Cordless>Dans l'ensemble du système.
6) Cliquez sur **Appliquer** puis sur **OK**.

18.3.3.2 Comment configurer les stations de base Cordless

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une station de base OpenScape Business est raccordée au système de communication.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Cordless**.
3) Dans l'arborescence du menu, cliquez sur **Cordless** > **Stations de base**. Toutes les stations de base raccordées sont présentées.
4) Si une ou plusieurs stations de base sont raccordées directement (sans module SLC) au système (SLUC), vous pouvez activer ou désactiver les stations de base à l'aide de la liste de sélection **Type**.
   a) **Station de base** : la station de base est activée et il est automatiquement préconfiguré 16 téléphones DECT et une ligne de mise en réseau SLC.
   b) **Aucun Port** : la station de base est désactivée avec tous les téléphones DECT correspondants et la ligne de mise en réseau SLC.
5) Si nécessaire, modifiez dans **Nom** le nom préconfiguré de la station de base (par ex. `Base 1`).
6) Dans **Niveau**, définissez le niveau de la station de base (50% ou 100%).
7) Cliquez sur **Appliquer** puis sur **OK**.

18.3.3.3 Comment configurer pour la première fois les abonnés DECT

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une station de base OpenScape Business est raccordée au système de communication.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Cordless**.
3) Dans l'arborescence du menu, cliquez sur **Cordless** > **SLC**. Tous les téléphones DECT déjà configurés sont affichés. Lors de la connexion d'une station de base, 16 téléphones DECT sont automatiquement préconfigurés.
4) Si nécessaire, modifiez dans **N° tél** le numéro de téléphone interne préconfiguré du téléphone DECT
5) Si nécessaire, modifiez dans **SDA** le numéro SDA préconfiguré du téléphone DECT.
6) Si nécessaire, modifiez dans **Nom** le nom préconfiguré du téléphone DECT.
7) Si nécessaire, modifiez dans **Code mobile** le code mobile (PIN) préconfiguré du téléphone DECT. Ce code doit être entré sur le téléphone DECT lors de la première connexion de la station de base.
8) Cliquez sur **Appliquer** puis sur **OK**.

Tâches associées

Comment configurer les abonnés DECT à la page 416

18.3.3.4 Comment connecter un téléphone DECT (combiné OpenStage/Gigaset) sur cordless

Avant l'enregistrement d'un téléphone DECT, vous devez ouvrir la fenêtre d'enregistrement sur un poste système au moyen d'un code d'enregistrement DECT. Entrez ensuite les numéros des téléphones DECT à enregistrer. Vous pouvez enregistrer au maximum 10 numéros de téléphone dans la même fenêtre d'enregistrement. Une fenêtre d'enregistrement reste ouverte pendant 10 minutes maximum.

Si aucun téléphone système n'est disponible, vous pouvez utiliser la fonctionnalité Hipath 3000 Manager **en ligne** pour effectuer vos actions au lieu d'utiliser un téléphone physique. Les étapes suivantes concernent le téléphone physique.

Les étapes suivantes concernent le téléphone physique.

Étape par étape

1) Ouvrez la fenêtre d'enregistrement dans le système de communication :
   a) Sur le téléphone physique, entrez le code *94 2 puis 19970707.
   b) Entrez ensuite les numéros des téléphones DECT à enregistrer.

2) Enregistrez le téléphone DECT :

a) A partir de l'écran d'accueil du téléphone DECT, appuyez sur la **touche Menu**.

b) Allez à **Paramètres > Enregistrement > Enregistrer le combiné**, puis sélectionnez **Base**.

c) Il vous sera demandé d'entrer le code PIN système de la station. Entrez le code à huit chiffres du téléphone mobile et validez.

Vous devrez attendre un ou deux appels silencieux, c'est-à-dire des appels automatiques (sur certains appareils, cela correspond à 2 sonneries).

Si vous enregistrez un numéro inactif (qui n'a jamais utilisé auparavant : aspect noir dans WBM et gris dans KDS), l'enregistrement sera terminé par un appel silencieux. Si vous enregistrez un numéro d'appel inactif qui n'a jamais été utilisé auparavant (aspect vert dans WBM et KDS), l'enregistrement sera terminé par deux appels silencieux.

N'effectuez aucune autre action (par ex. initialisation d'appels téléphoniques DECT) tant que ce processus n'est pas terminé !

Une fois l'enregistrement réussi, vous verrez le numéro de téléphone sur l'écran d'accueil, et vous serez en mesure d'utiliser l'appareil.

Exemple : inscription sur le téléphone système DECT 2 le téléphone mobile (numéro d'appel 125) avec le code de téléphone mobile/PIN 11112345 (configuré comme code mobile à l'aide de Manager E ou de WBM, comme nous l'avons indiqué dans le chapitre : Comment configurer pour la première fois les abonnés DECT à la page 907.)

1) Activez la fenêtre d'enregistrement à partir d'un téléphone physique raccordé au système entrant *942.

2) L'écran du téléphone s'affiche : **Code**

3) Entrez 19970707 et vous verrez s'afficher sur l'écran du téléphone : **N° tél.** : Entrez 125.

4) Si nécessaire, activez le combiné en appuyant pendant plus de 1 s sur la touche Raccrocher. Vous entendez ensuite la tonalité d'acquittement.

5) Effectuez les entrées suivantes en l'espace de 10 minutes. Appuyez sur la touche Menu.

6) Allez à **Paramètres** du menu téléphone et confirmez.

7) Allez à **Enregistrement** et confirmez le premier choix : **Enregistrement combiné** (ne sélectionnez pas la deuxième option : Sélectionner Base)

8) Sélectionnez une station (**Base 2** dans notre exemple) et validez. Vous verrez au milieu de l'écran **Enregistrement** et **Veuillez entrer le code PIN système**.

9) Entrez le code PIN à huit chiffres (code de téléphone mobile, dans ce cas **11112345**) et validez. Si l'enregistrement a réussi, vous devez attendre un « appel silencieux », c'est-à-dire un appel automatique (sur certains appareils, cela correspond à 2 sonneries). Si vous enregistrez un numéro inactif (qui n'a jamais utilisé auparavant : aspect noir dans WBM et gris dans KDS), l'enregistrement sera terminé par un appel silencieux. Si vous enregistrez un numéro d'appel inactif qui n'a jamais été utilisé auparavant (aspect vert dans WBM et KDS), l'enregistrement sera terminé par deux appels silencieux. N'effectuez aucune autre action (par ex. initialisation d'appels téléphoniques DECT) tant que ce processus n'est pas terminé ! Ensuite, sur le côté gauche de l'écran, vous verrez Base 2 (dans notre

exemple). Ensuite, vous verrez le numéro de téléphone (125) sur votre écran d'accueil.

10) Vous pouvez modifier le nom Base 2, si nécessaire. Pour cela, accédez à Paramètres et confirmez, allez à Enregistrement et confirmez, puis sélectionnez la deuxième option Sélectionner Base. Sélectionnez le nom de base qui doit être renommé, appuyez sur **Nom** et renommez le nom de base (par exemple, 125).

18.3.3.5 Comment ajouter d'autres téléphones DECT

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une station de base OpenScape Business est raccordée au système de communication.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Cordless**.

3) Dans l'arborescence du menu, cliquez sur **Cordless** > **SLC**.

4) Dans l'arborescence du menu, cliquez sur le module souhaité.

5) Cliquez sur l'onglet **Ajouter téléphones DECT**.

6) Dans **Nombre de téléphones DECT**, indiquez le nombre des nouveaux téléphones DECT ajoutés. Les nouveaux téléphones DECT ajoutés sont présentés dans l'onglet **Modifier les téléphones DECT**.

7) Cliquez sur **Appliquer** puis sur **OK**.

18.3.3.6 Comment effacer des téléphones DECT

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une station de base OpenScape Business est raccordée au système de communication.

Les téléphones DECT sont configurés.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Cordless**.

3) Dans l'arborescence du menu, cliquez sur **Cordless** > **SLC**. Tous les téléphones DECT déjà configurés sont affichés.

4) Dans la colonne **Effacer**, marquez les téléphones DECT à effacer.

5) Cliquez sur **Appliquer** puis sur **OK**.

18.3.3.7 Comment configurer le paramètre Multi-SLC

Conditions préalables

Vous êtes connecté à WBM avec le profil **Expert** ou à Hipath 3000 Manager. Les étapes ci-après concernent uniquement WBM, mais des opérations similaires peuvent être effectuées avec Hipath 3000 Manager.

Plusieurs modules SLMUC sont enfichés dans OpenScape Business X8.

Une station de base OpenScape Business est raccordée au système de communication.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Cordless**.
3) Dans l'arborescence du menu, cliquez sur **Cordless** > **Multi-SLC**.
4) Modifier les paramètres du module SLMUC :
   a) Si nécessaire, modifiez sous **N° SLC** l'identifiant unique du module SLMUC préconfiguré pour l'ensemble du système.

      Plage de valeurs : 1-15,17-31,33-47,...,127. Les multiples de 16 ne sont pas autorisés.
   b) Si nécessaire, modifiez sous **N° SLC** le numéro d'appel unique de la ligne de mise en réseau SLC du module SLMUC préconfiguré pour l'ensemble du système.

      Remarque : Pour chaque ligne de mise en réseau SLC, un abonné S_0 interne est créé. Le numéro SLC correspond au numéro de téléphone de l'abonné interne S_0.

      ---

   c) Vérifiez que l'indicateur abonné **Protégé intrusions** est désactivé pour l'abonné S_0 interne.
5) Si nécessaire répéter l'opération 4 pour les autres modules SLMUC.
6) Cliquez sur **Appliquer**, puis sur **OK**.

18.3.3.8 Comment interroger les données des stations de base

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une station de base OpenScape Business est raccordée au système de communication.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Cordless**.
3) Dans l'arborescence du menu, cliquez sur **Cordless** > **Stations de base**.
4) Dans l'arborescence du menu, cliquez sur la station de base souhaitée. Les données de la station de base sont affichées. Vous trouverez une explication sur les données dans Cordless>Station de base.

5) Vous pouvez sélectionner simultanément jusqu'à 10 canaux de fréquences différents pour une station de base. Vous trouverez une explication sur les canaux de fréquences dans Cordless>Station de base.
6) Cliquez sur **Appliquer** puis sur **OK**.

18.3.3.9 Comment activer Message Waiting Indication (MWI - indication de message en attente) pour les téléphones DECT

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Configur. de base** > **Système** > **Flags système**.
4) Dans la zone **Flags système**, cochez la case **Tonalité d'avertissement CMI MWI**.
5) Cliquez sur **Appliquer** puis sur **OK**.

18.3.3.10 Comment interroger l'état de connexion des téléphones DECT

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une station de base OpenScape Business est raccordée au système de communication.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Cordless**.
3) Dans l'arborescence du menu, cliquez sur **Cordless** > **SLC**. Tous les téléphones DECT déjà configurés sont affichés.
4) Dans la colonne **Actif**, il vous est présenté l'état de connexion de chaque téléphone DECT :
   - Vert : le téléphone mobile est actif.
   - Rouge : interrupteur de modules activé pour téléphone mobile déclaré.
   - Jaune : le téléphone mobile a été automatiquement désenregistré par modification du PIN.
   - Gris : Aucun téléphone mobile n’a encore été déclaré sur ce port.
5) Cliquez sur **Appliquer** puis sur **OK**.

18.3.4 Téléphones WLAN et points d'accès

Les téléphones WLAN et les téléphones dual mode permettent la communication mobile. Ces téléphones peuvent être intégrés dans des infrastructures WLAN existantes. Les points d'accès WLAN permettent de créer des réseaux sans fil et d'utiliser les services Voix et Données sur la même infrastructure. Il est recommandé de n'utiliser que des point d'accès WLAN hautes performances (par ex. d'Enterasys).

18.3.4.1 Exigences du WLAN

Lors de l'utilisation du WLAN, il faut vérifier si les exigences fondamentales de l'utilisation de Voice-over-WLAN sont bien réunies. Pour la mise en place de la partie sans fil du réseau, il faut si nécessaire procéder à une étude de la diffusion radio (étude sur le site).

Aides à la décision

- Les installations de petites tailles, avec jusqu'à 3 points d'accès, peuvent être évaluées de manière précise lors d'une visite du site ou en étudiant le plan du bâtiment. Dans ce cas, il n'est pas nécessaire de réaliser une étude de site.
- Pour les installations à partir de 4 AP, il faut dans tous les cas effectuer une étude radio. Cela s'applique spécialement aux installation qui intègrent plusieurs bâtiments ou plusieurs étages de bâtiments.
- Indépendamment du nombre de points d'accès, il est également nécessaire d'effectuer une étude de site dans le cas d'un environnement à forte densité RF (RF = radio fréquence) ou lorsque la solution doit être installée à proximité d'autres systèmes WLAN existants.

18.4 Mobilité à domicile

La mobilité à domicile est rendue possible grâce au télétravail. Pour cela, les téléphones non locaux (tels que les téléphones fixes ou mobiles) sont intégrés au réseau de communication OpenScape Business.

Les types de postes de télétravail suivants sont disponibles :

- Abonnés VPN

  OpenScape Business dispose d'une fonctionnalité VPN intégrée. Au total, 10 télétravailleurs peuvent être actifs simultanément via VPN. Il peut s'agir d'un PC domestique ou d'un téléphone mobile équipé d'un système d'exploitation Android ou iOS. La connexion VPN est établie entre le client VPN natif du PC ou du téléphone mobile et le serveur OpenVPN d'OpenScape Business.

  Les utilisateurs de UC Suite peuvent indiquer leur numéro de téléphone fixe depuis leur domicile via leur client UC, puis utiliser leur téléphone privé comme téléphone professionnel (CallMe).
- Device@Home : Stations SIP@Home ou stations System Device@Home

  Les téléphones SIP compatibles STUN (par exemple, Yealink T19) (stations SIP Device@Home) ou les téléphones HFA (stations System Device@Home) peuvent s'enregistrer eux-mêmes sur le système de

communication via Internet en utilisant la fonction SBC interne d'OpenScape Business. Pour ce faire, la fonction doit être activée dans les données de la station pour chaque téléphone SIP ou HFA via le WBM.

Un serveur STUN doit être spécifié en plus dans le WBM uniquement si aucun ITSP n'est utilisé ou si l'ITSP utilisé ne propose pas de serveur STUN.

SIP Device@Home ne prend pas en charge la transmission de signaux vidéo.

Remarque : Lorsque vous utilisez plusieurs appareils SIP/HFA @Home derrière le même routeur, les limitations NAT peuvent entraîner des problèmes de charge utile des appels en raison de conflits de réutilisation des ports ; pour éviter cela, configurez chaque appareil avec un port source (RTP) unique.

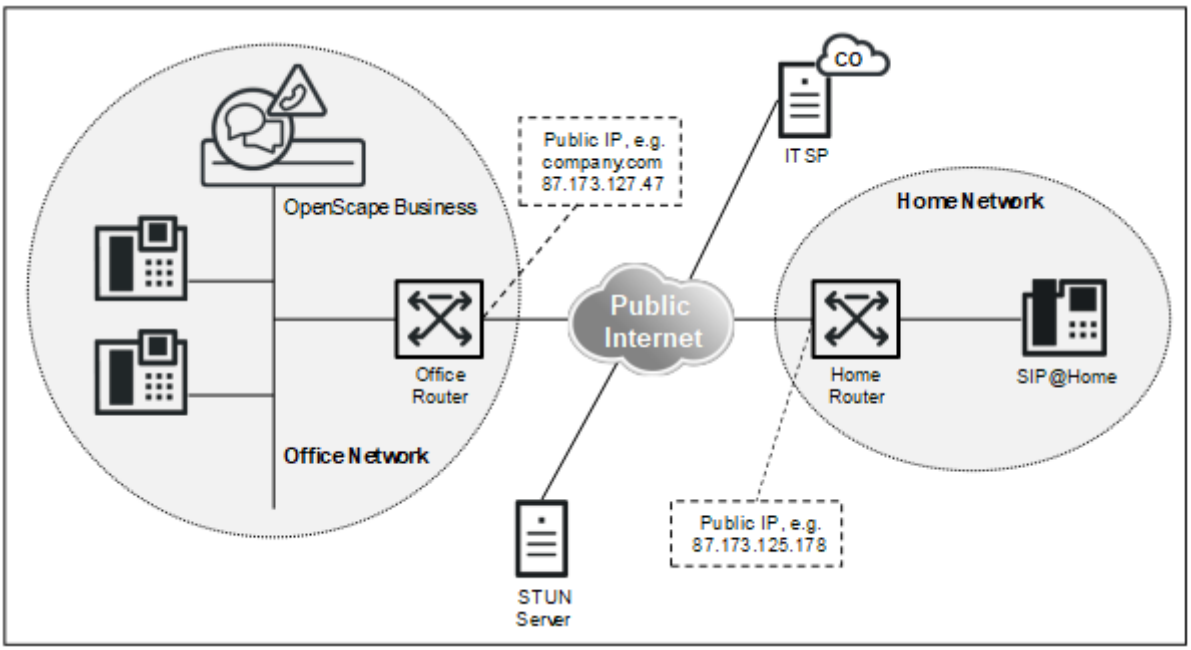


Illustration 8 : Composants Device@Home (SIP Device@Home ou System Device@Home)

18.4.1 Configuration pour VPN

Pour raccorder des abonnés au système de communication via la fonctionnalité VPN intégrée, il faut effectuer des configurations sur OpenScape Business et les abonnés VPN.

Configuration OpenScape Business

Pour la configuration VPN du système de communication, voir Comment configurer la connexion des télétravailleurs via VPN .

Configuration abonné VPN (client VPN)

Pour la configuration des clients VPN, voir Clients VPN .

18.4.2 Configuration de SIP Device@Home

Pour établir des connexions via Internet entre un téléphone SIP compatible STUN et OpenScape Business, il faut effectuer des configurations.

Configuration d'OpenScape Business

Afin qu'un abonné SIP puisse s'enregistrer sur le système de communication via Internet, il faut activer la fonction SBC intégrée pour l'abonné SIP (voir Comment activer Device@Home).

À l'aide d'un protocole STUN, la fonction SBC intégrée détecte l'adresse IP publique du système de communication et le port utilisé. Si le système de communication est relié à un fournisseur ITSP qui propose un serveur STUN, il n'est pas nécessaire d'effectuer d'autres configurations sur le système de communication. S'il n'est pas utilisé un ITSP ou si le ITSP utilisé n'offre pas de serveur STUN, il faut configurer un serveur STUN dans le système (voir Comment indiquer un serveur STUN pour Device@Home).

Configuration du routeur Internet Office

Afin que le téléphone SIP puisse atteindre le système de communication via Internet, il faut avoir paramétré sur le routeur Internet de bureau un renvoi de port pour le port SIP externe. Afin d'éviter les attaques SIP en provenance d'Internet, il faut utiliser comme port SIP un port SIP différent du standard.

Le protocole de transport doit être réglé sur le téléphone SIP.

Tableau 9 : Configurer le renvoi de port dans le routeur du bureau

Protocole de transport	Port SIP interne	Port SIP externe	Commentaire
UDP	5070	Entrée de 5090, par exemple.	Pour le renvoi de port, le port SIP externe et le port SIP interne doivent être différents. Il est possible d'indiquer comme port SIP externe une valeur différente du port SIP 5070 standard interne. C'est pourquoi UDP est recommandé.
TCP	5070 Modification en 5080, par exemple	Entrée de 5080 par exemple (= port SIP interne)	Pour le renvoi de port, le port SIP externe et le port SIP interne doivent être identiques. Pour utiliser un port SIP externe différent du port SIP standard 5070, il faut modifier le port SIP interne. Cela nécessite une reconfiguration de toutes les composantes qui utilisent SIP. Donc TCP n'est **pas** recommandé.

Protocole de transport	Port SIP interne	Port SIP externe	Commentaire
TLS	5071	Entrée de 5071 (= port SIP TLS interne)	Pour le renvoi de port, le port SIP TLS externe et le port SIP TLS interne doivent être identiques. Étant donné que le port interne SIP-TLS diffère déjà du port SIP-TLS par défaut, il est possible d'indiquer aussi comme port externe SIP-TLS 5071. C'est pourquoi TLS est recommandé.

Remarque : Dans un système mis à jour, aucun changement concernant les ports SIP n'est effectué automatiquement. Après la mise à niveau, les ports sont :

SIP_EXT = 5060

SIP_TLS_SUB_EXT = 5062

Ces valeurs doivent être modifiées manuellement par l'administrateur si Device@Home est utilisé dans un système migré.

Pour TLS, il faut activer les certificats valides dans le système de communication. Les connexions TLS pour abonnés SIP sont supportées au niveau de l'interface LAN du système de communication, mais pas au niveau de l'interface WAN. La charge utile SRTP avec signalisation SDES n'est pas supportée.

Si le routeur Internet Office est relié à Internet sans adresse IP fixe, il faut configurer DynDNS dans le routeur Internet Office de manière à ce que l'abonné SIPO puisse atteindre le système de communication via Internet. L'adresse IP actuelle est enregistrée à intervalles réguliers à l'aide du compte DynDNS. Dans les comptes DynDNS gratuits, qui expirent à intervalles réguliers, cela peut parfois provoquer une défaillance.

Configuration téléphone SIP

Vous trouverez sur Internet, dans Unify Experts Wiki, une liste de tous les téléphones SIP testés qui supportent STUN. Vous y trouverez les valeurs qu'il faut entrer sur le téléphone SIP.

Configuration du routeur Internet Home

Sur le routeur Internet Home, aucune configuration spéciale n'est nécessaire.

Le routeur Internet Home doit répondre aux exigences suivantes :

- Le routeur doit fournir la fonctionnalité VoIP avec la fonction NAT activée (NAT asymétrique).
- La fonction ALG doit être désactivée dans le routeur.

La connexion Internet doit fournir une bande passante suffisante pour la transmission de l'appel. Pour les connexions DLS asymétriques notamment, assurez-vous de disposer d'une bande passante suffisante pour le chargement.

Configuration de myPortal @work

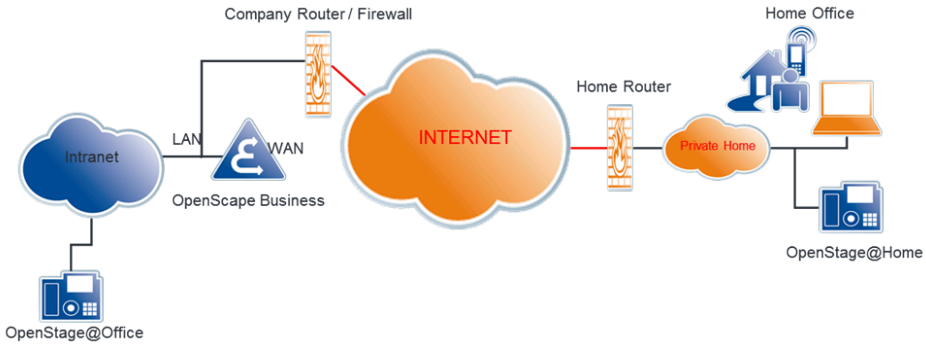
Pour permettre à myPortal @work d'accéder au système de communication par Internet, vous devez effectuer les opérations suivantes :

- Configurez le serveur STUN en fonction du système/client.
- Ouvrez et transmettez le port 8802 (les autres transmissions ne sont pas valables).
- L'indicateur SBC n'est pas nécessaire. Aucune authentification n'est nécessaire.

18.4.3 Configuration pour le périphérique système@Home

Pour établir une connexion entre un téléphone du système et OpenScape Business via Internet, certaines configurations doivent être effectuées sur OpenScape Business, le routeur Internet du bureau et le téléphone du système.

- **Illustration 9 : Exemple de cas d'utilisation de System Device@Home**



Configuration d'OpenScape Business

Pour permettre à une station System Device@Home de s'enregistrer auprès du système de communication via Internet, la fonction SBC intégrée doit être activée pour la station System Device@Home (voir Comme activer Equipement@Home à la page 919).

La fonction SBC intégrée détecte l'adresse IP publique du système de communication et le port utilisé à l'aide du protocole STUN. Si le système de communication est connecté à un fournisseur de services de communication (ITSP) qui propose un serveur STUN, aucune autre configuration ne doit être effectuée sur le système de communication. Toutefois, si aucun fournisseur de services de communication (ITSP) n'est utilisé ou si l'ITSP utilisé ne propose aucun serveur STUN, un serveur STUN doit être indiqué au système de communication (voir Comment spécifier un serveur STUN pour System Device@Home).

Configuration du routeur Internet du bureau

Pour permettre aux stations System Device@Home d'accéder au système de communication via Internet, la redirection de port pour le port System Device doit être configurée sur le routeur Internet du bureau. Pour pouvoir s'inscrire

depuis Internet, le routeur/pare-feu du bureau doit être configuré avec une règle de redirection de port :

- Port externe TCP/4060 vers port interne TCP/4062 (HFA), pour les connexions non-TLS

  Port externe TCP/4061 vers port interne TCP/4063 (HFA), pour TLS

  Remarque : Lors de la migration de la version V2R1 vers une version supérieure, le routeur Internet du bureau doit également être reconfiguré conformément à cette règle.

  Les ports mentionnés ci-dessus sont uniquement nécessaires pour les périphériques système (téléphone HFA).

- Plage de ports RTP dans OpenScape Business X : 30274-30529 ; plage de ports RTP dans OpenScape Business S : 30528-30887 (valeurs par défaut)

  Les clients de communications unifiées compatibles VoIP, tels que myPortal@work, ont également besoin de ces ports.

- TCP/8802 (HTTPS) (requis pour le client de communications unifiées (par exemple, mon portail au travail configuré comme périphérique système à domicile)

  Remarque : La zone du pare-feu interne doit être fermée.

Le protocole de transport est configuré au niveau de la station System Device@Home.

Si le routeur Internet du bureau est connecté à Internet sans adresse IP fixe, DynDNS doit être configuré sur ce routeur afin que les stations System Device@Home puissent accéder au système de communication via Internet. L'adresse IP actuelle est enregistrée à intervalles réguliers via le compte DynDNS. Avec les comptes DynDNS gratuits, qui expirent à intervalles réguliers, cela peut entraîner des interruptions temporaires.

Configuration du routeur Internet domestique

Aucune configuration particulière n'est nécessaire sur le routeur Internet domestique.

Le routeur Internet domestique doit répondre aux exigences suivantes :

- Le routeur doit fournir une fonctionnalité VoIP avec NAT activé (NAT non symétrique).
- La fonction ALG doit être désactivée sur le routeur.

La connexion Internet doit fournir une bande passante suffisante pour la transmission de l'appel. Pour les connexions DSL asymétriques, il est notamment indispensable de garantir la disponibilité d'une bande passante montante suffisante.

Configuration du téléphone HFA

La passerelle doit être configurée avec le nom DNS (par exemple mycompany.net) afin que le téléphone puisse accéder au système via Internet. L'adresse IP du DLI doit également être configurée. Un numéro de téléphone

interne doit être ajouté pour l'abonné. Le mot de passe de l'appareil doit également être défini.

Restrictions

- Il n'est pas possible de configurer des applications XML sur OpenStage.

18.4.4 Comme activer Equipement@Home

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés** > **Client IP** > **Clients SIP** ou **Clients système**
4) Dans l'arborescence du menu, cliquez sur l'abonné HFA ou SIP souhaité.
5) Cliquez sur l'onglet **Modifier les données du poste de travail Client**.
6) Assurez-vous qu'un mot de passe est saisi. Les valeurs indiquées ici doivent aussi être inscrites sur le téléphone SIP ou l'équipement système.

Remarque :

Dans une connexion par Internet, il faut absolument utiliser un mot de passe sûr (au moins 8 caractères y compris majuscules, chiffres et caractères spéciaux).

Remarque : Le mot de passe des clients Deskshare déclarés en tant que @Home ne doit contenir que des caractères numériques. Ce mot de passe est en fait le code PIN destiné à l'activation de la fonctionnalité de mobilité (code de service de la fonctionnalité : *9419). Les équipements prennent seulement en charge les codes PIN constitués de caractères numériques.

Une fois le mot de passe défini, l'**Enregistrement Internet avec SBC interne** est disponible pour être activé.

Remarque : Après une mise à niveau rapide ou un redémarrage du système, la case **Authentification active** est activée pour tous les terminaux SIP et elle est grisée de sorte que l'utilisateur ne puisse pas la désactiver lorsqu'au moins un abonné SIP dispose de l'indicateur **Enregistrement Internet avec SBC interne** activé.

18.4.5 Comment mettre à jour le logiciel pour l'équipement HFA @Home

La procédure de mise à jour logicielle normale du DLI pour un périphérique connecté en interne ne peut pas être utilisée pour un équipement HFA@Home car cela nécessite un accès direct à l'adresse IP du périphérique pour le transfert de fichier. Le DLI ne peut pas déterminer l'adresse IP de l'équipement HFA@Home pour les raisons suivantes :

- Device@Home réside dans un réseau domestique utilisant des adresses IP privées. L'accès à Internet s'effectue via un routeur domestique avec traduction d'adresse réseau (NAT).
- Le DLI au sein d'OpenScape Business se situe dans un réseau d'entreprise/de bureau utilisant des adresses IP privées. Le réseau d'entreprise est connecté à Internet via le routeur d'entreprise/de bureau.

Par conséquent, la procédure de mise à jour logicielle DLI utilise une connexion HTTPS supplémentaire via le port 8804 (paramètre par défaut) en combinaison avec le port DLI 18443 (paramètre par défaut) pour déterminer la version logicielle de Device@Home et effectuer la mise à jour logicielle.

La vérification de la version logicielle pour un Device@Home est uniquement effectuée si l'une des conditions suivantes s'applique :

- Redémarrage du périphérique
- Modification de la configuration localement ou à distance
- Changements d'inventaire sur le périphérique
- Connexion ou déconnexion d'un utilisateur mobile sur un périphérique.

Dans ces cas, le DLI vérifie la version logicielle du périphérique et effectue une mise à jour logicielle si une version plus récente est disponible dans OpenScape Business.

La mise à jour logicielle automatique d'un Device@Home par le DLI doit être configurée dans OpenScape Business. Elle est désactivée par défaut et doit être activée explicitement.

Les étapes suivantes doivent être exécutées.

Étape par étape

1) Vous êtes connecté à l'interface WBM avec le profil Expert.

2) Dans la barre de navigation, cliquez sur **Mode Expert**.

3) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie > Paramètres de base**.

4) Dans l'arborescence de navigation, cliquez sur **Paramètres de base > Déploiement des paramètres du téléphone**.

- En cliquant sur **Déployer le logiciel sur les équipements @Home**, les autorisations sont données pour la mise à jour logicielle via DLI pour les équipements HFA @Home. La valeur par défaut est « désélectionné ».
- Cliquez sur **Appliquer**, puis sur **OK**.

5) Paramètres de pare-feu

Aucun paramètre de pare-feu manuel n'est requis dans OpenScape Business. Le port 8804 est ouvert au démarrage du système et les demandes qui parviennent à ce port ne sont traitées par le système que si l'option **Déployer le logiciel sur les équipements @Home** est activée.

6) Ouvrez les ports utilisés 18443 et 8804 pour le DLI avec la configuration appropriée (redirection de port) dans le routeur de l'entreprise/du bureau.

Limitations

L'équipement HFA@Home réside derrière un pare-feu (routeur domestique). Le routeur ou le pare-feu induit une traduction d'adresse réseau (NAT), ce qui rend l'adresse IP impossible à voir depuis le monde extérieur. Par conséquent, les téléphones IP ne peuvent pas être vus à distance pour être administrés par le DLI.

L'effet secondaire de la restriction réseau ci-dessus est que tout événement géré par le DLI ne peut pas être accompli, car ces événements sont envoyés vers l'adresse IP locale (non accessible) de l'équipement.

Par conséquent, aucune mise à jour logicielle à la demande ne sera possible. D'autre part, la mise à jour du logiciel sera possible lorsque l'équipement initiera un échange de messages en ouvrant une session HTTPS vers le DLI. Les sessions sont ouvertes en raison d'événements spécifiques de l'équipement, tels que :

- le redémarrage de l'équipement ;
- un changement de configuration effectué sur l'équipement (via l'affichage local ou la gestion web) ;
- des changements d'inventaire sur l'équipement ;
- la connexion ou la déconnexion d'un utilisateur mobile sur un équipement.

Dans tous ces cas, le DLI vérifie le logiciel de l'équipement et, si nécessaire, l'équipement est mis à jour vers le logiciel officiel pris en charge par OSBiz.

Remarque : Le déploiement du logiciel a lieu au démarrage du téléphone (soit lorsqu'il est enregistré sur OSBiz, soit lorsque le système OSBiz entre en service).

18.4.6 Comment indiquer un serveur STUN pour Equipement@Home

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Il n'est pas utilisé d'ITSP ou l'ITSP utilisé ne propose pas de serveur STUN.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Passerelle vocale**.
3) Dans l'arborescence du menu, cliquez sur **Internet Telefonie Service Provider - fournisseur de services de téléphonie sur Internet**.
4) Cliquez sur l'onglet **Modifier la configuration STUN**.
5) Dans **Serveur STUN par défaut**, **Adresse IP / Nom d'hôte** indiquez l'adresse IP ou le nom d'hôte du serveur STUN (par ex. `stun.serviceprovider.com`).
6) Dans **Serveur STUN par défaut**, **Port**, indiquez le port du serveur STUN (par ex. `3478`).

7) Cliquez sur **Appliquer** puis sur **OK**.

19 Sécurité

La sécurité englobe la protection du système de communication et des données enregistrées et transmises par rapport aux accès non autorisés; Cela peut être assuré par une protection d'accès pour le réseau IP (pare-feu) ou par le chiffrement de la transmission (SSL, VPN).

Security Checklist

Le système de communication prend en compte la sécurité des communications dans ses réglages préalables. Lors de la mise en service, les fonctions doivent être adaptées à la situation individuelle du client et il doit donc être pris de nouvelles dispositions dans l'environnement client. Afin de développer la conscience des risques pour la sécurité et d'adopter des mesures adaptés, il est fourni dans la documentation produit une liste de contrôle de la sécurité (Security Checklist). Il est conseillé de manière urgente d'en discuter avec le client lors de la mise en service et de documenter les mesures.

19.1 Pare-feu

Un pare-feu est un système de composantes matérielles et logicielles qui limite l'accès entre différents réseaux d'ordinateurs pour mettre en oeuvre un concept de sécurité.

Les pare-feux se trouvent aux interfaces entre différents réseaux et contrôlent le trafic de données entre les sous-zones afin d'interdire un trafic non souhaité et laisser passer uniquement le trafic souhaité. L'emploi le plus fréquent d'un pare-feu consiste à contrôler le trafic entre un réseau local (LAN) et Internet.

Dans chaque réseau d'entreprise, un pare-feu découple le LAN interne de l'Internet.

Le système de communication offre des fonctions de sécurité intégrées ; dans ce cadre, OpenScape Business X et OpenScape Business S se différencient en matière de fonctionnalité.

OpenScape Business X offre les fonctionnalités suivantes :

- Pare-feu de port / NAT (pare-feu entre port WAN et LAN)
- Pare-feu application (pare-feu pour l'accès au système de communication)

OpenScape Business S utilise le pare-feu Linux.

19.1.1 Porthandling

Le Porthandling sert à valider un port (Port Mapping, Renvoi de port) dans le pare-feu du routeur intégré de OpenScape Business X.

Numéros de port

Remarque : N'ouvrez des ports que si cela est impérativement nécessaire pour une application définie.

Les ports (services) sont impératifs pour la communication par les protocoles TCP et UDP, car ils permettent à plusieurs applications d'échanger simultanément des données par une seule liaison.

Le terme pare-feu désigne généralement un pare-feu de port (c.-à-d. le blocage de certains service, également appelés ports). Le pare-feu de port n'agit que sur le raccordement WAN de OpenScape Business.

Dans OpenScape Business S, il est possible sous Linux d'activer un pare-feu de port sur la connexion LAN. Dans OpenScape Business X, le pare-feu du raccordement WAN est activé afin de protéger le réseau interne (au niveau du raccordement LAN) des attaques en provenance d'Internet. Si certains ports/services doivent toutefois demeurer joignables depuis Internet, ils doivent alors être validés (voir Validation de port). Tous les ports/services de la fonctionnalité de OpenScape Business X sont automatiquement validés au niveau de la connexion LAN (en direction du réseau de clients interne).

OpenScape Business S comprend une seule connexion LAN (dans le réseau de clients interne) et est protégé d'Internet par d'autres composantes/routeurs du réseau de clients. De plus, le pare-feu Linux interne au serveur est activé. Certains ports/services doivent être validés pour la fonctionnalité OpenScape Business (afin par ex. que les téléphones puissent communiquer avec OpenScape Business S). Cela se produit automatiquement, mais l'administrateur peut toutefois bloquer certains services.

Les numéros de ports peuvent avoir des valeurs entre 0 et 65535 et sont ainsi affectés aux différentes applications. Entre 0 et 1023 se trouvent des ports 'Well Known Ports', qui sont affectés de façon fixe par l'IANA (Internet Assigned Numbers Authority) et connus de façon générale. Vous pouvez consulter la liste de ces ports à l'adresse http://www.iana.org/assignments/port-numbers.

19.1.1.1 Validation de port

Si le système établit l'accès Internet (par le port WAN), seule est autorisée par défaut la communication qui mène de l'intérieur (du réseau d'entreprise ou du système de communication lui-même) vers Internet et les paquets de réponse correspondants. Les demandes qui sont à l'origine issues d'Internet sont bloquées. Ce paramètre de sécurité peut être contourné par la validation de port ciblée, pour par ex. faire fonctionner un serveur Web dans le réseau.

Remarque : Si le système de communication est utilisé comme routeur Internet, le port 5060 doit être fermé (paramètre par défaut). Dans le cadre de la téléphonie Internet via ITSP, le système de communication ouvre les ports correspondants et les maintient ouverts.

Même si l'on utilise un routeur externe ou un pare-feu, le port 5060 doit être fermé. Il est de la responsabilité du système de communication d'ouvrir ce port (si nécessaire).

19.1.1.2 Comment configurer la validation de port

Avec l'assistant **Pare-feu**, vous pouvez activer la validation de port de sorte que le système de communication ou le PC sur LAN soit joignable via le port WAN.

Les validations de port entraînent un risque d'accès par des personnes non autorisées. Il convient donc de ne valider que les ports qui sont nécessaires de manière urgente.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Cliquez dans l'arborescence de navigation sur **Assistants** > **Sécurité**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Pare-feu**. La fenêtre **Validation de port** s'ouvre.
4) Sur la ligne de l'application souhaitée ou du service souhaité, cochez la case **Règle NAT activée** pour laquelle vous souhaitez libérer les ports.
5) Dans les champs **Port global**, **Adresse IP locale** et **Port local** entrez les données à valider.
6) Pour la validation du port d'un service non inscrit, cliquez sur **Ajouter** et complétez les champs **Description**, **Règle NAT active**, **Port global**, **Adresse IP locale** et **Port local**.
7) Cliquez sur **OK&Suivant**.
8) Cliquez sur **Terminer**.

19.1.1.3 Gestion des ports

La Gestion des ports permet de modifier certains des ports que le système de communication utilise lui-même. Cela permet, dans un réseau, d'harmoniser la communication au réseau client, même si les ports sont déjà utilisés ailleurs.

Si des modifications sont apportées à la gestion des ports, il faut le faire normalement simultanément sur toutes les composantes (téléphones, système etc.) pour que la fonctionnalité soit garantie.

19.1.1.4 Comment modifier les paramètres de gestionnaire de ports généraux

Entrez ici les numéros de port des différentes fonctions.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Gestion des ports**. L'onglet **Modifier les paramètres de gestionnaire de ports généraux** s'ouvre.
4) Dans **Numéro de port** entrez le port pour la fonction correspondant ou conservez la valeur par défaut.
5) Cliquez sur **Appliquer** puis sur **OK**.

19.1.2 NAT

NAT (Network Address Translation) est une méthode de conversion d'adresse qui permet de remplacer une adresse IP dans un paquet de données par une autre. Dans un réseau interne, les clients utilisent des adresses IP privées. Comme les adresses IP privées ne sont pas transmises dans le réseau public, il est possible avec NAT de reproduire les adresses IP privées en une adresse IP publique. Ainsi, les clients internes ont accès au réseau public et la structure du réseau interne avec les adresses IP privées est invisible (masquée) pour le réseau public (par ex. Internet). NAT ou les règles NAT sont nécessaires pour la validation de port.

La conversion d'adresse est réalisée au niveau de la transition entre le réseau interne et le réseau public. NAT peut fonctionner sur un routeur Internet, un serveur ou un autre appareil spécialisé. Ainsi, par ex., un routeur Internet peut relier le réseau interne à Internet par Internet.

Vis-à-vis d'Internet, le réseau interne se présente avec une seule adresse IP publique, qui est affectée au routeur Internet par le fournisseur d'accès à Internet (FAI). Tous les accès à Internet à partir du réseau interne sont traités par cette adresse IP officielle avec différents numéros de ports. Le routeur Internet remplace les adresses IP privées par l'adresse IP officielle affectée par le FAI. Lorsque les paquets de données arrivent, l'adresse IP officielle est à nouveau remplacée par les adresses IP privées. Pour l'affectation, les numéros de ports sont décisifs. Seules les adresses IP privées validées spécifiquement peuvent être jointes directement à partir d'Internet.

Règles NAT

Les règles NAT permettent de définir si les adresses IP privées (locales) peuvent être jointes directement à partir d'Internet. Pour cela, des règles NAT propres peuvent être définies ou les règles NAT par défaut déjà prédéfinies pour les services Serveur FTP, Serveur HTTP, etc. peuvent être utilisées. Au total, 20 règles NAT peuvent être définies. Pour qu'une règle NAT puisse être utilisée, il faut entrer les données d'adresses locales du PC client qui fournira ces services pour Internet et la règle NAT doit être activée. Plusieurs règles NAT peuvent être configurées ensemble à l'aide d'un tableur. Les règles NAT qui ne sont plus nécessaires peuvent être effacées.

Ports

Au démarrage, les serveurs demandent au système d'exploitation l'attribution de certains ports afin d'être en mesure d'accepter les connexions. Serveur HTTP, le port 80, serveur FTP, le port 21, etc. Les clients demandent normalement au système d'exploitation un port aléatoire pour établir des connexions.

19.1.2.1 Comment configurer une règle NAT

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Routage**.
3) Configurez la règle NAT :
   - Si vous souhaitez définir une nouvelle règle NAT, cliquez dans l'arborescence de menu sur **NAT** puis sur l'onglet **Ajouter NAT**.
   - Si vous souhaitez modifier une règle NAT existante, cliquez dans l'arborescence de menu sur **NAT** et sélectionnez la règle NAT souhaitée.
4) Entrez dans **Description** un nom pour la règle NAT. S'il s'agit d'une règle NAT par défaut, ce nom ne peut pas être modifié.
5) Entrez dans **Adresse IP locale** l'adresse IP du client dans le réseau interne qui doit être validé.
6) Entrez dans **Port local** le numéro de port qui utilise l'application du client interne.
7) Entrez dans **Port global** le numéro de port qui utilise l'application du partenaire de communication externe.
8) Sélectionnez dans la liste déroulante **Protocole** le protocole de transport utilisé par l'application (**TCP** ou **UDP**). S'il s'agit d'une règle NAT par défaut, le protocole ne peut pas être modifié.
9) Si vous souhaitez appliquer la règle NAT, activez l'option **Règle NAT active**.
10) Cliquez sur **Appliquer** puis sur **OK**. La règle NAT activée est identifiée par un symbole vert sous l'option **NAT**.

19.1.2.2 Comment configurer plusieurs règles NAT avec le tableur NAT

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans la barre de navigation, cliquez sur **Téléphonie** > **Routage**.
3) Dans l'arborescence du menu, cliquez sur **Routage**.
4) Cliquez dans l'arborescence de menu sur **NAT** puis sur l'onglet **Tableur NAT**.
5) Configurez la règle NAT :
   - Si vous souhaitez définir une nouvelle règle NAT, remplissez les champs de la première ligne tels que décrits ci-dessous.
   - Si vous souhaitez modifier une règle NAT existante, cliquez dans les champs souhaités de la règle NAT et remplissez-les tels que décrits ci-dessous.
6) Entrez dans la colonne **Adresse IP locale** l'adresse IP du client dans le réseau interne qui doit être validé.
7) Entrez dans la colonne **Port local** le numéro de port qui utilise l'application du client interne.
8) Entrez dans la colonne **Port global** le numéro de port qui utilise l'application du partenaire de communication externe.

9) Sélectionnez dans la liste déroulante **Protocole** le protocole de transport utilisé par l'application (**TCP** ou **UDP**). S'il s'agit d'une règle NAT par défaut, le protocole ne peut pas être modifié.
10) Pour appliquer la règle NAT, cochez la colonne **Actif**.
11) Entrez dans la colonne **Description** un nom pour la règle NAT. S'il s'agit d'une règle NAT par défaut, ce nom ne peut pas être modifié.
12) Enregistrer la règle NAT :
    - Si vous avez configuré une nouvelle règle NAT, cliquez sur **Ajouter** puis sur **OK**. La nouvelle règle NAT est insérée à la fin du tableau.
    - Si vous avez modifié une règle NAT existante, passez au point 5.
13) Cliquez sur **Appliquer**. Une règle NAT activée est identifiée par un symbole vert sous l'option **NAT**.

19.1.2.3 Comment effacer une règle NAT

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Téléphonie** > **Routage**.
2) Dans l'arborescence de navigation, cliquez sur **Routage**.
3) Dans l'arborescence du menu, cliquez sur **NAT**.
4) Cliquez dans l'arborescence de menu sur la règle NAT à effacer et cliquez sur l'onglet **Effacer NAT**. Les règles NAT par défaut prédéfinies ne peuvent pas être effacées.
5) Validez l'avertissement avec **Effacer** puis cliquez sur **OK**. La règle NAT est effacée sous l'option de menu **NAT** de la liste des règles NAT.

19.1.3 Application pare-feu

Le pare-feu applicatif est utilisé pour restreindre l'accès à des services spécifiques tels que FTP ou LDAP. Il est désactivé par défaut et peut être activé en définissant des règles appropriées.

Les services suivants peuvent être bloqués ou limités à des adresses IP spécifiques ou à des plages d'adresses IP par le pare-feu d'application dans OpenScape Business X :

Service	Ports
FTP	21, 40000 - 40040
ssh (verrouillé par défaut)	22
LDAP	389
HTTPS	443
Postgres	5432
Manager E	7000
CSTA	7001 (FP), 7004 (FP), 8800 (CSP)

Service	Ports
OBSERVATEUR	Ce service permettait l'accès à partir d'une application OpenScape Observer qui n'est plus supportée.

Seuls les services listés peuvent être bloqués via un menu de sélection en mode Expert.

Les fonctions téléphoniques telles que SIP, HFA, etc. ne peuvent pas être bloquées à l'aide du pare-feu applicatif.

Un service peut être sélectionné plusieurs fois ; à chaque fois, des restrictions IP différentes peuvent être spécifiées.

Remarque : L'activation/désactivation ou la modification des paramètres du pare-feu peut restreindre considérablement la fonctionnalité de la carte (l'administration basée sur le LAN peut ne plus être possible, par exemple).

Remarque : Le pare-feu applicatif, lorsqu'il est activé, ne bloque pas les services par défaut jusqu'à ce qu'une règle soit ajoutée pour ce service, auquel cas seules les adresses IP incluses dans la règle peuvent accéder à ce service spécifique.

Le pare-feu applicatif peut restreindre l'accès aux fonctions inter-nœuds lorsque le système est relié à d'autres systèmes OpenScape Business. Par exemple, la fonction de survie nécessite le service POSTGRES pour fonctionner correctement. Dans ce cas, si une règle est ajoutée pour le service POSTGRES, ajoutez manuellement les adresses IP des autres nœuds OpenScape Business en réseau à la règle POSTGRES afin de garantir le bon fonctionnement de la fonction de survie.

19.1.3.1 Comment afficher la configuration de l'application pare-feu

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **Application pare-feu**.
4) Cliquez sur l'onglet **Afficher les services** pour afficher les services bloqués.
5) Dans le champ **Nom de la règle** il est présenté le nom de la règle.
6) Dans **Règle activée** vous voyez si la règle est activée ou non (cochée).
7) Dans le champ **Seuil inférieur de la plage d'adresses IP de source** figure le seuil inférieur des adresses IP bloquées.
8) Dans le champ **Seuil supérieur de la plage d'adresses IP de source** figure le seuil supérieur des adresses IP bloquées.

19.1.3.2 Comment restreindre les services via l'application pare-feu

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **Application pare-feu**.
4) Cliquez sur l'onglet **Ajouter un service** pour bloquer une plage d'adresses IP ou un service.
5) Dans **Nom de la règle**, donnez un nom à ce service (cette règle).
6) Dans **Plage d'adresses**, définissez le **Seuil inférieur** et le **Seuil supérieur** des adresses IP source admissibles.

   Il est possible de verrouiller entièrement l'accès en entrant 127.0.0.1.

   Conseil : N'activez une règle qu'un fois que vous êtes persuadé que les adresses IP autorisées ont été correctement configurées.

7) Cliquez sur **Sauvegarder**.

19.1.3.3 Comment effacer la configuration de l'application pare-feu

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **Application pare-feu**.
4) Cliquez sur l'onglet **Delete all Services** (Effacer tous les services) pour effacer tous les services.

19.1.4 Administration des services (OpenScape Business S)

Le pare-feu interne à Linux est activé par défaut, ce qui interdit tout accès à OpenScape Business S. Le système de communication propose toutefois des services (par ex. service Téléphonie) ce qui rend nécessaires des ports ouverts (services). Après l'installation d'OpenScape Business S ces ports/services sont ouverts dans le pare-feu. Si des service comme SNMP ne doivent pas être utilisés, ils peuvent être verrouillés dans le pare-feu Linux.

Remarque : Vous devez savoir que le verrouillage de services qui sont utilisés par OpenScape Business S peut provoquer des défaillances ou une panne des fonctionnalités du système de communication.

19.1.4.1 Comment ajouter ou verrouiller des services

Étape par étape

1) Dans la barre des tâches, cliquez sur **Computer**.
2) Dans l'arborescence du menu, cliquez sur **System** > **YaST**.
3) Entrez le mot de passe pour l'utilisateur root et cliquez sur **Continue** (poursuivre).
4) Dans l'arborescence du menu, cliquez sur **Security and Users** (sécurité et utilisateurs).
5) Dans la zone **Security and Users**, cliquez sur **Firewall** (pare-feu).
6) Dans l'arborescence du menu de la fenêtre **Firewall Configuration: Start-UP** (configuration du pare-feu: démarrer), cliquez sur **Allowed Services** (services autorisés).
7) Dans le champ **Allowed Services for Selectet Zone** (services autorisés dans la zone sélectionnée), sélectionnez la zone dans laquelle vous voulez modifier les services (**External Zone**, **Demilitarized Zone**, **Internal Zone**).
8) Dans le champ **Service to allow** (service à autoriser), sélectionnez les services que vous souhaitez valider (ajouter) de manière ciblée et cliquez sur **Add** (ajouter). Le menu déroulant indiquent tous les services actuellement autorisés.
9) Dans le champ **Allowed Service** (service autorisé), sélectionnez les services que vous souhaitez verrouiller et cliquez sur **Delete** (supprimer).
10) Cochez si nécessaire la case **Protect Firewall from Internal Zone** (Protéger pare-feu de la zone interne).
11) Cliquez sur **Advanced** pour ajouter si nécessaire des emplacements ou des protocoles numériques au pare-feu (**ports TCP**, **ports UDP**, **ports RPC** et **protocoles IP**). Pour finir, cliquez deux fois sur OK.
12) Cliquez sur **Next** (suivant). Les paramètres choisis pour le pare-feu s'affichent. Si nécessaire, vous pouvez consultez des informations supplémentaires à l'aide de **Show Details** (afficher détails).
13) Cliquez sur **Terminer**.

19.2 Cryptage de la signalisation et de la charge utile (SPE)

SPE sert à la sécurité lors de la transmission des données de signalisation et de la charge utile entre téléphones système IP et le système de communication. La fonctionnalité repose sur un processus de cryptage asymétrique où l'on utilise des clés publiques et privées.

Cryptage de données de signalisation et des données utiles

- Cryptage de la signalisation : la transmission du signal entre passerelle et clients est effectuée avec une clé 128 bits. Pour la transmission, on utilise le protocole TLS avec cryptage AES.
- Cryptage de la charge utile : les données utiles, également appelées données Voix ou charge utile, sont transmises à l'aide du protocole SRTP (Secure Real-time Transport Protocol). Elles sont cryptées à l'aide d'une clé 128 bits (AES). SRTP est également utilisé pour les réseaux IP. La procédure d'échange des clés pour SRTP s'appelle Multimedia Internet Keying, en abrégé MIKEY.

Pour SPE, il faut garantir l'identification univoque des téléphones système et des systèmes de communication associés. Cela est réalisé par des certificats qui fournissent également les clés publiques.

Les clés et les certificats sont distribués par le serveur DLS (distribution manuelle également possible).

Conseil : La fonctionnalité SPE n'est pas disponible pour les abonnées SIP et WL2.

Une connexion cryptée ne peut être établie que dans le cadre d'une liaison directe entre deux téléphones système ou pour les conférences.

Cryptage SRTCP

Le protocole SRTCP (Secure Real-Time Transport Control Protocol) est une extension du protocole SRTP et il assure la sécurité des données de gestion. L'extension comprend trois champs supplémentaires : un index SRTPC, un drapeau de cryptage et un tag d'authentification.

Conformité SPE

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

Légende :

Cryptage de la signalisation	
nv	Aucune sécurité VoIP
t	Par défaut : TLS côté VoIP ; pas de End-to-end Secure Payload (charge utile sécurisée de bout en bout)
s	Cryptage de la signalisation et de la charge utile (SPE)
*	Pas de End-to-end Signaling Encryption (cryptage de la signalisation de bout en bout) (TLS)
Payload Encryption (cryptage de la charge utile)	
y	Secure Payload (charge utile sécurisée) (SRTP)
n	Non-Secure Payload (charge utile non sécurisée) (RTP)

19.2.1 Comment activer ou désactiver SPE

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez utiliser le cryptage de la signalisation et de la charge utile, cochez la case **Assistance SPE**.
   - Si vous souhaitez désactiver le cryptage de la signalisation et de la charge utile, décochez la case **Assistance SPE**.
5) Cliquez sur **Appliquer** puis sur **OK**.

19.2.2 Comment modifier les paramètres de sécurité modification

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Sécurité** > **Signaling and Payload Encryption (SPE)** (Cryptage de la signalisation et de la charge utile).
3) Dans l'onglet **Modifier les paramètres de sécurité SPE**, **Longueur minimale de la clé RSA**, sélectionnez la longueur de clé minimale du protocole de sécurité (512, 1024 ou 2048).
4) Sélectionnez l'entrée **Contrôle de certificat avec contrôle CRL** si vous souhaitez une harmonisation avec les listes CRL (listes de révocation des certificats).

5) Dans **Intervalle max. de renouvellement de clé (Heures)**, indiquez l'intervalle (en heure) à l'issue duquel les paires de clés sont de nouveau attribuées.
6) Cliquez sur **Appliquer**.

19.2.3 Comment importer le certificat SPE et la clé privée (PKCS#12)

Si aucun certificat spécifique client n'est disponible,il est possible via SSL > Génération de certificats de générer un certificat CA signé par soi-même et ainsi de créer et enregistrer un certificat de serveur signé par CA (PKCS#12). Celui-ci est ensuite importé pour SPE.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Sécurité** > **Signaling and Payload Encryption (SPE)** (Cryptage de la signalisation et de la charge utile).
3) Dans Arborescence du menu, allez à **Certificat SPE**.
4) Dans **Importer le certificat SPE et la clé privée (PKCS#12)**, dans le champ **Mot de passe de déchiffrement**, entrez le mot de passe obtenu lorsque l'on a généré le fichier.
5) Dans **Fichier avec certificat et clé privée (format PEM ou PKCS#12)**, entrez le fichier de certificat ou le sélectionnez dans les répertoires à l'aide de **Parcourir**.

   Conseil : Lorsque vous installez pour la première fois un certificat alors que le cryptage SPE est activé, il est ensuite effectué automatiquement une réinitialisation !

6) Cliquez sur **Afficher l'empreinte digitale du certificat** si vous voulez contrôler l'intégrité.

19.2.4 Comment importer le certificat CA SPE

Cette étape n'est pas nécessaire lorsque l'on utilise des certificats qui ont été eux-mêmes été créés dans **Génération de certificats SSL**.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Sécurité** > **Signaling and Payload Encryption (SPE)** (Cryptage de la signalisation et de la charge utile).
3) Dans Arborescence du menu, allez à **Certificats CA SPE**.

4) Dans la fenêtre **Importer le certificat CA de confiance pour SPE (fichier X.509)**, dans **Fichier avec certificat (fichier PEM ou binaire)**, entrez le nom du fichier de certificat ou sélectionnez le fichier à l'aide de **Parcourir**.
5) Dans **Protocole CRL Distribution Point (CDP)**, sélectionnez le protocole des listes CRL (listes de révocation de certificats)(**LDAP** ou **HTTP**).
6) Dans **CDP (sans par ex. ldap://)** sélectionnez le serveur souhaité.
7) Cliquez sur **Afficher l'empreinte digitale du certificat**.

19.2.5 Comment activer ou désactiver SPE pour un abonné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, sélectionnez **Abonnés** > **Abonnés** > **Clients IP** pour accéder à l'abonné souhaité (client système)
3) Dans la fenêtre **Abonnés**, onglet **Modifier les paramètres de l'abonné**, allez à **Payload Security** (sécurité charge utile).
4) Sélectionnez une des possibilités suivantes :
   - Si vous voulez activer la fonction, sélectionnez dans **Payload Security** (Sécurité charge utile) l'entrée **Activé**.
   - Si vous voulez désactiver la fonction, sélectionnez dans **Payload Security** (Sécurité charge utile) l'entrée **Désactivé**.
5) Cliquez sur **Appliquer**.

19.3 Virtual Private Network VPN

Un réseau privé virtuel (VPN) est un réseau d'ordinateurs qui utilise un réseau public (par ex. Internet) pour le transport de données privées. Il permet ainsi une transmission sûre via un réseau qui n'est pas sûr. Le transfert des données se fait de façon chiffrée.

Présentation du VPN

VPN offre :

- Liaison sécurisée par un support non protégé (Internet)
- Protection des données confidentielles contre une manipulation
- Intégration sécurisée de partenaires externes dans le réseau d'entreprise
- Accès aux informations sur l'entreprise pour le service externe

Pour que la communication puisse se dérouler de façon sécurisée, VPN procède comme suit : un tunnel est établi entre les partenaires de communication. Lors de cet établissement de tunnel, il y a authentification et autorisation. Après l'établissement du tunnel, les données à proprement parler sont transférées de manière cryptée.

Un VPN peut être établi entre (au moins) deux ordinateurs ou réseaux (extrémités de tunnel).

Il existe 2 types de mise en réseau :

- Site-to-Site-VPN

  Le chiffrement entre deux passerelles VPN a lieu ici ; au sein du LAN, les données sont transférées de façon non cryptée.

- Réseau VPN End-to-Site

  VPN d'accès à distance (accès à distance de collaborateurs mobiles)

Informations spécifiques du système

L'administration des paramètres VPN est assurée principalement à l'aide de l'Assistant VPN.

Attention : la liaison avec le système de communication doit être effectuée à l'aide d'une connexion sécurisée par SSL. Celle-ci est réalisée via OpenSwan et OpenSSL.

Correspondances

Rubrique	Correspondance
DynDNS	Les points terminaux VPN doivent pouvoir être joints à l'aide d'un nom de domaine ou d'une adresse IP fixe. Si ce n'est pas le cas, on peut utiliser DynDNS.
DynDNS	Si une adresse IP se modifie pour le VPN, le système de communication actualise les données relatives au nom d'hôte (adresse IP) dans DynDNS.
DNS	Chaque partenaire VPN peut effectuer une résolution du nom d"hôte / de l'adresse IP à l'aide du protocole DNS standard. Tous les noms DNS (par ex. Nom d'hôte) doivent être des noms de domaines entièrement qualifiés (FQDN). Pendant l'actualisation de l'adresse IP par DNS, aucune liaison n'est possible par les tunnels IPSec.

19.3.1 Exigences pour VPN

Afin de garantir la qualité de transmission de la voix et des données, les réseaux utilisés doivent répondre à certaines exigences. En ce qui concerne le cryptage en particulier, il faut prévoir une bande passante plus importante que pour un autre type de mise en réseau.

Pour les exemples suivants des tableaux, on a utilisé comme mode de cryptage le "mode tunnel ESP avec authentification". Ce mode offre la sécurité la plus élevée aux VPN site-à-site.

Structure d'un paquet voix crypté :

Longueur de l'en-tête ESP

Padding

Calcul de bande passante pour l'algorithme de cryptage AES :

Calcul de bandes passantes pour l'algorithme de cryptage DES / 3DES :

Bande passante pour fax T.38

Protocole	octets	
Trailer ESP	12	
Padding ESP	varie (y)	crypté
En-tête padding ESP	2	crypté
Charge utile Voix	varie (x)	crypté
RTP	12	crypté
UDP	8	crypté
IP (original)	20	crypté
En-tête ESP	8 + iv	
IP (tunnel)	20	
802.1Q VLAN Tagging	4	
MAC (y compris préambule, FCS)	26	
Total	**112 + iv + x + y**	

La longueur de l'en-tête ESP dépend de l'algorithme de cryptage utilisé.

Nécessaire pour le Cipher Block Chaining (chaînage de blocs de chiffres). L'en-tête ESP comprend un vecteur d'initialisation (IV). La longueur de l'IV est identique à la longueur du bloc de chiffres.

Le padding (remplissage) est nécessaire car les algorithmes de cryptage reposent sur le chiffrement de bloc. Cela signifie que toute la partie cryptée du paquet (En-tête original IP/UDP/RTP + charge utile voix + padding en-tête ESP) est doit être un multiple entier de la longueur de bloc de chiffres.

Longueur du bloc de l'algorithme de cryptage :

Algorithme de cryptage	Longueur du bloc	Longueur iv du vecteur d'initialisation
AES	16 octets (128 bits)	16 octets (128 bits)
3DES	8 octets (64 bits)	8 octets (64 bits)

Calcul des octets de padding nécessaires pour les paquets voix.

(42 + x + y) (octets) = N x (0 ou 16 (octets)) (N entier)

Codec	Paramètre de mise en paquet	Taille de la trame (ms)	Charge utile (octets)	Padding (octets)	Longueur des paquets Ethernet (octets)	Rapport charge utile/ surdébit de paquet	Charge Ethernet (y compris) en-tête (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

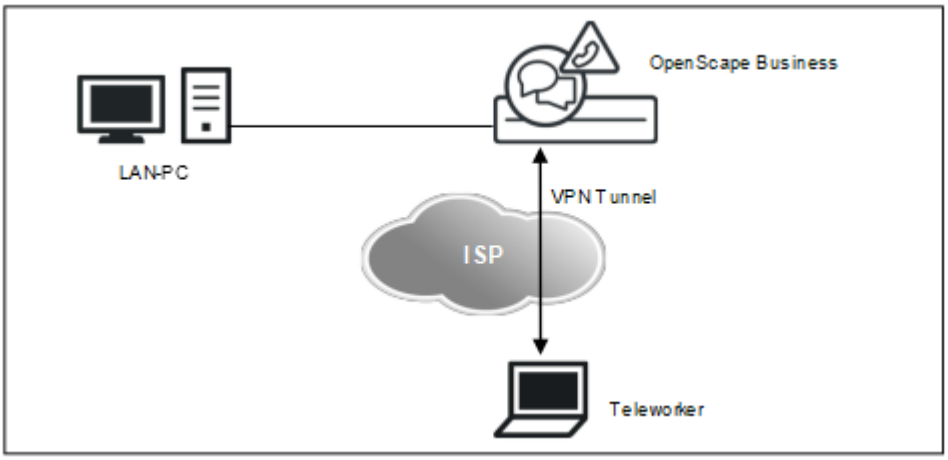
Codec	Paramètre de mise en paquet	Taille de la trame (ms)	Charge utile (octets)	Padding (octets)	Longueur des paquets Ethernet (octets)	Rapport charge utile/ surdébit de paquet	Charge Ethernet (y compris) en-tête (kbit/s)
G.711	20	20	160	6	286	75%	114,4
G.711	30	30	240	6	366	50%	97,6
G.711	40	40	320	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

Algorithme de cryptage	Taille de trame (ms)	Charge utile y (octets)	Padding x (octets)	Longueur des paquets Ethernet (octets)	Charge utile paquet (surdébit en pourcentage)	Charge Ethernet (y compris) en-tête (kbit/s)
DES / 3DES	30	169	1	278	64%	74,1
AES	30	169	9	294	74%	78.3

19.3.2 Connexion des télétravailleurs via VPN

Grâce à une liaison sécurisée via VPN, les télétravailleurs peuvent être raccordés au système de communication.

Système autonome avec connexion des télétravailleurs via VPN



Le système de communication dispose d'une fonctionnalité VPN intégrée (configuration par assistant). Jusqu'à 10 télétravailleurs par système de communication peuvent être simultanément actifs via VPN.

Les clients VPN suivants sont validés pour OpenScape Business :

- client NCP VPN
- client VPN Shrew Soft
- client VPN Android
- client iOS VPN
- client Mac OS-X VPN

Comment exporter les données de télétravailleur

Les données de télétravailleur peuvent être exportées sous forme de fichier ZIP (non crypté). Dans le fichier ZIP figure, pour chaque client VPN supporté, un fichier texte individuel avec les données de télétravailleur. Pour le client NCP VPN sous la forme d'un fichier `.ini`, pour le client Shrew Soft VPN sous la forme d'un fichier `.vpn` et pour le client OS-X VPN sous la forme d'un fichier `.networkConnect`. Ces fichiers texte peuvent être importés sur client VPN.

Conseil : Les inflexions ou accents éventuels ne sont pas traités dans les fichiers texte contenant les données de télétravailleur. Les caractères vides sont remplacés par des traits de soulignement.

Affichage de l'état des connexions VPN

Vous trouverez un affichage d'état de toutes les connexions VPN dans l'assistant **VPN**. Vous trouverez un aperçu détaillé de toutes les connexions VPN dans **Centre de service**, sous **Diagnostic** > **Etat** > **Etat du réseau VPN**.

VPN avec OpenScape Business S

Avec OpenScape Business S, un routeur externe termine le VPN. Le description des applications externes ne fait pas partie de ces instructions.

19.3.2.1 Comment configurer la connexion des télétravailleurs via VPN

L'Assistant **VPN** permet, via le VPN (Virtual Private Network), de donner aux télétravailleurs (partenaires VPN) l'accès au LAN interne et de connecter les systèmes de communication via VPN. Si le système de communication ne dispose pas d'une adresse IP externe fixe (adresse IP publique, adresse IP globale), il faut paramétrer un service DynDNS, par ex. sur www.DynDNS.org.

Conditions préalables

L'accès Internet via l'interface WAN est configuré.

Si l'interface WAN ne dispose pas d'adresse IP (publique) fixe, il faut alors que DynDNS soit configuré. Pour réaliser le test DynDNS, il faut une connexion Internet.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Configuration VPN**. Paramètre par défaut : **VPN désactivé**.
4) Cliquez sur **Configurer via VPN**.
5) Si vous voulez modifier une connexion VPN, cliquez sur **Modifier** pour la connexion VPN concernée.
6) Si vous voulez créer une nouvelle connexion VPN, cliquez sur **Ajouter**.
7) Dans le champ **Nom du système**, donnez un nom à la connexion VPN (par ex. `node2mch.dyndns.org`).
8) Entrez éventuellement un **commentaire** dans le champ prévu.
9) Cochez la case **activé** (paramètre par défaut).
10) Cochez la case **Utiliser les données du système personnel**.
11) Si nécessaire, sélectionnez le **Type d'adresse** :
    - Si l'interface WAN dispose d'une adresse IP fixe (publique), sélectionnez dans la liste déroulante **Type d'adresse** l'entrée **Adresse IP** et indiquez l'adresse IP fixe (publique) dans **Adresse IP globale / Nom DNS (WAN)**.
    - Si l'interface WAN ne dispose pas d'une adresse IP fixe (publique), sélectionnez dans la liste déroulante **Type d'adresse** l'entrée **Nom DNS**. Dans **Adresse IP globale / Nom DNS (WAN)**, il est affiché le nom DNS du système de communication déjà configuré pour DynDNS.
12) Si nécessaire seulement, modifiez l'**adresse IP locale (LAN)**.
13) Si nécessaire seulement, modifiez le**masque de sous-réseau local (LAN)**.
14) Si vous voulez modifier un télétravailleur déjà paramétré, cliquez dans **Télétravailleurs** sur **Modifier** pour le télétravailleur souhaité.
15) Si vous souhaitez configurer un nouveau télétravailleur, dans **Télétravailleurs**, cliquez sur **Ajouter**.
16) Dans le champ **Nom**, donnez un nom pour la configuration de ce télétravailleur.

17) Configurez le type de client VNP utilisé :

- Pour les télétravailleurs purement IPSec-VPN (clients NCP et Shrew Soft VPN) :

  Décochez la case **L2TP/IPSec**, sélectionnez comme **Type d'adresse**, l'entrée **Adresse IP**. Dans le champ **Adresse IP virtuelle /Nom DynDNS**, indiquez une adresse IP virtuelle pour le télétravailleur lorsque le client utilisé supporte des adresses IP virtuelles (indépendamment du fait que le télétravailleur établit sa connexion Internet avec un routeur DSL ou un modem DSL).
- Pour les télétravailleurs L2TP/IPSec-VPN (clients VPN iOS, Android et MAC OS X) :

  Cliquez la case **L2TP/IPSec** et attribuez le **nom utilisateur** et le **mot de passe** pour le télétravailleur.

18) Cochez la case **activé** (paramètre par défaut).

19) Cliquez sur **OK**. Le système affiche de nouveau la fenêtre avec un aperçu des télétravailleurs. Vous pouvez entrer d'autres télétravailleurs.

20) Une fois que vous avez paramétré tous les télétravailleurs, cliquez sur **OK & Suivant**. La fenêtre **Sélectionner le système** s'affiche.

21) Cliquez sur **OK&Suite**. La fenêtre **Paramètres de sécurité pour les liaisons** s'ouvre.

22) Attribuez à la connexion VPN qui vient d'être configurée une clé pour une connexion sécurisée dans **Secret prépartagé** et répétez cette clé dans **Répéter le secret prépartagé**. La clé doit comporter au moins 20 caractères.

23) Entrez si nécessaire un encore un **commentaire**.

24) Cliquez sur **OK**. Le système affiche la fenêtre **Informations sur l'état du VPN**.

25) Cliquez sur **Démarrer le VPN**.

26) Seulement s'il a été sélectionné comme type d'adresse Nom DNS : contrôlez les données déjà configurées du compte DynDNS et cliquez sur **Test connexion**. Les données d'accès DynDNS sont transmises au fournisseur de service. Cette opération dure environ 10 secondes. Si le test n'est pas effectué avec succès, vérifiez de nouveau vos données d'accès. Une fois le test effectué avec succès, cliquez sur **OK**.

27) Cliquez sur **OK&Suite**. Les télétravailleurs utilisent maintenant l'interface WAN du système de communication.

28) Cliquez sur **Quitter**.

19.3.2.2 Comment exporter les données des télétravailleurs

L'assistant **VPN** vous permet d'exporter les données de télétravailleur.

Conditions préalables

Une connexion VPN est configurée.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Configuration VPN**. Paramètre par défaut : **VPN désactivé**.
4) Cliquez sur **Exporter/Importer**.
5) Dans **Exporter les données de télétravailleur du système**, cliquez sur **Exporter**. Sauvegardez le fichier ZIP dans un répertoire de votre choix.

Conseil : Dans le fichier ZIP figure pour chaque client VPN supporté un fichier propre avec les données de télétravailleur. Les données télétravailleur ne sont pas cryptées. Veuillez utiliser les données de manière responsable.

---

6) Cliquez sur **OK&Suite** puis sur **Quitter**.

19.3.3 Mise en réseau de système de communication via VPN

Plusieurs systèmes de communication OpenScape Business peuvent être mis en réseau de manière sécurisée à l'aide d'un réseau VPN Site-to-Site.

Mise en réseau par VPN

Dans un système de communication, vous avez la possibilité de configurer les données permettant la mise en réseau de plusieurs systèmes, d'exporter sous formes cryptée ces données de topologie et de les importer dans tous les autres systèmes faisant partie de cette interconnexion de réseaux. Cela permet de disposer d'une configuration rapide et cohérente dans tous les systèmes de l'interconnexion de réseaux.

La différenciation entre les systèmes propres et les systèmes étrangers se fait par reconnaissance du propre nom DynDNS ou (lorsque l'on utilise des adresses IP fixes) via la propre adresse Internet.

- Exporter les données de télétravailleur du système
  - Toutes les données relatives à la mise en place du réseau VPN sont regroupées sous la forme d'un fichier XML crypté et fournies sous la forme d'un fichier ZIP pour exportation en direction d'un autre système.
- Importer les données de topologie dans le système
  - Toutes les données relatives à la mise en place du réseau VPN peuvent être importées sous la forme d'un fichier ZIP (contenant le fichier XML crypté) et être reprises pour ce système.

La clé (mot de passe) pour l'exportation est sélectionnable librement et doit être communiquée à un autre administrateur qui souhaite importer ces paramètres.

Affichage de l'état des connexions VPN

Vous trouverez un affichage d'état de toutes les connexions VPN dans l'assistant **VPN**. Vous trouverez un aperçu détaillé de toutes les connexions VPN dans **Centre de service**, sous **Diagnostic** > **Etat** > **Etat du réseau VPN**.

19.3.3.1 Comment configurer la mise en réseau via un VPN

L'assistant **VPN** vous permet de configurer tous les systèmes de communication du réseau VPN dans un système. Vous pouvez exportez ces données de topologie et les importer sur tous les systèmes de l'interconnexion de réseaux VPN.

Conditions préalables

L'accès Internet via l'interface WAN est configuré.

Si l'interface WAN ne dispose pas d'adresse IP (publique) fixe, il faut alors que DynDNS soit configuré. Pour réaliser le test DynDNS, il faut une connexion Internet.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Configuration VPN**. Paramètre par défaut : **VPN désactivé**.
4) Cliquez sur **Configurer via VPN**.
5) Cliquez sur **Ajouter**.
6) Dans le champ **Nom du système**, donnez un nom au premier système de l'interconnexion de réseaux VPN (par ex. `node1mch.dyndns.org`).
7) Entrez éventuellement un **commentaire** dans le champ prévu.
8) Cochez la case **activé** (paramètre par défaut).
9) Cochez la case **Utiliser les données du système personnel**. Les champs suivants sont complétés avec les données du système.
10) Si nécessaire seulement, sélectionnez le **Type d'adresse** prédéfini :
    - Si l'interface WAN dispose d'une adresse IP fixe (publique), sélectionnez dans la liste déroulante **Type d'adresse** l'entrée **Adresse IP** et indiquez l'adresse IP fixe (publique) dans **Adresse IP globale / Nom DNS (WAN)**.
    - Si l'interface WAN ne dispose pas d'une adresse IP fixe (publique), sélectionnez dans la liste déroulante **Type d'adresse** l'entrée **Nom DNS**. Dans **Adresse IP globale / Nom DNS (WAN)**, il est affiché le nom DNS du système de communication déjà configuré pour DynDNS.
11) Si nécessaire seulement, modifiez l'**adresse IP locale (LAN)** prédéfinie.
12) Si nécessaire seulement, modifiez le**masque de sous-réseau local (LAN)** prédéfini.
13) Cliquez sur **OK&Suite**. La fenêtre **Sélectionner le système** s'affiche.
14) Cliquez de nouveau sur **Ajouter**.
15) Dans le champ **Nom du système**, donnez un nom au second système de l'interconnexion de réseaux VPN (par ex. `node2mch.dyndns.org`).
16) Entrez éventuellement un **commentaire** dans le champ prévu.
17) Cochez la case **activé** (paramètre par défaut).

18) Sélectionnez le **Type d'adresse** du second système :
    - Si l'interface WAN dispose d'une adresse IP fixe (publique), sélectionnez dans la liste déroulante **Type d'adresse** l'entrée **Adresse IP** et indiquez l'adresse IP fixe (publique) dans **Adresse IP globale / Nom DNS (WAN)**.
    - Si l'interface WAN ne dispose pas d'une adresse IP fixe (publique), sélectionnez dans la liste déroulante **Type d'adresse** l'entrée **Nom DNS**. Dans **Adresse IP globale / Nom DNS (WAN)**, il est affiché le nom DNS du système de communication déjà configuré pour DynDNS.
19) Entrez l'**adresse IP locale (LAN)** du second système.
20) Entrez le **Masque de sous-réseau local (LAN)** du second système.
21) Cliquez sur **OK&Suite**. La fenêtre **Sélectionner le système** s'affiche.
22) Répétez les étapes 14 à 21 pour les autres systèmes de l'interconnexion de réseaux VPN.
23) Pour terminer, cliquez sur **OK&Suivant** La fenêtre **Paramètres de sécurité pour les liaisons** s'ouvre.
24) Pour chaque connexion VPN d'un système vers l'autre, attribuez une propre clé dans **Secret prépartagé** et répétez cette clé dans **Répéter le secret prépartagé**. La clé doit comporter au moins 20 caractères.
25) Entrez si nécessaire un **commentaire** pour chaque connexion VPN.
26) Cliquez sur **OK**. Le système affiche la fenêtre **Informations sur l'état du VPN**.
27) Cliquez sur **Exporter/Importer** pour exporter les données de topologie. La fenêtre **Exporter et importer les données de configuration VPN** s'affiche.
28) Dans **Exporter les données de topologie du système**, **Clé** et **Répéter la clé**, attribuez une clé (au moins 7 caractères) pour la sécurisation des données et cliquez sur **Exporter**. Sauvegardez le fichier ZIP dans un répertoire de votre choix.
29) Cliquez sur **OK&Suite**.
30) Cliquez sur **Démarrer le VPN**.
31) Seulement s'il a été sélectionné comme type d'adresse **Nom DNS** : contrôlez les données déjà configurées du compte DynDNS et cliquez sur **Test connexion**. Les données d'accès DynDNS sont transmises au fournisseur de service. Cette opération dure environ 10 secondes. Si le test n'est pas effectué avec succès, vérifiez de nouveau vos données d'accès. Une fois le test effectué avec succès, cliquez sur **OK**.
32) Cliquez sur **OK&Suite** puis sur **Quitter**.
33) Dans WBM du deuxième système, dans la barre de navigation, cliquez sur **Configuration** et dans l'arborescence de navigation sur **Assistants** > **Réseau / Internet**.
34) Cliquez sur **Modifier** pour lancer l'Assistant **Configuration VPN**. Paramètre par défaut : **VPN désactivé**.
35) Cliquez sur **Exporter/Importer** pour importer les données de topologie. La fenêtre **Exporter et importer les données de configuration VPN** s'affiche.
36) Cliquez sur **Importer les données de topologie dans le système** pour importer des données de topologie.
37) Entrez la **Clé** (mot de passe) que vous avez entrée lors de l'exportation des données sur le premier système.

38) Naviguez jusqu'à l'emplacement de stockage du fichier ZIP. Cliquez ensuite sur **Importer**.
39) Cliquez sur **OK&Suite**. Vous voyez les systèmes configurés.
40) Cliquez sur **Démarrer le VPN**.
41) Seulement s'il a été sélectionné comme type d'adresse **Nom DNS** : contrôlez les données déjà configurées du compte DynDNS et cliquez sur **Test connexion**. Les données d'accès DynDNS sont transmises au fournisseur de service. Cette opération dure environ 10 secondes. Si le test n'est pas effectué avec succès, vérifiez de nouveau vos données d'accès. Une fois le test effectué avec succès, cliquez sur **OK**.
42) Cliquez sur **OK&Suite** puis sur **Quitter**.
43) Répétez les étapes 33 à 42 pour les autres systèmes de l'interconnexion de réseaux VPN.

19.3.3.2 Comment exporter et importer les données de topologie d'une interconnexion de réseaux VPN

A l'aide de l'assistant **VPN**, vous pouvez exporter et importer les données de topologie du réseau via VPN.

Conditions préalables

Une connexion VPN est configurée.

Pour importer les données de topologie, vous devez connaître la clé attribuée lors de l'exportation.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Réseau/ Internet**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Configuration VPN**. Paramètre par défaut : **VPN désactivé**.
4) Cliquez sur **Exporter/Importer**.
5) Si vous voulez exporter les données de topologie, dans **Exporter les données de topologie du système**, **Clé** et **Répéter la clé**, attribuez une clé (au moins 7 caractères) pour la sécurisation des données et cliquez sur **Exporter**. Sauvegardez le fichier ZIP dans un répertoire de votre choix.
6) Si vous voulez importer les données de topologie, dans **Importer les données de topologie du système**, **Clé**, indiqué la clé de décryptage des données et naviguez jusqu'à l'emplacement de stockage du fichier ZIP. Pour finir, cliquez sur **Importer**.
7) Cliquez sur **OK&Suite** puis sur **Quitter**.

19.3.4 Mécanismes de sécurité VPN

Le chiffrement des données se fait pour VPN par différents mécanismes de sécurité comme Tunnel IPSec, associations de sécurité et méthodes d'authentification (Peer-to-Peer, signatures numériques).

Tunnel IPSec

IPSec sert à chiffrer les données et peut être utilisé en général avec et sans tunnel. IPSec est une possibilité pour réaliser VPN. Avec elle, il est possible de chiffre l'ensemble du paquet IP y compris l'en-tête IP : cela se fait en mode Tunnel.

Les tunnels doivent toujours être configurés chez les deux partenaires VPN.

Pour IPSec, la gestion de chiffrement automatique Internet Key Exchange (IKE) peut être utilisée. Il s'agit d'un standard qui est intégré à IPSec.

Security Associations SA

IKE-SA

SA de charge utile

Authentification

Une association de sécurité SA (Security Association) est une convention entre deux unités qui communiquent dans les réseaux d'ordinateurs. Elle décrit comment les deux parties appliquent les services de sécurité pour communiquer l'un avec l'autre.

Les liaisons VPN nécessitent toujours trois associations de sécurité SA qui sont négociées en deux phases :

- Phase 1 - Etablir la SA IKE

  Une pour l'authentification réciproque du début et pour l'échange des clés de session (IKE-SA)

- Phase 2 - Négocier les SA de charge utile

  Une par faisceau de la liaison établie pour le trafic de charge utile (SA de charge utile)

Le protocole IKE a pour l'essentiel deux tâches différentes. Il faut d'abord constituer une SA exclusivement utilisée par le protocole IKE (IKE-SA). Le système utilise ensuite la IKE-SA disponible pour gérer de manière sécurisée toutes les autres SA nécessaires au transfert des données utiles. IKE opère par conséquent en deux phases successives :

Lors de l'établissement de la liaison entre les partenaires VPN, divers paramètres doivent être négociés (par ex. fréquence de la génération de nouvelle clé ou mode de chiffrement utilisé). Ces paramètres sont enregistrés et gérés dans les SA IKE.

La phase IKE 2 sert à négocier tous les paramètres de sécurité pour les SA de charge utile entre les partenaires VPN.

Il faut toujours que deux SA soient établies, pour le transfert et la réception.

Pour l'essentiel, les opérations suivantes sont exécutées :

- Négocier les algorithmes pour le chiffrement et l'authentification
- Négocier les protocoles de sécurité appliqués (ESP et AH)
- Négocier le mode de fonctionnement des protocoles de sécurité
- Négocier la durée de vie de la SA
- Définir le matériel de clés

Dans VPN une communication Peer-to-peer a lieu. L'authentification des partenaires VPN se fait de deux façons :

- Clés pré-partagées

  La plupart du temps, dans VPN, ce sont aussi des clés distribuées auparavant (Preshared Keys) qui sont utilisées. Pour cela, une paire de clés est configurée pour chaque partenaire VPN. A partir de ces clés, une valeur de hachage est constituée pour l'authentification ; elle est contrôlée par le partenaire.
- Signatures numériques

  Un certificat est affecté à chaque partenaire VPN. Pour la réussite de l'authentification, les partenaires VPN aux deux extrémités du tunnel doivent contrôler la signature numérique du partenaire opposé pour être sûr que le CA soit de confiance.

Informations spécifiques du système

L'administration des paramètres VPN est assurée principalement à l'aide de l'Assistant.

Attention : la liaison administrateur avec doit être effectuée à l'aide d'une connexion sécurisée par SSL.

- Security Associations SA

  Le système de communication supporte les groupes Oakley 1, 2 et 5
- IPSec

  Le système de communication utilise le mode tunnel IPSec avec ESP (Encapsulating Security Payload). ESP est un protocole IPSec qui garantit le cryptage, l'intégrité et l'authenticité des paquets.
- SA de charge utile

  Le système de communication supporte les algorithmes de chiffrement DES, 3DES et AES

  Parmi les groupes connus d'algorithmes MAC (MAC=Message Authentication Codec) pour l'authentification de l'origine et de l'intégrité des donnés, HMAC-SHA1, HMAC-SHA2 et HMAC-MD5.
- Modes de fonctionnement conseillés
  - IKE en "mode principal" avec Perfect Forward Secrecy
  - Fonction de hachage avec SHA-2
  - Authentification avec certificats (RSA)
  - chiffrement avec AES (jusqu'à 256 bits)
  - support d'adresses IP publiques dynamiques par des adresses IP virtuelles ou des mécanismes d'actualisation DynDNS pour les PC des télétravailleurs

19.3.5 Certificats VPN

Un certificat associe une certaine clé publique à un certain client VPN ; le client peut être aussi bien un client du système de communication qu'un télétravailleur. La combinaison univoque entre clé publique et client VPN est la base de l'opération d'authentification.

Certificats et centre de certification

Lightweight CA

CRL Certificate Revocation Lists - Listes de révocation de certificats

Les certificats sont signés numériquement et émis par un centre de certification (CA). IPSec accepte un certificat lorsqu'il est émis par un centre de certification de confiance.

Dans un environnement VPN simple, la définition d'un seul centre de certification peut être suffisante ; ce CA fonctionne comme centre de certification racine de confiance pour l'ensemble du VPN et s'identifie par rapport à tous les clients VPN grâce à son certificat CA signé par lui-même.

Chaque client VPN a besoin d'un certificat émis par ce CA.

Les certificats à la norme X.509 (le standard le plus répandu aujourd'hui) incluent les éléments principaux suivants :

- Informations sur l'identité du propriétaire du certificat
- Clé publique du propriétaire du certificat
- Informations sur le CA qui a signé le certificat (numéro de série, durée de validité, informations sur l'identité du CA ainsi que sur la signature numérique du CA)

Pour les environnements dans lesquels le client n'utilise par déjà un PKI, une fonctionnalité CA Lightweight aide à la certification. Le CA Lightweight offre les possibilités suivantes :

- Créer des paires de clés privés/publiques
- Signer et émettre les certificats correspondants
- Enregistrer des paires de clés avec les certificats correspondants dans des fichiers

Dans la cryptographie, on appelle PKI (Public-Key-Infrastructure) un système qui permet d'émettre, de distribuer et de contrôler des certificats numériques.

Une situation critique se produit lorsqu'un certificat est connu (ou soupçonné d'être connu) et que ce certificat n'a plus la confiance pour l'authentification Peer. Dans ce cas, le centre de certification doit révoquer le certificat et tous les Peers doivent être informés le plus tôt possible de cette révocation. La tentative d'un Peer distant d'authentifier son identité à l'aide d'un certificat révoqué est rejetée.

Généralement, une CRL est une liste de tous les certificats révoqués. Les CRL doivent toujours être crées par la CA dont émanent les certificats.

Une CRL contient les éléments principaux suivants :

- Liste des certificats révoqués ; l'identification des certificats se fait par les numéros de série
- Moment de la publication de la prochaine CRL actualisée (indication de la durée de validité de la CRL)
- Informations sur le CA qui a généré le certificat (informations sur l'identité du CA ainsi que sur la signature numérique du CA)

Une actualisation et une distribution régulières des CRL doivent être réalisées manuellement par l'administrateur.

Informations spécifiques du système

L'authentification se fait sur la base d'algorithmes de cryptographie avec des clés publiques. Le système de communication supporte RSA comme algorithme de cryptographie avec des clés publiques. Le système de communication supporte uniquement les certificats qui sont conformes à la norme X.509.

Le système de communication agit pour l'authentification toujours comme client VPN.

- Lightweight CA

  Le système de communication offre une fonctionnalité CA restreinte (Lightweight CA). L'administrateur fournit pour un système le matériel de clés en importante manuellement par la liaison d'administration sécurisée SSL des paires de clés privées/publiques et des certificats dans tous les partenaires de communication impliqués.

- CRL

  Les CRL (Certificate Revocation Lists - liste de révocation de certificats) sont utilisées pour la révocation de certificats. L'importation de la CRL dans le système de communication se fait par l'administrateur via une liaison sécurisée SSL.

19.3.5.1 VPN - Comment générer les certificats Lightweight CA

Lightweight CA est une fonction sous licence servant à générer et gérer les certificats CA et Peer.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Lightweight CA**. Dans la fenêtre **Génération de certificats**, vous pouvez générer un propre certificat CA.
4) Attribuez dans **Nom du certificat** un nom au certificat demandé.
5) Dans **Numéro de série du certificat** attribuez un numéro de série pour le Certificat.

   Conseil : Un numéro de série déjà attribué ne peut pas être utilisé une nouvelle fois pour un autre certificat car le numéro de série de tous les certificats jamais générés doit être univoque.

6) Dans **Type d'algorithme de signature**, entrez l'algorithme souhaité pour le certificat (sha256RSA ou sha512RSA).
7) Dans **Longueur de la clé publique**, entrez la longueur de la clé publique (par ex. 2048).
8) Indiquez la date et l'heure de début de la période de validité dans **Début de la validité du certificat (GMT)**. La date est interprétée comme heure GMT (Greenwich Mean Time).

9) Entrez dans du sujet **Fin de la validité du certificat (GMT)** la date et l'heure de la fin de validité.
10) Dans **Demandeur**, entrez le **Pays (C)**, l'**Organisation (O)**, l'**Unité organisationnelle (OU)** et le **Nom général (CN)**.
11) En option, vous pouvez indiquer un autre demandeur dans **Autre nom de demandeur**. Vous devez ensuite indiquer un format (par ex. adresse IP ou nom DNS). La fenêtre de saisie dépend de la sélection du format.
12) Dans le champ **Point de distribution CRL** indiquez le point de distribution des listes CRL (affichage dans un menu déroulant).
13) Cliquez sur **Générer le certificat**.

19.3.5.2 VPN - Gestion des certificats - Comment afficher le certificat

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Gestion des certificats**. Le système ouvre la fenêtre **Afficher le certificat du fichier**.
4) Si nécessaire, cochez la case **Format PKCS#12**.
5) Entrez le **mot de passe de déchiffrement**.
6) Dans **Fichier avec le certificat**, entrez le fichier de certificat ou sélectionnez-en un par le champ **Parcourir**.
7) Cliquez sur **Charger**.

19.3.5.3 VPN - Comment importer le certificat CA Trusted (X.509)

X.509 est une norme pour les certificats. Sont également enregistrés dans le certificat le nom et la signature numérique de l'émetteur du certificat. X.509 fait partie du service d'annuaire X.500 pour systèmes distribués et ouverts dans le monde.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Gestion des certificats** > **Certificats CA Trusted** > **Certificats configurés**.
4) Attribuez dans **Nom du certificat** un nom au certificat demandé.
5) Dans le champ **Fichier avec le certificat**, entrez le fichier de certificat ou sélectionnez-en un par le champ **Parcourir**.
6) Confirmez et cliquez sur **Activer les tableaux VPN configurés.**

19.3.5.4 VPN - Certificats Peer - Comment générer une demande de certificat (CSR)

Vous pouvez générer un certificat Peer signé CA basé sur un certificat CA. Condition : au moins un certificat CA doit avoir été généré. Le certificat généré est enregistré dans un fichier PKCS#12. Les fichiers PKCS#12 (PKCS#12, Personal Information Exchange Syntax Standard) enregistrent les certificats avec la clé privée. Un fichier PKCS#12 contient ainsi les données décisives pour le déchiffrement et le chiffrement.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Certificats Peer**.
4) Dans l'onglet **Générer une demande de certificat (CSR)**, entrez les données nécessaires.
5) Entrez le **Nom de la demande de certificat**.
6) Dans **Type d'algorithme de signature**, entrez l'algorithme souhaité (sha256RSA ou sha512RSA).
7) Dans **Longueur de la clé**, entrez la longueur de la clé (2048).
8) Dans **Demandeur** entrez toutes les données de **Pays (C)**, **Organisation (O)**, **Unité organisationnelle (OU)** et **Nom général (CN)**.
9) Dans **Autre nom de demandeur** entrez le **Format du nom DNS**, ou bien un **Autre format** et l'**Autre nom de demandeur**.
10) Sauvegardez le fichier *.csr qui doit être signée par un CA.

19.3.5.5 VPN - Certificats Peer - Comment générer le certificat (PKCS#12)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Lightweight CA**.
4) Cliquez sur Certificat CA, puis sur **générer un certificat du pair signé CA (PKCS#12)**.
5) Entrez le **mot de passe de déchiffrement**.
6) Entrez un numéro de série de votre choix dans **Numéro de série du certificat**.
7) Dans **Longueur de la clé**, entrez la longueur de la clé (1024, 1536 ou 2048).

8) Indiquez la date et l'heure de début de la période de validité dans **Début de la validité du certificat (GMT)**. Cette indication est fournie en heure GMT (Greenwich Mean Time - Temps moyen de Greenwich).

Remarque : La durée de validité du certificat du pair devrait être soigneusement adaptée à la directive sécurité en vigueur dans l'entreprise. Un peu avant la fin de la période de validité, il faut prolonger le certificat ou bien établir un nouveau certificat.

---

9) Indiquez la date et l'heure de fin de la période de validité dans **Fin de la validité du certificat (GMT)**.
10) Dans **Demandeur** entrez toutes les données de **Pays (C)**, **Organisation (O)**, **Unité organisationnelle (OU)** et **Nom général (CN)**.
11) En option, vous pouvez indiquer un autre demandeur dans **Autre nom de demandeur**. Vous devez ensuite indiquer un format (par ex. adresse IP ou nom DNS). La fenêtre de saisie dépend de la sélection du format.
12) Entre le **Point de distribution CRL** (option).
13) Cliquez sur **Générer le certificat**.

19.3.5.6 VPN - Comment importer le certificat Peer (PKCS#12)

Les fichiers PKCS#12 (Personal Information Exchange Syntax Standard) enregistrent les certificats avec la clé privée. Un fichier PKCS#12 contient ainsi les données décisives pour le déchiffrement et le chiffrement.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Certificats Peer**.
4) Cliquez sur l'onglet **Importer le certificat Peer [PKCS#12]**.
5) Entrez un nom pour le certificat demandé dans **Nom du certificat**.
6) Dans **Mot de passe de déchiffrement** entrez votre mot de passe personnel pour décrypter ce certificat.
7) Dans le champ **Fichier avec le certificat**, entrez le nom du fichier ou recherchez le fichier avec le bouton **Parcourir**.
8) Cliquez sur **Afficher l'empreinte digitale du certificat**.
9) Cliquez sur **Importer le certificat du fichier**.

19.3.6 Clients VPN

A l'aide d'un tunnel VPN, un télétravailleur peut établir via Internet une connexion sécurisée VPN en direction du réseau de l'entreprise. Pour cela, il a besoin d'un client VPN sur son équipement (PC, tablette, smartphone). Toutes les données transmises entre le client VPN, le pare-feu de l'entreprise et le serveur VPN du système de communication sont cryptées.

Les clients VPN suivants sont supportés :

- **client NCP VPN**

  Les clients NCP peuvent être utilisés dans n'importe quel environnement VPN avec IPSec. C'est intéressant lorsqu'il faut accéder à partir d'un PC distant aux passerelles VPN de différents fabricants ou qu'une passerelle VPN centrale est déjà installée par un fabricant tiers dans le réseau d'entreprise. En cas de réseau de filiale, la passerelle NCP Secure Entreprise peut communiquer avec d'autres passerelles VPN sur la base de liaisons IPSec.

  Le client NCP est payant, mais il comprend une interface graphique et un affichage de l'état de la connexion.
- **Client VPN Shrew Soft**

  Le client VPN Shrew Soft est un client VPN gratuit avec interface graphique qui, à partir de la version 2.1.5, supporte également l'authentification hybride.

  Le client VPN Shrew Soft comprend notamment un support ISAKMP, Xauth et RSA, AES, Blowfish, les protocoles de cryptage 3DES et de nombreuses autres fonctionnalités qui ne se trouvent généralement que dans des solutions professionnelles.
- **Client VPN iOS et Android**

  Le système d'exploitation iOS ou Android a intégré le client VPN L2TP/IPSec.

  Les clients CPN L2TP/IPSec utilisent la plage d'adresses IP `10 254 253.x`. Si les adresses IP de cette plage sont déjà utilisées dans le réseau client, la plage des adresses IP doit être modifiée dans la WBM à l'aide de **Mode Expert** > **Maintenance** > **Diagnostics des applications** > **Test IPSec : programmes de test IPSec** > **Définir adresse IP pour L2TP** (par ex. De `10.254.253.1` à `10.254.252.1`).
- **Client Mac OS-X VPN**

  Le système d'exploitation MAC OS-X a intégré le client Mac OS-X-VPN.

Informations spécifiques du système

- Les données de télétravailleur d'un client VPN peuvent être exportées sous forme de fichier ZIP (non crypté). Dans le fichier ZIP figure, pour chaque client VPN supporté, un fichier texte individuel avec les données de télétravailleur. Pour le client NCP VPN sous la forme d'un fichier `.ini`, pour le client Shrew Soft VPN sous la forme d'un fichier `.vpn` et pour le client OS-X VPN sous la forme d'un fichier `.networkConnect`. Ces fichiers texte peuvent être importés sur client VPN.
- Infrastructure LAN avec plusieurs sous-réseaux

  Lorsque l'on doit utiliser un VPN dans une infrastructure LAN avec plusieurs sous-réseaux, il faut créer des règles pour ces sous-réseaux. Les règles ne peuvent pas être définies avec l'assistant, mais doivent être configurées en mode Expert.
- Tunnel-dans-Tunnel

  Il est impossible de créer un second tunnel VPN dans un tunnel VPN existant.

19.3.6.1 Paramètres du client NCP VPN

Pour une connexion VPN via le client NCP VPN, les paramètres indiqués ci-après doivent être respectés lorsque la configuration est réalisée manuellement. Via le système de communication, il es possible d'exporter un fichier texte `ncp_vpn.ini` avec les données client VPN configurées, et de l'importer sur client VPN. Ainsi, ces paramètres sont déjà configurés.

Configuration de base

- Nom du profil

  Choix libre, un nom évocateur est conseillé
- Type de liaison

  VPN vers poste IPSec
- Support de liaison

  Selon la liaison Internet utilisée

  par ex. LAN (via IP) ou xDSL (PPPoE)

Accès au réseau

Aucune configuration nécessaire.

Connexion HTTP

Aucune configuration nécessaire.

Modem

Aucune configuration nécessaire.

Gestion des lignes

- Etablissement de la liaison

  automatique ou manuel

  temporisation = 0

  Remarque : ainsi, la connexion n'est plus coupée en cas de vide !
- Priorité à la voix sur IP (VoIP)

  Cocher
- Authentification EAP

  Aucune configuration nécessaire
- Authentification HTTP

  Aucune configuration nécessaire

Paramètres IPSec

- Passerelle = adresse IP ou nom DNS du système de communication

  Vous pouvez accéder au système de communication par Internet à cette adresse IP ou sous ce nom DNS.

  Désignation dans l'Assistant VPN : **adresse IP / Nom DynDNS**

- Directive IKE = mode automatique
- Directive IPSec = mode automatique
- Mode Exchange = mode principal
- Groupe PFS = groupe DH 2 (1024 bits)
- Validité / Durée
  - Directive IKE : 000:00:07:00 (7 minutes)
  - Directive IPSec : 000:00:08:00 (8 minutes)
- Editeur

  Aucune configuration nécessaire

Options IPSec avancées

Aucune configuration nécessaire

Identité

- Type = adresse IP

  ID = adresse IP du PC du télétravailleur (voir aussi affectation d'adresse IP)

  Utiliser la clé pré-partagée

  Cocher

  Shared Secret = c'est le mot de passe pour la liaison VPN

  Désignation dans l'Assistant VPN : **Secret prépartagé**
- Authentification avancée (XAUTH)

  non utilisée, pas de configuration nécessaire

Affectation d'adresse IP

- Attribuer manuellement l'adresse IP

  Adresse IP = adresse IP du PC du télétravailleur

  Désignation dans l'Assistant VPN : **adresse IP virtuelle/nom DNS**
- DNS / WINS

  Cocher
- Serveur DNS : adresse IP du système de communication

  Désignation dans l'Assistant VPN : **adresse IP de sous-réseau locale (LAN)**

Réseaux IP VPN

Aucune configuration nécessaire

Contrôle de certificat

Aucune configuration nécessaire

Lien pare-feu

- Activer Stateful Inspection :

  en cours de liaison
- Autoriser uniquement la communication dans le tunnel :

  Cocher

19.3.6.2 Comment configurer un client NCP VPN

Pour disposer d'une connexion VPN sûre vers le système de communication, il faut installer et configurer un client NCP VPN sur l'appareil du télétravailleur.

Conditions préalables

L'administrateur de votre système de communication vous a paramétré en tant que télétravailleur, dans WBM de OpenScape Business, et vous a communiqué le fichier ZIP Export avec les données de télétravailleur.

L'administrateur de votre système de communication vous a communiqué la clé PSK pour la connexion VPN.

Le NCP VPN Client (LANCOM Advanced VPN-Client) est installé sur l'appareil du télétravailleur. Les informations nécessaires figurent dans la Documentation des clients NCP VPN.

L'appareil du télétravailleur dispose d'une connexion active avec Internet.

Étape par étape

1) Procédez à l'extraction des fichiers `ncp_readme.txt` et `ncp_VPN.ini` et les placer dans un répertoire local. Les entrées figurant dans le fichier `ncp_vpn.ini` se rapportent au profil `HOOME`.
2) Importez le profil `HOOME` dans le client NCP VPN.
3) Elargissez le profil `HOOME` avec un serveur DNS. L'adresse du serveur DNS est l'adresse IP privée (LAN) de votre système de communication.
4) Démarrez le client NCP VPN
5) Sélectionnez le profil `HOOME` et cliquez sur **Connect**.

19.3.6.3 Comment configurer un client Shrew Soft VPN

Pour disposer d'une connexion VPN sûre vers le système de communication, il faut installer et configurer un client Shrew Soft VPN sur l'appareil du télétravailleur.

Conditions préalables

L'administrateur de votre système de communication vous a paramétré en tant que télétravailleur, dans WBM de OpenScape Business, et vous a communiqué le fichier ZIP Export avec les données de télétravailleur.

L'administrateur de votre système de communication vous a communiqué la clé PSK pour la connexion VPN.

Le client Shrew Soft VPN est installé sur le système du télétravailleur. Vous trouverez un téléchargement du client VPN Shrew Soft dans `http://www.shrew.net`.

L'appareil du télétravailleur dispose d'une connexion active avec Internet.

Étape par étape

1) Procédez à l'extraction des fichiers `shrewsoft_readme.txt` et `shrewsoft_openswan.vpn` et les placer dans un répertoire local.
2) Démarrez **Shrew Soft VPN Client Access Manager** et effectuez la configuration. Enregistrez les indications.

3) Importez le fichier `shrewsoft_openswan.vpn` dans Shrew Soft Client.
4) Ensuite, vous verrez la connexion dans **Gestionnaire d'accès client VPN Shrew Soft**, **Connect (connexion)**.

19.3.6.4 Comment configurer un client iOS ou Android VPN

Pour disposer d'une connexion VPN sûre vers le système de communication, il faut configurer une connexion L2TP-VPN sur l'appareil du télétravailleur.

Conditions préalables

L'administrateur de votre système de communication vous a paramétré en tant que télétravailleur, dans WBM de OpenScape Business, et vous a communiqué un nom utilisateur, un mot de passe et une clé PSK pour la connexion VPN.

L'appareil du télétravailleur dispose d'une connexion active avec Internet.

Étape par étape

1) Sur l'appareil du télétravailleur iOS ou Android, ouvrez le menu **Paramètres** > **Général** > **VPN**.
2) A l'aide de **Ajouter VPN**, ajoutez une nouvelle connexion VPN.
3) Cliquez sur l'onglet **L2TP**.
4) Dans le champ **Description**, donnez un nom à cette connexion VPN.
5) Dans le champ **Serveur**, indiquez l'adresse IP publique ou le nom DNS du système de communication.
6) Dans le champ **Account** (compte), entrez le nom d'utilisateur du télétravailleur.
7) Dans le champ **Mot de passe**, entrez le mot de passe du télétravailleur.
8) Dans le champ **Shared Secret**, indiquez la clé (Preshared Secret) du tunnel VPN.
9) Activez l'option **Toutes les données**.
10) Dans le menu **Paramètres**, activez l'option **VPN**.

19.3.6.5 Comment configurer un client Mac OS-X VPN

Pour disposer d'une connexion VPN sûre vers le système de communication, il faut configurer une connexion L2TP-VPN sur l'appareil du télétravailleur.

Conditions préalables

L'administrateur de votre système de communication vous a paramétré en tant que télétravailleur, dans WBM de OpenScape Business, et vous a communiqué le fichier ZIP Export avec les données de télétravailleur.

L'administrateur de votre système de communication vous a communiqué le nom d'utilisateur, le mot de passe et la clé PSK pour la connexion VPN.

L'appareil du télétravailleur dispose d'une connexion active avec Internet.

Étape par étape

1) Procédez à l'extraction du fichier `.networkConnect` et placez-le dans un répertoire local.

2) Double-cliquez sur le fichier `.networkConnect`.
3) Cliquez sur **VPN (L2TP)**.
4) Dans le champ **Configuration**, sélectionnez la connexion VPN.
5) Dans le champ **Adresse du serveur**, indiquez l'adresse IP publique ou le nom DNS du système de communication.
6) Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur du télétravailleur.
7) Paramétrez les paramètres de sécurité :
   a) Cliquez sur **Paramètres d'authentification**.
   b) Dans le champ **Mot de passe**, entrez le mot de passe du télétravailleur.
   c) Dans le champ **Clé ("Shared Secret")**, indiquez la clé (Preshared Secret) du tunnel VPN.
   d) Cliquez sur **OK**.
8) Cliquez sur **Autres options** et cochez la case **Envoyer tout le trafic sur la connexion VPN**. Pour finir, cliquez sur **OK**.
9) Cliquez sur **Appliquer** puis sur **Connecter**. Lorsque la connexion est établie avec OpenScape Business, l'état **Connecté** s'affiche.

19.3.7 VPN - Services

La fonction Services configurés vous permet de gérer des services. Il faut toutefois activer les services configurés pour qu'ils deviennent des services actifs.

19.3.7.1 VPN - Services actifs - Comment afficher tous les services IPSec

Vous pouvez consulter une liste de tous les services IPSec actifs avec les données détaillées sous forme de tableau.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Services** > **Services actifs**.
4) Dans l'onglet **Afficher les services IPsec**, vous pouvez afficher les données détaillées pour les services IPsec actifs.

19.3.7.2 VPN - Services actifs - Comment afficher le service IPSec spécifique

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Services** > **Services actifs**.
4) Cliquez dans l'arborescence sur le service spécifique sur lequel vous souhaitez consulter toutes les informations (**Nom du service**, **Port source**, **Port de destination**, **Protocole IP**, **Règle ’pass’ correspondante**, **Règle 'deny' correspondante**).

19.3.7.3 VPN - Services configurés - Comment afficher tous les services IPSec

Vous pouvez consulter une liste de tous les services IPsec configurés avec les données détaillées sous forme de tableau.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Services** > **Services configurés**.
4) Dans l'onglet **Afficher les services IPsec**, vous pouvez afficher les données détaillées pour les services IPsec configurés.

19.3.7.4 VPN - Services configurés - Comment modifier le service IPSec

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Remarque : Avant de modifier ou d'activer le service IPsec, il faut effectuer une sauvegarde. Les règles IPSec ont le même effet que les entrées dans un pare-feu ; elles peuvent restreindre l'accès au système. S'il arrive que vous activiez IPsec et que vous n'ayez plus accès au système, vous pouvez réinitialiser le système de communication avec **Recharger** (Reload).

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Services** > **Services configurés**.
4) Cliquez dans l'arborescence de menu sur le service spécifique que vous souhaitez modifier.
5) Modifiez le nom du service dans **Nom du service**.
6) Modifiez le port source dans **Port source**.
7) Modifiez le port de destination dans **Port de destination**.

8) Dans **Protocole IP**, modifiez le service (par ex. UDP).
9) Après la configuration VPN globale, la modification est reprise à l'aide de **Activer les tableaux VPN configurés**

19.3.7.5 VPN - Services configurés - Comment renommer le service IPSec

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Services** > **Services configurés**.
4) Cliquez dans l'arborescence de menu sur le service spécifique que vous souhaitez renommer.
5) Dans **Nom du service**, modifiez le nom du service.
6) Après la configuration VPN globale, la modification est reprise à l'aide de **Activer les tableaux VPN configurés**

19.3.7.6 VPN - Services configurés - Comment effacer le service IPSec

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Services** > **Services configurés**.
4) Cliquez dans l'arborescence de menu sur le service spécifique que vous souhaitez effacer.
5) Après la configuration VPN globale, la modification est reprise à l'aide de **Activer les tableaux VPN configurés**

19.3.8 Tunnel VPN

Un tunnel correspond au transport de paquets de données cryptés vers un point terminal défini. Les tunnels actifs sont les tunnels configurés après activation de la configuration. Au total, il est possible de configurer jusqu'à 256 tunnels par passerelle.

19.3.8.1 VPN - Tunnels actifs - Comment afficher les données de tunnel générales

Vous pouvez afficher toutes les données de tunnel actives avec les informations détaillées sous forme de tableau.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Tunnel** > **Tunnels actifs**.
4) Dans l'onglet **Afficher les données de tunnel générales**, vous voyez les informations détaillées sur les tunnels actifs. Cela englobe :
   - **Nom du tunnel**
   - **Etat dans la pile IP**
   - **Type de point terminal du tunnel local**
   - **Adresse de point terminal du tunnel local**
   - **Type de point terminal du tunnel distant**
   - **Adresse de point terminal du tunnel distant**
   - **Durée de vie proposée des clés de session**
   - **Durée de vie proposée de la session d'échange de clés**
   - **Règles correspondantes Règle d'envoi correspondante**
   - **Règles correspondantes Règle de réception correspondante**

19.3.8.2 VPN - Tunnels actifs - Comment afficher les règles pour tous les tunnels

Vous pouvez afficher dans une fenêtre les règles pour tous les tunnels actifs.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Tunnel** > **Tunnels actifs**.
4) Dans l'onglet **Afficher les règles pour tous les tunnels**, vous voyez les informations détaillées sur les tunnels actifs, comme
   - **Données de tunnel**
   - **Données de règle**
   - **Adresse source**
   - **Adresse de destination**
   - **Données du service**

19.3.8.3 VPN - Tunnels configurés - Comment afficher les données de tunnel générales

Vous pouvez afficher toutes les données pour les tunnels configurés sous forme de tableau, avec les informations détaillées

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Tunnel** > **Tunnels configurés**.
4) Dans l'onglet **Afficher les données de tunnel générales**, vous voyez les informations détaillées sur les tunnels configurés. Cela englobe :
   - **Nom du tunnel**
   - **Type de point terminal du tunnel local**
   - **Adresse de point terminal du tunnel local**
   - **Type de point terminal du tunnel distant**
   - **Adresse de point terminal du tunnel distant**
   - **Durée de vie proposée des clés de session**
   - **Durée de vie proposée de la session d'échange de clés**
   - **Règles correspondantes Règle d'envoi correspondante**
   - **Règles correspondantes Règle de réception correspondante**

19.3.8.4 VPN - Tunnels configurés - Comment afficher les règles pour tous les tunnels

Vous pouvez afficher dans une fenêtre les règles pour tous les tunnels actifs.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Tunnel** > **Tunnels configurés**.
4) Dans l'onglet **Afficher les règles pour tous les tunnels**, vous voyez les informations détaillées sur les tunnels configurés, à savoir
   - **Données de tunnel**
   - **Données de règle**
   - **Données source**
   - **Données de destination**
   - **Données du service**

19.3.8.5 VPN - Comment ajouter un tunnel configuré

Vous pouvez configurer un nouveau tunnel IPSec. Au total, il est possible de configurer jusqu'à 256 tunnels par passerelle.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.

3) Dans l'arborescence du menu, allez à **VPN** > **Tunnel** > **Tunnels configurés**.
4) Dans l'onglet **Ajouter un tunnel**, vous obtenez la fenêtre de saisie pour le nouveau tunnel.
5) Sélectionnez **Données de tunnel**.
6) Entrez dans **Nom du tunnel** le nom souhaité pour le nouveau tunnel.
7) Dans la liste déroulante **Point terminal du tunnel local**, sélectionnez le type d'adresse de point terminal sur le côté émission du tunnel (il est possible d'indiquer un nom d'hôte ou nom DNS).
8) Entrez dans **Adresse de point terminal du tunnel local** l'adresse de l'émetteur, au format adapté au type de point terminal.
9) Dans la liste déroulante **Type de point terminal du tunnel distant** sélectionnez le type d'adresse de point terminal côté réception du tunnel (l'indication de l'adresse IP est supportée).
10) Entrez dans **Adresse de point terminal du tunnel distant** l'adresse du destinataire, au format adapté au type de point terminal. Si l'adresse 0.0.0.0 est paramétrée, cela signifie que le point terminal du tunnel est inconnu. Dans ce cas, l'établissement du tunnel doit toujours se faire par le côté opposé (par ex. télétravailleur).
11) Entrez dans **Négociation de clé de session** la méthode d'échange des clés (possibilités : Automatique, Avec le protocole IKE).
12) Dans **Algorithmes de chiffrement proposés**, sélectionnez les algorithmes qui peuvent être utilisés (AES, DES ou 3DES).
13) Dans **Algorithmes de hash proposés**, sélectionnez les algorithmes de contrôle qui peuvent être utilisés (MD5, SHA1 ou SHA2). Les algorithmes sélectionnés sont proposés par l'initiateur de la négociation IKE.
14) Entrez dans **Durée de vie proposée des clés de session** une durée de validité pour les clés de session utilisées. Après écoulement de ce délai, plus aucune donnée ne sera échangée au cours de cette session. En remplacement des clés de session devenues invalides, de nouvelles clés de session sont automatiquement échangées.
15) Entrez dans **Durée de vie proposée de la session d'échange de clés** une durée de validité. A la fin de la session d'échange des clés, de nouvelles clés sont automatiquement échangées par IKE.
16) Entrez dans **Volume de données proposé des clés de session** le volume de données maximum pour les clés de session. Lorsque le volume de données est dépassé, une nouvelle clé de session est automatiquement négociée avec IKE. Lorsque l'on sélectionne **illimité**, la validité des Session Keys (clés de session) n'est pas limitée par la quantité de données.
17) Dans la partie supérieure de la fenêtre, cochez la case **Données d'échange de clé**.

18) Entrez toutes les données d'échange de clé, **activer "Perfect Forward Secrecy" et sélectionnez la méthode d'authentification pour les pairs VPN, (clé pré-partagée** ou **signatures numériques.**

Conseil : Si vous avez sélectionné **Clés pré-partagées** comme méthode d'authentification, vous devez entrer une clé pré-partagée de 20 caractères (et la répéter).

Conseil : Si vous utilisez **Signatures numériques** (d'une Lightweight CA) comme méthode d'authentification dans un réseau VPN à plusieurs noeuds, vous devez configurer des étapes supplémentaires.

---

a) Créez un certificat LWCA sur un noeud.
b) Exportez le certificat (.crt) vers un fichier.
c) Créez et exportez une Certificate Revocation List (.CRL) dans un fichier.
d) Créer et exporter un certificat du pair (.p12), avec certificat CA pour chaque noeud.
e) Le certificat CA (.crt), la Certificate Revocation List (.crl) (liste de révocation des certificats) et les certificats du pair correspondants doivent être importés dans chaque noeud.

19) Entrez les **groupes Diffie-Hellman proposés** (Groupe DH 2, 5 ou 14).
20) Après la configuration VPN globale, la modification est reprise à l'aide de **Activer les tableaux VPN configurés**

19.3.9 Règles VPN

Les règles définissent ce qui doit se passer avec un paquet IP. L'action de règle *Pass* signifie que le paquet IP doit continué à être transporté. L'action de règle *Deny* signifie que le paquet IP ne doit pas continuer à être transporté. Il est possible de sélectionner si le paquet IP utilise ou pas un tunnel VPN (chiffré).

Le système de communication est en mesure de gérer 640 règles dont 6 sont prédéfinies (règles par défaut) et 634 sont libres d'attribution.

19.3.9.1 VPN - Règles actives - Comment afficher les règles

Vous pouvez afficher toutes les règles actives.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Règles** > **Règles actives**.

4) Cliquez sur l'onglet **Afficher les règles**. Le système affiche des informations détaillées sur les règles actives, comme

- **Priorité**
- **Service**
- **Action pour la règle**
- **Chiffrement nécessaire**
- **Etat de la règle**
- **Etat dans la pile IP**
- **Adresse source**
- **Adresse de destination**
- **Tunnel pour le chiffrement**

19.3.9.2 VPN - Règles actives - Comment afficher la règle spéciale

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Règles** > **Règles actives**.
4) Cliquez sur la règle de votre choix dans l'arborescence. La fenêtre **Afficher la règle** avec toutes les données détaillées apparaît pour cette règle (**Priorité**, **Service**, **Action pour la règle**, **Chiffrement nécessaire**, **Etat de la règle**, **Adresse source**, **Adresse de destination**)

19.3.9.3 VPN - Règles configurées - Comment afficher toutes les règles

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Règles** > **Règles configurées**.
4) Cliquez sur l'onglet **Afficher les règles**. Le système affiche des informations détaillées sur les règles actives, comme

- **Priorité**
- **Service**
- **Action pour la règle**
- **Chiffrement nécessaire**
- **Activer la règle**
- **Adresse source (Type et Adresse IP)**
- **Adresse de destination (Type et Adresse IP)**

19.3.9.4 VPN - Règles configurées - Comment ajouter une règle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Règles** > **Règles configurées** > **Ajouter des règles**.
4) Procédez au réglage des paramètres suivants.
   - **Priorité**
   - **Service**
   - **Action pour la règle (PASS, PASS_INCOMING, PASS_OUTGOING, DENY)**
   - **Chiffrement nécessaire**
   - **Etat de la règle**
   - **Adresse source - Type**
   - **Adresse source - Adresse (la plus basse de la plage)**
   - **Adresse source - Masque de sous-réseau (adresse supérieure de la zone)**
   - **Adresse de destination - Type**
   - **Adresse de destination - Adresse (inférieure de la plage)**
   - **Adresse cible - Masque de sous-réseau (adresse supérieure de la zone)**
   - **Tunnel côté réception**
   - **Tunnel côté émission**
5) Cliquez sur **Appliquer**.

19.3.9.5 VPN - Comment modifier la règle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Règles** > **Règles configurées**.
4) Dans l'arborescence du menu, sélectionnez la règle que vous voulez modifier.
5) Entrez dans **Priorité** la priorité.
6) Entrez dans **Service** le service (par ex. DNS).
7) Dans **Action pour la règle** entrez la règle (**PASS**, **PASS_INCOMING**, **PASS_OUTGOING**, **DENY**).
8) Si nécessaire, cochez la case **Chiffrement**.
9) Cochez la case **Activer la règle**.

10) Entrez dans **Adresse source** le **Type** et **l'adresse IP** de la règle modifiée.
11) Entrez dans **Adresse de destination** le **type** et **l'adresse IP** de la règle modifiée.
12) Après la configuration VPN globale, la modification est reprise à l'aide de **Activer les tableaux VPN configurés**

19.3.9.6 VPN - Comment ajouter une règle pour le sens opposé

Lorsque une règle IPSec est créée pour un sens de transmission, il convient d'ajouter immédiatement la règle pour le sens opposé. La fonction "Ajouter une règle pour le sens opposé" permet d'intégrer les entrées de la règle sélectionnée en intervertissant l'adresse source et l'adresse de destination et en modifiant en conséquence l'affectation du tunnel.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Règles** > **Règles configurées**.
4) Dans l'arborescence du menu, sélectionnez la règle que vous voulez traiter.
5) Cliquez sur l'onglet **Ajouter une règle pour le sens opposé**.
6) Cliquez sur **Appliquer**.
7) Après la configuration VPN globale, la modification est reprise à l'aide de **Activer les tableaux VPN configurés**

19.3.9.7 VPN - Comment effacer la règle

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Règles** > **Règles configurées**.
4) Dans l'arborescence du menu, sélectionnez la règle que vous voulez effacer.
5) Cliquez sur l'onglet **Effacer la règle**. La règle sélectionnée avec toutes les données est affichée.
6) Cliquez sur **Effacer**. Un avertissement apparaît pour vous indiquer que vous êtes sur le point d'effacer cette règle.
7) Après la configuration VPN globale, la modification est reprise à l'aide de **Activer les tableaux VPN configurés**

19.3.10 Serveur PKI

Le serveur PKI correspond à un serveur qui peut établir, distribuer et contrôler des certificats numériques. Les certificats établis à l'intérieur d'une infrastructure PKI (Public Key Infrastructure) sont utilisés pour sécuriser la communication.

A l'aide de la PKI-URL configurée par le serveur PKI, on tente de télécharger CRL en utilisant des certificats (signatures numériques).

19.3.10.1 VPN - Comment afficher le serveur PKI

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Public Key Infrastructure (PKI)**.
4) Cliquez sur l'onglet **Afficher le serveur PKI**. Le **nom du serveur PKI**, le **Type de serveur PKI** et l'**URL du serveur PKI** s'affichent.

19.3.10.2 VPN - Comment ajouter un serveur PKI

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **VPN** > **Public Key Infrastructure (PKI)**.
4) Cliquez sur l'onglet **Ajouter un serveur PKI**.
5) Entrez le **nom du serveur PKI**.
6) Indiquez le **Type de serveur PKI** (par ex. LDAP).
7) Entrez l'**URL du serveur PKI**.
8) Validez et cliquez sur **Appliquer**.

19.4 Gestion du certificat

La gestion du certificat (pour Secure Sockets Layer SSL) permet l'administration sécurisée du système de communication. Les données ne peuvent pas être lues ou manipulées par les postes non autorisés. L'autorisation est donnée par des certificats. Vous pouvez générer et gérer des certificats.

L'accès administration se produit de manière cryptée via HTTPS, en utilisant le protocole TLS 1.2. Les certificats servent à authentifier la connexion. Par

défaut, il est utilisé un certificat autosigné. Pour augmenter la sécurité, il est possible d'utiliser un certificat spécifique du client.

SSL fournit les services de sécurisation suivants :

- Authenticité (le partenaire de communication est bien celui qu'il prétend être)
- Confidentialité (les données ne peuvent pas être lues par un tiers)
- Intégrité (les données ont été reçues comme elles ont été envoyées)

Ces services de sécurité nécessitent une entente préalable sur un mécanisme de sécurité et l'échange de clés cryptographiques. Ces deux opérations sont réalisées lors de l'établissement de la liaison.

SSL utilise des certificats et des clés pour permettre un transfert de données sécurisé.

CRL (Certificate Revocation Lists)

Les listes Certificate Revocation Lists (CRL) sont des fichiers qui contiennent une liste des certificats verrouillés, avec leurs numéros de série et leurs données de verrouillage. De plus, la liste CRL contient le nom de l'émetteur de la liste de verrouillage des certifications et de la prochaine heure d'actualisation.

CDP (CRL Distribution Point)

CRL Distribution Point (CDP) est le répertoire (le lieu) dans lequel se trouve la version actuelle des CRL (par ex. http://sectestcal.microsoft.com/ErtEnvoll/SecTestCAL.crl).

Informations spécifiques du système

Lors d'une administration basée sur SSL, une communication client-serveur a lieu.

Le serveur s'authentifie par rapport au client à l'aide des certificats générés dans WBM ou importés. Un tel certificat peut être importé dans le navigateur comme certificat de confiance afin d'éviter les messages d'avertissement du navigateur en cas de liaison avec le serveur SSL.

Conseil : Le certificat SSL peut aussi être utilisé pour SPE.

19.4.1 Introduction

Que sont les certificats SSL ?

Les certificats TLS/SSL sont utilisés pour protéger les données lors de la communication entre des serveurs tels qu'Unify OpenScape Business et des clients basés sur le Web au moyen d'un cryptage et pour vérifier l'identité de l'entreprise appartenant au site Web afin que l'utilisateur puisse être sûr qu'il communique réellement avec le serveur réel.

Unify OpenScape Business émet lui-même un certificat SSL temporaire (« auto-signé ») lors de la Première Installation du système ou lors du changement de l'Adresse IP du réseau local, mais ce certificat ne contient pas suffisamment de données pour la vérification de l'identité en dehors de l'Adresse IP du réseau local de l'utilisateur.

Un tel certificat n'est pas conforme aux normes de sécurité en vigueur et doit être remplacé par un certificat SSL individuel digne de confiance délivré par une autorité de certification officielle (CA) dès que possible après la Première Installation d'OpenScape Business. C'est le seul moyen de répondre aux normes minimales des systèmes d'exploitation clients et des navigateurs Web actuels pour une communication Internet sécurisée.

Les CA offrent généralement des certificats SSL avec différents niveaux de confiance : validation de domaine (DV), validation d'organisation (OV) et validation étendue (EV). Pour Unify OpenScape Business, les certificats validés par domaine sont suffisants. C'est généralement l'option la moins chère, avec certains CA même gratuits.

Pour quels services Web Unify OpenScape Business utilise-t-il le certificat SSL ?

Le certificat SSL actif est utilisé pour l'accès administrateur via le portail d'administration ainsi que pour diverses autres applications Web (par exemple, la Programmation des touches) et les clients UC basés sur WSI tels que myPortal @work, Lanceur d'applications et myPortal for Teams.

Où puis-je obtenir un certificat SSL de confiance ?

Pour obtenir un certificat SSL, vous devez contacter une autorité de certification. Vous devez vérifier le nom de domaine utilisé pour atteindre Unify OpenScape Business afin de créer une demande de signature de certificat (CSR), qui est ensuite envoyée à l'autorité de certification pour validation.

Il convient de noter que les certificats SSL de confiance émis par CA n'ont qu'une durée de validité limitée de quelques mois à quelques années pour s'assurer qu'ils sont conformes aux normes de sécurité en vigueur. Il est important de garder un œil sur la date d'expiration et de renouveler les certificats SSL avant que la date d'expiration ne soit atteinte.

Le non-renouvellement des certificats SSL peut entraîner la classification du site Web par l'environnement client comme « non sécurisé » et empêcher la communication avec le serveur.

Veuillez noter que certains environnements clients ont des exigences particulières pour les certificats SSL, qui peuvent ne pas être remplies par toutes les autorités de certification. Ces exigences spéciales sont liées plus bas dans la zone « considérations côté client ». Lors de la sélection de votre CA, veuillez suivre les instructions correspondantes.

Pourquoi la question du certificat est-elle devenue si importante ?

L'utilisation de certificats SSL fiables, spécifiques au client ou au serveur est extrêmement importante et est de plus en plus appliquée par les principaux fabricants de systèmes d'exploitation et de navigateurs. La sécurité, le professionnalisme, l'intégrité et la confidentialité lors du traitement des données personnelles en sont les principaux arguments.

En raison de l'utilisation croissante des services et des clients basés sur le Web, y compris via Internet, l'utilisation permanente du certificat SSL par défaut temporaire, auto-signé (et donc non sécurisé) d'OpenScape Business est hors de question.

En outre, le certificat temporaire auto-signé d'OSBiz a une validité de plusieurs années, tandis que certains environnements clients ont commencé à limiter la validité du certificat – parfois à un an maximum.

De plus, dans de nombreuses installations de clients qui ont été configurées à l'origine avec des versions de logiciels plus anciennes avant V3R2.1, la validité de ces certificats temporaires auto-signés expire le 1er janvier 2024.

Le portail d'administration d'OpenScape Business fournit une gamme d'outils pour générer et gérer des certificats SSL et aide également l'administrateur système à créer des demandes de signature de certificats. Les fonctions les plus importantes à cet égard sont expliquées ci-dessous.

19.4.2 Comment générer un certificat CA

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Génération de certificat**.
4) Cliquez sur l'onglet **Générer le certificat CA**.
5) Spécifiez le **Nom du certificat**.
6) Attribuez également un numéro d'ordre dans le champ **Numéro de série du certificat**.
7) Dans **Type d'algorithme de signature** , sélectionnez l'algorithme (**sha256RSA** ou **sha512RSA**).
8) Dans **Longueur de la clé publique**, sélectionnez la clé publique.
9) Dans les champs correspondants, entrez le début et la fin de validité du certificat.
10) Ensuite, complétez les champs **Nom du sujet** ou **Nom alternatif du sujet**.
11) Entrez le **Point de distribution CRL**.
12) Cliquez sur **Appliquer**, puis sur **OK**.

19.4.3 Comment générer le certificat autosigné

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Génération de certificat**.
4) Cliquez sur l'onglet **Générer le certificat autosigné** dans la fenêtre **Génération de certificats**.
5) Attribuez dans le champ **Nom du certificat** un nom au certificat généré.
6) Attribuez également un numéro d'ordre dans le champ **Numéro de série du certificat**.
7) Dans **Type d'algorithme de signature** sélectionnez l'algorithme.
8) Dans **Longueur de la clé publique**, sélectionnez la clé publique.

9) Dans les champs correspondants, entrez le début et la fin de validité du certificat.
10) Ensuite, complétez les champs de **Demandeur** ou **Autre nom de demandeur**.
11) Entrez le **point de distribution CRL**.
12) Cliquez sur **Appliquer** puis sur **OK**.

19.4.4 - Comment générer une demande de certificat (CSR)

Selon l'autorité de certification choisie, il existe différentes options pour créer des demandes de signature de certificat en ligne (par exemple, via le portail Web d'une autorité de certification) ou hors ligne. Le portail OpenScape Business Admin offre la possibilité de créer une CSR à télécharger et à transmettre à l'autorité de certification.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Dans la page Générer une demande de certificat (CSR), les champs suivants doivent être remplis afin de générer les fichiers clé et CSR.

Général :

Nom de la demande de certificat : Un nom pour la CSR, qui sera utilisé dans le nom du fichier qui sera téléchargé.

Type d'algorithme de signature : Choisir entre sha256RSA et sha512RSA

Longueur de la clé publique : La seule option est 2048

Pays (P) : Utilisez un code de pays à deux lettres, par exemple DE

Organisation (O) : nom officiel de l'entité ou de l'entreprise à laquelle le certificat est attribué.

Unité organisationnelle (UO) : désigne une sous-unité ou un département spécifique au sein d'une organisation, offrant un degré de précision supplémentaire pour identifier la structure organisationnelle concernée.

Nom commun (NC) : un identifiant crucial, représentant généralement le nom de domaine pour lequel le certificat est émis, qui constitue un élément clé pour vérifier l'identité du détenteur du certificat.

Nom alternatif du sujet (facultatif) :

L'extension Nom alternatif du sujet (Subject Alternative Name, SAN) est une fonctionnalité des certificats X.509 utilisée dans le domaine de la cryptographie. X.509 est une norme qui définit le format des certificats de clé publique. L'extension SAN permet d'associer des identités supplémentaires, telles que des noms d'hôtes, des adresses IP ou des adresses e-mail, à un seul certificat X.509. Ceci est particulièrement utile dans les scénarios où il doit être possible d'accéder à un serveur en utilisant différents noms ou adresses.

Format de nom distinctif : Des informations similaires au nom du sujet, telles que le pays (P), l'organisation (O), l'unité organisationnelle (UO), le nom commun (NC), doivent être renseignées.

Autre format :

Extension Nom alternatif du sujet : Les options sont nom DNS, adresse IP, adresse e-mail, URI (identifiant uniforme de ressource), autres

Nom alternatif du sujet (SAN) : L'extension SAN permet de remédier aux limitations dans les cas où un seul nom commun ne suffit pas ou lorsqu'il est nécessaire d'inclure plusieurs identités dans un seul certificat. Ceci est important pour les services Web modernes, où un serveur peut être accessible par plusieurs noms de domaine ou adresses IP.

Voici un exemple illustrant comment une extension SAN peut se présenter dans un certificat :

Nom alternatif du sujet :

DNS : www.example.com

DNS : mail.example.com

Adresse IP : 192.168.1.1

Adresse e-mail :admin@example.com

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Gestion des certificats** > **Certificats de serveur**.
4) Dans l'onglet **Générer une demande de certificat (CSR)** :
5) Dans le champ **Nom de la demande de certificat**, entrez le nom du certificat.
6) Cliquez pour sélectionner **sha256RSA** ou **sha512RSA** dans la liste déroulante **Type d'algorithme de signature**.
7) La**Longueur de la clé publique** est fixée à **2048** caractères.
8) Entrez le pays **Pays (C).**
9) Entrez l'organisation **Organisation (O).**
10) Entrez l'**Unité organisationnelle (UO)**.
11) Entrez le **Nom commun (NC)**.
12) Cliquez sur **Format de nom distinctif** ou **Autre format**pour sélectionner le format du certificat.
13) Si vous le souhaitez, vous pouvez choisir l'une des valeurs de l'**Extension Nom alternatif du sujet**.
14) Si vous le souhaitez, vous pouvez cliquer sur le bouton **Ajouter** pour ajouter un **Nom alternatif du sujet** dans la CSR.
15) Cliquez sur **Appliquer**, puis sur **OK**.

19.4.5 Comment importer le certificat de serveur (PKCS#12)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l’arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Gestion des certificats** > **Certificats de serveur**.
4) Cliquez sur l'onglet **Importer le certificat de serveur (PKCS#12)** dans la fenêtre **Certificats de serveur**.

   Remarque : Si un autre format est sélectionné, il est possible de configurer plus d'une entrée SAN.

5) Indiquez le **Nom du certificat**.
6) Entrez le **Mot de passe de déchiffrement**.
7) Under **Fichier avec certificat**, entrez dans le fichier de certificat souhaité grâce au bouton **Choisir un fichier**.
8) Cliquez sur **Importer le certificat du fichier**, puis sur **OK**.

19.4.6 Comment importer les certificats de serveur (PEM)

Les certificats au format PEM sont également pris en charge. Pour ce faire, vous pouvez importer le certificat et le fichier clé sous la forme de deux fichiers distincts.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l’arborescence de navigation, cliquez sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Gestion des certificats** > **Certificats de serveur**.
4) Cliquez sur l'onglet **Importer le certificat de serveur (PKCS#12)** dans la fenêtre **Certificats de serveur**.

   Remarque : Si un autre format est sélectionné, il est possible de configurer plus d'une entrée SAN.

5) Dans la section **Importer le certificat et les fichiers clés** :
6) Indiquez le **Nom du certificat**. (Vous pouvez saisir un nom de votre choix).
7) Entrez le **Mot de passe de déchiffrement**. (Vous pouvez saisir une phrase de votre choix servant de mot de passe)
8) Sous **Fichier de certificat**, choisissez le fichier de certificat à l'aide du bouton **Choisir un fichier**.
9) Sous **Fichier clé**, choisissez le fichier clé à l'aide du bouton **Choisir un fichier**.
10) Cliquez sur **Importer le certificat et la clé**, puis sur **OK**.

19.4.7 Comment afficher les certificats

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Gestion des certificats** > **Certificats de serveur**.
4) Double-cliquez sur le certificat souhaité. La fenêtre **Certificats de serveur** s'affiche.
5) Cliquez sur l'onglet **Afficher le certificat** et vous pouvez consulter le certificat actuel.

19.4.8 Comment supprimer un certificat

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Gestion des certificats** > **Certificats de serveur**.
4) Double-cliquez sur le certificat souhaité. La fenêtre **Certificats de serveur** s'affiche.
5) Cliquez sur l'onglet **Effacer le certificat**. Le nom du certificat actuellement valide s'affiche avec l'avertissement que vous êtes sur le point de l'effacer.
6) Si vous souhaitez vraiment effacer le certificat, cliquez sur **Effacer**.

19.4.9 Comment exporter un certificat (X.509)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Gestion des certificats** > **Certificats de serveur**.
4) Double-cliquez sur le certificat souhaité. La fenêtre **Certificats de serveur** s'affiche.
5) Cliquez sur l'onglet **Exporter le certificat (X.509)**. Vous pouvez ouvrir ou enregistrer le certificat.

19.4.10 Comment importer un certificat prolongé (X.509)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **SSL** > **Gestion des certificats** > **Certificats de serveur**.
4) Double-cliquez sur le certificat souhaité. La fenêtre **Certificats de serveur** s'affiche.
5) Cliquez sur l'onglet **Importer le certificat prolongé (X.509)**. Le nom du certificat actuellement valide s'affiche.
6) Dans le champ **Fichier avec le certificat**, entrez le certificat souhaité ou sélectionnez-le par le champ **Parcourir**.
7) Mettez fin à vote entrée avec **Empreinte digitale de**.

19.4.11 Comment activer les certificats

Avec cette fonction, vous spécifiez le certificat à utiliser pour l'administration basée sur le Web.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Sécurité**.
3) Naviguez dans l'arborescence des menus jusqu'à **SSL** > **Certificate Management** > **Server Certificates**.
4) Cliquez sur l'émoji désiré.
5) Cliquez sur l'onglet **Activer le certificat**. Un avertissement s'affiche indiquant que cette action interrompra toutes les connexions HTTP en cours.
6) Sélectionnez le système souhaité (Unify OpenScape Business) pour lequel vous souhaitez activer le certificat dans la liste déroulante **Système**.

Remarque : Pour fonctionner correctement, l'adresse IP du système doit être saisie dans le champ **Nom commun** de chaque certificat. Assurez-vous d'activer le bon certificat pour le système sélectionné.

---

7) Cliquez sur **Activer maintenant**.

Remarque : Le certificat de serveur importé doit être émis directement à partir d'une autorité de certification racine. Les AC intermédiaires ne doivent pas être utilisées.

19.5 Sécurité web

Le filtre d'accès au web figure dans Sécurité web. Il vous permet de gérer les autorisations client ainsi que le journal admin qui garde la trace de tous les accès ou toutes les modifications dans le système de communication.

19.5.1 Connexions au serveur Web

Les connexions des clients au serveur web interne du système de communication peuvent être soit cryptées (HTTPS), soit non cryptées (HTTP).

19.5.1.1 Comment configurer les connexions vers le serveur Web (UC Suite)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu allez à **Accès Web**.
4) Configurez la connexion avec le serveur Web :
   - Si vous souhaitez autoriser des connexions cryptées, cochez la case **HTTPS**.
   - Si vous souhaitez autoriser des connexions sans cryptage, cochez la case **HTTP**.
5) Activez évent. le champ **Enregistrer les données de connexion dans le terminal** si vous souhaitez autoriser cette fonction. Ici, à l'aide des cookies, les données de connexion sont enregistrées dans le navigateur Web du téléphone mobile.
6) Cliquez sur **Sauvegarder**.

19.5.1.2 Comment configurer les connexions vers le serveur Web (UC Smart)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Applications** > **UC Smart** > **Configuration de base**.
3) Contrôlez si UC Smart est **actif**.
4) Configurez la connexion avec le serveur Web :
   - Si vous souhaitez autoriser des connexions cryptées, cochez la case **HTTPS**.
   - Si vous souhaitez autoriser des connexions sans cryptage, cochez la case **HTTP**.

5) Cliquez sur **Appliquer** puis sur **OK**.

19.5.2 Protocole Admin

Le protocole d'administration vous donne la possibilité quand et quelles modifications ont été apportées au système de communication et qui en est l'auteur.

19.5.2.1 Comment effacer le protocole d'administration

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance**.
3) Dans l'arborescence du menu, allez à **Protocole Admin** > **Données du protocole d'admin**.
4) Dans la fenêtre **Données du protocole d'admin.** apparaît le message "Le protocole Admin va être chargé depuis le système. Merci de confirmer".
5) Cliquez sur **Charger**.

19.5.2.2 Comment modifier la langue du protocole d'administration

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Service**.
3) Dans l'arborescence du menu, allez à **Protocole Admin** > **Configuration**.
4) Dans la fenêtre **Modifier la configuration** dans **Langue du protocole d'admin.**, régler la langue souhaitée.
5) Cliquez sur **Appliquer**.

19.6 Sécurité SQL

OpenScape Business stocke les données de configuration du système, les enregistrements de données d'appels, les informations d'identification des comptes d'utilisateurs, les données UC, etc. dans une base de données SQL interne. L'accès à la base de données est protégé par des identifiants de connexion.

Jusqu'à la version logicielle V2R2, les identifiants de connexion utilisés sont protégés par un mot de passe, qui ne peut pas être modifié par un

administrateur OpenScape Business. À partir de V2R2, le mot de passe peut être modifié. Le mot de passe est généré par la machine et il n'est pas montré à l'administrateur. Pour la compatibilité à l'intérieur des scénarios multinoeuds utilisant d'anciennes versions de logiciel, il est possible de changer un mot de passe modifié en le replaçant à sa valeur "ancienne". La configuration du mot de passe d'accès SQL peut être trouvée sous Sécurité SQL. La configuration du mot de passe d'accès SQL peut être utilisée à la fois dans les environnements réseau et dans les environnements à nœud unique. La gestion des scénarios spécifiques à nœud unique ou à nœuds multiples est décrite dans les chapitres suivants.

19.6.1 Noeud unique

Mise à jour logicielle à partir de V2R1 ou antérieure

Après une mise à jour logicielle à partir de V2R1, l'ANCIEN mot de passe de la base de données SQL est actif. Le mot de passe SQL doit être modifié à l'intérieur de la nouvelle version de logiciel par l'administrateur du système, à l'aide du portail Administration (WBM).

Configuration d'un nouveau système

Lorsque la date est configurée pour la première fois dans le système, un nouveau mot de passe SQL sera généré. C'est seulement la première fois où la date et l'heure sont définies que le mot de passe est automatiquement modifié.

Configuration d'un système à "nœud unique" rechargé

Après chaque rechargement du système, l'ANCIEN mot de passe de base de données SQL est actif dans le système. Le mot de passe SQL doit être modifié à l'intérieur de la nouvelle version de logiciel par l'administrateur du système, à l'aide du portail Administration (WBM).

19.6.2 Multinoeud

Le système à nœud unique est configuré et intégré dans le réseau de la manière connue. Après la configuration du système, le nouveau nœud esclave synchronise son mot de passe SQL avec le nœud maître. Aucune action n'est nécessaire pour adapter le mot de passe SQL dans le nœud esclave.

Recharger un nœud V2R2 ou ultérieure dans le réseau V2R2 ou ultérieur

Après un rechargement d'un nœud de réseau dans le réseau, le nœud doit être reconfiguré et intégré à nouveau dans le réseau.

Rechargement du noeud maître

Dans le cas du noeud maître, le mot de passe SQL doit être modifié par l'administrateur système à l'aide du portail Administration (WBM). Tous les noeuds esclaves synchronisent leur mot de passe SQL avec le nouveau mot de passe du noeud maître. Aucune action n'est nécessaire pour modifier le mot de passe SQL dans les nœuds esclaves.

Rechargement du noeud esclave

Dans le cas d'un nœud esclave, aucune action n'est nécessaire car le nœud esclave synchronise son mot de passe SQL avec celui du nœud maître.

Nouveau nœud esclave V2R2 ou ultérieure dans le réseau V2R1 (scénario non recommandé)

Le système à nœud unique est configuré et intégré dans le réseau de la manière connue. Après la configuration du système, le nouveau nœud esclave détecte que le nœud maître utilise l'ancien mot de passe SQL et utilise aussi l'ancien mot de passe SQL. Aucune action n'est nécessaire pour adapter le mot de passe SQL dans le nœud esclave.

Remarque : Il est fortement recommandé de mettre à niveau le réseau entier dans la dernière version du logiciel.

Nouveau nœud maître V2R2 ou ultérieure dans le réseau V2R1 (scénario non recommandé)

Le système à nœud maître est configuré et intégré dans le réseau de la manière connue. Après la configuration du système, le nouveau noeud maître utilise l'ancien mot de passe SQL. L'administrateur système ne doit pas modifier l'ancien mot de passe, car les esclaves V2R1 ne peuvent pas se synchroniser avec un nouveau mot de passe SQL figurant dans le noeud maître. Dans ce cas, le nœud ne fonctionnerait pas à l'intérieur du réseau. Si l'administrateur système a changé le mot de passe SQL par hasard, il doit revenir au mot de passe "par défaut" dans la configuration du noeud maître.

Remarque : Il est fortement recommandé de mettre à niveau le réseau entier dans la dernière version du logiciel.

19.6.3 Configurer les mots de passe de la base de données SQL

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Cliquez dans l'arborescence de navigation sur **Serveur de téléphonie** > **Sécurité**.
3) Dans l'arborescence du menu, allez à **Sécurité SQL**.
4) Configurer les mots de passe de la base de données SQL :
   - Si vous souhaitez générer un nouveau mot de passe inconnu de l'utilisateur, cochez la case **Générer nouveau**.
   - Si vous voulez que le mot de passe par défaut soit activé, sélectionnez la case **Activer la valeur par défaut**.

Remarque : Dans la zone de notification de la page de destination, le message suivant s'affiche si le mot de passe

sql par défaut est utilisé (ou un mot de passe généré avec l'ancien algorithme de génération de mot de passe) :

"`Le mot de passe SQL par défaut est utilisé. Veuillez envisager de le modifier via le mode Expert`"

Le message est un lien URL qui conduit à la page Sécurité SQL afin de la modifier.

19.7 Protection contre les attaques SIP (SIP Attack Protection)

Les attaques dites SIP sont une nouvelle forme d'attaque dirigées contre les systèmes de communication, via la téléphonie IP. Les attaques peuvent se produire aussi à partir du LAN qu'à partir d'Internet (via des routeurs mal configurés). La protection contre les attaques SIP offre un accès SIP protégé par mot de passe.

Pour un accès abonné SIP, il faut respecter les règles ci-après.

- Authentification active
- Mot de passe qualifié,
- – entre 8 et 20 caractères,
  – contenant une ou plusieurs majuscules (A à Z),
  – une ou plusieurs minuscules (a à z)
  – un ou plusieurs chiffres (0 à 9),
  – un ou plusieurs caractères spéciaux (par ex. : %),
  – pas plus de 3 caractères répétés.
- Définition d'un ID abonné SIP qui se distingue du numéro de téléphone.

Lorsque un nouvel abonné SIP est configuré, l'authentification est activée par défaut et un mot de passe aléatoire est généré. Comme ce mot de passe aléatoire n'est pas connu, il doit être modifié par l'administrateur.

Dans le système de communication, les paramètres correspondants sont réalisés à l'aide de l'assistant "Téléphonie centrale" ou à l'aide de Manager E.

Durant le démarrage du système, la liste des mots de passe est vérifiée et une entrée EventLog (affichage d'événement) est effectuée si un abonné SIP a été configuré sans mot de passe.

Conseil : Si le système de communication est utilisé comme routeur Internet, le port 5060 doit être fermé (paramètre par défaut). Dans le cadre de la téléphonie Internet via ITSP, le système de communication ouvre les ports correspondants et les maintient ouverts.

Même si l'on utilise un routeur externe ou un pare-feu, le port 5060 doit être fermé. Il est de la responsabilité du système de communication d'ouvrir ce port (si nécessaire).

20 Mise en réseau de OpenScape Business

Les systèmes de communication OpenScape Business peuvent être mis en réseau les uns avec les autres ainsi qu'avec les systèmes de communication OpenScape 4000 (HiPath 4000) et OpenScape Voice. A l'intérieur d'un réseau homogène OpenScape Business, les abonnés sont en mesure d'utiliser des fonctionnalités comme Etat Présence, Messagerie vocale, Conférences, et bien d'autres, de la manière dont on pouvait le faire uniquement dans un seul système de communication OpenScape Business jusqu'ici.

Mises en réseau possible :

- Pure mise en réseau vocale d'OpenScape Business X
- Mise en réseau OpenScape Business X et OpenScape Business S (en option avec UC Suite ou UC Smart).
- OpenScape Business X avec OpenScape 4000 (fonctionnalité UC avec OpenScape Business uniquement dans certaines conditions)
- OpenScape Business X avec OpenScape Voice (sans fonctionnalité UC avec OpenScape Business)
- Association de connexions externes à OpenScape Business via interconnexion SIP.
- Mise en réseau par RNIS
- Interconnexion de réseaux OpenScape Business avec raccordement réseau ITSP central

Les systèmes de communication sont préparés pour la mise en réseau à l'aide de l'assistant **Configuration de la mise en réseau**. Dans cet assistant, il est indiqué s'il s'agit d'un noeud maître ou esclave. De plus, il est affecté automatiquement 16 lignes au faisceau 16 (Mise en réseau).

Tous les réseaux qui utilisent les fonctionnalités communications unifiées (comme UC Smart ou UC Suite) doivent faire référence à un plan de numérotation fermé. Les réseaux sans fonctionnalités Unified Communications peuvent être basées sur un plan de numérotation ouvert ou fermé. Pour être en mesure de répondre de manière flexible aux souhaits d'extension des clients, il est conseillé d'utiliser la numérotation fermée lors de la création d'une nouvelle interconnexion de réseaux.

Conseil : La configuration d'un réseau IP est une procédure complexe et ne devrait donc être effectuée que par des techniciens de maintenance expérimentés.

Il ne peut pas y avoir de réseau OpenScape Business X1 pur car un système X1 ne peut pas être un système maître. Il faut nécessairement un système maître dans un réseau.

La mise en réseau de OpenScape Business avec les systèmes ci-après n'est pas supportée.

- HiPath 3000 SIP-Q, uniquement supporté mise en réseau TDM sur base S_0/ S_{2M} avec CorNet NQ, voir Mise en réseau par RNIS.
- HiPath 5000 RSM
- OpenScape Office MX
- OpenScape Office LX

La migration de HiPath 3000 (y compris HiPath 5000 RSM) vers OpenScape Business est décrite au chapitre Migration.

Remarque : Pour plus d'informations sur les licences et la mise à niveau ou la migration des systèmes dans un réseau, voir la section **Réseau - Licences** du chapitre Mises à jour .

20.1 Plan de mise en réseau

Avant d'effectuer la mise en réseau, il est recommandé d'établir un plan du réseau après avoir consulté le client.

Le plan du réseau doit comprendre les données suivantes :

- ID de noeud (Node-ID) et adresses IP correspondantes
- Plan de numérotation

20.1.1 Réseaux homogènes et hétérogènes

En général, on distingue dans la mise en réseau les réseaux homogènes (où tous les composants appartiennent à une seule famille de systèmes) et les réseaux hétérogènes (avec des systèmes différents).

Réseau homogène (natif)

Réseau hétérogène (hybride)

Un réseau homogène (natif) est constitué de composants de la famille de systèmes OpenScape Business.

Un réseau hétérogène (hybride) est constitué de composants de la famille de systèmes OpenScape Business et d'un OpenScape 4000 ou d'un OpenScape Voice, par exemple.

Vue d'ensemble de tous les nœuds métier OpenScape du réseau

Tous les nœuds Unify OpenScape Business d'un inter-réseau peuvent être affichés via l'entrée **Réseau** dans la barre de navigation du Web based Management (Web admin). De plus, tous les terminaux Unify OpenScape Business de l'inter-réseau peuvent être affichés triés par nœud.

Les informations suivantes peuvent être affichées :

- **ID de nœud** : ID de nœud
- **M** / **S** : Identification pour savoir si le nœud est Maître ou Esclave
- **Nom net** : nom du nœud
- **Type** : type du nœud (**OSBiz X** : modèle matériel, **OSBiz S** : softswitch)
- **OSBiz X / OSBiz S** : adresse IP du nœud, à cliquer (ouvre le WBM du nœud)
- **Statut de l'enregistrement** : statut de l'enregistrement
- **Alive** : indique si le noeud est actif ou non

20.1.1.1 Comment afficher la présentation de tous les noeuds OpenScape Business

Conditions préalables

Plusieurs systèmes de communication OpenScape Business sont mis en réseau les uns avec les autres.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mise en réseau**.
2) Dans l'arborescence de navigation, cliquez sur **Vue des noeuds**. Tous les noeuds OpenScape Business sont listés dans l'interconnexion de réseaux.

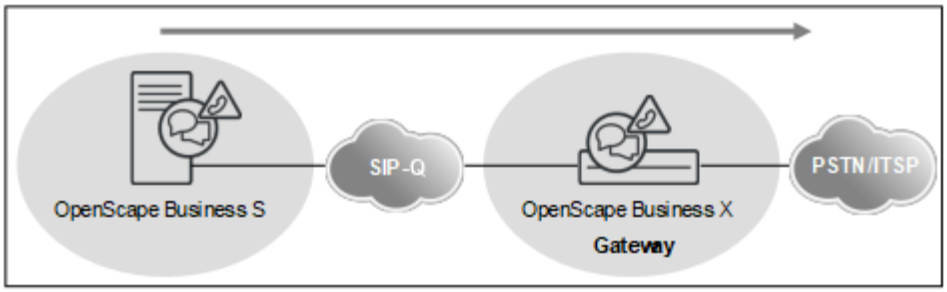
20.1.2 Mono-passerelle et multi-passerelle

Lors de la mise en réseau d'OpenScape Business, on fait la distinction entre passerelle unique et multipasserelle. La passerelle unique décrit la mise en réseau avec une seule passerelle tandis que la multipasserelle décrit la mise en réseau avec plusieurs passerelles.

Mono-passerelle

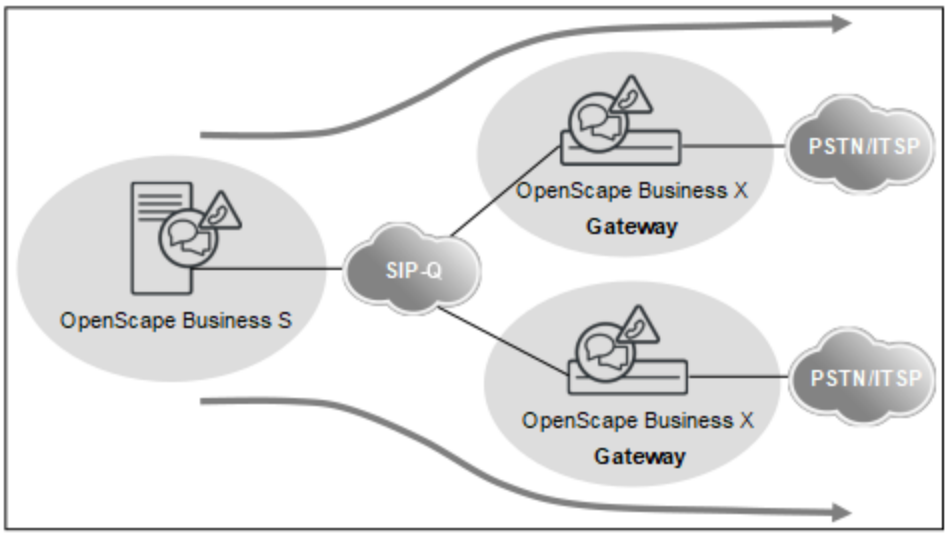
Multi-passerelle

Dans un réseau mono-passerelle, les appels en provenance et en direction du serveur sont acheminés via une seule passerelle. Tous les abonnés IP qui sont enregistrés sur le serveur utilisent cette passerelle.



- Est supporté lorsqu'un ou plusieurs OpenScape Business S se trouvent dans le réseau.
- Les abonnés IP sont raccordés aux systèmes de communication les plus divers.
- OpenScape Business X est utilisé comme passerelle.

Dans un réseau multi-passerelle, les appels sont acheminés via plusieurs passerelles OpenScape Business différentes.



- Un seul fournisseur RTC ou un numéro réseau par passerelle
- Les abonnés de différents sites sont enregistrés sur un système central (OpenScape Business S).
- Il est affecté à chaque abonné d'OpenScape Business S une passerelle définie (OpenScape Business X).
- Il doit y avoir un seul OpenScape Business S par réseau.
- OpenScape Business et OpenScape Business S se trouvent dans le même fuseau horaire et dans le même pays (même code de pays).
- Il y a uniquement un indicatif réseau sur l'ensemble du réseau.
- Au niveau des passerelles, il est possible de paramétrer localement des abonnés RNIS et analogiques.

20.2 Fonctionnalités sur l'ensemble du réseau

Les fonctionnalités Voix sur l'ensemble du réseau sont pour l'essentiel déterminées par le protocole de mise en réseau SIP-Q. Les fonctionnalités UC sur l'ensemble du réseau sont déterminés par la mise en réseau de la solution UC (UC Suite ou UC-Smart) et de leurs clients UC.

20.2.1 Fonctionnalités à l'échelle du réseau des solutions UC

Le tableau suivant vous donne un aperçu des fonctionnalités réseau des deux solutions UC, UC Smart et UC Suite.

L'interfonctionnement UC utilisant à la fois OpenScape 4000 et OpenScape Voice n'est pas possible. Dans un réseau OpenScape Business, il convient d'utiliser soit UC Smart, soit UC Suite. Les solutions UC mixtes ne sont pas prises en charge.

Fonctionnalités de communications unifiées à l'échelle du réseau	UC Smart	Suite UC	
	myPortal au travail	myPortal pour ordinateur de bureau / Outlook	myPortal au travail
Visibilité à l'échelle du réseau du statut de présence (gestion de la présence)	x	x	x
Modification de son propre statut de présence via le client	x	x	x
Modification de son propre statut de présence via le TUI	x	x	x
Transfert d'appel basé sur le statut	x	x	Via des destinations définies dans d'autres clients UC Suite
Affichage de l'état du réseau dans les favoris	x	x	x
Affichage de l'état du réseau dans les répertoires	x	x	x
Affichage de l'état du réseau dans le Journal	-	x	-
Activer le service CallMe	-	x	x
Intégration du calendrier (Outlook)	-	x	-
Intégration du calendrier (iCal) (uniquement avec myPortal pour ordinateur)	-	x	-
Affichage à l'échelle du réseau de l'état des appels (libre, occupé, en sonnerie)	x	x	x
Création de groupes à l'échelle du réseau	x	x	-
Affichage compact des favoris	-	x	-
Conversations	x	-	x

Fonctionnalités de communications unifiées à l'échelle du réseau	UC Smart	Suite UC	
	myPortal au travail	myPortal pour ordinateur de bureau / Outlook	myPortal au travail
Annuaire personnel	Locale	Locale	Locale
Répertoire interne	Locale	Locale	Locale
Répertoire externe	-	x	x
Recherche dans les annuaires à l'échelle du réseau	x	x	x
Accès aux destinations en numérotation abrégée définies dans le système (SSD)	Locale	-	Locale
Importer/Gérer les contacts personnels (CSV/XML)	x	x	-
Accès aux contacts Outlook	x	x	-
Importer les contacts personnels (Mac OS) (myPortal pour ordinateur)	-	x	-
Intégration d'un serveur d'annuaire externe via LDAP	-	x	-
Tous les appels	x	x	x
Appels à candidatures ouverts	-	x	-
Appels manqués	x	x	x
Répondre aux appels	x	x	x
Appels programmés	-	x	-
appels VoIP	x	x	x
Journal de télécopie	-	x	-
numérotation manuelle	x	x	x
Composeur de bureau (cliquer pour appeler)	-	x	-
Expéditeur	x	x	x
Mettre l'appel en attente	x	x	x

Fonctionnalités de communications unifiées à l'échelle du réseau	UC Smart	Suite UC	
	myPortal au travail	myPortal pour ordinateur de bureau / Outlook	myPortal au travail
Enregistrement des appels (enregistrement vocal)	-	x	-
Envoyer un courriel	x	x	x
Envoyer un SMS	-	-	-
Fenêtres contextuelles	x	x	x
Conférence ad hoc	x	x	x
Conférences programmées	-	x	-
Conférences permanentes et ouvertes (conférence par glisser-déposer)	x	x	-
Intégration de la collaboration Web	x	x	x
Boîte vocale (messagerie vocale visuelle)	x	x	x
Écouter les messages vocaux par téléphone	x	x	x
Écouter les messages vocaux via la carte son du PC	-	x	-
Comment envoyer un message vocal par e-mail	x	x	-
Télécopie (pour les systèmes d'exploitation Windows)	-	x	-
Messagerie instantanée (chat) à l'échelle du réseau	x	x	-

20.2.2 Fonctionnalités Voix sur l'ensemble du réseau

Dans une mise en réseau à l'aide du protocole SIP-Q, les fonctionnalités vocales suivantes sont supportées pour OpenScape Business et les autres systèmes de communication.

Fonctionnalité	SIP-Q (réseau IP)
Appel de base	Oui
Rappel sur occupation	Oui
Rappel sur non réponse	Oui
Entrée en tiers	Oui
Avertissement	Oui
Deuxième appel	Oui
Calling Line Identification Presentation CLIP (présentation du numéro de l'appelant)	Oui
Calling Line Identification Restriction CLIR (restriction de présentation du numéro de l'appelant)	Oui
Connected Line Identification Presentation COLP	Oui
Connected Line Identification Restriction COLR	Oui
Calling / Connected Name Identification Presentation CNIP (Appel/Présentation du nom de l'appelant)	Oui
Calling / Connected Name Identification Restriction CNIR (Appel/Restriction de la présentation du nom de l'appelant)	Oui
Ne pas déranger	Oui
Renvoi d'appel	Oui
Renvoi temporisé sur occupation	Oui
Renvoi temporisé sur non réponse	Oui
Call Deflection (renvoi d'une liaison)	Oui
Service de télétaxation lors de l'établissement de l'appel	non
Service de télétaxation durant l'appel	Oui
Service de télétaxation à la fin de l'appel	Oui
Optimisation route	non
Reroutage	non
Message Waiting Indication / Info	Oui
Appels malveillants	Oui
Mise en garde	Oui
Va-et-vient	Oui
Transfert	Oui
Conférence	Oui
Retour d'appel	Oui
Appel d’urgence	Oui
Renvoi distinct	Oui
Private Numbering Plan PNP (plan de numérotation privé)	non

Fonctionnalité	SIP-Q (réseau IP)
Interception d'appel	non
Groupe de recherche	Oui
SPE (sauf conférence et applications)	oui

20.3 Procédure de licence d'une interconnexion de réseaux

Pour un système de communication en réseau, on peut choisir une procédure de licence centralisée.

Toutes les licences des sytèmes individuels sont regroupées en une licence pour l'ensemble du réseau dans le serveur de licences. Dans l'interconnexion de réseaux les licences peuvent être attribuées librement aux différents noeuds, via le WBM.

Informations supplémentaires, voir Procédure de licence de plusieurs systèmes de communication (interconnexion de réseaux).

20.4 Exigences pour la mise en réseau

Afin de garantir la qualité de la transmission de la voix, les réseaux IP utilisés et le système de communication doivent répondre à certaines exigences. La qualité vocale et la fiabilité de la communication voix dépendent de la technologie utilisée sur le réseau.

Paramètres réseau, exigences pour LAN et WAN

Paramètres	Exigence minimale	Remarque
Delay (one way) (temps d'aller simple)	50 ms	Des valeurs plus élevées dégradent la qualité de la voix.
Round Trip Delay (temps de propagation aller-retour)	100 ms	Des valeurs plus élevées dégradent la qualité de la voix.
Gigue	20 ms	Des valeurs plus élevées dégradent la qualité de la voix.
Packet Loss (perte de paquet)	3%	En cas de transmission par fax ou modem via G.711, la perte de paquets ne doit pas dépasser 0,05 % (dans le cas où aucun T.38 n'est possible).
Consecutive Packet Loss (perte de paquet consécutive)	3 avec G.711	Des valeurs plus élevées dégradent la qualité de la voix.

Recommandation pour le calcul de la bande passante

- Dans une interconnexion de réseaux, il faut disposer d'une bande passante d'au moins 256 bit/s (dans le sens émission et dans le sens réception).
- Le calcul de la bande passante doit se baser sur l'hypothèse d'une part de 50% maxi. pour la voix par rapport à la bande passante totale. Sur un WAN 1 Mbit, il faut donc affecter au maximum 500 kbits/s à la voix. Pour le codec G.711, il s'agit par exemple de 5 lignes IP au maximum.
- Indépendamment de cela, il faut tenir compte des caractéristiques réseau comme QoS (qualité de service), Delay (retard), Packet Loss (pertes de paquets) etc.

20.4.1 Exigences pour la mise en réseau LAN.

Afin de garantir la qualité de transmission de la voix et des données, les réseaux IP utilisés et le système de communication doivent répondre à certaines exigences concernant le LAN.

Exigences relatives au LAN

Le réseau de données doit être de type Ethernet.

- Sont recommandés au moins les câbles Cat.5 (câbles multifils blindés/ non blindés jusqu'à 100 MHz, pour montage horizontal et vertical selon EN 50288).
- Assistance pour QoS : IEEE 802.1p, DiffServ (RFC 2474).
- Tous les ports LAN activés doivent supporter 100 / 1000 Mbit/s et la communication en duplex intégral.

Chaque système de communication doit être raccordé via un commutateur ou via un port dédié d'un routeur. Les hubs ou répéteurs ne sont pas supportés.

Connexions Payload avec RTP (Realtime Transport Protocol) dans un environnement LAN.

La bande passante nécesssaire pour la transmission de la voix dans un réseau IP peut être calculée à l'aide du tableau ci-après.

Type de codec	Paramètre de mise en paquet	Taux d'échantillonn (ms)	Charge utile (octets)	Longueur des paquets Ethernet (octets)	Charge utile paquet (surdébit en pourcentage)	Charge Ethernet (y compris l'en-tête) (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

La charge dans le LAN s'applique à la direction Envoi comme à la direction Réception.

Le calcul englobe le VLAN-Tagging selon IEEE 802 1q. Sans VLAN-Tagging, la longueur d'un paquet est inférieure de 4 octets.

Le surdébit se calcule de la manière suivante.

Protocole	octets
En-tête RTP	12
En-tête UDP	8
En-tête IP	20
802.1Q VLAN Tagging	4
MAC (y compris préambule, FCS)	26
Total	70

Transport Payload en environnement LAN T.38

	Taux d'échantillonnag (ms)	Charge utile (octets)	Longueur des paquets Ethernet (octets)	Charge utile paquet (surdébit en pourcentage)	Charge Ethernet (y compris l'en-tête) (kbit/s)
T.38	30	169	227	34%	60,5

Liaisons Payload avec SRTP (Secure Realtime Transport Protocol) dans un environnement LAN :

Type de codec	Taux d'échantillonna (ms)	Charge utile (octets)	Longueur des paquets Ethernet (octets)	Longueur de paquet SRTP-Ethernet (kbit/s)	Longueur de paque RTP-Ethernet (kbit/s	Large de bande supplémentaire pour SRTP (%)
G.711	20	160	244	97,6	92	6,1
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

20.4.2 Plan de numérotation dans le réseau

Le plan de numérotation est une condition importante pour la mise en réseau. En fonction du plan de numérotation, la configuration des réseaux interconnectés est plus ou moins lourde. Open Scape Business supporte dans l'interconnexion de réseaux la numérotation ouvert comme la numérotation fermée, toutefois l'intégralité des fonctionnalités UC ne peut être utilisée qu'en numérotation fermée.

Numérotation fermée

En numérotation cachée (fermée), un abonné du réseau est identifié de manière univoque par son numéro d'abonné. Chaque abonné du réseau peut joindre un autre abonné en composant directement son numéro d'appel.

La numérotation fermée présente l'avantage de ne pas exiger la composition du numéro du nœud pour joindre un abonné dans un autre système de communication en réseau.

Tableau 10 : Exemple de numérotation fermée

	Noeud 1	Noeud 2	Noeud 3	Noeud 4
Numéros de téléphone	100	200	300	400
	101	201	301	401
	102	202	302	402
	103	203	303	403
	104	204	304	404

Numérotation ouverte

Dans le cas de la numérotation ouverte, chaque abonné est identifié de façon univoque par le numéro de téléphone du nœud et le numéro d'abonné. Des utilisateurs de différents systèmes de communication (nœuds) à l'intérieur de l'interconnexion de réseaux peuvent donc avoir le même numéro de téléphone.

Dans le cas de la numérotation ouverte, outre le numéro d'appel de l'abonné, il est nécessaire composer également le numéro de téléphone du nœud. Pour cela, il est possible d'employer à plusieurs reprises les plages de numéros d'appel et, par conséquent d'utiliser davantage de numéros.

Les fonctionnalités UC suivantes ne sont pas supportées localement avec une numérotation ouverte :

- UC Smart
- UC Suite
- CSP sur l'ensemble du réseau (CSTA Service Provider)
- Serveur DSS
- CMD (CSTA Message Dispatcher)

Tableau 11 : Exemple de numérotation ouverte :

	Noeud 1	Noeud 2	Noeud 3	Noeud 4
Numéro de téléphone du nœud (numéro PABX)	15	96	97	98
Numéros de téléphone	100	100	100	100
	101	101	101	101
	102	102	102	102
	103	103	103	103
	104	104	104	104

20.4.2.1 Sélection des numéros de téléphone publics dans le réseau

Indépendamment de la numérotation fermée ou ouverte, il est judicieux de sélectionner des destinations interne au noeud comme des destinations internes au réseau via des numéros d'appel publics. (Par ex. en tant que UC Client qui sélectionne les contacts au format pleinement qualifié à partir des répertoires).

20.5 Optimisation de route (Path Replacement)

A l'aide de l'optimisation de route (Path Replacement), on évite les doubles occupation de lignes IP sur les systèmes de communication en réseau.

Lorsque plusieurs systèmes OpenScape Business sont mis en réseau, le problème suivant peut par exemple survenir : Tout d'abord, supposons que l'abonné A appelle l'abonné B qui, à son tour, a transféré tous les appels à l'abonné C. Les abonnés A et C sont connectés au même nœud de réseau, mais l'abonné B est connecté à un autre nœud de réseau. C'est pourquoi, l'appel avec renvoi occupe tout d'abord deux lignes entre les deux noeuds de réseau. Pour éviter cette double occupation, il faut activer l'optimisation de l'acheminement.

Conseil : Le drapeau système de l'optimisation de route doit être activé sur tous les systèmes OpenScape Business en réseau !

: Il est fortement conseillé de ne pas utiliser la fonction Path Replacement dans les réseaux où des stations de fax analogiques sont utilisées. Cette limitation sera levée avec une prochaine version du logiciel.

L'optimisation de route est effectuée :

- A l'intérieur de la partie réseau OpenScape Business
- Après établissement de la liaison (pas durant la phase d'appel) !
- Après les scénarios de transfert
- Après renvoi temporisé ou renvoi d'appel

L'optimisation de route n'est pas effectuée :

- Avec un pilotage ou un appel de groupe
- Dans les conférences
- Si une autre fonctionnalité est activée durant l'optimisation d'une route, cette optimisation est interrompue.
- Dans un réseau non homogène, les systèmes tiers sont configurés via l'interconnexion SIP. Dans ce cas, indépendamment de la configuration du flag, aucun remplacement de chemin possible (par ec. OpenScape 4000, OpenScape Voice, serveurs SIP externes).

20.5.1 Comment activer ou désactiver l'optimisation de route (Path Replacement) Activer ou désactiver

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous voulez que l'interception des retours d'appel soit possible, cochez la case **Optimisation de route**.
   - Si vous ne voulez pas que l'interception des retours d'appel soit possible, décochez la case **Optimisation de route**.
5) Cliquez sur **Appliquer** puis sur **OK**.

20.6 Scénarios de mise en réseau

Il existe plusieurs scénarios pour mettre en réseau les systèmes OpenScape Business les uns avec les autres et avec d'autres systèmes de communication.

- Mise en réseau de plusieurs OpenScape Business X
- Mise en réseau de OpenScape Business X et OpenScape Business S (passerelle unique)
- Mise en réseau de OpenScape Business X et OpenScape Business S (multipasserelle)
- Mise en réseau de OpenScape Business S dans un environnement d'hébergement
- Mise en réseau de OpenScape Business X et OpenScape 4000
- Mise en réseau de OpenScape Business X et OpenScape Voice
- Association de connexions externes à OpenScape Business via interconnexion SIP
- Numérotation ouverte dans les réseaux OpenScape Business X
- Mise en réseau par RNIS
- Interconnexion de réseaux OpenScape Business avec raccordement réseau ITSP central

Les données de communication ne peuvent être appelées que par noeud de réseau, et non pas pour l'ensemble du réseau.

20.6.1 Fonctions et restrictions

Pour les scénarios de mise en réseau, il faut tenir compte de différentes dépendances et restrictions.

Fonctions et restrictions

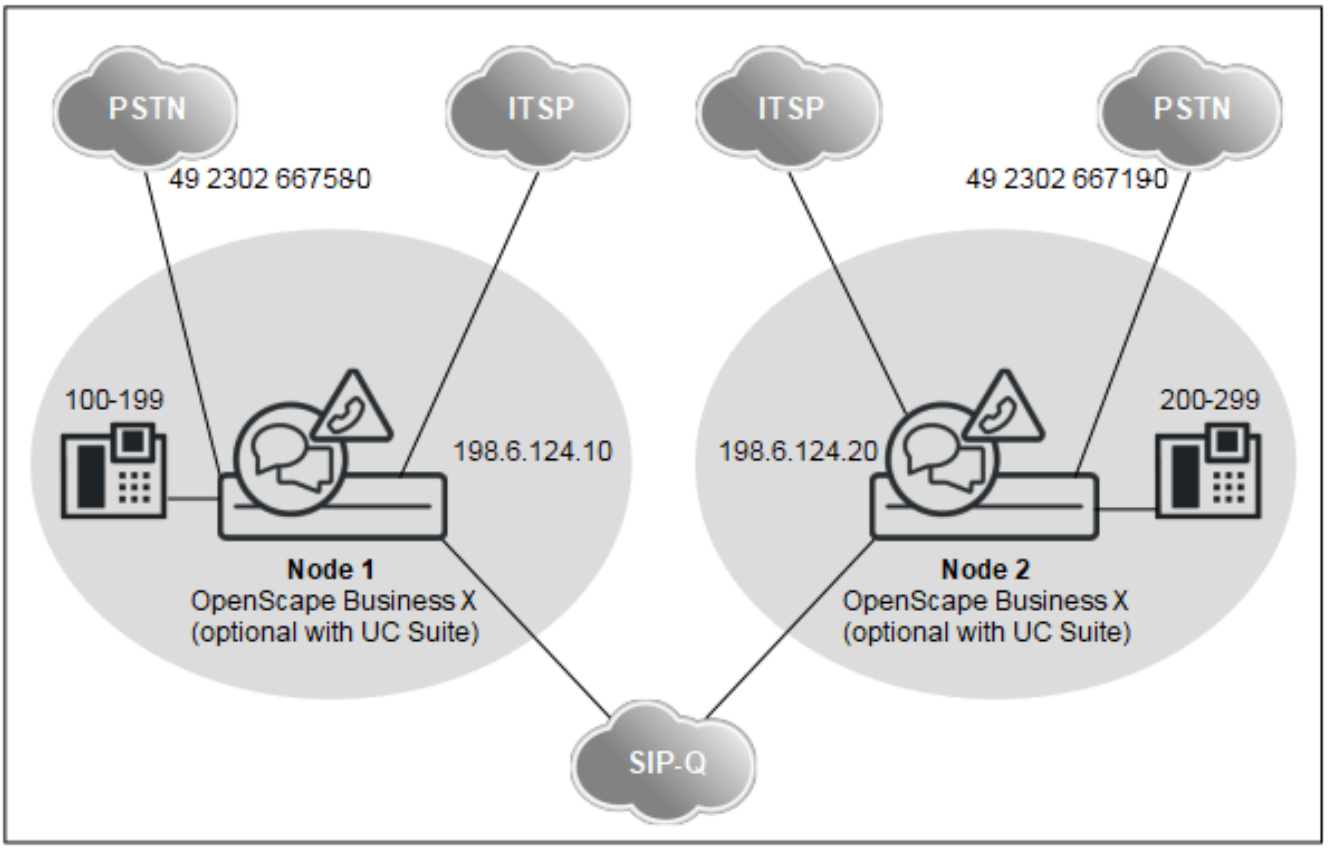
- Chaque système de l'interconnexion de réseaux est affecté à son propre fuseau horaire. Tous les abonnés d'un système sont donc dans le même fuseau horaire.
- Les mises en réseau multi-passerelle OpenScape Business S ne sont validées qu'à l'intérieur d'un pays (même fuseau horaire, même code d'accès CO).
- D'une manière générale, les interconnexions de réseaux de OpenScape Business sont configurées par des assistants. OpenScape Voice et OpenScape 4000 en réseau sont configurés en mode Expert par noeud.
- Le gestionnaire de présence (fonctionnalité DSS Server = affichage sur l'ensemble du réseau des états Présence sur les touches DSS + interception d'appel) est disponible dans les réseau OpenScape Business.
- Les lignes SIP-Q avec voie 16 (dernière voie) sont utilisées afin de configurer à l'aide de l'assistant **Configuration du réseau** des systèmes de communication OpenScape Business homogènes. Les lignes SIP externes (interconnexion SIP) sont utilisées pour la mise en réseau de OpenScape 4000, OpenScape Voice ou autres systèmes de communication ; la configuration est effectuée à l'aide du mode Expert.
- Si le système est configuré comme Esclave ou Maître à l'aide de l'assistant **Configuration du réseau**, il est vérifié si des lignes sont affectées à la voie "Mise en réseau". Si ce n'est pas le cas, il est affecté automatiquement 16 lignes à la voie "Mise en réseau". Si le système est retiré de l'interconnexion de réseaux, ces affectations demeurent.
- Dans chaque noeud, UN SEUL système de messagerie vocale peut être utilisé. D'une manière générale, différents systèmes de messagerie vocale sont autorisés dans une interconnexion de réseaux OpenScape Business :
  - Lorsque UC Suite est utilisé, les autres systèmes de messagerie vocale existant dans l'interconnexion de réseaux doivent être désactivés par l'administrateur.
  - Une interconnexion de réseaux HiPath 3000 disposant de différents systèmes de messagerie vocale peut migrer 1:1 vers OpenScape Business.
- Pour des raisons techniques, les systèmes OpenScape Business X1 ne peuvent pas être configurés comme maîtres. Étant donné qu'un système maître est nécessaire dans chaque réseau OpenScape Business, au moins un système doit être supérieur à X1.

Conseil : Les limites opérationnelle peuvent différer de ces indications (ainsi que des indications suivantes figurant dans les différents scénarios). Veuillez tenir compte des indications figurant dans les informations commerciales.

20.6.2 Mise en réseau de plusieurs systèmes OpenScape Business X

Il est possible de mettre en réseau jusqu'à 32 systèmes de communication OpenScape Business X.

Données réseau



- Avec une solution UC (UC Smart ou UC Suite) : seule la numérotation fermée est possible.
- Sans solution UC : numérotation fermée ou ouverte possible
- Configuration via WBM (assistants) lors de l'utilisation d'une numérotation fermée
- Jusqu'à 32 systèmes en réseau et 1500 utilisateurs sans solution de communications unifiées
- Jusqu'à 8 systèmes en réseau et 1500 utilisateurs avec solution de communications unifiées

Fonctionnalités à l'échelle du réseau

Réseautage UC	Numérotation fermée	Numérotation ouverte
Nombre maximal de nœuds	8 avec solution UC et 32 sans solution UC	
Nombre maximal de stations dans un seul système de communication	Selon OpenScape Business X	
Nombre maximal de stations dans le réseau	1500	

Administration	Numérotation fermée	Numérotation ouverte
WBM	Administration à l'échelle du réseau à l'aide d'assistants	Administration du réseau en mode Expert
Gestionnaire E	Administration à l'échelle du réseau pour les tâches spéciales	Administration à l'échelle du réseau pour les tâches spéciales

Administration	Numérotation fermée	Numérotation ouverte
Administration de UC Suite	Administration à l'échelle du réseau à l'aide d'assistants	Non pris en charge
Importation massive de données via des fichiers CSV (numéros d'appel, numéros DID, noms)	Séparément pour chaque nœud du réseau	

Licence	Numérotation fermée	Numérotation ouverte
structure de licence	Une licence réseau est requise pour chaque nœud.	

Configuration

Cette configuration (avec numérotation fermée et UC Suite) illustre les étapes nécessaires à la mise en place du réseau à l'aide d'un exemple.

Prérequis :

- Un forfait réseau est disponible. Le plan de réseau a été utilisé pour garantir que chaque numéro d'appel interne du réseau ne soit utilisé qu'une seule fois pour la numérotation fermée. La longueur des numéros de station peut varier. Seuls les numéros de station DID peuvent apparaître plus d'une fois (par exemple, les numéros de station CO 49 2302 66758 100 et 49 2302 66719 100 ont le même numéro DID 100).

  Conseil : Il pourrait être nécessaire d'adapter la numérotation des stations. Aucun système de numérotation ouvert n'est mis en œuvre !

- Le réseau IP a été configuré et tous les nœuds peuvent être contactés par ping avec succès.
- Tous les nœuds ont été mis à niveau vers la même version du logiciel.

Transfert d'appel entre nœuds : pour les appels entrants via des lignes IP déjà transférés, aucun autre transfert vers la messagerie vocale n'est effectué. En effet, il est impossible autrement d'attribuer une adresse vocale unique à cette boîte vocale.

Si des règles de délégation inter-nœuds (extensions de référence) sont nécessaires, celles-ci doivent être configurées via les profils des stations OpenScape Business ou des groupes de sonnerie. Les appels inter-nœuds correspondants ne sont pas signalés comme étant transférés dans ce cas, mais comme des appels DSS (sélection directe de station). Les transferts d'appels du député sont donc redirigés vers la messagerie vocale.

Tableau 12 : Configuration des données de localisation pour le nœud 1

Nœud 1	
G.-Pays de localisation	49
G.-Localisation Réseau local	2302
Système de géolocalisation G.	66758
Préfixe international	00
Préfixe national	0

Nœud 1		
Itinéraires		
ISDN	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 1 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 13 : Aperçu des entrées du LCR pour le nœud 1

Plan de numérotation		Table de routage			règle à cadran		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Noeud 2 Internat	0C0049230266719-Z	Réseautage	Obligatoire	2	D49230266719E3A	Réseau d'entreprise	International
NAT du nœud 2	0C0230266719-Z						
Station Node 2	0C66719-Z						
CO	0CZ	ISDN	Non		UN	Fournisseur principal de réseau	Inconnu
Divers	-Z	Réseautage	Non		UN	Réseau d'entreprise	Inconnu

Tableau 14 : Configuration des données de localisation pour le nœud 2

Nœud 2		
G.-Pays de localisation		49
G.-Localisation Réseau local		2302
Système de géolocalisation G.		66719
Préfixe international		00
Préfixe national		0
Itinéraires		
ISDN	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		

Nœud 2		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 2 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 15 : Aperçu des entrées du LCR pour le nœud 2

Plan de numérotation		Table de routage			règle à cadran		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Nœud 1 Internat	0C0049230266758-Z	Réseautage	Obligatoire	1	D49230266758E3A	Réseau d'entreprise	International
NAT du nœud 1	0C0230266758-Z						
Station du nœud 1	0C66758-Z						
CO	0CZ	ISDN	Non		UN	Fournisseur principal de réseau	Inconnu
Divers	-Z	Réseautage	Non		UN	Réseau d'entreprise	Inconnu

Procédure de configuration du réseau :

1) Configurer l'installation de base pour le nœud 1 (maître)
2) Configuration du réseau pour le nœud 1
3) Configurer l'installation de base pour le nœud 2 (esclave)
4) Configuration du réseau pour le nœud 2
5) Vérifiez la fonction réseau du maître.
6) Vérifier les itinéraires et les paramètres de routage (maître)
7) Vérifier les itinéraires et les paramètres de routage (Trk. Grp. 16) (maître)
8) Configurer LCR pour la mise en réseau (maître)
9) Vérifier les itinéraires et les paramètres de routage (esclave)
10) Configurer LCR pour la mise en réseau (esclave)

20.6.2.1 Comment configurer l'installation de base pour noeud 1 (Maître)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Installation de base**.
4) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
5) Entrez l'**indicatif local** et le **numéro de l'installation**.
6) Cochez la case **Intégration réseau**.
7) Dans le champ **ID de noeud** attribuez à OpenScape Business un ID de noeud univoque à l'intérieur de l'interconnexion de réseaux ("**1**" dans l'exemple de configuration présenté).
8) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.
9) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
10) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

---

11) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.
12) Configurez maintenant les clients IP.
13) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
14) Configurez maintenant l'envoi d'e-mails.
15) Cliquez sur **Quitter**.

20.6.2.2 Comment configurer la mise en réseau pour le noeud 1 (Maître)

Dans l'étape suivante, l'assistant de mise en réseau est configuré.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.

3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.
5) Définissez le type de noeud (**Maître**).
6) Dans **ID noeud**, entrez les numéros de noeud respectifs des systèmes OpenScape Business correspondants (dans l'exemple de configuration, ceux des Esclaves avec ID de noeud 2).
7) Dans **Adresse IP**, entrez les adresses IP des systèmes OpenScape Business correspondants (dans l'exemple de configuration, ceux des Esclaves avec ID de noeud 2).
8) Dans **Nom**, indiquez le type correspondant de sous-installation.
9) Si nécessaire, cochez la case **Chiffrement**.

Conseil : Le cryptage est basé sur SPE et ne s'applique pas aux applications.

Remarque : Le fait de cocher la case ne signifie pas que le cryptage est configuré. Voir Cryptage de la signalisation et de la charge utile SPE .

---

10) Cliquez sur **Terminer**.

20.6.2.3 Comment configurer l'installation de base pour le noeud 2 (Esclave)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
4) Entrez l'**indicatif local** et le **numéro de l'installation**.
5) Cochez la case **Intégration réseau**.
6) Dans le champ **ID de noeud** pour OpenScape Business S, attribuez un ID de noeud univoque à l'intérieur de l'interconnexion de réseaux ("**2**" dans l'exemple de configuration présenté).
7) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.

8) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
9) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

---

10) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.
11) Configurez maintenant les clients IP.
12) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
13) Configurez maintenant l'envoi d'e-mails.
14) Cliquez sur **Quitter**.

20.6.2.4 Comment configurer la mise en réseau pour le noeud 2 (Esclave)

Dans l'étape suivante, l'assistant de mise en réseau est configuré.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.
5) Dans **Type de noeud** , cochez la case **Ce système est un noeud ESCLAVE**.
6) Dans **Adresse IP**, entrez l'adresse IP du maître.

Conseil : Une fois que vous aurez cliqué sur **OK&Suivant**, cette action ne pourra plus être annulée.

---

7) L'**Etat de l'enregistrement** est affiché avec l'**Etat succès** (ou avec un message d'erreur correspondant). La tâche de l'assistant est maintenant terminée.
8) Cliquez sur **Terminer**.

20.6.2.5 Comment contrôler la fonction de mise en réseau pour Maître

Vous pouvez contrôler l'état du réseau en général et les différents numéros de téléphone.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Réseau**.
2) Dans la ligne d'état figure l'**État de la synchronisation** pour le réseau. Vert signifie que le réseau n'a pas de problème, rouge signale des problèmes dans le réseau.
3) Sélectionnez dans la fenêtre **Réseau** l'onglet **Affichage du noeud** ; le système indique tous les noeuds disponibles avec **ID du noeud**, **Nom**, **Type de système**, **Adresse du serveur**, **Etat de l'enregistrement** et **Etat de disponibilité**.
4) Sélectionnez dans la fenêtre **Réseau** l'onglet **Numéros de téléphone** ; le système ouvre une fenêtre avec toutes les indications sur :
   - **Numéro de téléphone**
   - **SDA**
   - **Nom**
   - **Type de port**
   - **Noeud**

20.6.2.6 Comment configurer les faisceaux et les paramètres du faisceau (réseau RNIS pour le maître)

Les étapes suivantes permettent de configurer les faisceaux pour la mise en réseau du maître.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Dir. 1` pour la ligne réseau.
5) Dans **Préfixes faisceaux** entrez `0`.
6) Dans **Numéro de l'installation-entrant** , dans le champ **Indicatif national** entrez `49`.
7) Dans **Numéro de l'installation-entrant**, dans le champ **Indicatif du réseau local** entrez `2302`.
8) Dans **Numéro de l'installation-entrant**, dans le champ **Numéro de l'installation** entrez `66758`.

9) Cochez la case **Numéro de l'installation-entrant**, dans le champ **Numéro de site**.
10) Cliquez sur **Appliquer** puis sur **OK**.

20.6.2.7 Comment configurer les faisceaux et les paramètres de faisceau (faisc. 16) (Maître)

Pour le faisceau 64 (mise en réseau) il est indispensable de remplir l'entrée correspondant au 2e indicatif pour Maître et Esclave. Le faisceau 16 est le faisceau par défaut pour la mise en réseau avec OpenScape Business.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur le dernier **faisceau** (**Faisc. 16**).
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Mise en réseau` pour le sens de la mise en réseau.
5) Dans **Préfixes faisceaux**, n'indiquez rien.
6) Dans **Indicatif réseau (2e indicatif réseau)** entrez 0.
7) Il est possible de reprendre les paramètres par défaut du faisceau (type de n °, sortant, type de numéro de téléphone.
8) Cliquez sur **Appliquer** puis sur **OK**.

20.6.2.8 Comment configurer LCR pour la mise en réseau (Maître)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33 et 34 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour le noeud 2. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal for Desktop).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.

4) Entrez les valeurs suivants sur les emplacements vides (ici 35 à 37) après les valeurs par défaut :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	14
35	Noeud 2 interne	0C0049230266719-Z	16
36	Noeud 2 Nat	0C0230266719-Z	16
37	Noeud 2 Abo	0C66719-Z	16

5) Cliquez sur **Appliquer** puis sur **OK**.
6) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 2.
   a) Dans **Nom de la règle**, entrez **Noeud 2**.
   b) Dans **Format de la règle de numérotation**, entrez **D49230266719E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.
7) Dans l'arborescence du menu, cliquez sur **Table de routage**.
8) Cliquez sur la table de routage 16.
   a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   b) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 2**.
   c) Dans **Discrimination mini.**, sélectionnez **15**.
   d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   e) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **2**.
   g) Cliquez sur **Appliquer** puis sur **OK**.

20.6.2.9 Comment configurer le faisceau et les paramètres du faisceau (Esclave)

A l'aide des étapes suivantes, configurez le faisceau et les paramètres de faisceau pour la mise en réseau de l'Esclave.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Dir. 1` pour le sens de la mise en réseau.
5) Dans **Préfixes faisceaux** entrez `0`.

6) Dans **Numéro de l'installation-entrant** , dans le champ **Indicatif national** entrez `49`.
7) Dans **Numéro de l'installation-entrant**, dans le champ **Indicatif du réseau local** entrez `2302`.
8) Dans **Numéro de l'installation-entrant**, dans le champ **Numéro de l'installation** entrez `66719`.
9) Cochez la case **Numéro de l'installation-entrant**, dans le champ **Numéro de site**.
10) Il est possible de reprendre les paramètres par défaut du faisceau (type de n°, sortant, type de numéro de téléphone.
11) Cliquez sur **Appliquer** puis sur **OK**.

20.6.2.10 Comment configurer LCR pour la mise en réseau (Esclave)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33, 34 et 35 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour le noeud 2. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal for Desktop).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.
4) Entrez les valeurs suivants sur les emplacements vides (ici 35 à 37) après les valeurs par défaut :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	14
36	Noeud 1 interne	0C0049230266758-Z	16
37	Noeud 1 Nat	0C00230266758-Z	16
38	Noeud 1 Abo	0C66758-Z	16

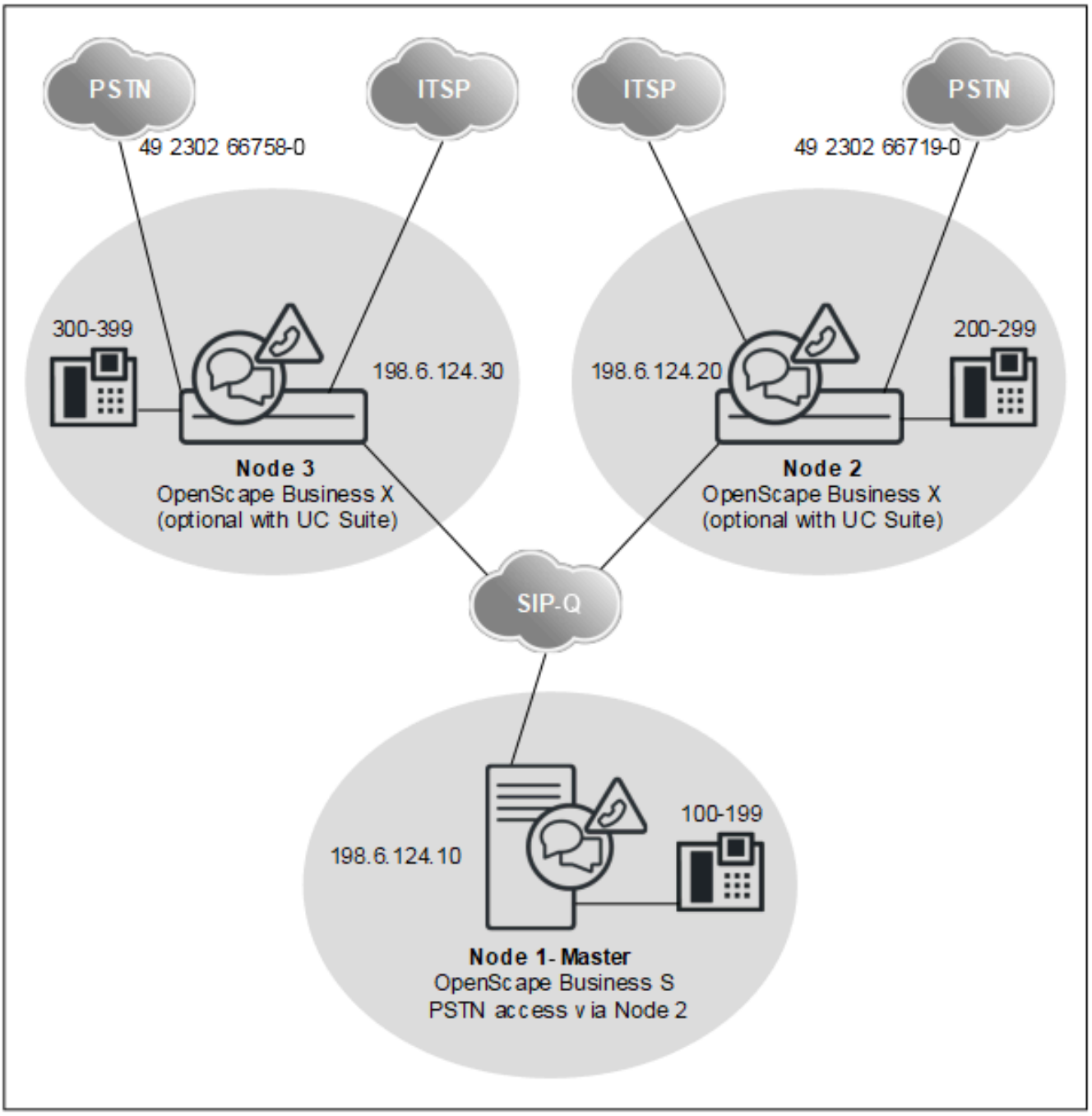
5) Cliquez sur **Appliquer** puis sur **OK**.

6) Dans l'arborescence du menu, cliquez sur **Règle de numérotation** pour **Noeud 2**.
   a) Dans **Nom de la règle**, entrez **Noeud 1**.
   b) Dans **Format de la règle de numérotation**, entrez **D49230266758E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.
7) Cliquez sur la table de routage 16.
   a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   b) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 1**.
   c) Dans **Discrimination mini.**, sélectionnez **15**.
   d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   e) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **2**.
   g) Cliquez sur **Appliquer** puis sur **OK**.
8) Dans l'arborescence du menu, cliquez sur **Table de routage**.

20.6.3 Mise en réseau d'OpenScape Business X et d'OpenScape Business S (passerelle unique)

Jusqu'à 32 systèmes de communication OpenScape Business X/S peuvent être mis en réseau entre eux. Plusieurs systèmes OpenScape Business S sont autorisés dans un réseau. Passerelle unique signifie que toutes les stations IP enregistrées auprès d'OpenScape Business S utilisent une seule passerelle vers le réseau téléphonique public commuté (RTPC) ou le fournisseur de services de télécommunications (ITSP).

Données réseau



- Numérotation fermée
- Fonctionnalités vocales et de communications unifiées à l'échelle du réseau avec configuration UC Suite via WBM (assistants)
- Plusieurs instances d'OpenScape Business S sont autorisées au sein d'un même réseau.
- Jusqu'à 32 systèmes en réseau et 1500 utilisateurs sans solution de communications unifiées
- Jusqu'à 8 systèmes en réseau et 1500 utilisateurs avec solution de communications unifiées

Fonctionnalités à l'échelle du réseau

Réseautage UC	Numérotation fermée	Numérotation ouverte
Nombre maximal de nœuds	8 avec solution UC et 32 sans solution UC	
Nombre maximal de stations dans un seul système de communication	Selon OpenScape Business X	
Nombre maximal de stations dans le réseau	1500	

Administration	Numérotation fermée	Numérotation ouverte
WBM	Administration à l'échelle du réseau à l'aide d'assistants	Non pris en charge
Gestionnaire E	Administration à l'échelle du réseau pour des tâches spécifiques (non compatible avec OpenScape Business S)	Non pris en charge
Administration de UC Suite	Administration à l'échelle du réseau à l'aide d'assistants	Non pris en charge
Importation massive de données via des fichiers CSV (numéros d'appel, numéros DID, noms)	Séparément pour chaque nœud du réseau	Non pris en charge

Licence	Numérotation fermée	Numérotation ouverte
structure de licence	Une licence réseau est requise pour chaque nœud.	Non pris en charge

Configuration

Cette configuration (avec numérotation fermée et UC Suite) illustre les étapes nécessaires à la mise en place du réseau à l'aide d'un exemple.

Prérequis :

- Un forfait réseau est disponible. Le plan de réseau a été utilisé pour garantir que chaque numéro d'appel interne du réseau ne soit utilisé qu'une seule fois pour la numérotation fermée. La longueur des numéros de station peut varier. Seuls les numéros de station DID peuvent apparaître plus d'une fois (par exemple, les numéros de station CO 49 2302 66758 100 et 49 2302 66719 100 ont le même numéro DID 100).
- Le réseau IP a été configuré et tous les nœuds peuvent être contactés par ping avec succès.

Transfert d'appel entre nœuds : pour les appels entrants via des lignes IP déjà transférés, aucun autre transfert vers la messagerie vocale n'est effectué. En effet, il est impossible autrement d'attribuer une adresse vocale unique à cette boîte vocale.

Si des règles de délégation inter-nœuds (extensions de référence) sont nécessaires, celles-ci doivent être configurées via les profils des stations OpenScape Business ou des groupes de sonnerie. Les appels inter-nœuds correspondants ne sont pas signalés comme étant transférés dans ce cas, mais comme des appels DSS (sélection directe de station). Les appels transférés au poste du député sont donc redirigés vers sa messagerie vocale.

Dans un réseau où la période d'activation est utilisée, le CLA d'OpenScape Business S doit toujours être utilisé comme CLA central !

En raison des différentes limites supérieures, deux fichiers de période d'activation différents sont nécessaires pour OpenScape Business et OpenScape Business S. Le fichier de période d'activation pour OpenScape Business S inclut la base OpenScape Business ainsi que la base S pour les scénarios de mise en réseau.

Dans ce scénario, chaque fois qu'une entreprise OpenScape demande une licence à un CLA de l'entreprise OpenScape S pendant la période d'activation, ce sont les limites de l'entreprise OpenScape S qui sont utilisées.

En revanche, si le CLA d'OpenScape Business était utilisé à la place, AUCUNE période d'activation ne serait accordée à aucun OpenScape Business S demandeur, étant donné qu'aucune base pour OpenScape Business S n'est incluse dans ce fichier.

Tableau 16 : Configuration des données de localisation pour le nœud 1, OpenScape Business S

Nœud 1		
G.-Pays de localisation		49
G.-Localisation Réseau local		2302
Système de géolocalisation G.		66719
Préfixe international		00
Préfixe national		0
Itinéraires		
Trk. Groupe 1	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 1 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 17 : Aperçu des entrées du LCR pour le nœud 1

Plan de numérotation		**Table de routage**			**règle à cadran**		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Noeud 2 Internat	0C0049230266719-2Z	Réseautage	Obligatoire	2	D49230266719E3A	Réseau d'entreprise	International

Plan de numérotation		Table de routage			règle à cadran		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
NAT du nœud 2	0C0230266719-2Z						
Station Node 2	0C66719-2Z						
Noeud 3 Internat	0C0049230266758-3Z	Réseautage	Obligatoire	3	D49230266758E3A	Réseau d'entreprise	International
NAT du nœud 3	0C0230266758-3Z						
Station du nœud 3	0C66758-3Z						
CO	0CZ	Réseautage	Obligatoire	2	E1A	Fournisseur principal de réseau	Inconnu
Divers	-Z	Réseautage	Non		UN	Réseau d'entreprise	Inconnu

Tableau 18 : Configuration des données de localisation pour le nœud 2, OpenScape Business

Nœud 2		
G.-Pays de localisation		49
G.-Localisation Réseau local		2302
Système de géolocalisation G.		66719
Préfixe international		00
Préfixe national		0
Itinéraires		
ISDN	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 2 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 19 : Aperçu des entrées du LCR pour le nœud 2

Plan de numérotation		Table de routage			règle à cadran		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Nœud 1 Internat	0C0049230266719-1Z	Réseautage	Obligatoire	1	D49230266719E3A	Réseau d'entreprise	International
NAT du nœud 1	0C0230266719-1Z						
Station du nœud 1	0C66719-1Z						
Noeud 3 Internat	0C0049230266758-3Z	Réseautage	Obligatoire	3	D49230266758E3A	Réseau d'entreprise	International
NAT du nœud 3	0C0230266758-3Z						
Station Node 3	0C66758-3Z						
CO	0CZ	ISDN	Non		UN	Fournisseur principal de réseau	Inconnu
Divers	-Z	Réseautage	Non		UN	Réseau d'entreprise	Inconnu

Tableau 20 : Configuration des données de localisation pour Node 3, OpenScape Business

Nœud 3		
G.-Pays de localisation		49
G.-Localisation Réseau local		2302
Système de géolocalisation G.		66758
Préfixe international		00
Préfixe national		0
Itinéraires		
ISDN	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 3 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 21 : Aperçu des entrées du LCR pour le nœud 3

Plan de numérotation		Table de routage			règle à cadran		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Nœud 1 Internat	0C0049230266719-1Z	Réseautage	Obligatoire	1	D49230266719E3A	Réseau d'entreprise	International
NAT du nœud 1	0C0230266719-1Z						
Station du nœud 1	0C66719-1Z						
Noeud 2 Internat	0C0049230266719-2Z	Réseautage	Obligatoire	2	D49230266719E3A	Réseau d'entreprise	International
NAT du nœud 2	0C0230266719-2Z						
Station Node 2	0C66719-2Z						
CO	0CZ	ISDN	Non		UN	Fournisseur principal de réseau	Inconnu
Divers	-Z	Réseautage	Non		UN	Réseau d'entreprise	Inconnu

Procédure de configuration du réseau :

1) Configurer l'installation de base pour le nœud 1 (maître)
2) Configuration du réseau pour le nœud 1
3) Configurer l'installation de base pour le nœud 2 (esclave)
4) Configuration du réseau pour le nœud 2
5) Configurer l'installation de base pour le nœud 3 (esclave)
6) Configurer le réseau pour le nœud 3 (esclave)
7) Vérifiez la fonction réseau du maître.
8) Configurer LCR pour la mise en réseau (nœud 1, maître)
9) Configurer LCR pour la mise en réseau (nœud 2)
10) Configurer les routes et les paramètres de routage (nœud 3)
11) Configurer les itinéraires et les paramètres de routage (Trk. Grp. 16) (Nœud 3)
12) Configurer LCR pour la mise en réseau (nœud 3)

20.6.3.1 Comment configurer l'installation de base pour noeud 1 (Maître)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
4) Entrez l'**indicatif local** et le **numéro de l'installation**.
5) Cochez la case **Intégration réseau**.
6) Dans le champ **ID de noeud**, attribuez à OpenScape Business S un ID de noeud univoque dans l'interconnexion de réseaux. L'ID de noeud doit être situé entre "**1**" et "**100**" (sélectionner "**1**" pour l'exemple de configuration).
7) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.
8) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
9) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

   Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

10) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.
11) Importez les clients IP.
12) Configurez maintenant la téléphonie Internet.
13) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
14) Configurez maintenant l'envoi d'e-mails.
15) Cliquez sur **OK&Suivant**.
16) Cliquez sur **Terminer**.

20.6.3.2 Comment configurer la mise en réseau pour le noeud 1 (Maître)

Lors de l'étape suivante, l'assistant pour la mis en réseau du noeud 1 (maître) est configuré.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.
5) Définissez le type de noeud (**Maître**).
6) Dans **ID noeud**, entrez les numéros de noeud respectifs des systèmes OpenScape Business correspondants (dans l'exemple de configuration, ceux des Esclaves avec ID de noeud 2).
7) Dans **Adresse IP**, entrez les adresses IP des systèmes OpenScape Business correspondants (dans l'exemple de configuration, ceux des Esclaves avec ID de noeud 2 et 3).
8) Cochez la case **passerelle**.
9) Dans **Nom**, indiquez le type d'installation.
10) Dans **Type**, indiquez le type de sous-installation.
11) Si nécessaire, cochez la case **Chiffrement**.

Conseil : Le cryptage est basé sur SPE et ne s'applique pas aux applications.

Remarque : Le fait de cocher la case ne signifie pas que le cryptage est configuré. Voir Cryptage de la signalisation et de la charge utile SPE .

---

12) Cliquez sur **Terminer**.

20.6.3.3 Comment configurer l'installation de base pour le noeud 2 (Esclave)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
4) Entrez l'**indicatif local** et le **numéro de l'installation**.
5) Cochez la case **Intégration réseau**.
6) Dans le champ **ID de noeud** attribuez à OpenScape Business un ID de noeud univoque à l'intérieur de l'interconnexion de réseaux ("**2**" et "**3**" dans l'exemple de configuration présenté).

7) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.
8) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
9) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

---

10) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.
11) Configurez maintenant les abonnés RNIS et analogiques.
12) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
13) Configurez maintenant l'envoi d'e-mails.
14) Cliquez sur **OK&Suivant**.
15) Cliquez sur **Terminer**.

20.6.3.4 Comment configurer la mise en réseau pour le noeud 2 (Esclave)

Lors de l'étape suivante, il est effectué la configuration de la mise en réseau du noeud 2 à l'aide de l'assistant.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.
5) Dans **Type de noeud** , cochez la case **Ce système est un noeud ESCLAVE**.
6) **Entrer l'adresse IP du noeud MAITRE** (dans notre exemple de configuration, l'adresse IP du noeud 1).

Conseil : Une fois que vous aurez cliqué sur **OK&Suite**, cette action ne pourra plus être annulée.

---

7) L'**Etat de l'enregistrement** est affiché avec l'**Etat succès** (ou avec un message d'erreur correspondant). La tâche de l'assistant est maintenant terminée.

8) Cliquez sur **Terminer**.

20.6.3.5 Comment configurer l'installation de base pour le noeud 3 (Esclave)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
4) Entrez l'**indicatif local** et le **numéro de l'installation**. (identique système passerelle correspondant).
5) Cochez la case **Intégration réseau**.
6) Dans le champ **ID de noeud** attribuez à OpenScape Business un ID de noeud univoque à l'intérieur de l'interconnexion de réseaux ("**3**" dans l'exemple de configuration présenté).
7) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.
8) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
9) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

---

10) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.
11) Configurez maintenant les abonnés RNIS et analogiques.
12) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
13) Configurez maintenant l'envoi d'e-mails.
14) Cliquez sur **OK&Suivant**.
15) Cliquez sur **Terminer**.

20.6.3.6 Comment contrôler la fonction de mise en réseau pour Maître

Vous pouvez contrôler l'état du réseau en général et les différents numéros de téléphone.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Réseau**.
2) Dans la ligne d'état figure l'**État de la synchronisation** pour le réseau. Vert signifie que le réseau n'a pas de problème, rouge signale des problèmes dans le réseau.
3) Sélectionnez dans la fenêtre **Réseau** l'onglet **Affichage du noeud** ; le système indique tous les noeuds disponibles avec **ID du noeud**, **Nom**, **Type de système**, **Adresse du serveur**, **Etat de l'enregistrement** et **Etat de disponibilité**.
4) Sélectionnez dans la fenêtre **Réseau** l'onglet **Numéros de téléphone** ; le système ouvre une fenêtre avec toutes les indications sur :
   - **Numéro de téléphone**
   - **SDA**
   - **Nom**
   - **Type de port**
   - **Noeud**

20.6.3.7 Configurer la mise en réseau pour le noeud 3 (Esclave)

Lors de l'étape suivante, il est effectué la configuration de la mise en réseau du noeud 3 à l'aide de l'assistant.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.
5) Dans **Type de noeud** , cochez la case **Ce système est un noeud ESCLAVE**.
6) **Entrer l'adresse IP du noeud MAITRE** (dans notre exemple de configuration, l'adresse IP du noeud 1).

Conseil : Une fois que vous aurez cliqué sur **OK&Suite**, cette action ne pourra plus être annulée.

---

7) L'**Etat de l'enregistrement** est affiché avec l'**Etat succès** (ou avec un message d'erreur correspondant). La tâche de l'assistant est maintenant terminée.
8) Cliquez sur **Terminer**.

20.6.3.8 Comment configurer LCR pour la mise en réseau (Noeud 3, Esclave)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33, 34 et 35 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour les noeuds 1 et 2. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local. Les entrées 36, 37 et 39 pour l'interworking avec le noeud 1 (numéros de téléphone 100 > 199) et les entrées 39, 40 et 41 pour l'interworking avec le noeud 2 (numéros de téléphone 200 > 299) doivent être complétées. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal for Desktop).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.
4) Entrez les valeurs suivants sur les emplacements vides (ici 35 à 40) après les valeurs par défaut :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
31	Appl-Suite	-371	12
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	14
36	Noeud 1 interne	0C0049230266719-1Z	16
37	Noeud 1 Nat	0C0230266719-1Z	16
38	Noeud 1 Abo	0C66719-1Z	16
39	Noeud 2 interne	0C0049230266719-2Z	17
40	Noeud 2 Nat	0C0230266719-2Z	17
41	Noeud 2 Abo	0C66719-2Z	17

5) Cliquez sur **Appliquer** puis sur **OK**.

6) Dans l'arborescence du menu, cliquez sur la **Règle de numérotation** correspondante pour noeuds 1 et 2.
   a) Dans **Nom de la règle**, entrez **Noeuds 1 + 2**.
   b) Dans **Format de la règle de numérotation**, entrez **D49230266719E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.

7) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 16 pour le networking et l'affecter directement au noeud 1.

8) Cliquez sur la table de routage 16.
   a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   b) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeuds 1+2**.
   c) Dans **Discrimination mini.**, sélectionnez **15**.
   d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   e) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **1**.
   g) Cliquez sur **Appliquer** puis sur **OK**.

9) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 17 pour le networking et l'affecter directement au noeud 2.

10) Cliquez sur la table de routage 17.
   a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   b) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeuds 1+2**.
   c) Dans **Discrimination mini.**, sélectionnez **15**.
   d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   e) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **2**.
   g) Cliquez sur **Appliquer** puis sur **OK**.

20.6.3.9 Comment configurer LCR pour la mise en réseau (Noeud 2)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33, 34 et 35 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour les noeuds 1 et 3. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local. Les entrées 36, 37 et 38 pour l'Interworking avec le noeud 1 (numéros de téléphone 100 > 199) et les entrées 39, 40 et 41 pour l'Interworking avec le noeud 3 (numéros de téléphone 300 > 399) doivent être complétées. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal for Desktop).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.
4) Entrez les valeurs suivants sur les emplacements vides (ici 35 à 40) après les valeurs par défaut :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
31	Appl-Suite	-271	12
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	14
36	Noeud 1 interne	0C0049230266719-1Z	16
37	Noeud 1 Nat	0C0230266719-1Z	16
38	Noeud 1 Abo	0C66719-1Z	16
39	Noeud 3 interne	0C0049230266758-3Z	17
40	Noeud 3 Nat	0C0230266758-3Z	17
41	Noeud 3 Abo	0C66758-3Z	17

5) Cliquez sur **Appliquer** puis sur **OK**.
6) Dans l'arborescence du menu, cliquez sur **Table de routage**.
7) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 1.
   a) Dans **Nom de la règle**, entrez **Noeud 1**.
   b) Dans **Format de la règle de numérotation**, entrez **D49230266719E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.
8) Cliquez sur la table de routage 16 afin de la configurer pour le Networking avec le noeud 1.
   a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   b) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 1**.
   c) Dans **Discrimination mini.**, sélectionnez **1**.
   d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   e) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **1**.
   g) Cliquez sur **Appliquer** puis sur **OK**.
9) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 3.
   a) Dans **Nom de la règle**, entrez **Noeud 3**.
   b) Dans **Format de la règle de numérotation**, entrez **D49230266758E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.

10) Dans l'arborescence du menu, cliquez sur **Table de routage**.
11) Cliquez sur la table de routage 17 afin de la configurer pour le Networking avec le noeud 3.
    a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
    b) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 3**.
    c) Dans **Discrimination mini.**, sélectionnez **1**.
    d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
    e) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
    f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **3**.
    g) Cliquez sur **Appliquer** puis sur **OK**.

20.6.3.10 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 1, Maître)

Dans le noeud 1, configurez les paramètres pour la ligne réseau ainsi que le numéro de site, le préfixe faisceau et les paramètres de faisceau. Il faut inscrire ici le numéro de l'installation pour définir le site de la passerelle. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Dir. 1` pour la ligne réseau.
5) Dans **Préfixes faisceaux** entrez `0`.
6) Dans **Numéro de l'installation-entrant** , dans le champ **Indicatif national** entrez `49`.
7) Dans **Numéro de l'installation-entrant**, dans le champ **Indicatif du réseau local** entrez `2302`.
8) Dans **Numéro de l'installation-entrant**, dans le champ **Numéro de l'installation** entrez `66719`.
9) Cochez la case **Numéro de l'installation-entrant**, dans le champ **Numéro de site**.
10) Il est possible de reprendre les paramètres par défaut du faisceau (type de n°, sortant, type de numéro de téléphone.
11) Cliquez sur **Appliquer** puis sur **OK**.

20.6.3.11 Comment configurer les faisceaux et les paramètres de faisceau (Faisc. 16) (Noeud 1)

Pour le faisceau 16 (mise en réseau) il est indispensable de remplir l'entrée correspondant au 2e indicatif pour Maître et Esclave.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur le dernier **faisceau** (**Faisc. 16**).
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Mise en réseau` pour le sens de la mise en réseau.
5) Dans **Préfixes faisceaux**, n'indiquez rien.
6) Dans **Indicatif réseau (2e indicatif réseau)** entrez 0.
7) Il est possible de reprendre les paramètres par défaut du faisceau (type de n °, sortant, type de numéro de téléphone.
8) Cliquez sur **Appliquer** puis sur **OK**.

20.6.3.12 Comment configurer LCR pour la mise en réseau (Noeud 1)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33, 34 et 35 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour les noeuds 2 et 3. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal for Desktop).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.
4) Entrez les valeurs suivants sur les emplacements vides (ici 35 à 40) après les valeurs par défaut :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
16	Par défaut	0CZ	1
17	Par défaut	0C1Z	1
18	Par défaut	0CNZ	1
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	14
36	Noeud 2 interne	0C0049230266719-2Z	16
37	Noeud 2 Nat	0C0230266719-2Z	16

Plan de numérotatio	Nom	Chiffres composés	Table de routage
38	Noeud 2 Abo	0C66719-2Z	16
39	Noeud 3 interne	0C0049230266758-3Z	17
40	Noeud 3 Nat	0C0230266758-3Z	17
41	Noeud 3 Abo	0C66758-3Z	17

5) Cliquez sur **Appliquer** puis sur **OK**.

6) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 2.

a) Dans **Nom de la règle**, entrez **Noeud 2**.
b) Dans **Format de la règle de numérotation**, entrez **D49230266719E3A**.
c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
e) Cliquez sur **Appliquer** puis sur **OK**.

7) Dans l'arborescence du menu, cliquez sur **Table de routage**.

8) Cliquez sur la table de routage 16 afin de la configurer pour le Networking avec le noeud 2.

a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
b) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 2**.
c) Dans **Discrimination mini.**, sélectionnez **1**.
d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
e) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **2**.
g) Cliquez sur **Appliquer** puis sur **OK**.

9) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 3.

a) Dans **Nom de la règle**, entrez **Noeud 3**.
b) Dans **Format de la règle de numérotation**, entrez **D49230266719E1A**.
c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
e) Cliquez sur **Appliquer** puis sur **OK**.

10) Dans l'arborescence du menu, cliquez sur **Table de routage**.

11) Cliquez sur la table de routage 17 afin de la configurer pour le Networking avec le noeud 3.

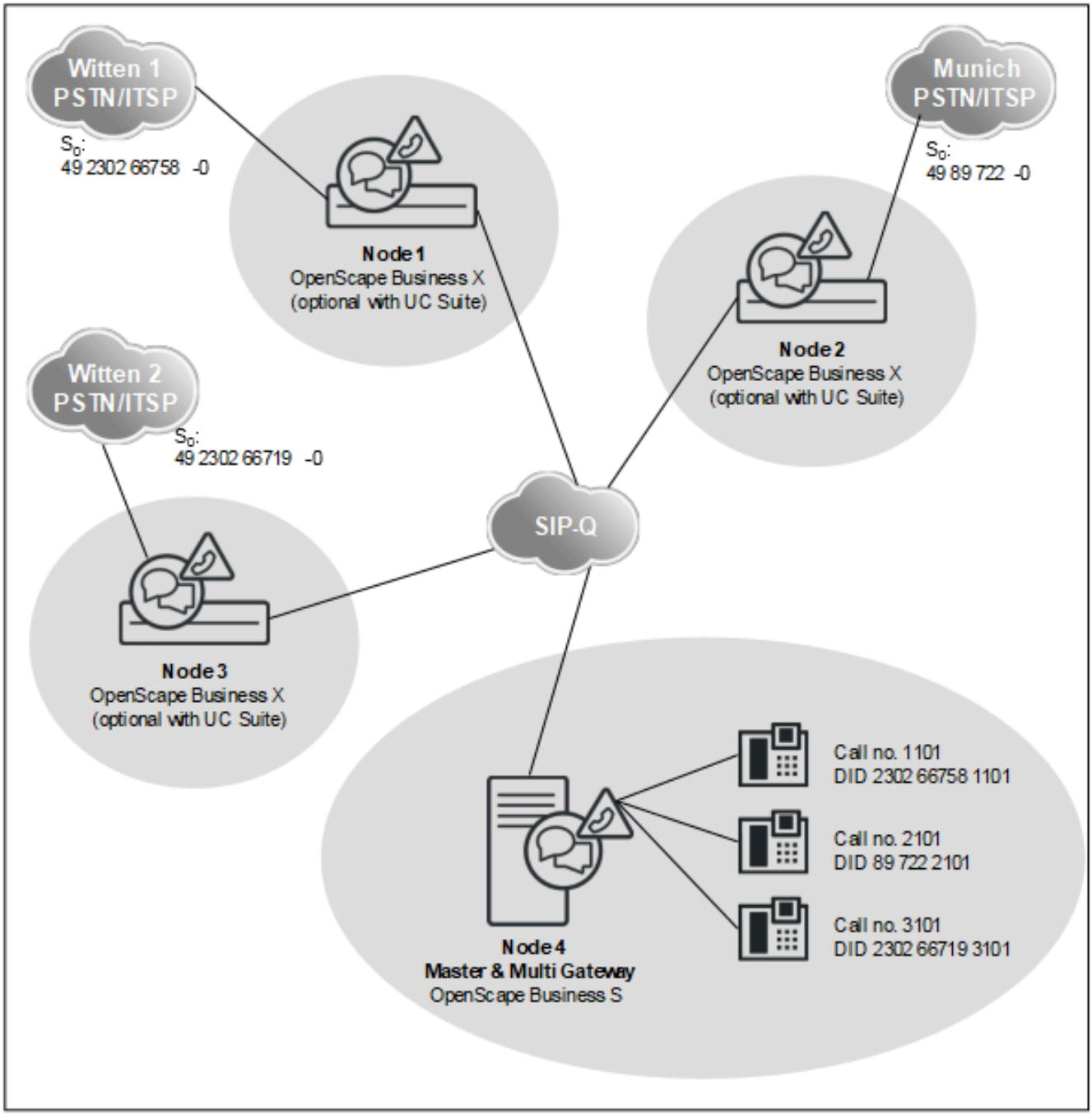
a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
b) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 3**.
c) Dans **Discrimination mini.**, sélectionnez **1**.
d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
e) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **3**.
g) Cliquez sur **Appliquer** puis sur **OK**.

12) Dans l'arborescence du menu, cliquez sur **Table de routage**.

20.6.4 Mise en réseau d'OpenScape Business X et d'OpenScape Business S (Multi-Gateway)

Il est possible de mettre en réseau jusqu'à 32 systèmes de communication OpenScape Business X et OpenScape Business S. Le terme « passerelle multiple » signifie que chaque station IP enregistrée auprès d'OpenScape Business S est affectée à une passerelle spécifique.

Données réseau



- Numérotation fermée

- Fonctionnalités vocales et de communications unifiées à l'échelle du réseau avec configuration UC Suite via WBM (assistants)
- Un seul OpenScape Business S est autorisé dans le réseau.
- Tous les systèmes doivent avoir le même code pays.
- Tous les systèmes doivent être situés dans le même fuseau horaire.
- Un seul code d'accès CO (par exemple, 0) doit exister pour l'ensemble du réseau.
- Jusqu'à 32 systèmes en réseau et 1500 utilisateurs sans solution de communications unifiées
- Jusqu'à 8 systèmes en réseau et 1500 utilisateurs avec solution de communications unifiées

Fonctionnalités à l'échelle du réseau

Réseautage UC	Numérotation fermée	Numérotation ouverte
Nombre maximal de nœuds	8 avec solution UC et 32 sans solution UC	
Nombre maximal de stations dans un seul système de communication	Selon OpenScape Business X	
Nombre maximal de stations dans le réseau	1500	

Administration	Numérotation fermée	Numérotation ouverte
WBM	Administration à l'échelle du réseau à l'aide d'assistants	Non pris en charge
Gestionnaire E	Administration à l'échelle du réseau pour des tâches spécifiques (non compatible avec OpenScape Business S)	Non pris en charge
Administration de UC Suite	Administration à l'échelle du réseau à l'aide d'assistants	Non pris en charge
Importation massive de données via des fichiers CSV (numéros d'appel, numéros DID, noms)	Séparément pour chaque nœud du réseau	Non pris en charge

Licence	Numérotation fermée	Numérotation ouverte
structure de licence	Une licence réseau est requise pour chaque nœud.	Non pris en charge

Configuration

Cette configuration (avec numérotation fermée et UC Suite) illustre, à l'aide d'un exemple, les étapes nécessaires à la mise en place d'un réseau multi-passerelles.

Prérequis :

- Un forfait réseau est disponible. Le plan de réseau a été utilisé pour garantir que chaque numéro d'appel interne du réseau ne soit utilisé qu'une seule fois pour la numérotation fermée. La longueur des numéros de station peut varier. Seuls les numéros de poste DID peuvent apparaître plus d'une fois.
- Le réseau IP a été configuré et tous les nœuds peuvent être contactés par ping avec succès.

- Tous les nœuds ont été mis à niveau vers la même version du logiciel.

Transfert d'appel entre nœuds : pour les appels entrants via des lignes IP déjà transférés, aucun autre transfert vers la messagerie vocale n'est effectué. En effet, il est impossible autrement d'attribuer une adresse vocale unique à cette boîte vocale.

Si des règles de délégation inter-nœuds (extensions de référence) sont nécessaires, celles-ci doivent être configurées via les profils des stations OpenScape Business ou des groupes de sonnerie. Les appels inter-nœuds correspondants ne sont pas signalés comme étant transférés dans ce cas, mais comme des appels DSS (sélection directe de station). Les transferts d'appels du député sont donc redirigés vers la messagerie vocale.

Tableau 22 : Configuration des données de localisation pour le nœud 1

Nœud 1		
G.-Pays de localisation		49
G.-Localisation Réseau local		2302
Système de géolocalisation G.		66758
Préfixe international		00
Préfixe national		0
Itinéraires		
ISDN	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 1 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 23 : Aperçu des entrées du LCR pour le nœud 1

Plan de numérotation		**Table de routage**			**règle à cadran**		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Noeud 2 Internat	0C004989722-Z	Réseautage	Obligatoire	2	D4989722E3A	Réseau d'entreprise	International
NAT du nœud 2	0C089722-Z						
Station Node 2	0C722-Z						

Plan de numérotation		Table de routage			règle à cadran		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Noeud 3 Internat	0C0049230266719-Z	Réseautage	Obligatoire	3	D49230266719E3A	Réseau d'entreprise	International
NAT du nœud 3	0C0230266719-Z						
Station Node 3	0C66719-Z						
Noeud 4 Internat	0C0049230266758-Z	Réseautage	NON		D230266758E3A	Réseau d'entreprise	National
NAT du nœud 4	0C0230266758-Z						
Station Node 4	0C66758-Z						
Divers	-Z	Réseautage	Non		BA	Réseau d'entreprise	Inconnu
CO International	0C0049-Z	ISDN	Non		D0E3A	Fournisseur principal de réseau	Inconnu
CO	0CZ	ISDN	Non		UN	Fournisseur principal de réseau	Inconnu

Tableau 24 : Configuration des données de localisation pour le nœud 2

Nœud 2		
G.-Pays de localisation		49
G.-Localisation Réseau local		89
Système de géolocalisation G.		722
Préfixe international		00
Préfixe national		0
Itinéraires		
ISDN	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 2 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de

station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 25 : Aperçu des entrées du LCR pour le nœud 2

Plan de numérotation		Table de routage			règle à cadran		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Nœud 1 Internat	0C0049230266758-Z	Réseautage	Obligatoire	1	D492302667E3A	Réseau d'entreprise	International
NAT du nœud 1	0C0230266758-Z						
Station du nœud 1	0C66758-Z						
Noeud 3 Internat	0C0049230266719-Z	Réseautage	Obligatoire	3	D49230266719E3A	Réseau d'entreprise	International
NAT du nœud 3	0C0230266719-Z						
Station du nœud 3	0C66719-Z						
Noeud 4 Internat	0C004989722-Z	Réseautage	NON		D89722E3A	Réseau d'entreprise	National
NAT du nœud 4	0C089722-Z						
Station Node 4	0C722-Z						
Divers	-Z	Réseautage	Non		BA	Réseau d'entreprise	Inconnu
CO International	0C0049-Z	ISDN	Non		D0E3A	Fournisseur principal de réseau	Inconnu
CO	0CZ	ISDN	Non		UN	Fournisseur principal de réseau	Inconnu

Tableau 26 : Configuration des données de localisation pour le nœud 3

Nœud 3		
G.-Pays de localisation		49
G.-Localisation Réseau local		2302
Système de géolocalisation G.		66719
Préfixe international		00
Préfixe national		0
Itinéraires		
ISDN	Code de tronc	0

Nœud 3		
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 3 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 27 : Aperçu des entrées du LCR pour le nœud 3

Plan de numérotation		**Table de routage**			**règle à cadran**		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Nœud 1 Internat	0C0049230266758-Z	Réseautage	Obligatoire	1	D49230266758E3A	Réseau d'entreprise	International
NAT du nœud 1	0C0230266758-Z						
Station du nœud 1	0C66758-Z						
Noeud 2 Internat	0C004989722-Z	Réseautage	Obligatoire	2	D4989722E3A	Réseau d'entreprise	International
NAT du nœud 2	0C089722-Z						
Station Node 2	0C722-Z						
Noeud 4 Internat	0C004989230266719-Z	Réseautage	Non		D230266719E3A	Réseau d'entreprise	National
NAT du nœud 4	0C0230266719-Z						
Station Node 4	0C66719-Z						
Divers	-Z	Réseautage	Non		BA	Réseau d'entreprise	Inconnu
CO International	0C0049-Z	ISDN	Non		D0E3A	Fournisseur principal de réseau	Inconnu
CO	0CZ	ISDN	Non		UN	Fournisseur principal de réseau	Inconnu

Configuration des données de localisation pour le nœud 4 : Associer les données de localisation à un tronc CO factice (Trk. Grp. 1) incl. Code d'accès CO = 0 et Type = CO, puisque le nœud 4 n'a pas de connexion directe à un bureau central.

Tableau 28 : Nœud 4, faux tronc CO

Nœud 4		
G.-Pays de localisation		49
G.-Localisation Réseau local		
Système de géolocalisation G.		
Préfixe international		00
Préfixe national		0
Itinéraires		
ISDN	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	Inconnu	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Les numéros de toutes les stations situées en dehors du nœud 1 sont automatiquement saisis dans les tables de routage. Cela inclut les numéros de station internes ainsi que les numéros de station DID, qui diffèrent des numéros de station internes respectifs.

Tableau 29 : Nœud 4, Route de mise en réseau

Nœud 4		
G.-Pays de localisation		
G.-Localisation Réseau local		
Système de géolocalisation G.		
Préfixe international		00
Préfixe national		0
Itinéraires		
ISDN	Code de tronc	0
Réseautage	2e code de tronc	0
Paramètres de routage		
Itinéraire	Non et type, sortant	Type RNR
Réseautage	National	Int/DID
ISDN	(Aucun changement d'inscription)	A FAIT

Tableau 30 : Aperçu des entrées du LCR pour le nœud 4

Plan de numérotation		Table de routage			règle à cadran		
Nom	**chiffres composés**	**Itinéraire**	**Passerelle dédiée**	**ID de passerelle**	**règle à cadran**	**Procédure**	**Taper**
Nœud 1 Internat	0C0049230266758-Z	Réseautage	Obligatoire	1	D49230266758E3A	Réseau d'entreprise	International
NAT du nœud 1	0C0230266758-Z						
Noeud 2 Internat	0C004989722-Z	Réseautage	Obligatoire	2	D4989722E3A	Réseau d'entreprise	International
NAT du nœud 2	0C089722-Z						
Noeud 3 Internat	0C004989230266719-Z	Réseautage	Obligatoire	3	D49230266719E3A	Réseau d'entreprise	International
NAT du nœud 3	0C0230266719-Z						
Divers	-Z	Réseautage	NON		UN	Réseau d'entreprise	Inconnu
CO	0CZ	Réseautage	PASSERELLE MULTIPLE	1	E1A	Fournisseur principal de réseau	Inconnu

Procédure de configuration du réseau :

1) Configurer l'installation de base pour le nœud 4 (maître)
2) Configurer le réseau pour le nœud 4 (maître)
3) Configurer l'installation de base pour le nœud 1 (esclave)
4) Configurer le réseau pour le nœud 1 (esclave)
5) Configurer l'installation de base pour le nœud 2 (esclave)
6) Configurer le réseau pour le nœud 2 (esclave)
7) Configurer l'installation de base pour le nœud 3 (esclave)
8) Configurer le réseau pour le nœud 3 (esclave)
9) Vérifiez la fonction réseau du maître.
10) Configurer une passerelle multiple pour le nœud 4 (maître)
11) Configurer les routes et les paramètres de routage (nœud 1, esclave)
12) Configurer LCR pour la mise en réseau (nœud 1, esclave)
13) Configurer les routes et les paramètres de routage (nœud 2, esclave)
14) Configurer LCR pour la mise en réseau (nœud 2, esclave)
15) Configurer les routes et les paramètres de routage (nœud 3, esclave)
16) Configurer LCR pour la mise en réseau (nœud 3, esclave)
17) Configurer les routes et les paramètres de routage (nœud 4, maître)
18) Configurer LCR pour la mise en réseau (nœud 4, maître)

20.6.4.1 Comment configurer l'installation de base pour noeud 4 (OpenScape Business S, maître)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
4) N'effectuez pas d'entrée pour les champs **Indicatif local** et **Numéro de l'installation**!.
5) Cochez la case **Intégration réseau**.
6) Dans le champ **ID de noeud**, attribuez à OpenScape Business S un ID de noeud univoque dans l'interconnexion de réseaux. L'ID de noeud doit être situé entre "**1**" et "**100**" (la valeur "**4**" a été choisie pour l'exemple de configuration).
7) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.
8) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
9) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

   Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

10) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.
11) Importez maintenant les clients IP.
12) Configurez les clients IP.
13) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
14) Configurez maintenant l'envoi d'e-mails.
15) Cliquez sur **Quitter**.

20.6.4.2 Comment configurer la mise en réseau pour le noeud 4 (Maître)

Lors de l'étape suivante, il est effectué la configuration de la mise en réseau du noeud 3 à l'aide de l'assistant.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.
5) Cochez la case **Ce système est le noeud Maître**.
6) Dans **ID noeud**, entrez les numéros de noeud respectifs des systèmes OpenScape Business correspondants (dans l'exemple de configuration, ceux des Esclaves avec ID de noeud 1, 2 et 3).
7) Dans **Adresse IP**, entrez les adresses IP des systèmes OpenScape Business correspondants (dans l'exemple de configuration, ceux des Esclaves avec ID de noeud 1, 2 et 3).
8) Cochez la case **passerelle**.
9) Dans **Nom**, indiquez le type d'installation (par ex. Esclave 1).
10) Dans **Type**, indiquez le type de sous-installation.
11) Si nécessaire, cochez la case **Chiffrement**.

Conseil : Le cryptage est basé sur SPE et ne s'applique pas aux applications.

Remarque : Le fait de cocher la case ne signifie pas que le cryptage est configuré. Voir Cryptage de la signalisation et de la charge utile SPE .

---

12) Cliquez sur **Terminer**.

20.6.4.3 Comment configurer l'installation de base pour le noeud 1 (Esclave)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
4) Entrez l'**indicatif local** et le **numéro de l'installation**.
5) Cochez la case **Intégration réseau**.
6) Dans le champ **ID de noeud** attribuez à OpenScape Business S un ID de noeud univoque à l'intérieur de l'interconnexion de réseaux ("**1**" dans l'exemple de configuration présenté).
7) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.
8) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
9) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

---

10) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.
11) Configurez maintenant les abonnés RNIS et analogiques.
12) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
13) Configurez maintenant l'envoi d'e-mails.
14) Cliquez sur **Quitter**.

20.6.4.4 Comment configurer la mise en réseau pour le noeud 1 (Esclave)

Dans l'étape suivante, l'assistant de mise en réseau est configuré.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.

5) **Entrez l'adresse IP du noeud MAITRE** (Un OpenScape Business est configuré comme noeud Esclave et l'adresse IP correspondante du noeud Maître, OpenScape Business S, est inscrite. Maître et Multi-Location sont toujours affectés au même système, dans l'exemple de paramétrage d'OpenScape Business S).

   Conseil : Une fois que vous aurez cliqué sur **OK&Suivant**, cette action ne pourra plus être annulée.

6) L'**Etat de l'enregistrement** est affiché avec l'**Etat succès** (ou avec un message d'erreur correspondant). La tâche de l'assistant est maintenant terminée.
7) Cliquez sur **Terminer**.

20.6.4.5 Comment configurer l'installation de base pour le noeud 2 (Esclave)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
4) Entrez l'**indicatif local** et le **numéro de l'installation**.
5) Cochez la case **Intégration réseau**.
6) Dans le champ **ID de noeud** pour OpenScape Business S, attribuez un ID de noeud univoque à l'intérieur de l'interconnexion de réseaux ("**2**" dans l'exemple de configuration présenté).
7) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.
8) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
9) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

   Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

10) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez

harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.

11) Configurez maintenant les abonnés RNIS et analogiques.
12) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
13) Configurez maintenant l'envoi d'e-mails.
14) Cliquez sur **Quitter**.

20.6.4.6 Comment configurer la mise en réseau pour le noeud 2 (Esclave)

Lors de l'étape suivante, il est effectué la configuration de la mise en réseau du noeud 2 à l'aide de l'assistant.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.
5) Dans **Type de noeud** , cochez la case **Ce système est un noeud ESCLAVE**.
6) **Entrez l'adresse IP du noeud MAITRE** (Un OpenScape Business est configuré comme noeud Esclave et l'adresse IP correspondante du noeud Maître, OpenScape Business S, est inscrite. Maître et Multi-Location sont toujours affectés au même système, dans l'exemple de paramétrage d'OpenScape Business S).

   Conseil : Une fois que vous aurez cliqué sur **OK&Suivant**, cette action ne pourra plus être annulée.

7) L'**Etat de l'enregistrement** est affiché avec l'**Etat succès** (ou avec un message d'erreur correspondant). La tâche de l'assistant est maintenant terminée.
8) Cliquez sur **Terminer**.

20.6.4.7 Comment configurer l'installation de base pour le noeud 3 (Esclave)

Pour l'intégration dans une interconnexion de réseaux, il faut que l'indicatif national et l'ID de noeud aient été attribués. Les numéros de téléphone internes doivent être configurés de manière univoque sur l'ensemble du réseau. L'entrée des numéros de téléphones nationaux et locaux est importante car ce numéro est paramétré dans Fsc1 du réseau RNIS et sert à la normalisation en tant que numéro de téléphone de site.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.
3) Dans le champ **Indicatif national**, entrez l'indicatif national correspondant, par ex. 49 pour l'Allemagne.
4) Entrez l'**indicatif local** et le **numéro de l'installation**.
5) Cochez la case **Intégration réseau**.
6) Dans le champ **ID de noeud** attribuez à OpenScape Business un ID de noeud univoque à l'intérieur de l'interconnexion de réseaux ("**3**" dans l'exemple de configuration présenté).
7) Cliquez sur **Exécuter la fonction**. Vous accédez à la fenêtre **Fonctions centrales pour les abonnés**.
8) Comme tous les numéros de téléphone doivent être univoques à l'intérieur d'un réseau, il faut effacer les numéros de téléphone par défaut. Activez le champ d'option **Supprimer tous les numéros**.
9) Cochez **Effacer tous les numéros** et cliquez sur **OK&Suivant**. Vous accédez à la fenêtre **Modifier les numéros d'appel préconfigurés**.

Remarque : Les indicatifs de fonction doivent être univoques dans l'interconnexion de réseaux. Des doublons dans les numéros de téléphone ne sont pas admis !

---

10) Harmonisez les numéros de téléphone préconfiguré au numéros de téléphone du réseau et cliquez sur **OK & Suivant**. Vous pouvez harmoniser les numéros de téléphone manuellement à l'aide de l'assistant ou importer un fichier csv avec les numéros de téléphone préparés en conséquence.
11) Configurez maintenant les abonnés RNIS et analogiques.
12) Modifiez les paramètres d'une conférence "Rendez-vous". Vous devez entrer un indicatif univoque dans l'interconnexion de réseaux.
13) Configurez maintenant l'envoi d'e-mails.
14) Cliquez sur **Quitter**.

20.6.4.8 Comment configurer la mise en réseau pour le noeud 3 (Esclave)

Lors de l'étape suivante, il est effectué la configuration de la mise en réseau du noeud 3 à l'aide de l'assistant.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Installation de base**.

3) Cliquez sur **Modifier** pour démarrer l'Assistant **Configuration de Mise en réseau**.
4) Sélectionnez le paramètre **Réseau avec OSBiz X / OSBiz S**.
5) Dans **Type de noeud** , cochez la case **Ce système est un noeud ESCLAVE**.
6) **Entrez l'adresse IP du noeud MAITRE** (Un OpenScape Business est configuré comme noeud Esclave et l'adresse IP correspondante du noeud Maître, OpenScape Business S, est inscrite. Maître et Multi-Location sont toujours affectés au même système, dans l'exemple de paramétrage d'OpenScape Business S).

   Conseil : Une fois que vous aurez cliqué sur **OK&Suite**, cette action ne pourra plus être annulée.

7) L'**Etat de l'enregistrement** est affiché avec l'**Etat succès** (ou avec un message d'erreur correspondant). La tâche de l'assistant est maintenant terminée.
8) Cliquez sur **Terminer**.

20.6.4.9 Comment contrôler la fonction de mise en réseau pour Maître

Vous pouvez contrôler l'état du réseau en général et les différents numéros de téléphone.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Réseau**.
2) Dans la ligne d'état figure l'**État de la synchronisation** pour le réseau. Vert signifie que le réseau n'a pas de problème, rouge signale des problèmes dans le réseau.
3) Sélectionnez dans la fenêtre **Réseau** l'onglet **Affichage du noeud** ; le système indique tous les noeuds disponibles avec **ID du noeud**, **Nom**, **Type de système**, **Adresse du serveur**, **Etat de l'enregistrement** et **Etat de disponibilité**.
4) Sélectionnez dans la fenêtre **Réseau** l'onglet **Numéros de téléphone** ; le système ouvre une fenêtre avec toutes les indications sur :
   - **Numéro de téléphone**
   - **SDA**
   - **Nom**
   - **Type de port**
   - **Noeud**

20.6.4.10 Comment configurer la multi-passerelle pour noeud 4 (Maître)

La configuration de l'interconnexion de réseaux en tant que réseau passerelle est effectuée sur le noeud Maître.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Configuration de la mise en réseau**.
3) Dans **Configuration du réseau**, sélectionnez le paramètre **Configuration multi-emplacement**. Dans la fenêtre **Configuration multi-emplacement**, il est déterminé l'affectation des abonnés au site. L'affectation du plan de numérotation) l'ID de noeud (Node-ID) est par ex. utilisée pour la prise de réseau sortante sur le noeud de site correspondant.
4) Pour l'exemple de configuration, indiquez les affectations suivantes dans **Configuration multi-emplacement**. (Tous les téléphones sont enregistrés sur OpenScape Business S) :

Numéro d'abonné	Nom	NodeId
1101	1101KN1	1-Esclave Witten1
1102	1102KN1	1-Esclave Witten1
1103	1103KN1	1-Esclave Witten1
2101	2101KN2	2-Esclave Munich
2102	2102KN2	2-Esclave Munich
2103	2103KN2	2-Esclave Munich
3101	3101KN3	3-Esclave Witten 2
3102	3102KN3	3-Esclave Witten 2
3103	3103KN3	3-Esclave Witten 2

5) Cliquez sur **Terminer**.

20.6.4.11 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 1, Esclave)

A l'aide des étapes suivantes, configurez le faisceau et les paramètres de faisceau pour la mise en réseau de l'Esclave.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Dir. 1` pour la ligne réseau.
5) Dans **Préfixes faisceaux** entrez `0`.

6) Dans **Numéro de l'installation-entrant** , dans le champ **Indicatif national** entrez `49`.
7) Dans **Numéro de l'installation-entrant**, dans le champ **Indicatif du réseau local** entrez `2302`.
8) Dans **Numéro de l'installation-entrant**, dans le champ **Numéro de l'installation** entrez `66758`.
9) Cochez la case **Numéro de l'installation-entrant**, dans le champ **Numéro de site**.
10) Il est possible de reprendre les paramètres par défaut du faisceau (type de n°, sortant, type de numéro de téléphone.
11) Cliquez sur **Appliquer** puis sur **OK**.

20.6.4.12 Comment configurer LCR pour la mise en réseau (Noeud 1, Esclave)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33, 34 et 35 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour les noeuds 2 et 3, ainsi que pour le noeud multi passerelle 4. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.
4) Entrez les valeurs suivantes sur les emplacements vides (ici 36 à 43) après les valeurs par défaut :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
31	Appl-Suite	-171	12
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	14
36	Noeud 2 interne	0C004989722-Z	16
37	Noeud 2 Nat	0C089722-Z	16
38	Noeud 3 interne	0C0049230266719-Z	17
39	Noeud 3 Nat	0C0230266719-Z	17
40	Noeud 3 Abo	0C66719-Z	17
41	Noeud 4 interne	0C0049230266758-Z	18
42	Noeud 4 Nat	0C0230266758-Z	18
43	Noeud 4 Abo	0C66758-Z	18

Plan de numérotatio	Nom	Chiffres composés	Table de routage
44			-

5) Cliquez sur **Appliquer** puis sur **OK**.

6) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 2.

a) Dans **Nom de la règle**, entrez **Noeud 2**.
b) Dans **Format de la règle de numérotation**, entrez **D4989722E3A**.
c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
e) Cliquez sur **Appliquer** puis sur **OK**.

7) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 16 pour le networking et l'affecter directement au noeud 2.

a) Cliquez sur la table de routage 16.
b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 2**.
d) Dans **Discrimination mini.**, sélectionnez **15**.
e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **2**.
h) Cliquez sur **Appliquer** puis sur **OK**.

8) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 3.

a) Dans **Nom de la règle**, entrez **Noeud 3**.
b) Dans **Format de la règle de numérotation**, entrez **D49230266719E3A**.
c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
e) Cliquez sur **Appliquer** puis sur **OK**.

9) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 17 pour le networking et l'affecter directement au noeud 3.

a) Cliquez sur la table de routage 17.
b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 3**.
d) Dans **Discrimination mini.**, sélectionnez **15**.
e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **3**.
h) Cliquez sur **Appliquer** puis sur **OK**.

10) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 4.
    a) Dans **Nom de la règle**, entrez **Noeud ML 4**.
    b) Dans **Format de la règle de numérotation**, entrez **D230266758E3A**.
    c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
    d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
    e) Cliquez sur **Appliquer** puis sur **OK**.
11) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 18 pour le networking et l'affecter directement au noeud 4.
    a) Cliquez sur la table de routage 18.
    b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
    c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 4**.
    d) Dans **Discrimination mini.**, sélectionnez **15**.
    e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
    f) Cliquez sur **Appliquer** puis sur **OK**.

20.6.4.13 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 2, Esclave)

A l'aide des étapes suivantes, configurez le faisceau et les paramètres de faisceau pour la mise en réseau de l'Esclave.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Dir. 1` pour la ligne réseau.
5) Dans **Préfixes faisceaux** entrez `0`.
6) Dans **Numéro de l'installation-entrant** , dans le champ **Indicatif national** entrez `49`.
7) Dans **Numéro de l'installation-entrant**, dans le champ **Indicatif du réseau local** entrez 89.
8) Dans **Numéro de l'installation-entrant**, dans le champ **Numéro de l'installation** entrez `722`.
9) Cochez la case **Numéro de l'installation-entrant**, dans le champ **Numéro de site**.
10) Il est possible de reprendre les paramètres par défaut du faisceau (type de n°, sortant, type de numéro de téléphone.
11) Cliquez sur **Appliquer** puis sur **OK**.

20.6.4.14 Comment configurer LCR pour la mise en réseau (Noeud 2, Esclave)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33, 34 et 35 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour les noeuds 1 et 2. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local. Les entrées 36, 37 et 38 pour l'Interworking avec le noeud 1 (numéros de téléphone 100 > 199) et les entrées 39, 40 et 41 pour l'Interworking avec le noeud 3 (numéros de téléphone 300 > 399) doivent être complétées. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal for Desktop).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.
4) Entrez les valeurs suivantes sur les emplacements vides (ici 36 à 43) après les valeurs par défaut :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
31	Appl-Suite	-171	12
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	14
36	Noeud 1 interne	0C0049230266758-Z	16
37	Noeud 1 Nat	0C0230266758-Z	16
38	Noeud 3 interne	0C0049230266719-Z	17
39	Noeud 3 Nat	0C0230266719-Z	17
40	Noeud 3 Abo	0C66719-Z	17
41	Noeud 4 interne	0C004989722-Z	18
42	Noeud 4 Nat	0C089722-Z	18
43	Noeud 4 Abo	0C722-Z	18
44			-

5) Cliquez sur **Appliquer** puis sur **OK**.

6) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 1.

a) Dans **Nom de la règle**, entrez **Noeud 1**.
b) Dans **Format de la règle de numérotation**, entrez **D49230266758E3A**.
c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
e) Cliquez sur **Appliquer** puis sur **OK**.

7) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 16 pour le networking et l'affecter directement au noeud 1.

a) Cliquez sur la table de routage 16.
b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 1**.
d) Dans **Discrimination mini.**, sélectionnez **15**.
e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **1**.
h) Cliquez sur **Appliquer** puis sur **OK**.

8) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 3.

a) Dans **Nom de la règle**, entrez **Noeud 3**.
b) Dans **Format de la règle de numérotation**, entrez **D49230266719E3A**.
c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
e) Cliquez sur **Appliquer** puis sur **OK**.

9) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 17 pour le networking et l'affecter directement au noeud 3.

a) Cliquez sur la table de routage 17.
b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 3 direct**.
d) Dans **Discrimination mini.**, sélectionnez **15**.
e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **3**.
h) Cliquez sur **Appliquer** puis sur **OK**.

10) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 4.

a) Dans **Nom de la règle**, entrez **Noeud 4**.
b) Dans **Format de la règle de numérotation**, entrez **D89722E3A**.
c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
d) Dans **Type** sélectionnez l'entrée **Indicatif du réseau local**.
e) Cliquez sur **Appliquer** puis sur **OK**.

11) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 18 pour le networking et l'affecter directement au noeud 4.

a) Cliquez sur la table de routage 18.
b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 4**.
d) Dans **Discrimination mini.**, sélectionnez **15**.
e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
f) Cliquez sur **Appliquer** puis sur **OK**.

20.6.4.15 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 3, Esclave)

A l'aide des étapes suivantes, configurez le faisceau et les paramètres de faisceau pour la mise en réseau de l'Esclave.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Dir. 1` pour la ligne réseau.
5) Dans **Préfixes faisceaux** entrez `0`.
6) Dans **Numéro de l'installation-entrant** , dans le champ **Indicatif national** entrez `49`.
7) Dans **Numéro de l'installation-entrant**, dans le champ **Indicatif du réseau local** entrez `2302`.
8) Dans **Numéro de l'installation-entrant**, dans le champ **Numéro de l'installation** entrez `66719`.
9) Cochez la case **Numéro de l'installation-entrant**, dans le champ **Numéro de site**.
10) Il est possible de reprendre les paramètres par défaut du faisceau (type de n°, sortant, type de numéro de téléphone.
11) Cliquez sur **Appliquer** puis sur **OK**.

20.6.4.16 Comment configurer LCR pour la mise en réseau (Noeud 3, Esclave)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33, 34 et 35 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour les noeuds 1 et 2. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal for Desktop).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.
4) Entrez les valeurs suivantes :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
31	Appl-Suite	-171	12
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	14
36	Noeud 1 interne	0C0049230266758-Z	16
37	Noeud 1 Nat	0C00230266758-Z	16
38	Noeud 1 Abo	0C66758-Z	16
39	Noeud 2 interne	0C004989722-Z	17
40	Noeud 2 Nat	0C0089722-Z	17
41	Noeud 4 interne	0C0049230266719-Z	18
42	Noeud 4 Nat	0C0230266719-Z	18
43	Noeud 4 Abo	0C66719-Z	18
44			-

5) Cliquez sur **Appliquer** puis sur **OK**.
6) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 1.
   a) Dans **Nom de la règle**, entrez **Noeud 1**.
   b) Dans **Format de la règle de numérotation**, entrez **D49230266758E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.
7) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 16 pour le networking et l'affecter directement au noeud 1.
   a) Cliquez sur la table de routage 16.
   b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 1**.
   d) Dans **Discrimination mini.**, sélectionnez **15**.
   e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **1**.
   h) Cliquez sur **Appliquer** puis sur **OK**.

8) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 2.
   a) Dans **Nom de la règle**, entrez **Noeud 2**.
   b) Dans **Format de la règle de numérotation**, entrez **D4989722E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.
9) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 17 pour le networking et l'affecter directement au noeud 2.
   a) Cliquez sur la table de routage 17.
   b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 2**.
   d) Dans **Discrimination mini.**, sélectionnez **15**.
   e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **2**.
   h) Cliquez sur **Appliquer** puis sur **OK**.
10) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 4.
   a) Dans **Nom de la règle**, entrez **Noeud ML 4**.
   b) Dans **Format de la règle de numérotation**, entrez **D230266719E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif du réseau local**
   e) Cliquez sur **Appliquer** puis sur **OK**.
11) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 18 pour le networking et l'affecter directement au noeud 4.
   a) Cliquez sur la table de routage 18.
   b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 4**.
   d) Dans **Discrimination mini.**, sélectionnez **15**.
   e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   f) Cliquez sur **Appliquer** puis sur **OK**.

20.6.4.17 Comment configurer les faisceaux et les paramètres de faisceau (Noeud 4, Maître)

A l'aide des étapes suivantes, configurez le faisceau et les paramètres de faisceau pour la mise en réseau de l'Esclave.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Lignes/ Routage**.
3) Dans l'arborescence du menu, cliquez sur **Sens**.
4) Dans la fenêtre **Modifier le faisceau**, champ **Nom du faisceau**, entrez un nom, par ex. `Dir. 1` pour la ligne réseau.
5) Dans **Préfixes faisceaux** entrez `0`.
6) Dans **Numéro de l'installation-entrant** , dans le champ **Indicatif national** entrez `49`.
7) N'effectuez aucune entrée dans les champs **Indicatif du réseau local** et Numéro de l'installation.
8) Cochez la case **Numéro de l'installation-entrant**, dans le champ **Numéro de site**.
9) Il est possible de reprendre les paramètres par défaut du faisceau (type de n°, sortant, type de numéro de téléphone.
10) Cliquez sur **Appliquer** puis sur **OK**.

20.6.4.18 Comment configurer LCR pour la mise en réseau (Noeud 4, Maître)

Dans le plan de numérotation LCR, il faut compléter les entrées par défaut dans index 32, 33, 34 et 35 par des entrées pour la sélection des numéros de téléphone au format "International, National et Participants" pour les noeuds 1 et 2. "International" et "National" sont toujours nécessaires. "Participants" uniquement pour les noeuds partenaire qui se trouvent dans le même noeud local. Ces indications sont utilisées pour la sélection à partir d'applications (par ex. myPortal for Desktop).

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Plan de numérotation**.
4) Entrez les valeurs suivantes sur les emplacements vides (ici 36 à 43) après les valeurs par défaut :

Plan de numérotatio	Nom	Chiffres composés	Table de routage
1	Appel d’urgence	0C112	19
2	Appel d’urgence	0C110	19
3	Télétravail	0C0137Z	19
4	Télévote	0C0138Z	19
5	Premium Services	0C0900Z	19
6	Service d'information	0C118Z	19
7	Numéro spécial	0C116116	19
16	Par défaut	0CZ	19

Plan de numérotatio	Nom	Chiffres composés	Table de routage
17	Par défaut	0C1Z	19
18	Par défaut	0CNZ	19
31	Appl-Suite	-471	12
32	Par défaut	88CZ	1
33	Réseau IP	-Z	13
34	RésInternat	0C0049-Z	15
36	Noeud 1 interne	0C0049230266758-Z	16
37	Noeud 1 Nat	0C0230266758-Z	16
38	Noeud 1 Abo	0C66758-Z	16
39	Noeud 2 interne	0C004989722-Z	17
40	Noeud 2 Nat	0C089722-Z	17
41	Noeud 3 interne	0C0049230266719-Z	18
42	Noeud 3 Nat	0C0230266719-Z	18
43	Noeud 3 Abo	0C66719-Z	18
44			-

5) Cliquez sur **Appliquer** puis sur **OK**.

6) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 1.

a) Dans **Nom de la règle**, entrez **Noeud 1**.
b) Dans **Format de la règle de numérotation**, entrez **D49230266758E3A**.
c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
e) Cliquez sur **Appliquer** puis sur **OK**.

7) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 16 pour le networking et l'affecter directement au noeud 1.

a) Cliquez sur la table de routage 16.
b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 1**.
d) Dans **Discrimination mini.**, sélectionnez **15**.
e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **1**.
h) Cliquez sur **Appliquer** puis sur **OK**.

8) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 2.
   a) Dans **Nom de la règle**, entrez **Noeud 2**.
   b) Dans **Format de la règle de numérotation**, entrez **D4989722E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.
9) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 17 pour le networking et l'affecter directement au noeud 2.
   a) Cliquez sur la table de routage 17.
   b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 2**.
   d) Dans **Discrimination mini.**, sélectionnez **15**.
   e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **2**.
   h) Cliquez sur **Appliquer** puis sur **OK**.
10) Dans l'arborescence du menu, cliquez sur la **règle de numérotation** correspondante pour le noeud 3.
   a) Dans **Nom de la règle**, entrez **Noeud ML 3**.
   b) Dans **Format de la règle de numérotation**, entrez **D230266719E3A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Indicatif national**.
   e) Cliquez sur **Appliquer** puis sur **OK**.
11) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 18 pour le networking et l'affecter directement au noeud 3.
   a) Cliquez sur la table de routage 18.
   b) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
   c) Dans **Règle de numérotation**, sélectionnez l'entrée **Noeud 3**.
   d) Dans **Discrimination mini.**, sélectionnez **15**.
   e) Dans **Avertissement** sélectionnez l'entrée **Néant**.
   f) Dans **Passerelle dédiée**, sélectionnez l'entrée **Forcée**.
   g) Dans **ID noeud Passerelle**, sélectionnez l'entrée **3**.
   h) Cliquez sur **Appliquer** puis sur **OK**.
12) Dans l'arborescence du menu, cliquez sur la **Règle de numérotation** correspondant aux communications réseau. Il s'agit de la règle de numérotation prédéfinie "Gateway Call" (appel passerelle).
   a) Dans **Nom de la règle**; entrez **Gateway Call**.
   b) Dans **Format de la règle de numérotation**, entrez **E1A**.
   c) Dans **Procédures de l'opérateur**, sélectionnez l'entrée **Corporate Network** (réseau d'entreprise).
   d) Dans **Type** sélectionnez l'entrée **Inconnu**.
   e) Cliquez sur **Appliquer** puis sur **OK**.
13) Dans l'arborescence du menu, cliquez sur **Table de routage** pour configurer la table de routage 19 pour la sortie réseau des esclaves. Sur la

base de l'inscription Multi-Passerelle, l'affectation de l'abonné au noeud est déterminée et il est effectué sur ce noeud la sortie du réseau.

14) Cliquez sur la table de routage 19.

a) Dans **Faisceau** sélectionnez l'entrée **Mise en réseau**.
b) Dans **Règle de numérotation**, sélectionnez l'entrée **Gateway Call** (numéro passerelle).
c) Dans **Discrimination mini.**, sélectionnez **15**.
d) Dans **Avertissement** sélectionnez l'entrée **Néant**.
e) Dans **Passerelle dédiée**, sélectionnez **Multi-passerelle**.
f) Dans **ID noeud Passerelle**, sélectionnez l'entrée **1**.
g) Cliquez sur **Appliquer** puis sur **OK**.

20.6.5 Mise en réseau de OpenScape Business dans un environnement d'hébergement

Dans un environnement de plusieurs sites, (environnement d'hébergement), il peut être affecté à chaque site un faisceau et à chaque faisceau un enregistrement ITSP. Il est possible de gérer 8 enregistrements ITSP maxi. Un enregistrement par ITSP est possible ainsi que plusieurs enregistrements dans un ITSP. A chaque enregistrement ITSP il est possible d'affecter une préfixe de réseau local et ensuite plusieurs abonnés. Le raccordement des abonnés aux différents sites du système de communication est réalisé via VPN ou MPLS. Si les sites se trouvent dans différents pays, il faut utiliser pour chaque pays un OpenScape Business S spécifique (scénario 1a). Si tous les sites sont dans un même pays, il est possible d'utiliser un OpenScape Business S. (Scénario 1b).

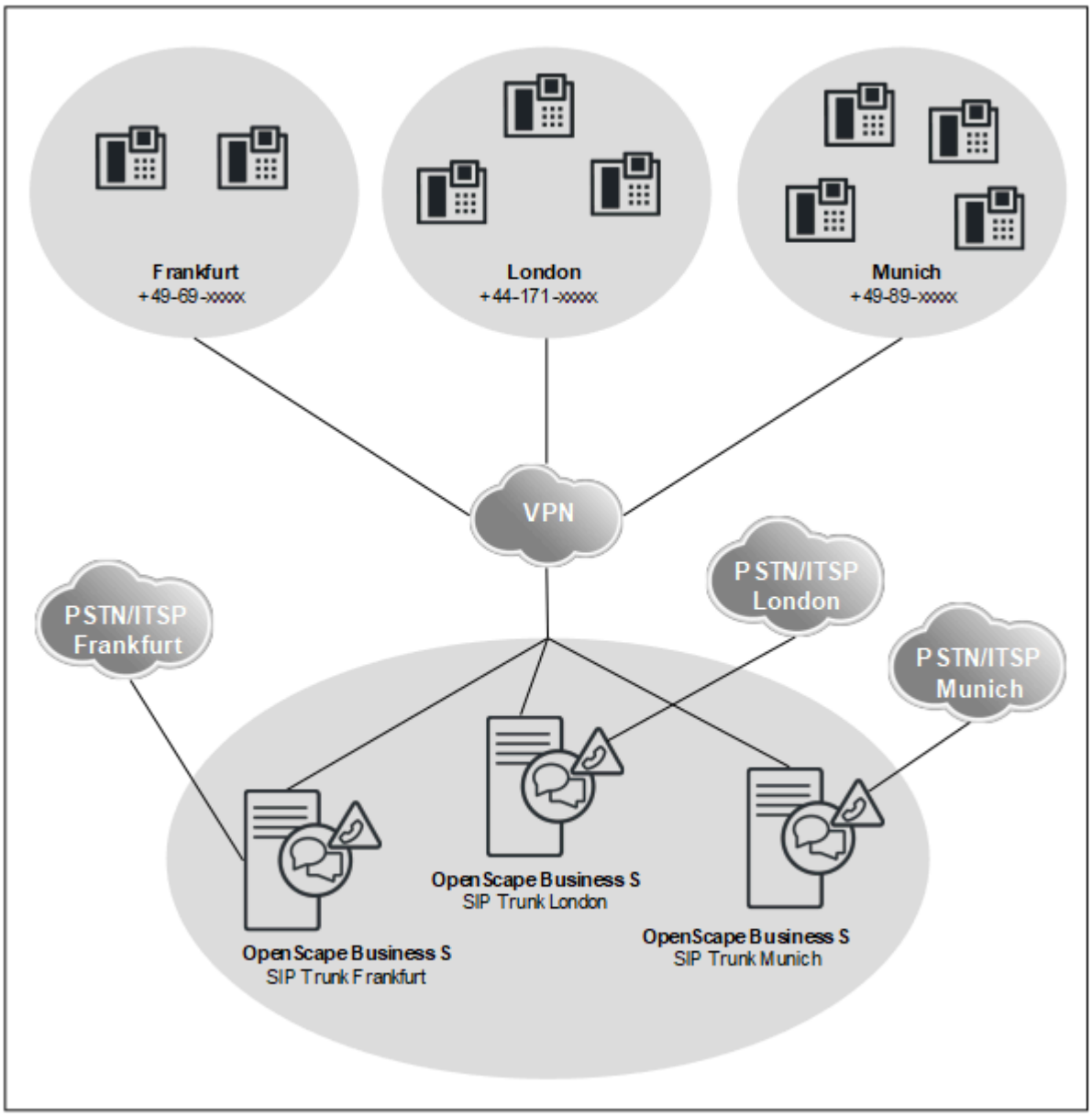
Les deux scénarios sont aussi réalisables avec les modèles matériels OpenScape Business X (par ex. pour les petites installations). Sur un même site, il est également possible d'utiliser les composantes TDM.

Les scénarios Hosting indiqués ci-après sont décrits d'une manière générale. Les variantes suivantes sont réalisables.

- Utilisation de OpenScape Business S et OpenScape Business X dans le centre de données du client ou hébergeur
- OpenScape Business S sur serveur matériel ou virtualisé
- Condition : une infrastructure VPN MPLS, en particulier lorsqu'il existe plusieurs sites client (aucun routeur NAT spécifique à un site servant d'accès Internet)
- Jusqu'à 8 ITSP par système et pays, fournisseur MSN ou de n° SDA
- Jusqu'à 8 préfixes de site (area codes) par système et pays, affectés à jusqu'à 8 sites client (multi-site)
- Scénarios multi-site combinables avec une mise en réseau classique (Voix et UC)
- Multi-site >8 sites réalisables dans interconnexions de réseau (x fois réseau multi-site)
- Multi-site réalisable sur l'ensemble du pays dans le cadre de réseaux (x fois réseau multi-site)
- Scénarios de mise en réseau avec passerelles RNIS entièrement intégrables
- La condition technique est de pouvoir utiliser de la même manière les numéros SDA pour le fournisseur RNIS comme pour le fournisseur SIP.

Scénario a : hébergement avec un OpenScape Business S par site

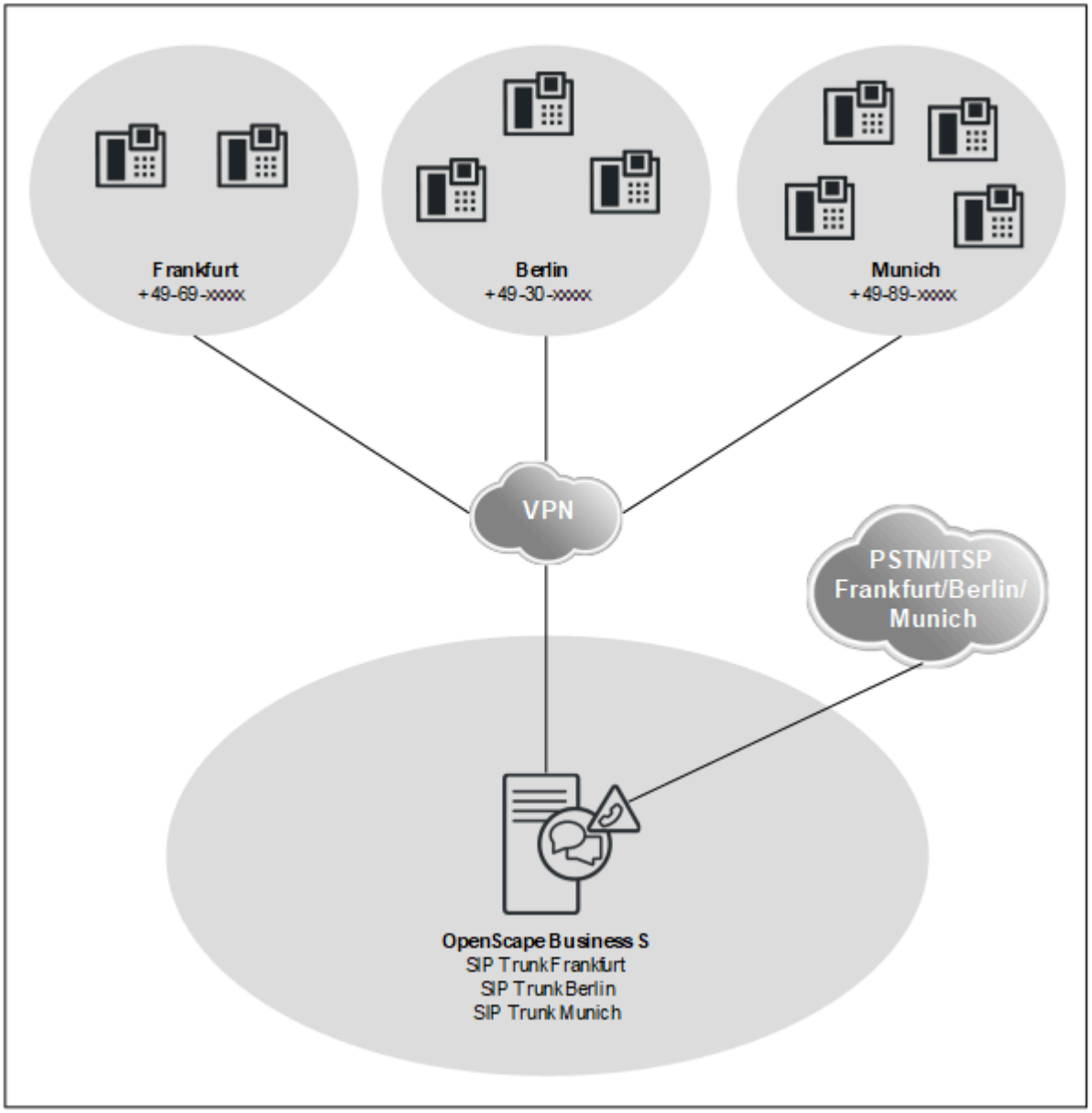
Données réseau



- Client à l'intérieur d'un VPN ou MPLS.
- Un OpenScape Business S par site.
- Les sites peuvent être répartis à l'intérieur d'un pays ou dans plusieurs pays.
- Jusqu'à 1000 utilisateurs et 180 tronçons SIP par OpenScape Business S.
- Mise en réseau OpenScape Business en option, jusqu'à 1500 utilisateurs au total. Des installations de plus grandes tailles sont possibles dans le cadre de projets spécifiques.

Scénario b : hébergement avec un OpenScape Business S pour plusieurs sites

Données réseau



- Client à l'intérieur d'un VPN ou MPLS.
- Un OpenScape Business S pour tous les sites.
- Sites uniquement à l'intérieur d'un pays.
- Jusqu'à 8 sites avec différents préfixes.
- Jusqu'à 8 fournisseurs SIP par OpenScape Business S.
- Un fournisseur SIP par site.
- Jusqu'à 1000 utilisateurs et 180 jonctions SIP.
- Mise en réseau de OpenScape Business avec plusieurs OpenScape Business S à l'intérieur d'un VPN en option (OS Biz S 1 dans pays 1, OS Biz S 2 dans pays 2, etc.), jusqu'à 1500 utilisateur au total. Des installations de plus grandes tailles sont possibles dans le cadre de projets spécifiques.

- Exemple de configuration, voir Unify Experts Wiki dans Internet, *ITSP Configuration Guide*.

20.6.6 Mise en réseau d'OpenScape Business X et d'OpenScape 4000

La mise en réseau d'OpenScape Business X avec OpenScape 4000 peut prendre deux formes différentes. Premièrement, avec un adressage direct entre les nœuds OpenScape Business (scénario 4a), et deuxièmement, avec le routage de toutes les connexions via OpenScape 4000 (scénario 4b).

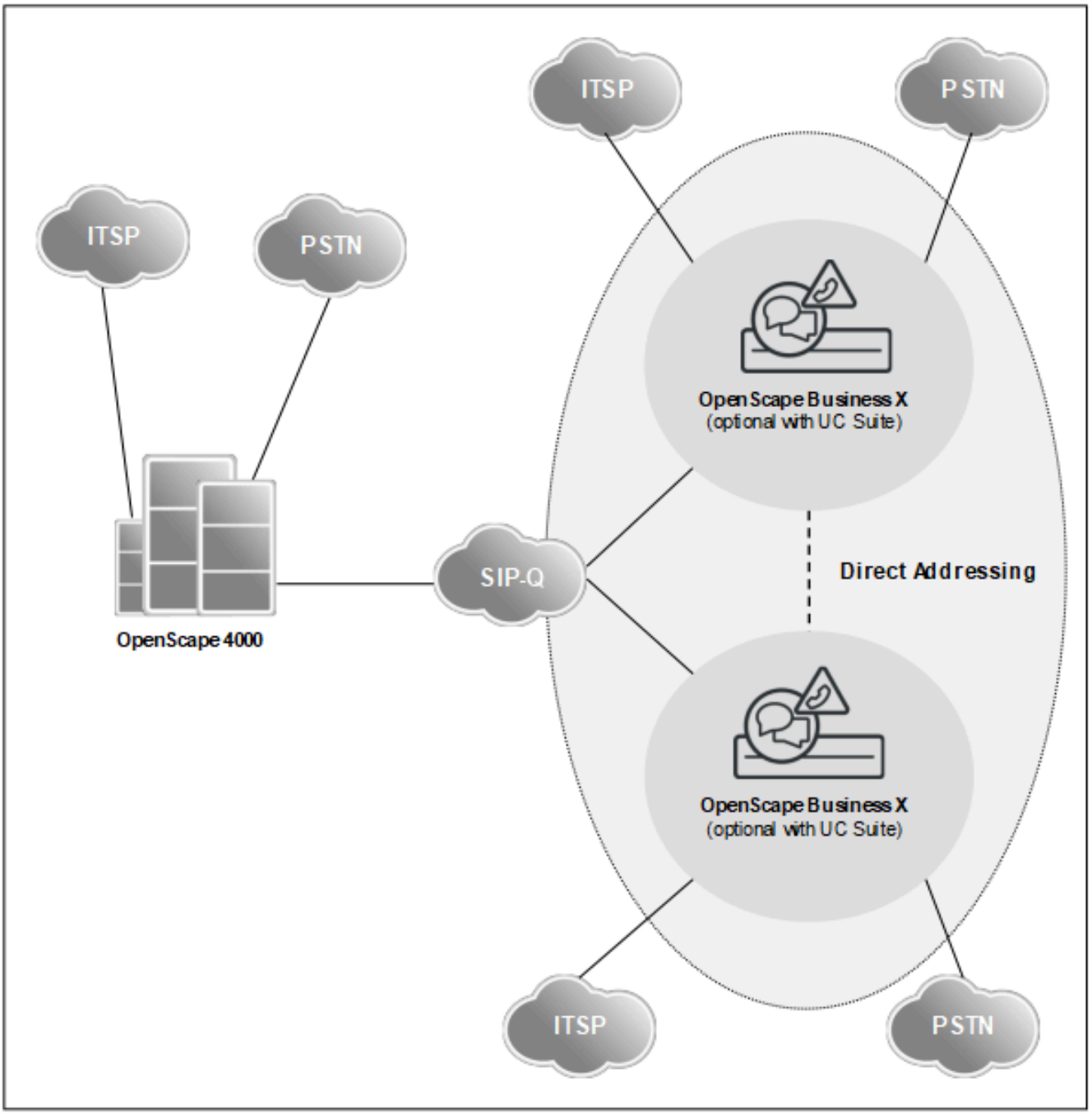
Remarque : Vous trouverez un exemple de configuration réseau pour OpenScape Voice dans le wiki des experts Unify à l' `adresse http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Scénario a : Travail sur Internet avec OpenScape 4000 et adressage direct entre les nœuds OpenScape Business X

Données réseau

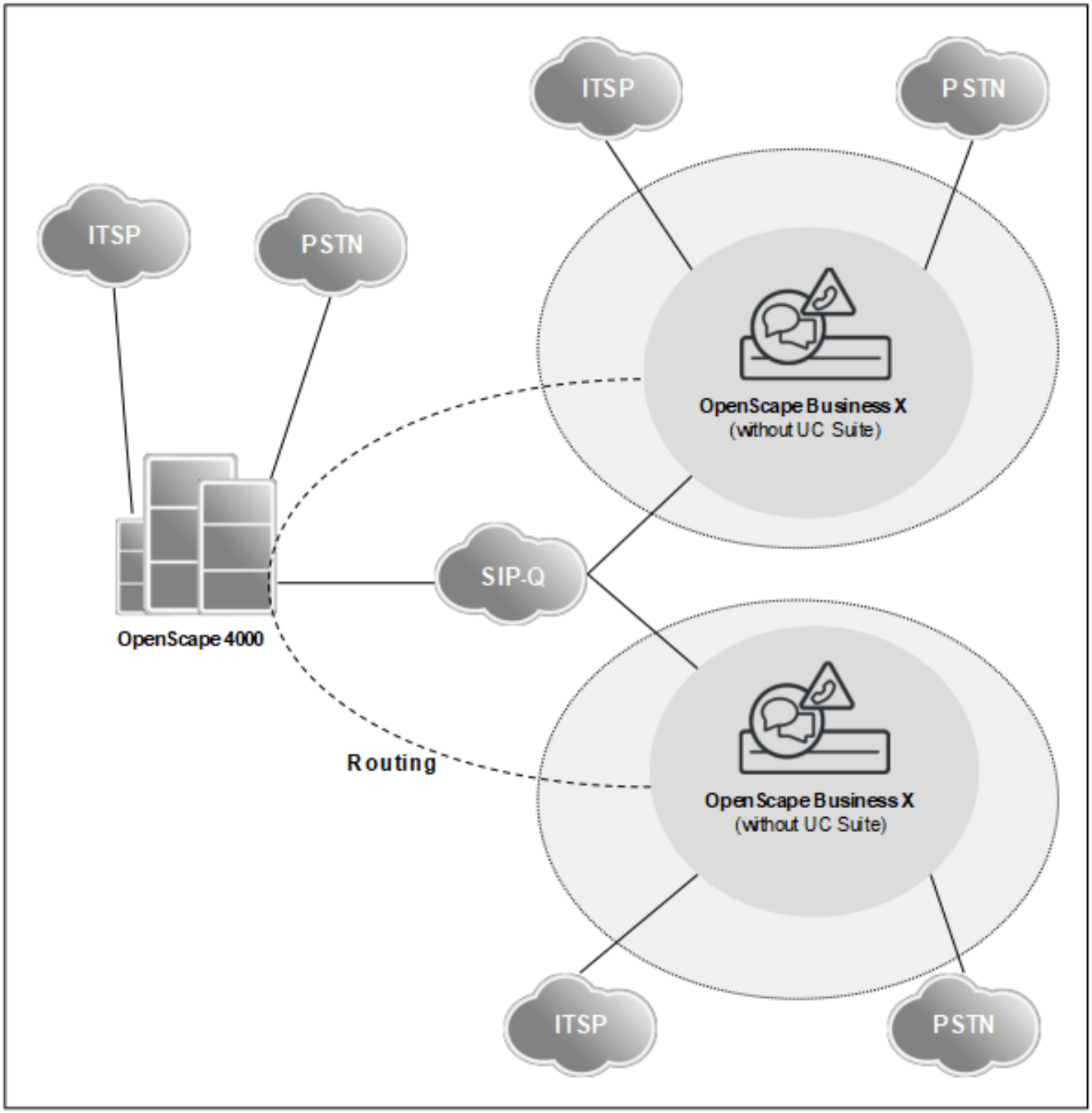
Scénario b : Travail sur Internet avec OpenScape 4000 et routage de toutes les connexions via OpenScape 4000

Données réseau



- Numérotation fermée au sein du réseau OpenScape Business
- Fonctionnalités vocales et de communications unifiées à l'échelle du réseau au sein de l'interconnexion OpenScape Business

- Configuration du réseau OpenScape Business avec l'assistant de configuration réseau
- Configuration des composants réseau OpenScape 4000 en mode Expert
- Le concept de petit site distant (SRS) n'est pas pris en charge.
- OpenScape Business S peut être intégré en mode passerelle unique ou multiple.



- Numérotation ouverte
- Fonctionnalité vocale à l'échelle du réseau
- Chaque appel vers un autre nœud est acheminé via OpenScape 4000.
- Aucune solution de communications unifiées n'est disponible dans OpenScape Business car le réseau utilise une numérotation ouverte.

- Le concept de petit site distant (SRS) n'est pas pris en charge.
- La configuration doit être effectuée en mode expert pour chaque nœud.

Fonctionnalités à l'échelle du réseau

Expansion	Numérotation fermée au sein du réseau OpenScape Business (scénario 4a)	Numérotation ouverte (scénario 4b)
Nombre maximal de nœuds	100 (32 publiés, selon OpenScape 4000)	
Nombre maximal de stations par système	Selon le modèle OpenScape Business X	
Nombre maximal de stations dans le réseau	1500 pour le segment de réseau OpenScape Business	Selon OpenScape 4000
Réseau vocal	SIP-Q	

Réseautage UC	Numérotation fermée (Scénario 4a)	Numérotation ouverte (scénario 4b)
	Fonctionnalités à l'échelle du réseau au sein d'OpenScape Business	Non pris en charge
OpenScape Business S	Soutenu	Non pris en charge

Administration	Numérotation fermée (Scénario 4a)	Numérotation ouverte (scénario 4b)
	WBM avec assistants pour les nœuds OpenScape Business ; OpenScape 4000 est administré via le mode Expert d'OpenScape Business.	Administration du réseau en mode Expert
WBM	WBM avec des sorciers	WBM avec mode expert
Gestionnaire E	Non recommandé	Non recommandé
Administration de UC Suite	WBM avec assistants pour les nœuds OpenScape Business	Non pris en charge
Importation massive de données via des fichiers CSV (numéros d'appel, numéros DID, noms)	Séparément pour chaque nœud du réseau	

Licence	Numérotation fermée (Scénario 4a)	Numérotation ouverte (scénario 4b)
structure de licence	Une licence réseau est requise pour chaque entreprise OpenScape.	

myPortal pour ordinateur de bureau / myPortal pour Outlook (UC Suite)	Numérotation fermée (Scénario 4a)	Numérotation ouverte (scénario 4b)
	Réseau avec fonctionnalité UC via OpenScape Business S	Non pris en charge

myPortal pour ordinateur de bureau / myPortal pour Outlook (UC Suite)	Numérotation fermée (Scénario 4a)	Numérotation ouverte (scénario 4b)
Messagerie instantanée	Sur l'ensemble du réseau, à l'intérieur d'un réseau OpenScape Business	Non pris en charge
Messagerie vocale	Les abonnés utilisent leur système de messagerie vocale local ; il n'y a pas de messagerie vocale centrale pour l'ensemble de l'interconnexion de réseaux.	Non pris en charge
État de présence	Sur l'ensemble du réseau, à l'intérieur d'un réseau OpenScape Business	Non pris en charge
Indication d'occupation	Sur l'ensemble du réseau, à l'intérieur d'un réseau OpenScape Business	Non pris en charge
Répertoire interne/favoris	Sur l'ensemble du réseau, à l'intérieur d'un réseau OpenScape Business	Non pris en charge
Annuaire externe	Local par importation de fichiers csv	Non pris en charge
Recherche dans les répertoires externes d'autres nœuds	Impossible	Non pris en charge
Répertoire hors ligne externe (LDAP)	via LDAP	Non pris en charge

myAttendant	Numérotation fermée (Scénario 4a)	Numérotation ouverte (Scénario 4b)
	Avec fonctionnalité UC via Unify OpenScape Business S	Non pris en charge
Messagerie instantanée	Sur l'ensemble du réseau, à l'intérieur d'un réseau OpenScape Business	Non pris en charge
Messagerie vocale	Les abonnés utilisent leur système de messagerie vocale local ; il n'y a pas de messagerie vocale centrale pour l'ensemble de l'interconnexion de réseaux.	Non pris en charge
État de présence	Sur l'ensemble du réseau, à l'intérieur d'un réseau OpenScape Business	Non pris en charge
Indication d'occupation	Sur l'ensemble du réseau, à l'intérieur d'un réseau OpenScape Business	Non pris en charge
Répertoire interne/favoris	Sur l'ensemble du réseau, à l'intérieur d'un réseau OpenScape Business	Non pris en charge

myAttendant	Numérotation fermée (Scénario 4a)	Numérotation ouverte (Scénario 4b)
Annuaire externe	Local par importation de fichiers csv	Non pris en charge
Recherche dans les répertoires externes d'autres nœuds	Impossible	Non pris en charge
Répertoire hors ligne externe (LDAP)	via LDAP	Non pris en charge

Company AutoAttendant (UC Suite)	Numérotation fermée (Scénario 4a)	Numérotation ouverte (Scénario 4b)
Company AutoAttendant : une fois que le standard automatique (AutoAttendant) a répondu à un appel, l'appelant doit composer le numéro avec lequel il souhaite être joint.	Les scripts ccv permettent de composer des numéros provenant du répertoire interne à l'intérieur de l'interconnexion de réseaux.	Non pris en charge
Standard automatique personnel : une fois que le standard automatique a répondu à un appel, l'appelant doit sélectionner un chiffre pour être en liaison avec sa destination d'appel.	Tous les numéros de téléphone préconfigurés par un abonné UC sont possibles	Non pris en charge

Company AutoAttendant (UCSmart)	Numérotation fermée (Scénario 4a)	Numérotation ouverte (Scénario 4b)
Company AutoAttendant (UCSmart)	Local	Local

myAgent	Numérotation fermée (Scénario 4a)	Numérotation ouverte (Scénario 4b)
	Avec la fonctionnalité UC via Unify OpenScape Business S. Tous les agents sont enregistrés sur UN nœud. Appels CC entrants via le réseau RTC, ITSP et les joncteurs réseau SIP-Q.	Non pris en charge
Messagerie instantanée	En réseau	Non pris en charge
Messagerie vocale (enregistrement, indication de message en attente, interrogation)	Les abonnés utilisent leur système de messagerie vocale local ; il n'y a pas de messagerie vocale centrale pour l'ensemble de l'interconnexion de réseaux.	Non pris en charge
État de présence	En réseau	Non pris en charge
Indication d'occupation	En réseau	Non pris en charge
État de l'agent	Local	Non pris en charge
Annuaire interne	En réseau	Non pris en charge
Annuaire externe	Local par importation de fichiers csv	Non pris en charge
Recherche dans les répertoires externes d'autres nœuds	Impossible	Non pris en charge

myAgent	Numérotation fermée (Scénario 4a)	Numérotation ouverte (Scénario 4b)
Répertoire hors ligne externe (LDAP)	via LDAP	Non pris en charge
Contacts Outlook	Local	Non pris en charge
Transférer un appel	Local	Non pris en charge
Information client	Local	Non pris en charge
Reporting	Local	Non pris en charge

Applications externes	Numérotation fermée (Scénario 4a)	Numérotation ouverte (Scénario 4b)
OpenScape Business Application TAPI	Voir Application Connectivity	
Applications CSTA externes		
Application Launcher		
OpenScape Contact Center	Voir Centre de contacts multimédia.	

Téléphonie	Numérotation fermée (Scénario 4a)	Numérotation ouverte (Scénario 4b)
Fournisseur SIP (ITSP)	Local	Local
Fournisseur de réseau téléphonique public commuté (RTPC)	Les nœuds de réseau locaux, dépourvus de fournisseur PSTN propre, sont accessibles via SIP-Q ou la passerelle associée.	
Survie (redondance en cas de panne du réseau ou d'OpenScape Business S)	Compatible entre OpenScape Business X et OpenScape Business S	Non pris en charge
Composez un numéro public dans votre propre nœud	Soutenu	
Composez un numéro public dans un nœud en réseau	À l'échelle du réseau, au sein de l'interconnexion OpenScape Business	

Mobilité	Numérotation fermée (Scénario 4a)	Numérotation ouverte (scénario 4b)
Partage de bureau	Au sein d'un nœud ; à l'échelle du réseau, au sein de l'interconnexion OpenScape Business (avec DLS)	Non pris en charge
Mobilité avec commande DTMF du système	Local (non pris en charge pour OpenScape Business S)	Locale

Autres fonctionnalités	Numérotation fermée (Scénario 4a)	Numérotation ouverte (scénario 4b)
Chiffrement de la signalisation et de la charge utile (SPE)	Non pris en charge sur les réseaux OpenScape 4000 / OpenScape Business. Non pris en charge pour les connexions et conférences UC	Non pris en charge sur les réseaux OpenScape 4000 / OpenScape Business. Non pris en charge pour les conférences

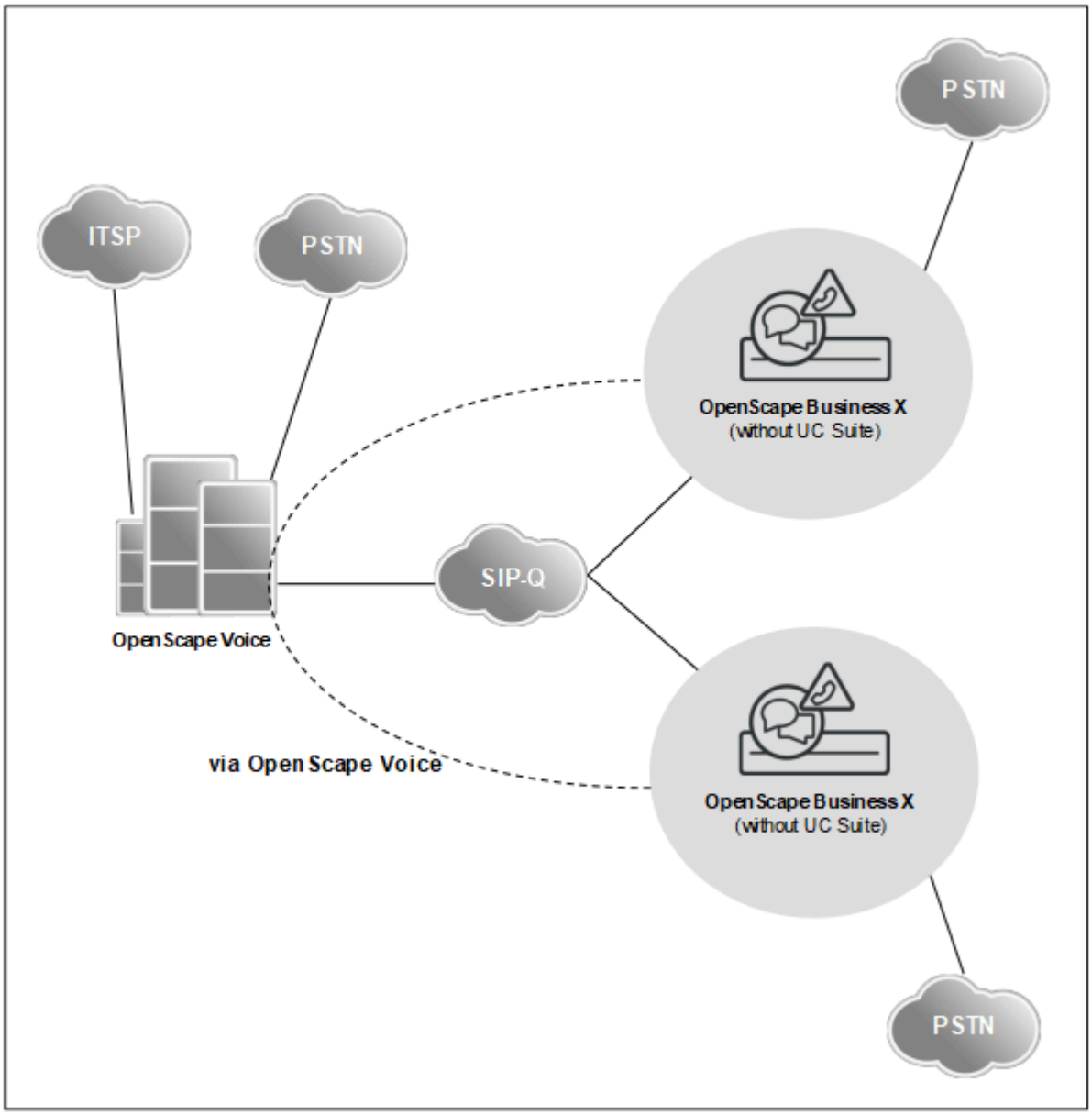
Autres fonctionnalités	Numérotation fermée (Scénario 4a)	Numérotation ouverte (scénario 4b)
Serveur DSS	À l'échelle du réseau, au sein de l'interconnexion OpenScape Business	Non pris en charge
Prise d'appel	Non pris en charge	Non pris en charge

20.6.7 Mise en réseau de OpenScape Business X et OpenScape Voice

OpenScape Business X peut être mis en réseau avec OpenScape Voice.

Remarque : Vous trouverez un exemple de configuration pour la mise en réseau avec OpenScape Voice dans Unify Experts Wiki sous `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Données réseau



- OpenScape Business X propose à OpenScape Voice une fonctionnalité Voix et Passerelle sur l'ensemble du réseau
- Un ou plusieurs OpenScape Business X peuvent être utilisés comme passerelle pour les centraux numériques (RNIS, T1, CAS)
- Sur les passerelles OpenScape Business X, les terminaux suivants peuvent être exploités : numériques / analogiques / DECT / IP (HFA)
- Dans ce réseau, UC n'est généralement pas supporté par OpenScape Business X.
- Chaque communication d'un noeud à un autre est acheminée par OpenScape Voice.
- La configuration de chaque noeud est effectuée en mode Expert.
- Le plan de numérotation de OpenScape Voice est basé sur E.164, donc, il n'y a pas de numérotation ouverte ou fermée.

Fonctionnalités sur l'ensemble du réseau

Configuration maximum	
Nombre maximum de noeuds	en fonction de OpenScape Voice
Nombre maximum d'abonnés dans un système de communication individuel	en fonction de OpenScape Business X
Nombre maximum d'abonnés dans le réseau	en fonction de OpenScape Voice

Administration	
WBM	L'assistant Mise en réseau ne peut pas être utilisé. OpenScape Voice est géré à l'aide du mode Expert de OpenScape Business, noeud par noeud.
Manager E	Non recommandé
UC-Administration	UC non pertinent en connexion avec OpenScape Voice
Importation de grandes quantités de données via fichiers csv (numéros d'appel, numéros de sélection directe à l'arrivée, noms)	Séparément pour chaque noeud de OpenScape Business dans l'interconnexion de réseaux

Procédure de licence	
Structure des licences	Chaque noeud individuellement, une licence réseau est nécessaire pour chaque noeud OpenScape Business

Restrictions et remarques sur les fonctionnalités

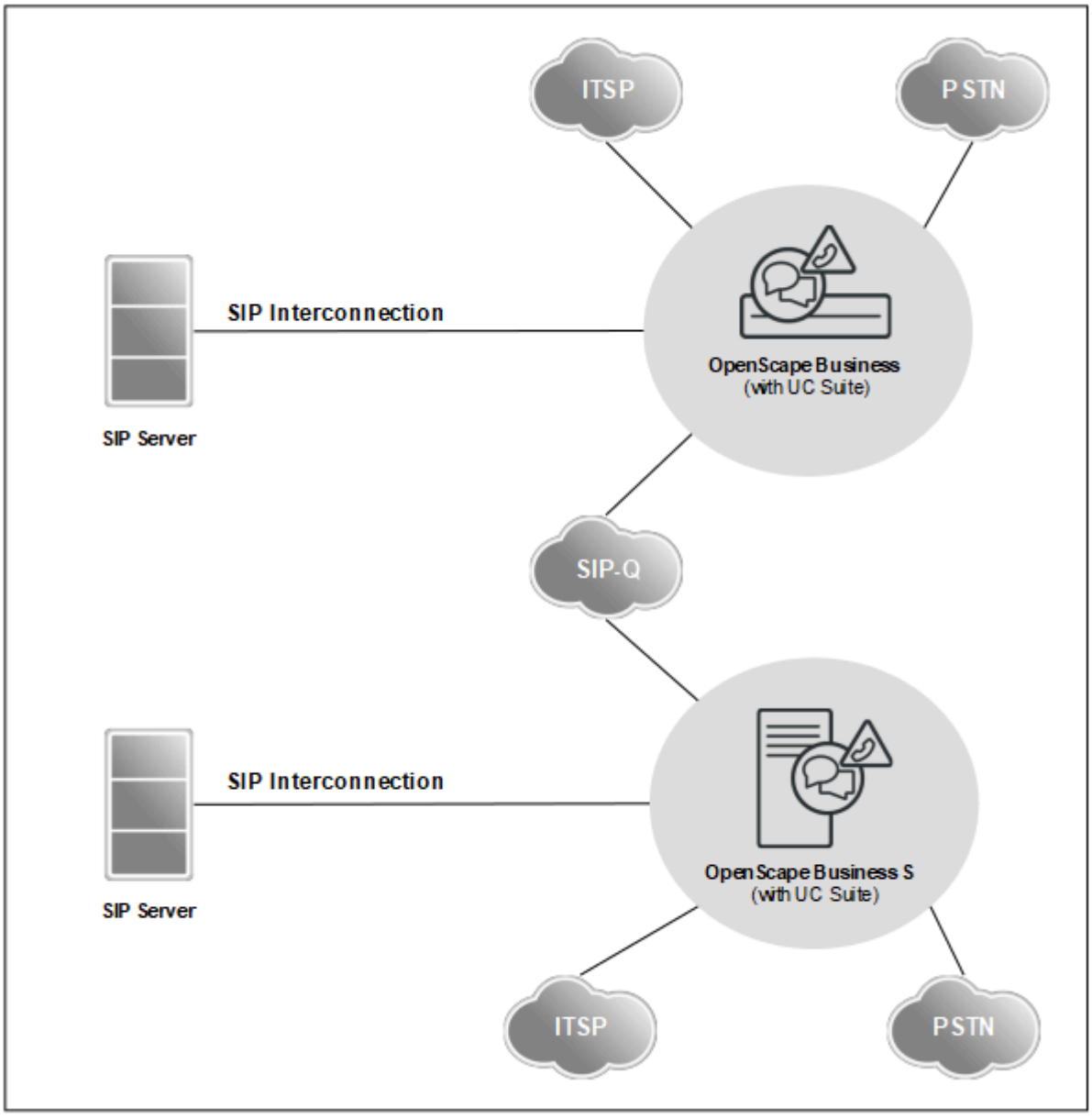
- La connexion des lignes réseau analogiques aux passerelles OpenScape Business est validée **uniquement** au Brésil (car Line Reversal et la libération vers l'arrière des lignes réseau analogiques sont réalisés dans les centraux brésiliens).
- Une mise en réseau de passerelles OpenScape Business les unes avec les autres ou avec d'autres systèmes qu'OpenScape Voice n'est pas supportée. La mise en réseau de passerelles OpenScape Business avec OpenScape Voice doit se faire par une structure de réseau en étoile.
- Path Replacement (Optimisation route) via SIP-Q n'est pas supporté pour les terminaux raccordés sur une passerelle OpenScape Business.
- Pour éviter une mauvaise qualité de la voix sur les connexions par ligne de transit, il est conseillé d'utiliser un codec voix G.711. Le Codec G.729 n'est pas recommandé car les fonctionnalités comme Conférence et Renvoi d'appel peuvent créer des liaisons de transit et que Path Replacement (optimisation de l'acheminement) n'est pas supporté.
- Pas de prise en charge inter-systèmes de fonctionnalités, telles que groupes d'interception, appels collectifs et groupements entre OpenScape Voice et les passerelles OpenScape Business. Les groupes doivent comprendre soit des abonnés OpenScape Voice, soit des abonnés OpenScape Business.
- Le cryptage (Signaling & Payload Encryption, SPE) entre OpenScape Voice et les passerelles OpenScape Business 3000 n'est pas supporté. La connexion entre OpenScape Voice et OpenScape Business doit être réalisée avec un protocole de cryptage TLS. SRTP (SDES) n'est pas supporté dans le cas d'une mise en réseau avec OpenScape Voice V7R1.
- Seule la mise en réseau avec plan de numérotation E.164 est supportée.

- Pour les terminaux IP raccordés aux passerelles OpenScape Business : sur chaque connexion active OpenScape Business/OpenScape Voice, 2 canaux B sont nécessaires par terminal HFA (1 canal B par terminal TDM). La nécessité de ces ressources SDP supplémentaires doit faire l'objet d'un contrôle et d'une prise en compte.

20.6.8 Association de connexions externes à OpenScape Business via interconnexion SIP

Il est possible d'associer à OpenScape Business des connexions externes via interconnexion SIP afin de pouvoir par ex. utiliser des applications comme OpenScape Alarm Server, OpenScape 4000, OpenScape Voice ou d'autres serveurs SIP certifiés.

Conditions



- Seules des applications certifiées peuvent être raccordées, par ex. OScAR.
- Un serveur externe SIPO peut être raccordé via protocole SIP d'origine ou SIP-Q.
- On dispose au maximum de deux faisceaux SIP-Q (un est utilisé pour UC Suite si disponible) et de 10 faisceaux d'origine SIP maxi. (jusqu'à 8 faisceaux d'origine SIP peuvent être utilisés pour ITSP).

Vous trouverez plus d'informations dans

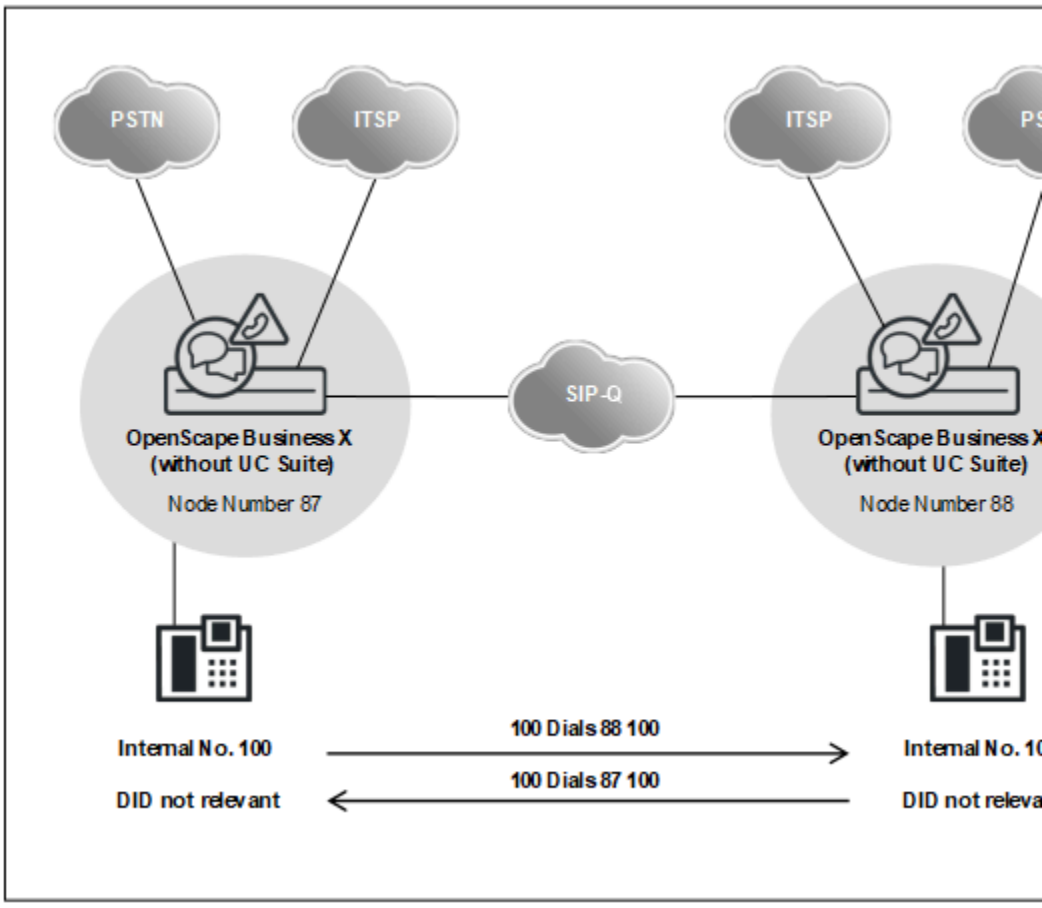
- Wiki experts pour téléphones, systèmes de communication et UC :

  `http://wiki.unify.com`

20.6.9 Numérotation ouverte dans les réseaux OpenScape Business X

Une interconnexion de réseaux avec numérotation ouverte peut être paramétrée lorsque deux (ou plusieurs) systèmes de communication sont mis en réseau et que leur numérotation se recoupe (n'est pas de manière univoque dans l'interconnexion de réseaux).

Données réseau



- Mise en réseau de la voix sur l'ensemble du réseau avec OpenScape Business.
- Les fonctionnalités UC ne sont pas supportées.

- Chaque appel à l'intérieur d'un noeud est effectué avec numéro de téléphone interne.
- Chaque appel vers un autre noeud a lieu avec le numéro de noeud (plus le numéro de téléphone interne).
- Configuration de chaque noeud à l'aide du mode Expert. L'assistant Mise en réseau est bloqué dès qu'un numéro de noeud a été configuré pour une numérotation ouverte.
- Ligne extérieure RTC ou ITSP est local sur chaque noeud.

Remarque : Dans le cas de l'extension d'une fonctionnalité UC sur l'ensemble du réseau, il est nécessaire de passer d'une numérotation ouverte à une numérotation fermée afin d'adapter les numéros internes. Donc, la numérotation ouverte doit être désactivée tandis que le numéro de noeud doit être effacé et ensuite ajouté comme préfixe (par exemple numéro interne étendu 87100 à la place de 100 et 88100 à la place de 100).

Différences :

- La sélection des participants dans leur propre noeud est effectuée avec le numéro interne étendu.

- Le numéro d'appel interne et le numéro SDA peuvent différer si nécessaire, mais les numéros SDA ne doivent pas être modifiés.

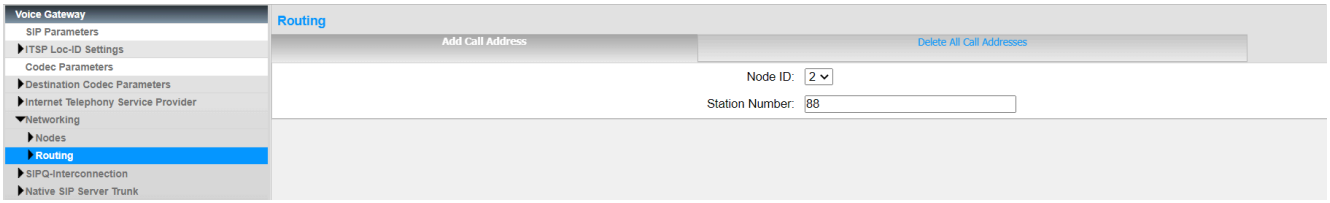
20.6.9.1 Comment configurer la numérotation ouverte

Paramétrer la numérotation ouverte

1) Activer la numérotation ouverte pour le système de communication à l'aide de l'indicateur système **Numérotation ouverte**
2) Inscrire son prore numéro de noeud (dans notre exemple "87")

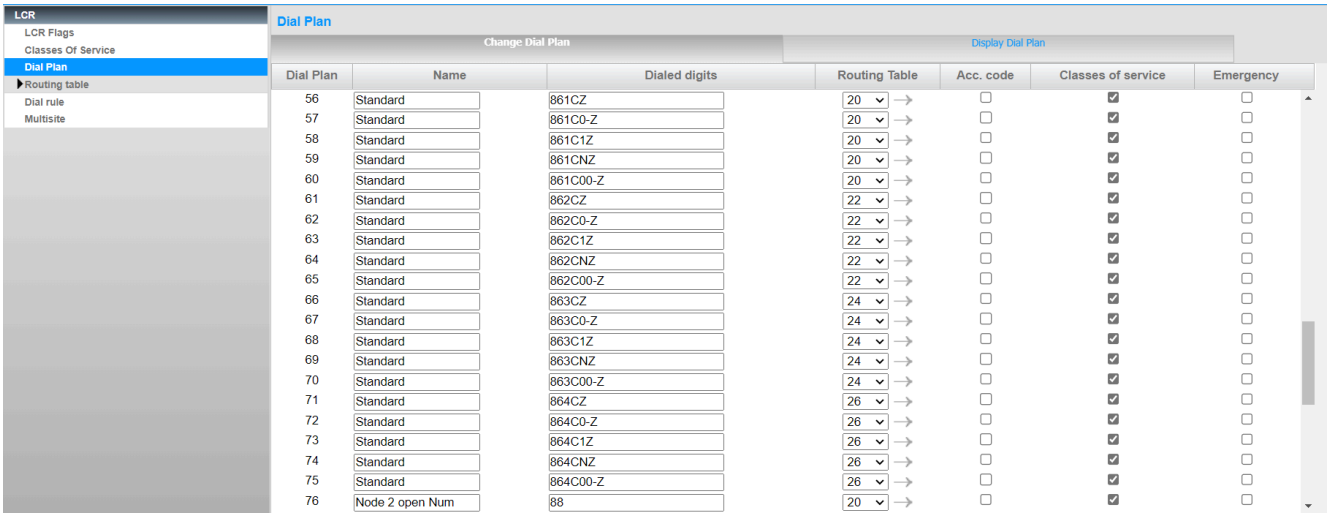
Paramétrer les noeuds (Routage)

1) Les noeuds de destination sont atteints avec l'acheminement suivant : Passerelle vocale > Mise en réseau > Noeud > Routage (dans nore exemple "88").
2) Dans un modèle à numérotation ouverte, il n'est pas possible d'utiliser l'assistant **Mise en réseau**, qui est bloqué par l'indicateur système **Numérotation ouverte**.

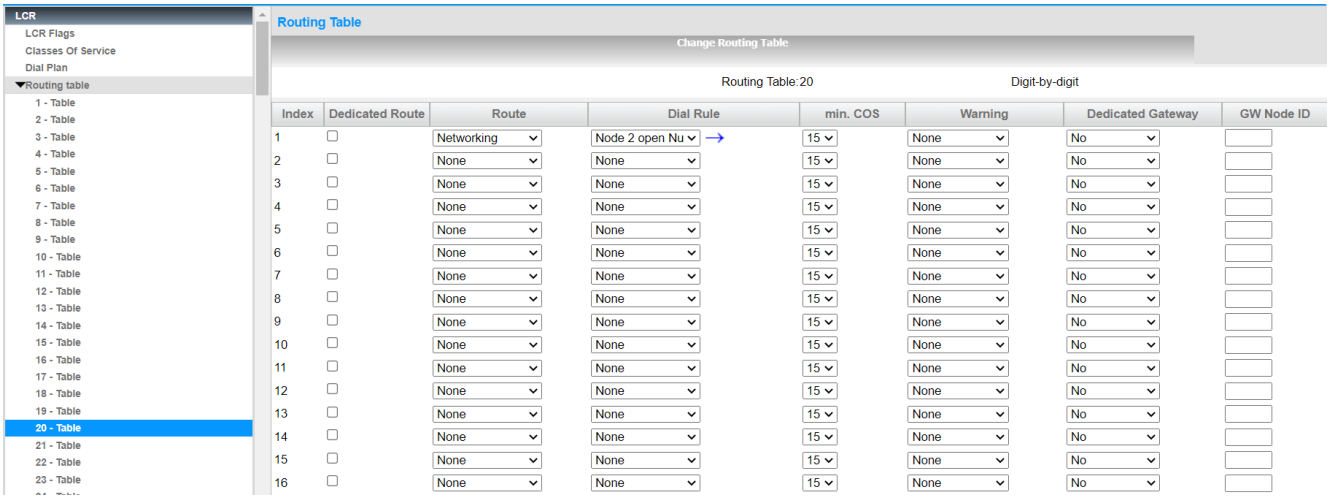


Paramétrer LCR

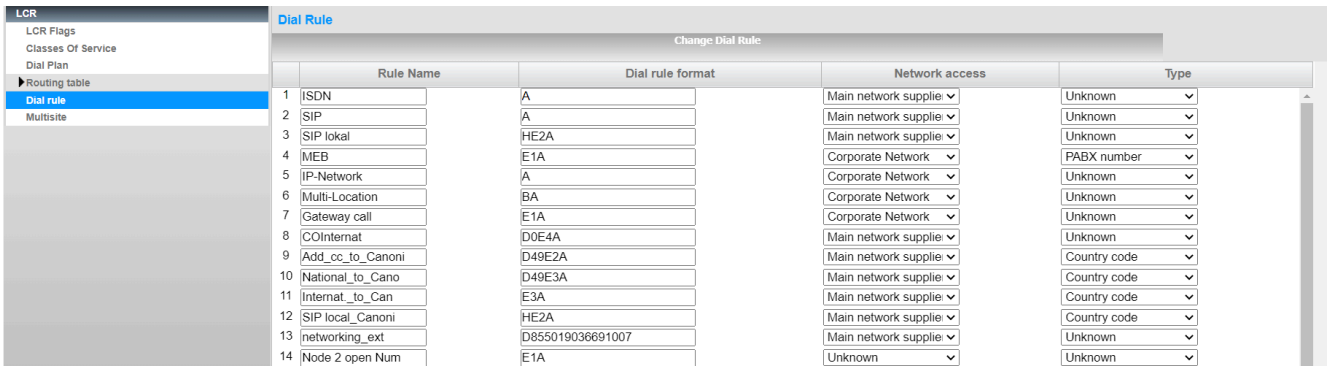
1) Définir la règle de numérotation, "Node 2 Open Num" pour le numéro de noeud et sélectionner la table de routage correspondante.



2) Affichage de la route configurée



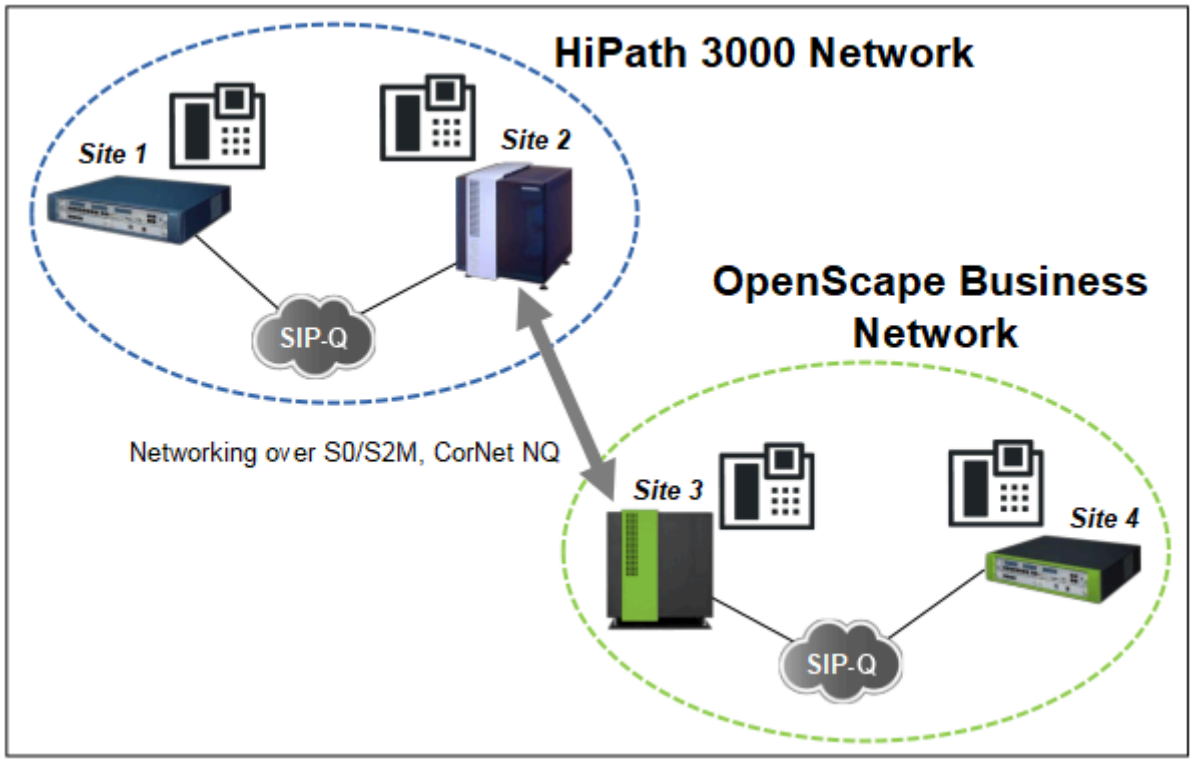
3) Entrer le noms de la route "Mise en réseau" et la règle de numérotation correspondante "Node 2 Open Num".



20.6.10 Mise en réseau par RNIS

Les systèmes OpenScape Business peuvent être mis en réseau les uns avec les autres, mais aussi avec les systèmes de communication HiPath 3000 et OpenScape 4000 à l'aide de lignes de connexion numériques. Le raccordement peut être réalisé à l'aide de lignes S_0 comme S_{2M}.

Réseau avec HiPath 3000



Le réseau HiPath 3000 existant reste (dans un premier temps) inchangé. L'extension du réseau est réalisée avec OpenScape Business. Si nécessaire, il est possible d'effectuer un migration pas à pas des noeuds HiPath 3000 vers le réseau OpenScape Business.

Tout appel HiPath 3000/OpenScape Business adressé au-delà est réalisé via des passerelles TDM correspondantes (S_0 ou S_{2M} avec protocole CorNet NQ, le cas échéant QSIG en tant que protocole indépendant du constructeur).

Les conditions annexes suivantes s'appliquent :

- Licence séparée HiPath 3000 / OpenScape Business
- Administration séparée HiPath 3000 / OpenScape Business
- Recommandé : numérotation fermée sur l'ensemble du réseau. En cas de numérotation ouverte, il peut se produire éventuellement des défaillances concernant avec CLIP ainsi qu'avec les entrées journal/listes des appelants.
- Recommandé : utiliser exclusivement un codec G.711 afin de garantir une bonne qualité de la voix sur l'ensemble du réseau.
- Le nombre des canaux B doit être défini en fonction de la quantité de communications à attendre.
- OpenScape Business nécessite dans tous les cas une licence réseau.

Raccordement de systèmes tiers via QSIG

Lorsque l'on raccorde des systèmes tiers avec le protocole QSIG il faut tenir compte des aspects suivants.

- Contrôler les variantes QSIG des systèmes tiers concernés en ce qui concerne la compatibilité (QSIG V1, appelé également QSIG selon norme ECMA ou QSIG V2 appelé également QSIG selon norme ISO).
- Comparaison entre les groupes de fonctionnalités des systèmes concernés. On peut voir dans quelle mesure l'étendue des fonctionnalités, c.-à-d. la partie identique des deux groupes de fonctionnalités répond aux souhaits du client.
- Pour s'assurer que les fonctionnalités attendues sont bien disponibles, il est recommandé d'effectuer un essai de raccordement sur site. Dans ce cadre, il faut tenir compte en particulier de l'interfonctionnement avec d'autres protocoles de mise en réseau ou protocoles réseau.

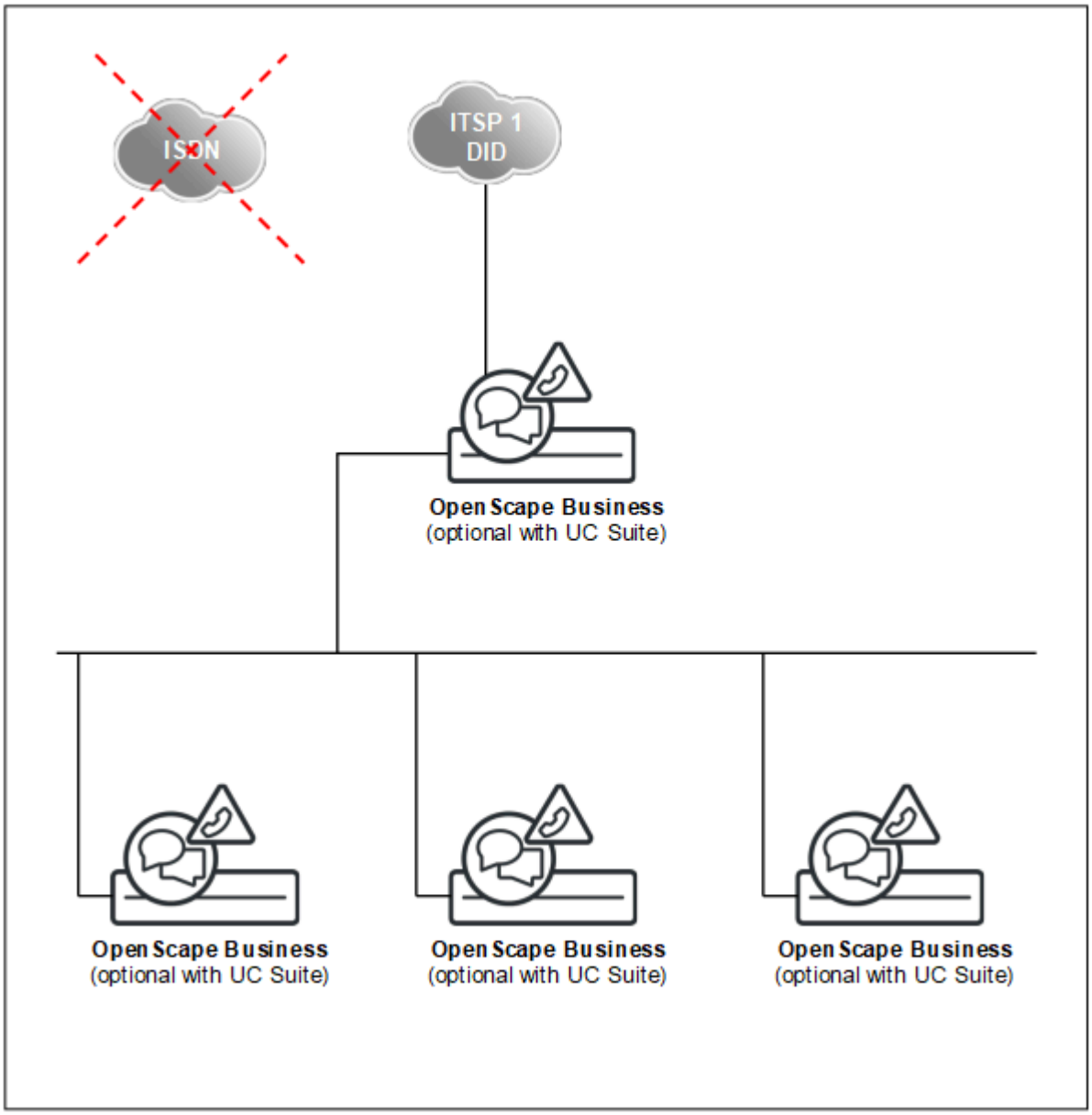
Remarque :

Le groupe de lignes QSIG doit être configuré comme type de route PABX dans le système OpenScape Business. Par conséquent, les appels provenant du réseau QSIG seront considérés comme internes et suivront le CDL interne.

20.6.11 Interconnexion de réseaux OpenScape Business avec raccordement réseau ITSP central

Une interconnexion de réseaux OpenScape Business pure peut être réalisée avec un raccordement de réseau ITSP central compatible SDA à la place du RNIS.

Mise en réseau avec raccordement réseau ITSP central, compatible SDA



Il faut tenir compte des aspects suivants lors de la planification des réseaux client :

- **Un** raccordement réseau ITSP central, compatible SDA pour le réseau OpenScape Business complet.
- Enregistrement exactement sur un réseau local, c.-à-d. que tous les noeuds du réseau utilisent exactement un numéro de réseau, par ex. 0049 89 7007-xxxxx.
- Dans les cas d'urgence, par ex. en cas de défaillance de l'accès central ITSP, les noeuds en réseau peuvent disposer de connexions réseau propres pour les liaisons sortantes. Dans certaines circonstances, l'identification correcte de l'appelant vers l'extérieur n'est pas possible dans ce cas. Le cas échéant, les appels d'urgence peuvent ne pas être adressés correctement. La capacité d'être joint via cette connexion locale peut également être soumise à des restrictions. Pour ces raisons, les connexions locales ne

sont pas recommandées, mais elles ne sont pas rendues techniquement impossibles.
- Pour la même raison, il n'est pas non plus recommandé de créer des raccordements RNIS supplémentaire sur le noeud central, mais cela n'est pas rendu techniquement impossible.
- Toutes les règles pour l'évaluation de la numérotation et l'acheminement des appels, relatives aux systèmes individuels et réseaux OpenScape Business s'appliquent. Dans ce cas, l'affectation de numéro d'appel des numéros de réseau ITSP est réalisée exclusivement dans le cadre de la configuration du numéro SDA de l'abonné (et non pas à l'aide de la table de mappage, voir Configuration ITSP, chapitre 9.2 et voir Unify Experts Wiki sur Internet).

20.7 Poste de renvoi central dans l'interconnexion de réseaux (pas pour les Etats-Unis)

Afin qu'aucun appel ne se perde, OpenScape Business permet de renvoyer vers un poste de renvoi distinct (à définir) les appels entrants qui ne peuvent pas être affectés à un abonné ou qui ne reçoivent pas de réponse.

Lorsque le poste de renvoi central de l'interconnexion de réseaux est configuré via RNIS, le fonctionnement est identique au fonctionnement sans mise en réseau.

Dans un réseau ITSP, il existe certaines restrictions pour le poste de renvoi central car chaque noeud a par principe son propre ITSP.

- Les critères de renvoi ITSP s'appliquent uniquement pour le noeud concerné.
- Le renvoi distinct est effectué sur non réponse, si occupé, si numérotation incomplète, sur fausse numérotation et en cas de retour d'appel sans réponse.
- Les renvois distincts "Fausse numérotation" et "Numérotation incomplète" ne fonctionnent pas avec ITSP.
- Les numéros de téléphone incomplets ou faux sont renvoyés à l'ITSP avec le signal Occupé.

Lorsque l'on doit utiliser un poste de renvoi central dans une interconnexion de réseaux, il faut configurer dans chaque noeud des abonnés virtuels. Ces abonnés virtuels sont renvoyés de manière fixe vers l'utilisateur myAttendant via l'interconnexion de réseaux.

Exemple pour le réseau ITSP : le numéro de l'installation ITSP est 0211-23456789 + n° SDA ITSP ; le numéro 0211-23456789-0 est diffusé publiquement comme numéro central du système de communication.

- L'abonné 100 est myAttendant avec son propre n° SDA ITSP 100 et l'abonné virtuel 199 avec n° SDA ITSP "0".
- Dans la liste de mapping ITSP de chaque noeud, le n° SDA ITSP "0" est affecté au propre abonné virtuel.
- Dans **Appels entrants/Renvoi temporisé**, les abonnés virtuels sont adressé à l'abonné 100.

  Première destination : propre abonné virtuel

  Deuxième destination : abonné 100 dans le noeud de destination

  Temps d'appel 5 Secondes

Pour mieux identifier les appels, il est recommandé d'attribuer leur numéro de téléphone (SDA) et un nom (par ex. entreprise) aux abonnés virtuels de tous les noeuds à l'aide de l'application myAttendant (dans **Configuration**/**myAttendant**/**SDA**). Ainsi, il est possible d'effectuer une identification complète de l'appelant dans la fenêtre **Appels actifs** de myAttendant.

20.7.1 Comment configurer un poste de renvoi central dans une interconnexion de réseaux multi-passerelle

Exemple de configuration d'un poste de renvoi central en interconnexion de réseaux multi passerelle via les passerelles OpenScape Business en amont. Tous les appels qui parviennent à un noeud et répondent aux critères de renvoi doivent être acheminés vers OpenScape Business S où se trouve le standard automatique central.

Conditions préalables

OpenScape Business S est maître (tous les abonnés HFA et SIP sont inscrits ici).

Plusieurs OpenScape Business X sont configurés comme noeud Esclave (avec RTC ou ITSP en tant qu'accès réseau). Les noeuds peuvent se trouver au même endroit ou à des endroits différents.

Étape par étape

1) Configuration d'un abonné virtuel dans OpenScape Business.
   a) Configuration d'un abonné virtuel avec nom "Renvoi distinct 22 Système2"

2) Configuration d'un poste de renvoi centralisé avec critères de renvoi à OpenScape Business.
   a) **Mode Expert**
   b) **Paramétrage de base** > **Système** > **Renvoi/P.O/Hotline**
   c) Sélectionner l'abonné virtuel 22 dans **Poste de renvoi** de **jour et de nuit**.
   d) Entrer les paramètres suivants pour l'abonné 22 dans **Poste de renvoi**, **Renvoi distinct** :

Nom	Renvoi distinct 22 Système2
SDA	xxxxxxx22
Type de terminal	Virtuel

   e) Activer les paramètres entrés dans **Poste de renvoi**, **Renvoi distinct**.
   f) Configuration de l'abonné virtuel dans **Poste de renvoi** dans **Code verrouillage**.

3) Configuration du renvoi temporisé dans OpenScape Business.

a) Configurer le renvoi temporisé de l'abonné virtuel 22 à l'aide de l'interconnexion de réseaux avec OpenScape Business S.
b) **Mode Expert**
c) **Appels entrants** > **Renvoi temporisé**
d) Sélectionner l'abonné virtuel 22
e) Suivant vers **Paramétrer le renvoi temporisé pour l'abonné**
f) puis à : **destination externe** (entrer numéros d'appel de file d'attente standard automatique, par ex. 7410)
g) **Faisceau** = Sélectionner réseau (Le numéro de file d'attente standard automatique 7410 doit être acheminé de manière ciblée dans LCR en contournant la règle -Z défaut 33).

4) Configuration du routage pour OpenScape Business.

Le numéro de file d'attente standard automatique 7410 doit être acheminé de manière ciblée dans LCR, en contournant la règle -Z défaut 33.

Dans **Plan de numérotation** :	Configurer **Nom** (VSL pilote file d'attente)
	Entrer le numéro de téléphone dans **Chiffres composés** (7410)
	Sélectionner la **table de routage** (XX)
Dans **Table de routage** XX :	**Faisceau** = Sélectionner réseau
	Affecter **Règle de numérotation**
	Dans **Passerelle dédiée**, sélectionner l'entrée **Forcé**.
	Inscrire **ID noeud Passerelle** d'OpenScape Business S
dans **Règle de numérotation** :	Entrer **Nom de la règle**
	Entrer le **Format de la règle de numérotation** D7410 (numéro pilote file d'attente)
	Procédures de l'opérateur, sélectionnez Corporate Network (réseau d'entreprise).
	Type : sélectionner Inconnu

5) Configurer une file d'attente OpenScape Business S.

a) Configuration d'une file d'attente (pilote file d'attente) avec CCV, par ex. **Composer par poste**, **Numérotation par nom**, **Action d'après chiffres**.

6) Configuration d'un renvoi temporisé sur OpenScape Business S.

a) Configurer le renvoi temporisé de pilote file d'attente 7410 dans OpenScape Business S.
b) **Mode Expert**
c) **Appels entrants** > **Renvoi temporisé**
d) Sélectionner pilote file d'attente 7410
e) Suivant vers **Paramétrer le renvoi temporisé pour l'abonné**
f) tout d'abord à : **destination externe** (Standard automatique entrer les numéros d'appel des files d'attente, par ex. 7410)
g) puis à : sélectionner **boîte vocale**

20.8 Gestionnaire de présence

Le gestionnaire de présence permet de signaler les états de l'abonné « Libre », « Occupé » et « Sonnerie » sur l'ensemble du réseau via les voyants LED des téléphones HFA. Cela nécessite une numérotation fermée et un OpenScape Business S comme nœud maître. Une licence réseau est requise pour chaque nœud.

En veille, la LED correspondante est éteinte ; en activité, elle est constamment allumée ; et en sonnerie, la LED clignote. Lorsque l'appareil sonne, l'appel peut être pris en appuyant sur le bouton correspondant.

Les états de traitement des appels ne peuvent être signalés pour une station que si le gestionnaire de présence peut définir un point de surveillance CSTA sur la station concernée.

Les touches sont configurées par l'utilisateur. Lorsque les numéros de poste sont programmés directement sur le téléphone, aucune distinction n'est faite entre les numéros internes et les numéros de réseau.

Le Gestionnaire de présence est un service et ne possède pas d'interface utilisateur. Aucun réglage n'est nécessaire, car toutes les données sont automatiquement obtenues par synchronisation.

Les groupes ne sont pas pris en charge par Presence Manager. La signalisation par LED n'est pas assurée et la prise d'appel n'est pas possible. Les MULAP ne sont toutefois pas pris en charge par Presence Manager.

Presence Manager ne prend pas en charge activement les téléphones SIP et S_0.

20.9 État de la synchronisation dans l'interconnexion de réseaux

Dans une interconnexion de réseaux, l'état de la synchronisation dans le portail Admin et l'état d'enregistrement des différents noeuds sont indiqués par des boutons de couleur. L'affichage de l'état de la synchronisation concerne les noeuds de réseau du système de communication et non pas les noeuds OpenScape 4000 et OpenScape Voice.

Afficher de l'état de la synchronisation

Affichage	Couleur	Signification pour le maître	Signification pour l'esclave
Etat de synchronisations (affichage sur la page de démarrage du portail Admin)	rouge	-	L'adresse IP du noeud Maître est configurée mais le système Esclave n'a pas pu s'enregistrer. A intervalles cycliques, l'esclave tente de s'enregistrer sur le maître.
	jaune	-	Esclave est enregistré dans Maître, mais les numéros de téléphone ne sont pas cohérents dans l'interconnexion de réseaux. Cela peut être le cas après une sauvegarde/restauration ou après le premier enregistrement.

Affichage	Couleur	Signification pour le maître	Signification pour l'esclave
	vert	Lorsque un noeud est configuré comme Maître, l'état est vert.	
Etat d'enregistrement des différents noeuds (affichage dans la boîte de dialogue Réseau>Vue du noeud)	rouge	Esclave est configuré ; le système ne s'est toutefois par encore enregistré.	Esclave est configuré ; le système ne s'est toutefois par encore enregistré.
	vert	Le système est enregistré.	Le système est enregistré.
Alive (affichage de la boîte de dialogue Réseau>Vue du noeud)	rouge	Vue des noeuds sur l'interconnexion de réseaux : tous les noeuds qui sont en rouge ne peuvent pas être joints. Les raisons peuvent être les suivantes : problèmes de réseau ou défaillance du système de communication.	
	vert	Le noeud (tiers) est joignable par le réseau. Le propre noeud est toujours représenté en vert.	

20.9.1 Synchronisation manuelle dans interconnexion de réseaux

Après la configuration des numéros de téléphone / noms (numéros internes ou numéros SDA) si ceux-ci ne sont pas automatiquement synchronisés dans les autres systèmes de l'interconnexion de réseaux, il est possible de lancer une synchronisation manuelle. La synchronisation manuelle dans interconnexion de réseaux fonctionne uniquement dans les réseaux homogènes.

Maître

Esclave

L'opération de synchronisation transmet uniquement les modifications de configuration.

Si l'affichage d'état dans le portail Admin est en "rouge", il est possible, en activant le bouton synchronisation, d'essayer de lancer manuellement la synchronisation des données sur le Maître.

Dans le cas où des systèmes déjà configurés du réseau ne peuvent plus téléphoner les uns avec les autres, il faut recherche la cause de cette défaillance ailleurs. Si l'état Alive de certains noeuds est "rouge", cela indique qu'il existe des problèmes de réseaux ou bien il existe d'autres raisons pour lesquelles le noeud du réseau n'est pas joignable. Dans ces cas, l'activation du bouton de synchronisation n'apporte aucune aide.

Lors de l'activation sur le noeud Maître, les noeuds Esclave sont invités à actualiser les numéros d'appel et les noms du système à partir du maître.

Lors de l'activation sur un noeud Esclave, les numéros d'appel et les noms du système sont actualisés sur le Maître. Simultanément, un nouvel enregistrement du noeud Esclave auprès du noeud Maître a lieu.

20.9.2 Comment démarrer la synchronisation manuelle

Conditions préalables

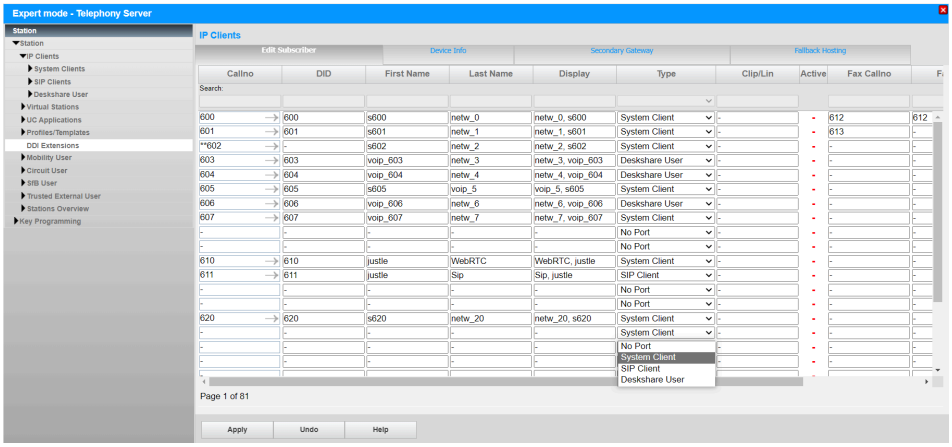
Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Redémarrer/Recharger**.
3) Activez le bouton **Sync Network** (synchronisation réseau) pour lancer la synchronisation manuelle.

20.10 Survivabilité

La capacité de survie est une fonction d'un réseau de nœuds OpenScape Business. Si un nœud OpenScape Business tombe en panne ou ne peut être atteint en raison d'erreurs de réseau, les téléphones système (HFA) connectés au nœud OpenScape Business peuvent se connecter à l'autre nœud OpenScape Business du réseau à la place. Les numéros de téléphone des téléphones système sont conservés après la nouvelle connexion. Cela permet d'assurer la continuité de la téléphonie de base ; cependant, les fonctions des applications telles que myPortal, la messagerie vocale et le CTI seront temporairement indisponibles.



Lorsque le nœud OpenScape Business défaillant est à nouveau accessible en toute sécurité, les téléphones du système reviennent automatiquement sur le nœud OpenScape Business.

Le temps de basculement vers la passerelle de secours peut durer jusqu'à 30 minutes.

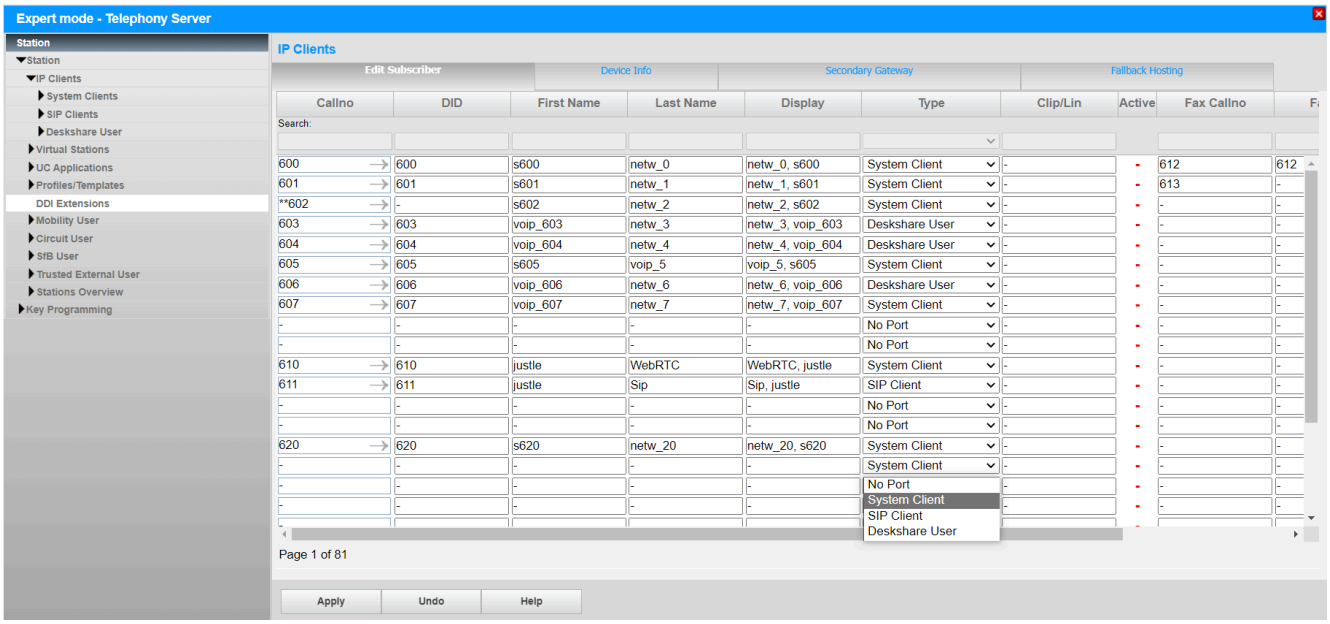
En cas de défaillance du nœud OpenScape Business, on tente d'abord de l'atteindre à nouveau pendant une durée déterminée (10 minutes ; non modifiable). Ce n'est qu'à l'issue de ce délai que les téléphones système prévus à cet effet sont enregistrés sur la passerelle de secours. L'état actuel des téléphones enregistrés peut être consulté en **mode Expert** > **journaux de diagnostic**.

Les paramètres de survie sont configurés sur les téléphones système. En cas de défaillance du nœud OpenScape Business, les téléphones essaient d'abord de le joindre à plusieurs reprises. Un délai d'attente ou la fréquence à laquelle le téléphone tente de se reconnecter peut être configuré via le paramètre "Redondance du système" dans le menu d'administration des téléphones. Par défaut, le délai d'attente est de 30 secondes avec une seule tentative. Ensuite, les téléphones s'enregistrent sur la passerelle de secours. L'enregistrement automatique au nœud OpenScape Business doit également être configuré sur les téléphones système.

Remarque : La fonction de survie nécessite le service POSTGRES pour fonctionner correctement. Si le pare-feu applicatif est activé avec une règle pour le service POSTGRES, vous devez vous assurer que les adresses IP des autres nœuds OpenScape Business en réseau sont ajoutées manuellement à cette règle, sinon la fonction de survivabilité ne fonctionnera pas.

Les conditions suivantes doivent être remplies pour la survivabilité :

- Un nombre suffisant de ports IP libres doit être disponible sur la passerelle de secours pour les téléphones système connectés au nœud OpenScape Business qui doivent être "sauvegardés" en cas de défaillance d'un nœud du réseau.
- Pour ces ports libres sur la passerelle de secours, les stations doivent être configurées sans nom ni numéro de téléphone.

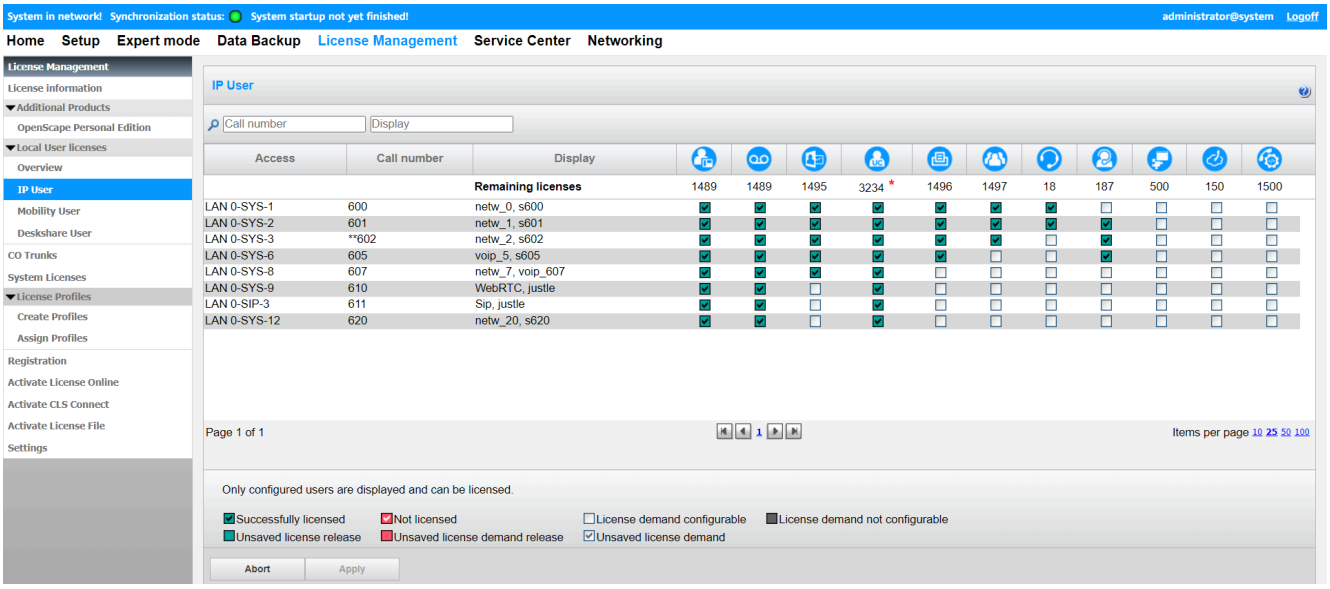


- Les stations doivent être configurées comme des téléphones système (clients système) et disposer d'une licence utilisateur Fallback. Si les licences Fallback ne sont pas disponibles dans le fichier de licence activé, des licences utilisateur IP peuvent être utilisées à la place. En cas de survivabilité, les stations ne peuvent utiliser que les fonctions de téléphonie.

Remarque : Pendant le temps d'arrêt du nœud maître, les numéros d'appel des clients de la redondance HFA entrent

en conflit jusqu'à ce que le nœud maître soit à nouveau opérationnel.

Remarque : Si des licences utilisateur Fallback sont attribuées au système, les licences utilisateur IP ne peuvent pas être utilisées en cas de défaillance.



20.10.1 Configuration de la survivabilité

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, allez à **Abonnés** > **Clients IP**. Dans un système Maître OpenScape Business, la fenêtre **Secondary Gateway** (passerelle secondaire) s'affiche.
3) Dans **ID noeud**, sélectionnez le OpenScape Business qui accueillera en cas d'urgence les abonnés d'OpenScape Business S.
4) Cochez la case **Emergency** pour les abonnés en situation d'urgence.
5) Les entrées pour **Emergency Call no** (n° d'urgence) et **Call no DID** (n° SDA) sont préconfigurées et peuvent être si nécessaire adaptées.
6) Cliquez sur **Appliquer** puis sur **OK**.

20.11 Retirer un noeud de l'interconnexion de réseaux

Si un noeud doit être retiré de l'interconnexion de réseaux, il est important que ce noeud ne puisse plus être joint dans la configuration du réseau. Sinon, le noeud essaie de manière indépendante de se connecter de nouveau dans le réseau et le noeud maître essaie de synchroniser les données.

Procédure

L'effacement d'un noeud est effectué à l'aide de l'assistant Mise en réseau ; tous les noeuds associés doivent être supprimés.

- Interrompre tous les circuits (routage) en direction des noeuds à supprimer.
- Administration de l'interconnexion de réseaux
- Entrer "Aucun réseau" pour le noeud esclave impliqué dans l'assistant de mise en réseau du nœud esclave.
- Supprimer le noeud esclave de la liste d'enregistrement dans l'assistant de mise en réseau du noeud maître.

Si un noeud n'est pas effacé correctement, des données continuent à être envoyées d'un OpenScape Business vers l'autre, ce qui peut produire des incohérences dans le répertoire interne, c.-à-d. que les utilisateurs n'apparaissent pas dans le répertoire utilisateur et ne peuvent donc pas par ex. utiliser myPortal for Desktop.

21 Autres équipements

Les connexions correspondent à des équipements externes (par ex. un équipement d'annonce ou un poste de portier avec dispositif d'ouverture de porte) qui sont raccordés aux interfaces du système de communication.

21.1 Dispositif d'annonce analogique

Un appareil d'annonce analogique peut être connecté à une interface a/b pour diffuser des annonces personnalisées (par exemple, pour le standard automatique central ou en remplacement de la musique d'attente).

Remarque : Avant d'utiliser des annonces ou de la musique provenant d'autres sources, assurez-vous de ne pas enfreindre les droits d'auteur.

Jusqu'à 16 sources d'annonces (par exemple, serveurs multimédias, lecteurs d'annonces ou appareils d'annonces analogiques) peuvent être configurées pour chaque système de communication.

Les types de dispositifs d'annonce suivants peuvent être utilisés :

- Dispositifs d'annonce qui démarrent toujours au début du message lorsqu'ils sont activés (comme les messages de salutation).
- Dispositifs de lecture continue (par exemple, pour la musique d'attente)

Le dispositif d'annonce doit se comporter comme une station, c'est-à-dire s'annoncer lui-même, diffuser l'annonce et basculer l'appel (mettre en attente de consultation, composer un numéro et raccrocher).

Types d'annonces

Les types d'annonces suivants sont disponibles :

- Message d'accueil (annonce avant la réponse)

  Un message d'accueil peut être diffusé aux appelants avant de répondre à leurs appels.
- Répondeur automatique

  Lorsque le standard automatique est activé, de la musique et/ou d'autres annonces peuvent être diffusées aux appelants s'ils ne peuvent pas être transférés immédiatement.
- DTMF DID

  Lorsque la numérotation directe entrante DTMF est activée, un message informe les appelants qu'ils peuvent utiliser le numéro DID pour composer un autre poste. Pendant l'annonce, un récepteur de code détecte si l'appelant utilise la numérotation par suffixe, puis transfère l'appel vers le numéro composé.

Alternatives à l'interface A/B (cartes SLA)

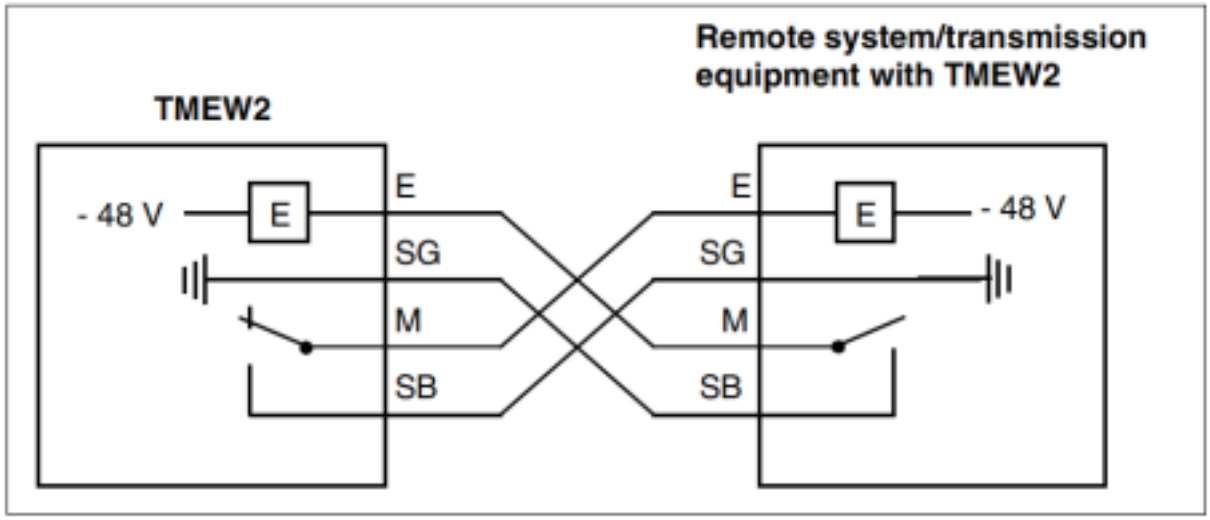
- OpenScape Business X8 : carte TMEW2
- OpenScape Business X5 : Carte STRB optionnelle

Délai d'annonce

Le délai d'annonce est le temps (0 - 600 s, configurable) qui doit s'écouler avant qu'un appel en attente ne soit transféré vers un dispositif d'annonce.

Dispositif d'annonce - Génie

La carte TMEW2 peut être installée sur une interface de type 2 pour connecter le dispositif d'annonce Genius. Vous trouverez une description de la carte TMEW2 et l'affectation des connecteurs SIVAPAC sur le fond de panier lors de la connexion du dispositif d'annonce Genius dans la documentation de service, Installation matérielle, Chapitre « Cartes ».



La configuration du dispositif d'annonce Genius est effectuée dans Manager E via **System View** > **Settings** > **Auxiliary Equipment** > **Announcement**.

21.1.1 Comment ajouter un équipement d'annonce analogique

Conditions préalables

L'équipement d'annonce est raccordé à une interface analogique.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphones/ Abonnés**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Terminaux analogiques**. Le système affiche une liste de tous les abonnés analogiques.
4) Dans la ligne de l'équipement d'annonce, inscrivez les noms et les numéros de téléphone.
5) Si nécessaire, procédez à d'autres réglages dans la ligne de l'équipement d'annonce.
6) Cliquez sur **OK & Suivant** puis sur **Quitter**.

21.1.2 Comment modifier le retard de l'annonce

La configuration est réalisée dans Manager E (voir aussi Aide en ligne de Manager E) :

Étape par étape

Aperçu de l'installation, Menu **Paramètres** > **Paramètres système** > **Temporisations** : dans le tableau, entrée **Délai pour annonce avant réponse**, définir le retard de l'annonce en fonction de ses propres besoins, en agissant sur la **Base** et le **Facteur de multiplication** (par défaut : 100 ms x 20).

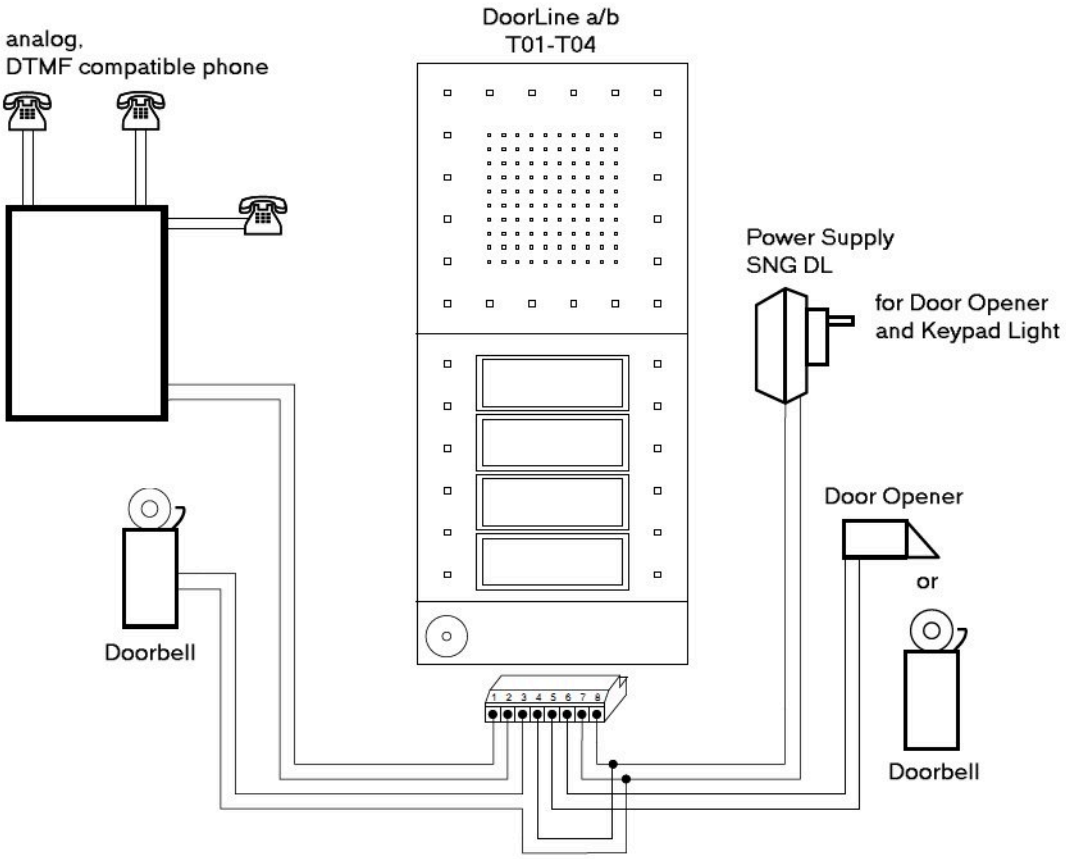
21.2 Poste de portier et Ouverture de porte

Les dispositifs d'ouverture de porte (TFE) sont aujourd'hui proposés dans un très large choix par différents fabricants. Les variantes de raccordement sont déterminantes pour la commande et la fonctionnalité de chaque TFE. Il est décrit en exemple le Doorline a/b T01-T04, mais les systèmes d'ouverture de porte de Behnke, Keil, 2N EntryCom, Auerswald, etc sont ressemblants.

21.2.1 DoorLine a/b T01-T04

Le poste de portier DoorLine a/b T01-T04 est raccordé à une interface analogique. Equipé de 1 à 4 touches de sonnerie (selon la version), il peut atteindre plusieurs zones d'habitation et d'activité indépendantes. Il peut non seulement être commandé à partir de chaque téléphone, mais dispose de plus de la connexion pour la raccordement de l'alimentation électrique de l'ouverture de porte.

Grâce à la technologie 2 fils a/b, le poste DoorLine a/b T01-T04 est rapide et simple à monter. Pour l'harmonisation avec le système de communication, il est possible d'arrêter la numérotation et de régler la communication vocale. L'ouverture de la porte est commandé par l'indicatif Doorline (par ex. #9). Il n'est plus nécessaire de disposer d'un module d'activation spéciale comme Doorline M02, M03, M06 et M06/1.



Remarque : Aucun autre paramétrage dans OpenScape Business n'est nécessaire pour ce poste de portier. Pour des raisons de sécurité, il est recommandé de configuré le poste comme "hors réseau" ou "appels entrants".

21.2.1.1 Comment configurer le port abonné de DoorLine a/b T01-T04

La configuration est réalisée dans Manager E (voir aussi Aide en ligne de Manager E) :

Étape par étape

1) **Vue de l'installation**, Menu **Paramètres** > **Configurer station** > **Abonnés** : pour le port d'abonné, sélectionner le type **Par défaut**.
2) **Vue abonné**, Onglet **Flags** : pour le port abonné, activer le flag **Protégé intrusions**.
3) **Vue de l'installation**, Menu **Paramètres** > **Paramètres système**, Onglet **Flags** : activer le flag **Surnum. DTMF auto.**.

21.2.1.2 Comment configurer le poste pour la Doorline a/b T01-T04

La configuration est réalisée dans Manager E (voir aussi Aide en ligne de Manager E) :

Étape par étape

1) **Vue abonné**, Onglet **Flags**: désactiver le flag **Protégé intrusions** pour le poste.
2) **Vue abonné**, Onglet **Flags**: activer le flag **Editer la liste des appelants** pour le poste.

21.2.2 DoorCom Analog

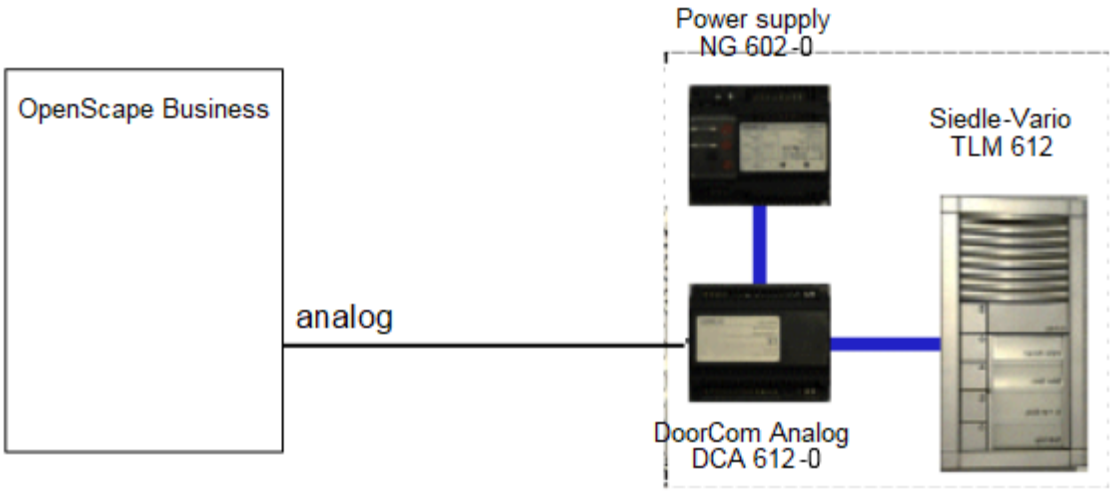
DoorCom® Analog est un boîtier adaptateur TFE universel pour les portiers de la société Siedle (par exemple Vario TLM 612).

DoorCom® Analog est raccordé à une interface analogique du système de communication. Il se comporte comme un téléphone analogique avec numérotation MF, identification MF et commande MF. La commande n'est possible que par des caractères MF.

DoorCom Analog est fonctionnel exclusivement en association avec les composantes suivantes :

- DoorCom Analog DCA 612-0
- portier et interphone Siedle-Vario TLM 612
- interface de commande à distance DCSF 600

  Pour la communication vocale d'un abonné interne au portier et à l'interphone. Sans ce module, aucun rappel du portier n'est possible, par exemple si un appel a été déclenché par mégarde du portier/de l'interphone.
- Bloc-secteur NG 602-0



Il est possible de programmer les fonctions de commande de l'appareil (ouvrir la porte, sélectionner le poste de portier, ...) sur les touches de procédure d'un

téléphone. La séquence de caractères MF ainsi sauvegardé peut ensuite être envoyée au poste de portier/au système d'ouverture de porte.

Remarque : Aucun autre paramétrage dans OpenScape Business n'est nécessaire pour ce poste de portier. Pour des raisons de sécurité, il est recommandé de configuré le poste comme "hors réseau" ou "appels entrants".

21.2.2.1 Comment configurer le port abonné de DoorCom Analog

La configuration est réalisée dans Manager E (voir aussi Aide en ligne de Manager E) :

Étape par étape

1) **Vue de l'installation**, Menu **Paramètres** > **Configurer station** > **Abonnés** : pour le port d'abonné, sélectionner le type **Par défaut**.
2) **Vue abonné**, Onglet **Flags** : pour le port abonné, activer le flag **Protégé intrusions**.
3) **Vue de l'installation**, Menu **Paramètres** > **Paramètres système**, Onglet **Flags** : activer le flag **Surnum. DTMF auto.**.

21.2.2.2 Comment configurer le poste pour DoorCom Analog

La configuration est réalisée dans Manager E (voir aussi Aide en ligne de Manager E) :

Étape par étape

1) **Vue abonné**, Onglet **Flags**: désactiver le flag **Protégé intrusions** pour le poste.
2) **Vue abonné**, Onglet **Flags**: activer le flag **Editer la liste des appelants** pour le poste.

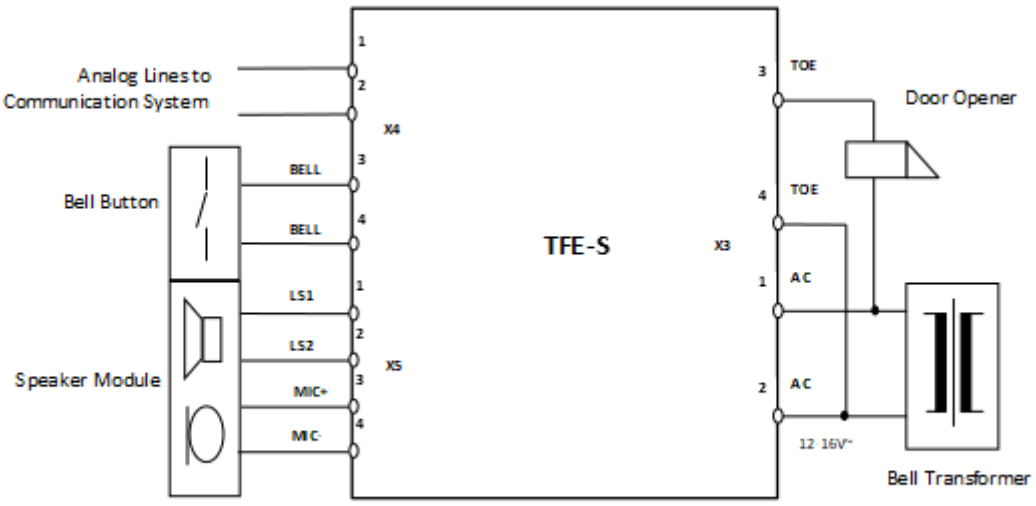
21.2.3 Poste de portier avec amplificateur (TFE-S)

Le module TFE-S (S30122-K7696-T313) relie une interface analogique du système de communication à un poste de portier, un équipement d'ouverture de porte et une touche de sonnerie. La gestion est réalisée via le système de communication.

Cela rend possible la connexion à des postes de portier passifs, comparables aux modèles suivants :

- Sté Siedle (TLM511-01, 611-01)
- Sté Rito (5760)
- Sté Grothe (TS6216)

L'amplification est réglable manuellement. Le module TFE-S a besoin d'une propre alimentation électrique.



Caractéristiques techniques

Paramètres	Valeur
Alimentation électrique	Transformateur de sonnerie 12V - 16V AC, 50Hz
Puissance consommée	150 mA maxi.
Interface OpenScape Business	abonné analogique
Dimensions	100mm x 160mm
Température ambiante	0°C à +45°C

Description de la fonction

L'appui sur la sonnette de porte est signalé à un abonné défini (destination de l'appel de portier), sur son poste en tant qu'appel. Si l'abonné accepte l'appel, il est établie une liaison voix avec le poste de portier. De plus, l'abonné peut activer le dispositif d'ouverture de porte à l'aide de son téléphone.

Si le poste de destination de l'appel de portier n'est pas joignable, il y a renvoi d'appel. Si le poste de renvoi n'est pas libre non plus, une recherche système est effectuée sur tous les téléphones système.

Conseil : Lors de la signalisation d'un appel de portier, le renvoi de nuit n'est pas pris en compte.

Conseil : KWZ n'est pas utilisable sur le poste de portier.

Possibilités de configuration

Les possibilités de configuration suivantes sont disponibles.

- Ouverture de porte :

  L'ouverture de la porte est configurée par une interface a/b. Pour cela, il faut raccorder un adaptateur au poste de portier. L'abonné peut ainsi ouvrir la porte en cours de communication avec le poste de portier, par une simple pression de touche sur le téléphone.
- MF (DTMF) :

  Il est défini ici si l'ouverture de porte est activée avec un émetteur MF (MF : multifréquences), c'est-à-dire si le poste de destination de l'appel de portier peut ouvrir la porte par surnumérotation MF.
- Renvoi d'appel:

  On définit ici si l'appel émanant du poste de portier doit suivre ou non un renvoi d'appel externe du poste de destination.

21.2.3.1 Comment configurer le poste de portier

A l'aide de l'assistant **Poste de portier** vous pouvez déterminer les abonnés autorisés à actionner l'ouverture de la porte. Vous pouvez configurer jusqu'à dix téléphones d'entrée.

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Portier**. La fenêtre **Modifier l'ouverture porte** s'affiche.
4) Sélectionnez un ou plusieurs **portiers**.
5) Indiquez la **destination**.
6) Cochez les cases des fonctions correspondantes comme **Ouverture de porte**, **DTMF** et **Renvoi**.
7) Cliquez sur **OK&Suivant** puis sur **Terminer**.
8) Suivre les étapes 1 à 7 pour configurer chaque téléphone d'entrée.

21.2.4 Haut-parleur

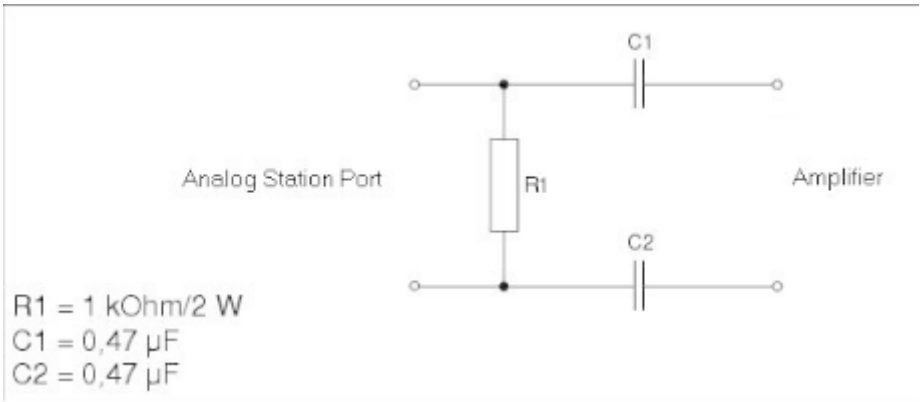
Il est possible de raccorder les haut-parleurs au système de communication via un amplificateur.

On dispose des possibilités suivantes pour le raccordement d'un amplificateur avec haut-parleur :

- **Raccordement de l'amplificateur à une interface abonné analogique**

  Il est éventuellement nécessaire d'effectuer une adaptation du niveau de l'amplificateur.

  Il est éventuellement nécessaire d'utiliser une résistance de boucle après le circuit suivant :



- **Raccordement de l'amplificateur au module TFE S**

  Il est possible de raccorder un amplificateur / système amplificateur via le module TFE S. L'entrée amplificateur est raccordée à la sortie haut-parleur du module TFE S.

  Il est éventuellement nécessaire de disposer d'un contact du module STRB pour activer l'amplificateur ou pour transmettre le signal d'entrée (suppression des bruits parasites).

21.2.4.1 Comment configurer l'interface abonné analogique pour un haut-parleur

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Abonnés**.
3) Dans l'arborescence du menu, cliquez sur **Abonnés** > **Abonnés analogiques**.
4) Sélectionnez l'abonné analogique souhaité (par ex. 3011).
5) Dans l'onglet **Modifier les paramètres d'abonné**, modifiez le données de l'abonné analogique comme nécessaire.

6) Dans la liste déroulante **Type d'abonné**, sélectionnez l'entrée **Haut-parleur**.
7) Cliquez sur **Appliquer**.

21.2.4.2 Comment configurer l'interface d'abonné analogique pour le raccordement d'un amplificateur au module TFE S

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Portier**. La fenêtre **Modifier l'ouverture porte** s'affiche.
4) Sélectionnez un **portier**.
5) Sélectionnez la **destination**.
6) Cliquez sur **OK&Suivant** puis sur **Terminer**.

21.3 Relais

Les actionneurs sont des sorties de commande qui sont activées ou désactivées par des signaux de commande provenant du système de communication. Ils entraînent une modification de l'état des équipements connectés et des fonctions de support pour la surveillance, l'alerte, le contrôle et la régulation. Ils sont principalement utilisés dans les systèmes de sécurité et de gestion des bâtiments (par exemple, pour les ouvre-portes).

Les actionneurs sont contenus dans des modules de relais de commande optionnels. Tous les modules de relais de commande comprennent quatre sorties de commande (actionneurs).

Modules de relais de commande possibles :

- REALS (OpenScape Business X8)
- STRBR (OpenScape Business X5R)

La description détaillée de ces commissions, y compris les affectations, se trouve dans la documentation de service, dans la section intitulée « Commissions ».

Les actionneurs peuvent être commandés de l'une des manières suivantes :

- depuis le téléphone en saisissant des codes
- depuis le téléphone système en appuyant sur une touche
- à distance via une ligne CO (DISA) par la station affectée à la fonction de relais
- à distance via la fonction « Services associés »

Les actionneurs peuvent être activés ou désactivés à l'aide des fonctions suivantes :

Remarque : Les codes de contrôle se trouvent dans la section « Mode expert ».

- **Aucune fonction**

  L'actionneur est soit hors service, soit enregistré comme sonnerie/sonnerie de nuit commune (sous « Paramètres » - « Appels entrants » - « Listes de destinations d'appel »).
- **Marche/arrêt manuelle**

  L'actionneur peut être activé ou désactivé à l'aide d'une clé ou via le code « Activer/désactiver le commutateur sélectionné ». Cette fonction peut être attribuée à une station, à un groupe ou à toutes les stations.
- **Arrêt automatique après délai.**

  L'actionneur fait office de minuterie et peut être activé ou désactivé à l'aide d'une clé ou du code « Activer/désactiver l'interrupteur sélectionné ». Cette fonction peut être attribuée à une station, à un groupe ou à toutes les stations. Si une valeur supérieure à 0 est saisie pour le temps de commutation, l'actionneur est désactivé uniquement lorsque le temps de commutation est écoulé.
- **ouvre-porte**

  L'actionneur fait office d'ouvre-porte et peut être activé ou désactivé à l'aide d'une clé ou du code « Activer/désactiver l'interrupteur sélectionné ». Cette fonction peut être attribuée à une station, à un groupe ou à toutes les stations. Si une valeur supérieure à 0 est saisie pour le temps de commutation, l'actionneur est désactivé uniquement lorsque le temps de commutation est écoulé. Le texte « Ouvre-porte » s'affiche sur l'écran de tous les téléphones associés. Exemple de facteur de multiplication du temps de commutation : 30 × 100 ms = 3 s
- **Amplificateur de haut-parleur**

  L'actionneur est activé lorsqu'une connexion est établie avec le téléphone d'entrée/l'ouvre-porte/le haut-parleur. Elle se désactive dès que la connexion est interrompue. Cela permet de contrôler un amplificateur téléphonique d'entrée afin qu'il ne soit activé qu'en cas de besoin. Un téléphone d'entrée ou le port du haut-parleur doit être affecté à cette fonction.
- **Indication d'occupation**

  L'actionneur est activé lorsque le poste associé quitte l'état inactif (c'est-à-dire, lorsqu'il décroche, active le haut-parleur ou reçoit un appel entrant). L'actionneur est désactivé une fois que la station associée repasse en état d'inactivité. L'actionneur peut également être activé directement via une clé ou via le code « Activer/désactiver l'interrupteur sélectionné ». Dans ce cas, l'état de la station associée est ignoré et l'actionneur ne peut être désactivé que par une clé ou un code. Une station spécifique doit être affectée à cette fonction. Exemple – Voyant d’occupation de la porte : Si le cadre est au téléphone, le voyant d’occupation de la porte s’allume pour indiquer qu’il ou elle ne souhaite pas être dérangé(e).
- **Musique en attente**

  L'actionneur est activé si au moins une station ou une ligne du système de communication n'est pas à l'état inactif. Dans ce cas, un appareil de sonorisation ou un lecteur CD est activé. L'actionneur est désactivé si toutes les stations et lignes du système de communication sont à l'état inactif. Cette fonction ne peut être attribuée qu'à toutes les stations et ne doit être utilisée

qu'une seule fois dans le système de communication. La valeur du temps de commutation doit être supérieure à 0 (par exemple, 600*100 ms = 60 s). L'actionneur reste actif et joue de la musique jusqu'à ce que le temps de commutation soit écoulé ou jusqu'à ce qu'il soit désactivé par un signal de commande.

- **Cloche secondaire**

  L'actionneur est activé pour la station désignée si cette station est appelée. L'actionneur est désactivé lorsque le correspondant répond ou lorsque l'appel est terminé. L'actionneur n'est pas synchronisé. Une station spécifique doit être affectée à cette fonction. Si une valeur supérieure à 0 est saisie pour le temps de commutation, l'arrêt peut être retardé. Le temps de commutation est un multiple de 3 secondes.
- **impulsion de coût d'appel**

  L'actionneur est cadencé en fonction du numéro de la station attribuée, sur la base des impulsions ou des signaux de facturation d'appel entrants. Une station spécifique doit être affectée à cette fonction. Le temps de commutation est de 150 ms pour l'impulsion et de 150 ms pour la pause, et ne peut pas être modifié.
- **Station active**

  L'actionneur est activé lorsque le poste associé est actif (décroché ou activé par haut-parleur). L'actionneur est désactivé une fois que la station associée repasse en état d'inactivité. Une station spécifique doit être affectée à cette fonction.

Noms des actionneurs

Tous les noms (jusqu'à 16 caractères) peuvent être attribués aux actionneurs.

21.3.1 Comment configurer un actionneur

Conditions préalables

Un module de relais de commande est enfiché.

La configuration est réalisée dans Manager E (voir aussi Aide en ligne de Manager E) :

Étape par étape

1) **Vue de l'installation**, Menu **Paramètres** > **Connexions** > **Relais** : dans la **liste des relais** sélectionner le relais à configurer.
2) **Vue de l'installation**, Menu **Paramètres** > **Connexions** > **Relais** : dans le **type de relais** sélectionner la fonction pour le relais.
3) **Vue de l'installation**, Menu **Paramètres** > **Connexions** > **Relais** : dans le champ **Nom du relais** entrez un nom (choix libre) pour le relais (16 caractères maxi.).
4) Si un abonné, un groupe ou tous les postes doivent être affectés à la fonction, il faut sélectionner le numéro de l'abonné ou le numéro d'appel de groupe dans la zone **Abonné affecté**, liste **Numéros d'abonné**.

   Pour tous les abonnés, il faut choisir l'entrée **Aucun**.

5) Si la fonction nécessite un temps de commutation, il faut indiquer le facteur multiplié par la valeur affichée dans la zone **Temps de commutation**, champ **Facteur**.

Les valeurs affichées possibles sont 100 ms et 3 s.

21.4 Capteurs

Les capteurs sont des entrées de commande et détectent un changement d'état de l'appareil connecté. Vous pouvez activer ou désactiver les fonctions du système de communication et ainsi prendre en charge les fonctions de surveillance, d'alerte, de contrôle et de régulation. Ils sont principalement utilisés dans les systèmes de sécurité et de gestion des bâtiments (par exemple, pour le contrôle de la température ou la détection de mouvement).

Les capteurs sont intégrés dans des modules de relais de commande optionnels. Tous les modules de relais de commande comprennent quatre entrées de commande.

Modules de relais de commande possibles :

- REALS (OpenScape Business X8)
- STRBR (OpenScape Business X5R)

La description détaillée de ces commissions, y compris les affectations, se trouve dans la documentation du service, dans la section intitulée « Commissions ».

Les capteurs peuvent activer ou désactiver les fonctions suivantes :

Remarque : Les codes de contrôle se trouvent dans la section « Mode expert ».

- Signalisation des appels sur les téléphones
- Afficher le message sur les téléphones du système
- Activer ou désactiver un dispositif d'annonce
- Contrôle du répondeur
- Numérotation automatique avec un numéro de téléphone prédéfini (numéro de téléphone interne, numéro de groupe ou numéro d'appel externe)
- Activation des services suivants pour un STN (avec code + STN) :
  - Actionneur marche/arrêt
  - Ne pas déranger
  - Renvoi d'appel activé/désactivé
  - Verrouillage par code activé/désactivé
  - Envoyer des SMS
  - Retirer les SMS
  - Service de nuit activé/désactivé
  - Transfert de sonnerie activé/désactivé
- Activation directe des services suivants (uniquement avec le numéro de la station) :
  - Actionneur marche/arrêt
  - Utilisez le système de numérotation abrégée

- Signalisation d'erreur - Les possibilités suivantes s'offrent à vous :
  - Affichage d'un message d'erreur programmable (nom du capteur, 10 caractères maximum : par exemple, Alarme de température) sur l'écran d'un téléphone système spécifique (pas de signalisation sonore).
  - Affichage des appels sur un téléphone système spécifique avec message d'erreur pendant l'appel (numéro de l'appel de destination)
  - Entrée d'erreur dans l'historique des erreurs (entrée dans la mémoire des erreurs = activée)

Numéro d'appel de destination

Un port analogique associé est programmable pour les capteurs. Ce port est appelé par le système une fois qu'un signal de configuration a été reçu. L'appelant remplace alors cette connexion. Un message enregistré peut être activé via un répondeur connecté à ce port, informant ainsi le poste composé de la réponse du capteur. Un port analogique programmé de cette manière ne peut pas être contacté de l'extérieur. Si un numéro d'appel externe a été programmé pour un capteur, mais qu'aucun port analogique ne l'a été, la connexion externe sera établie, mais aucun signal sonore relatif à la réponse du capteur ne sera transmis. Toutefois, si nécessaire, le STN appelé peut identifier l'origine de l'appel sur la base du numéro d'appel (CLIP).

Données de contrôle de la boîte de texte des messages

Saisie de la chaîne de contrôle avec un maximum de 24 caractères pour le système Phonemail (numéro d'appel de la messagerie vocale). Si la connexion est établie, la chaîne de contrôle est transmise au port d'annonce enregistrée. Si aucun port d'annonce enregistrée n'est disponible, la chaîne de contrôle est transmise à la destination.

22 Application Connectivity

Le système prend en charge Application Connectivity, par ex. avec CSTA, TAPI et Application Launcher.

22.1 CSTA

L'interface CSTA permet de connecter à OpenScape Business des applications CTI hautes performances, des centres de contact et des communications unifiées, etc.

CSTA utilise le protocole de contrôle de transmission (TCP). Une connexion permanente est établie. La perte de paquets de données est détectée et corrigée automatiquement.

normes

Le protocole CSTA mis en œuvre est basé sur :

- ECMA 269 Services pour les applications de télécommunications assistées par ordinateur (CSTA) Phase III
- ECMA-285ASN.1 pour les applications de télécommunications assistées par ordinateur (CSTA) Phase III
- extensions spécifiques

Prérequis

L'utilisation de CSTA nécessite OpenScape Business S pour le système connecté aux applications CSTA. Les identifiants de connexion aux applications CSTA doivent être configurés dans le système pour activer automatiquement l'interface CSTA. Les applications CSTA externes doivent utiliser ces identifiants pour accéder au système.

Caractéristiques

CSTA offre les fonctionnalités suivantes :

- Accès via réseau local Ethernet (TCP/IP)
- CSTA Phase III, encodage ASN.1
- Prise en charge du protocole XML CSTA pour les applications certifiées
- Large gamme de téléphones système compatibles
- Surveillance et contrôle à l'échelle du réseau de toutes les ressources
- Multiplexage pour les points de contrôle

Appareils compatibles

En plus des téléphones pris en charge par le système, CSTA prend en charge les appareils suivants :

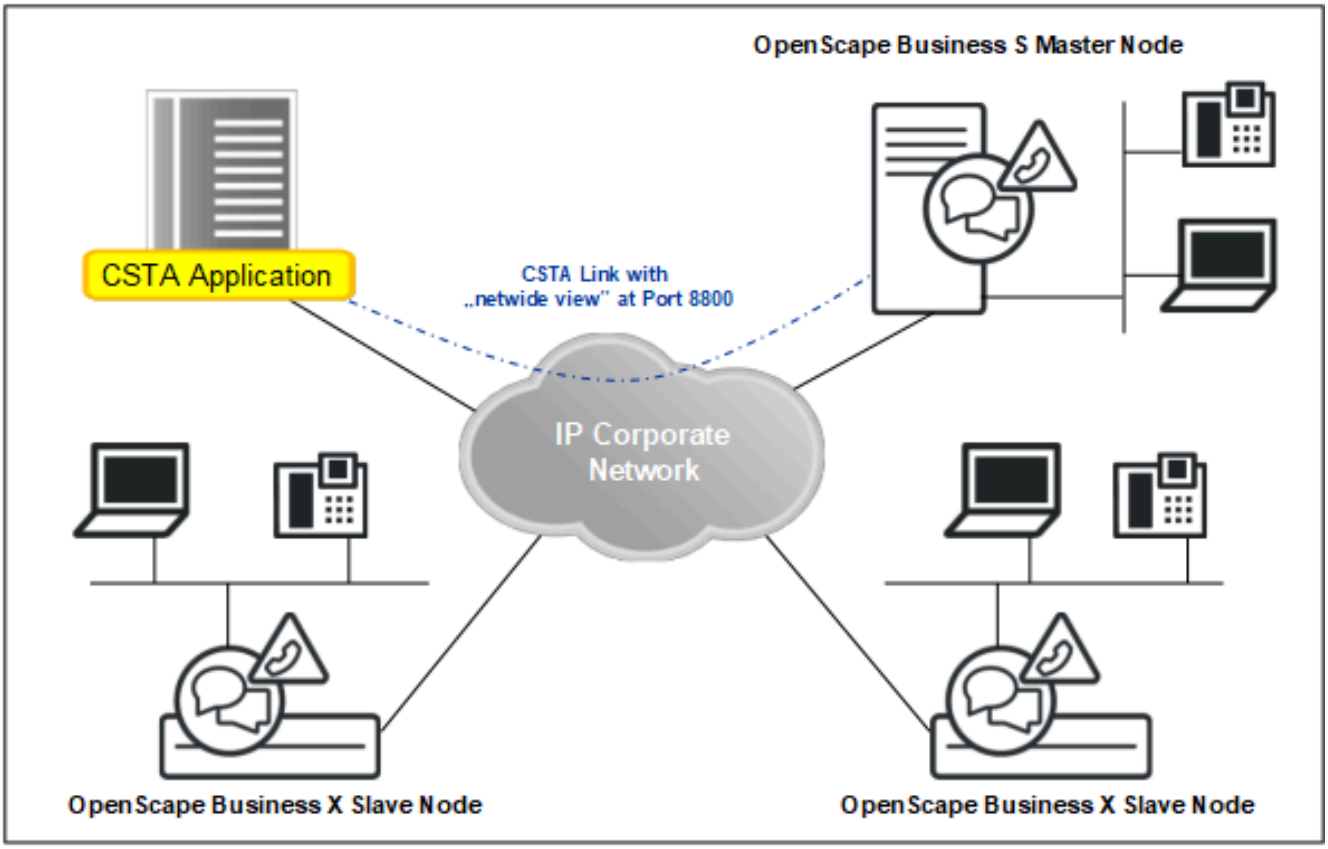
- ITSP

  Cela permet d'utiliser les applications de centre d'appels avec des liaisons SIP.
- ISDN
- Lignes analogiques CO
- Stations virtuelles

- Groupes UCD
- MULAPs

Remarque : Vous trouverez plus de détails sur les fonctionnalités et les équipements surpportés dans le Manuel de l'interface CSTA

Connexion pour une vue à l'échelle du réseau



Ports

Les numéros de port suivants sont disponibles par défaut :

Port	Numéro de port	Usage
CSP	8800	toute demande CSTA
CMD	8900	réservé aux clients TAPI 120 ; quel que soit le nombre de clients, une seule liaison CSTA logique est utilisée.

Les applications CSTA externes et les fournisseurs de services TAPI 120 doivent utiliser l'adresse IP du serveur UC ou du système avec le numéro de port approprié afin d'établir la connexion. L'adresse IP correspondante est affichée dans le WBM sous Sélection de l'application.

Liens CSTA

Par défaut, une liaison CSTA du port CSP est disponible pour les applications CSTA externes. Trois autres liens CSTA sont attribués par défaut aux applications ou services CSTA intégrés suivants :

- CMD (CSTA Message Dispatcher) pour les clients TAPI 120 au port CMD
- DSS (Serveur de station directe)
- Suite UC

Si ces applications ou services CSTA ne sont pas nécessaires, les liens CSTA correspondants peuvent être attribués à des applications CSTA externes si nécessaire.

Remarque : Une liaison CSTA fournit le service TDS uniquement aux appareils locaux. Les clients doivent disposer d'une liaison CSTA vers chaque nœud sur lequel le service TDS est requis.

En général, les applications CSTA peuvent être connectées à un système OpenScape Business via CSP, via LAS (un composant système) ou via PCC (un composant LDH).

Remarque : Si une application est connectée via CSP, il est également nécessaire de configurer les informations d'identification auprès du CSP.

Plus précisément :

- UC Suite, OSCC, TAPI 170 et les applications tierces (externes) sont connectées via un CSP.

  La connexion d'applications CSTA tierces (externes) nécessitant des informations sur les jonctions ne peut être effectuée qu'en mode UC Suite ou en interrogeant les points de surveillance des jonctions eux-mêmes via CSTA, dans leur propre application.
- UC Smart est connecté via LAS

Produits supplémentaires

Les options suivantes sont toujours activées dans le système :

- Toujours transmettre l'indicatif régional avec le numéro de téléphone
- Gestion améliorée des CSTA-CAUSE
- Signalisation CSTA CSP
- Surveillance MULAP

Concepts associés

Téléphones compatibles à la page 79

22.1.1 Comment modifier le numéro de port pour CSTA

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configuration de base** > **Gestion des ports**.
4) Dans la ligne pour **CSP** dansle champ de saisie de la colonne **Numéro de port**, saisissez le numéro de port souhaité.
5) Cliquez sur **Appliquer** puis sur **OK**.
6) Redémarrez le système.

Concepts associés

OpenScape Business TAPI 120 à la page 1102

22.1.2 Comment activer ou désactiver CMD pour l'utilisation de TAPI 120

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Middleware**.
3) Dans l'arborescence du menu, cliquez sur **Middleware** > **CSTA Message Dispatcher (CMD)**.
4) Cliquez sur l'onglet **Paramètres - CSTA Message Dispatcher (CMD)**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer le CMD, cochez dans la zone **Activation** la case **Le service sera lancé automatiquement**.
   - Si vous souhaitez désactiver le CMD, décochez dans la zone **Activation** la case **Le service sera lancé automatiquement**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous voulez utiliser Auto Registration (enregistrement automatique) pour les clients, dans la zone **Enregistrement automatique** cochez la case **Enregistrement automatique client est activé**.
   - Si vous ne voulez pas utiliser Auto Registration (enregistrement automatique) pour les clients, dans la zone **Enregistrement automatique** décochez la case **Enregistrement automatique client est activé**.
7) Cliquez sur **Appliquer**.

Concepts associés

OpenScape Business TAPI 120 à la page 1102

22.1.3 Comment activer ou désactiver le serveur DSS pour l'utilisation des touches DSS sur l'ensemble du réseau

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Middleware**.
3) Dans l'arborescence du menu, cliquez sur **Middleware** > **Serveur DSS**.
4) Cliquez sur l'onglet **Paramètres - Serveur DSS**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer le serveur DSS, cochez dans la zone **Activation** la case **Le service sera lancé automatiquement**.
   - Si vous souhaitez désactiver le serveur DSS, décochez dans la zone **Activation** la case **Le service sera lancé automatiquement**.
6) Cliquez sur **Appliquer**.

22.1.4 Comment activer ou désactiver le CSP

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Middleware**.
3) Dans l'arborescence du menu, cliquez sur **Middleware** > **CSTA Service Provider (CSP)**.
4) Cliquez sur l'onglet **Paramètres - CSTA Service Provider (CSP)**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer le CSP, cochez dans la zone **Activation** la case **Le service sera lancé automatiquement**. Indiquez aussi un ID utilisateur CSTA et un mot de passe utilisateur CSTA pour pouvoir utiliser une application CSTA.
   - Si vous souhaitez désactiver le CSP, décochez dans la zone **Activation** la case **Le service sera lancé automatiquement**.

     Remarque : Si CSP est désactivé, il n'est pas possible d'utiliser TAPI 120 (via CMD), TAPI 170, DSS-Server et UC Suite !
6) Cliquez sur **Appliquer**.

22.1.5 Comment activer ou désactiver Media Extension Bridge

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Middleware**.
3) Dans l'arborescence du menu, cliquez sur **Middleware** > **Media Extension Bridge (MEB)**.
4) Cliquez sur l'onglet **Paramètres - Media Extension Bridge (MEB)**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez utiliser Media Extension Bridge, cochez dans la zone **Activation** la case **Le service sera lancé automatiquement**.
   - Si vous souhaitez libérer ce lien CSTA, décochez dans la zone **Activation** la case **Le service sera lancé automatiquement**.
6) Cliquez sur **Appliquer**.

22.2 OpenScape Business TAPI 120/170

OpenScape Business tapi 120 et OpenScape Business tapi 170 sont deux fournisseurs de services tapi (TSP) optimisés pour l'architecture système et la topologie réseau d'OpenScape Business. Ces TSP fournissent l'interface tapi Microsoft aux applications tapi pour la connexion au système de communication OpenScape Business.

La connexion à OpenScape Business se fait exclusivement via le LAN. Des composants matériels et logiciels supplémentaires tels que le répartiteur de messages CSTA (CMD) ou le fournisseur de services CSTA (CSP) ne sont plus nécessaires pour fonctionner avec Unify OpenScape Business. La gestion des licences est basée sur les terminaux et ne fait pas de distinction entre les terminaux TAPI 120 ou TAPI 170 d'OpenScape Business. L'exigence de gestion des licences commence avec le premier terminal TAPI.

Le choix du Prestataire tapi approprié dépend essentiellement du nombre de PC clients à connecter aux applications tapi ainsi que de l'infrastructure informatique existante et des téléphones utilisés.

- **OpenScape Business Application TAPI**

  est utilisé comme fournisseur de services tapi de première partie préféré dans les réseaux Microsoft avec ou sans contrôleur de domaine lorsque les téléphones analogiques, sans fil et système sans interface USB/IP doivent également être utilisés conjointement avec l'application tapi. Le fournisseur de services tapi 120 est installé sur chaque client PC exécutant une application tapi.

  Les connexions TAPI via Unify OpenScape Business TAPI 120 sont soumises à licence au sein d'Unify OpenScape Business. Pour se connecter à OpenScape Business, en fonction du mode de fonctionnement ou du type de connexion, un lien CSTA ou un lien vers l'interface Web Services est nécessaire, quel que soit le nombre de clients tapi 120 exploités. L'étendue des fonctionnalités côté tapi dépend du mode de fonctionnement et du type de connexion.

- **OpenScape Business Application TAPI**

  est un Prestataire tapi « tiers » classique. Il est installé sur un serveur sur le réseau local et connecté de manière centralisée au système d'entreprise OpenScape Business. Tapi 170 peut être utilisé comme alternative à tapi 120 s'il existe un contrôleur de domaine dans le réseau Microsoft. Lors de l'utilisation de la fonction tapi dite à distance, il n'est pas nécessaire d'installer le fournisseur de services tapi sur les PC clients. Cela offre un gain de temps important dans les installations avec de nombreux PC clients. Veuillez toutefois noter que l'utilisation d'OpenScape Business tapi 170 est obligatoire dans les constellations suivantes :

  – Connexion des terminaux TAPI aux systèmes OpenScape Business en réseau lorsque les terminaux TAPI sont situés dans différents nœuds.
  – Connexion aux applications tapi s'exécutant sur un serveur de terminaux.
  – Connexion aux applications tapi basées sur le serveur.

  Les connexions TAPI via Unify OpenScape Business TAPI 170 sont soumises à licence au sein d'Unify OpenScape Business. Pour se connecter à OpenScape Business, une liaison CSTA est nécessaire, quel que soit le nombre de terminaux TAPI 170 exploités.

22.2.1 OpenScape Business TAPI 120

OpenScape Business TAPI 120 est un fournisseur de services de téléphonie de première partie qui prend en charge la fonctionnalité Microsoft TAPI V2.1. OpenScape Business TAPI 120 permet aux applications CTI sous Windows de surveiller et de contrôler un système téléphonique connecté à OpenScape Business.

OpenScape Business TAPI 120 peut également être connecté à OpenScape Business via l'interface CSTA (mode CSTA) ou l'interface des services Web (mode UC Smart). Il n'est pas possible de réaliser un fonctionnement mixte en utilisant les deux interfaces du système. Les exigences du système, le nombre maximal de stations TAPI et l'étendue des fonctionnalités côté TAPI dépendent des modes de fonctionnement.

OpenScape Business TAPI 120 Connexions

Le logiciel OpenScape Business TAPI 120 est installé sur un PC client Microsoft Windows. La connexion au système OpenScape Business System s'effectue via le réseau local (LAN). Aucune connexion physique entre l'ordinateur Windows et le téléphone n'est requise.

- **Mode TAPI 120 CSTA**

  Tous les PC clients TAPI 120 sont connectés à la même liaison CSTA d'OpenScape Business. OpenScape Business multiplexe en interne toutes les connexions TAPI 120.

  TAPI 120 en mode CSTA prend en charge OpenScape Business X5/X8 et OpenScape Business S.

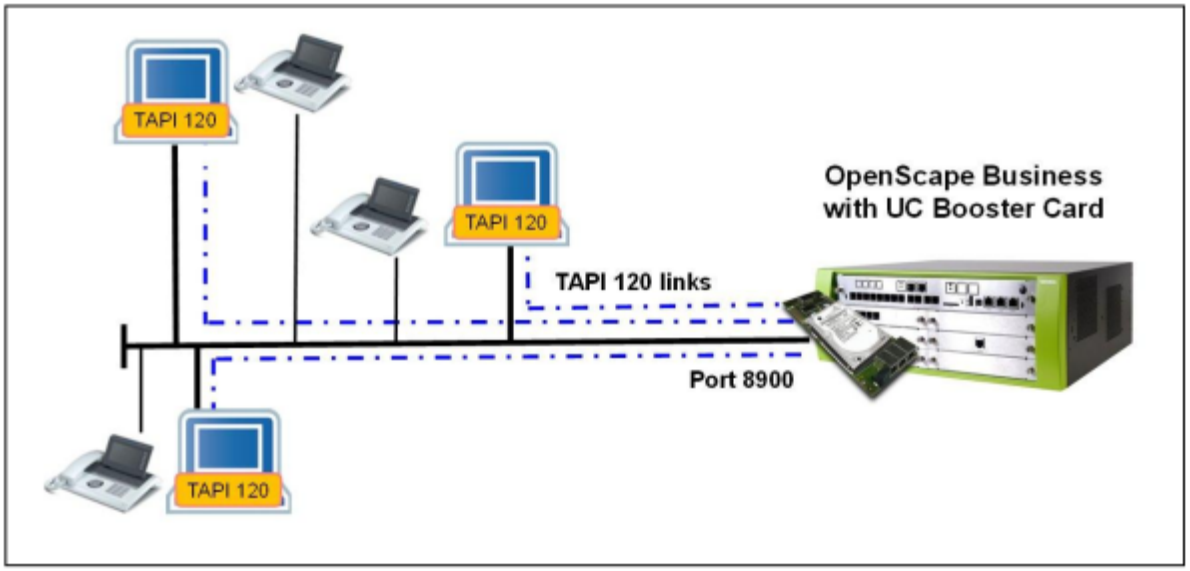


Illustration 10 : TAPI 120 en mode CSTA avec OpenScape Business X5R et carte UC Booster

- **Mode intelligent TAPI 120 UC**

  Tous les PC clients TAPI 120 sont connectés à la carte mère d'OpenScape Business via l'interface LAN et serveur Web. OpenScape Business multiplexe en interne toutes les connexions TAPI 120.

  TAPI 120 en mode CSTA prend en charge OpenScape Business X1/X5/X8.

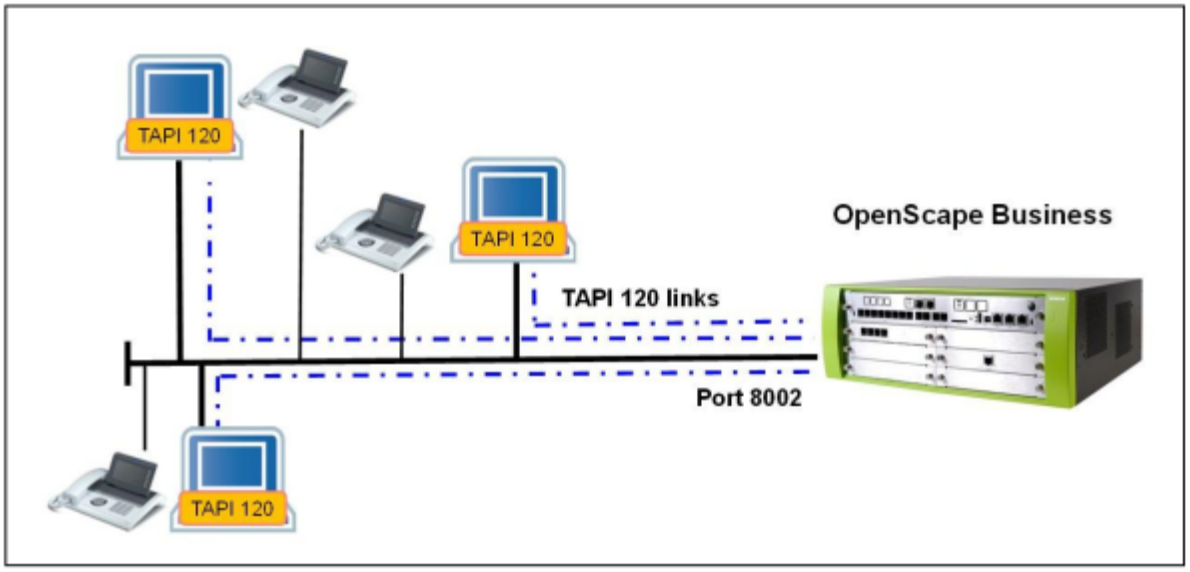


Illustration 11 : TAPI 120 en mode UC Smart avec OpenScape Business X5R

Caractéristiques

Les fonctionnalités suivantes sont prises en charge :

Fonctionnalité	TAPI 120 CSTA	TAPI 120 UC Smart
Fournisseur de services TAPI central de première partie connecté via un réseau local	X	X
Compatible avec la norme Microsoft TAPI 2.1	X	X
Connexion au système OpenScape Business autonome	X	X
Prise en charge du pare-feu OpenScape Business CTI	X	-
Fonctionnalités prises en charge via TAPI		
Signalisation des appels entrants et sortants avec identification des numéros d'appel et de l'origine de l'appel	X	X
Informations supplémentaires dans la signalisation des appels redirigés	X	X
Répondre aux appels internes et externes	X	X
Établissement d'une connexion contrôlée avec les parties appelées internes et externes	X	X
Numérotation manuelle / Numérotation par suffixe DTMF	X	X
Libérer les appels existants	X	X
Organiser une réunion de consultation avec les parties internes et externes	X	X
Alternative (basculer/connecter)	X	X
Transfert d'appel filtré	X	X
Transfert d'appel filtré avec numérotation ultérieure du lieu de consultation (transfert en une étape)	X	X
Transfert d'appel non filtré (transfert aveugle)	X	-
Configurer et supprimer le transfert d'appel	X	X
Activer et désactiver le mode Ne pas déranger	X	X
Lancer une conférence	X	-
Conférence élargie	X	-
Transférer l'appel entrant	X	-
Prise en charge dirigée (prise en charge d'appel)	X	-
Signalisation et prise en charge en groupe	X	-
Les appels en cours de stationnement	X	-
Reprendre les appels en attente	X	-
Mettre manuellement les appels en cours en attente	X	-

Fonctionnalité	TAPI 120 CSTA	TAPI 120 UC Smart
Reprendre manuellement les appels mis en attente	X	-
Définir le rappel	X	-
Prise en charge des fonctions pilotées par le code	X	-
Échange de données relatives aux appels entre applications TAPI	X	-
Contrôle des touches sur les téléphones du système (HFA)	X	-
Contrôle du gain du microphone sur les téléphones du système (HFA)	X	-
Contrôle/sélection de l'utilisation du combiné/haut-parleur/casque pour les téléphones du système (HFA)	X	-
Réglage du volume du combiné/haut-parleur/casque/clavier sur les téléphones du système (HFA)	X	-
Accès aux écrans et LED optiPoint/OpenStage (avec une limite de 50 écrans actifs par système)	X	-

Valeurs maximales

Le nombre maximal de PC clients TAPI 120 pouvant être connectés à OpenScape Business dépend du modèle (voir Niveaux d'extension disponibles via les ventes).

Systèmes d'exploitation publiés

Les systèmes d'exploitation actuellement disponibles pour Microsoft Windows Server, Terminal Server et PC client distant sont répertoriés dans les dernières informations commerciales.

Seuls les systèmes d'exploitation Microsoft Windows peuvent être utilisés conjointement avec TAPI 120.

Pour les installations sur serveurs de terminaux, OpenScape Business TAPI 170 doit être utilisé à la place d'OpenScape Business TAPI 120.

Licence

L'utilisation d'OpenScape Business TAPI 120 est soumise à une licence d'abonnement. Les licences TAPI sont gérées au sein du système OpenScape Business et peuvent être utilisées pour les deux modes de TAPI 120. Lors de l'utilisation de la fonctionnalité MULAP, une licence TAPI est requise pour chaque station au sein du MULAP.

Remarque : Aucune licence utilisateur UC n'est requise pour TAPI 120 en mode UC Smart.

Provisionnement de logiciels

Le logiciel OpenScape Business TAPI 120 est fourni sur un support de données séparé. Il ne fait pas partie du logiciel système OpenScape Business.

Configuration matérielle requise

Le PC doit au moins respecter les exigences système spécifiées par Microsoft pour le système d'exploitation utilisé ainsi que les exigences de l'application TAPI. De plus, une interface LAN Ethernet est requise.

- Pour TAPI 120 CSTA

  Un lien CSTA d'OpenScape Business est requis, quel que soit le nombre de clients TAPI 120 connectés. Un module OpenScape UC Business Booster (carte ou serveur) est obligatoire à cet effet.
- Pour TAPI 120 UC Smart

  L'interface des services Web est requise. Aucun module OpenScape UC Business Booster (carte ou serveur) ne doit être présent dans/au niveau du système.

Appareils compatibles

Les périphériques pris en charge ainsi que les fonctionnalités prises en charge sur ces périphériques dépendent de la fonctionnalité CSTA ou WSI du système OpenScape Business utilisé. Ces informations sont contenues dans les informations commerciales d'OpenScape Business.

Port IP par défaut / Adresse IP occupée par TAPI 120

En mode de fonctionnement TAPI 120 CSTA, la liaison CSTA vers OpenScape Business occupe le port IP 8900.

En mode de fonctionnement TAPI 120 UC Smart, la liaison WSI vers OpenScape Business occupe le port IP 8802 pour une connexion chiffrée (HTTPS) ou 8801 pour une connexion non chiffrée (HTTP).

Dans la configuration TAPI 120, l'adresse IP du système OpenScape Business doit être saisie conformément au mode de fonctionnement. Cette adresse IP est affichée dans le WBM sous **Sélection de l'application** .

Tâches associées

Comment modifier le numéro de port pour CSTA à la page 1098

Comment activer ou désactiver CMD pour l'utilisation de TAPI 120 à la page 1099

22.2.2 OpenScape Business TAPI 170

OpenScape Business TAPI 170 est un 3rd Party Telephony Service Provider qui supporte l'étendue des fonctions Microsoft TAPI V2.1. TAPI 170 permet aux applications CTI basées sur Microsoft Windows de surveiller et commander plusieurs téléphones raccordés à OpenScape Business.

Fonctionnalités

OpenScape Business TAPI 170 offre les fonctionnalités suivantes :

- 3rd Party TAPI Service Provider raccordé centralement
- Compatible avec standard Microsoft TAPI 2.1
- Les fonctions téléphonie sont disponibles sur chaque PC client raccordé via l'architecture TAPI 2.1 Client/Serveur
- logiciel TSP Client supplémentaire non nécessaire

- Fonctions téléphonie supportées :
  - Sélection entrante/sortante à partir du PC
  - Transmission des numéros de téléphone entrants, si signalisation
  - Double appel et transfert
  - Va-et-vient
  - Conférence
  - Renvoi d'appel
  - Rediriger l'appelant
  - Acceptation d'un appel par l'application
  - Libération d'un appel par l'application
  - Transfert avant/après réponse
  - Transmission de codes de fonctionnalité
  - Surveillance du téléphone (états d'appel, défaillance, etc.)
  - Fourniture d'une interface ACD
  - Surveillance/Accès clavier pour téléphones système (HFA)
  - Commande d'écran/LED sur les téléphones système (HFA)
  - Connexion à des systèmes OpenScape Business individuels ainsi qu'à des systèmes en réseau
  - Supporte des abonnés/numéros MULAP

Connexions OpenScape Business TAPI 170

Le logiciel OpenScape Business TAPI 170 est installé sur un Microsoft Windows Server dans le réseau. La connexion avec OpenScape Business est réalisée via un lien CSTA. Une liaison physique entre le PC Windows et le téléphone n'est pas nécessaire. OpenScape Business TAPI 170 peut, dans différents modes d'exploitation, être configuré sur des systèmes individuels ou sur un réseau OpenScape Business. Le serveur TAPI et les clients doivent être gérés par le même Domain Controller de réseau.

- **Connexion à OpenScape Business d'applications TAPI basées sur serveur, via TAPI 170**

  L'application Server et le logiciel TAPI 170 sont installés dans le "serveur téléphonie" du réseau. L'application Server met à disposition de ses clients correspondants, dans le réseau, les fonctions téléphonie pour les abonnés qui sont configurés à l'intérieur de OpenScape Business TAPI 170. Le logiciel TAPI 170 est relié via LAN à l'interface CSTA de OpenScape Business. Pour cette connexion, il est nécessaire d'avoir un lien CSTA de

OpenScape Business ainsi qu'une licence TAPI pour chaque abonné TAPI configuré.

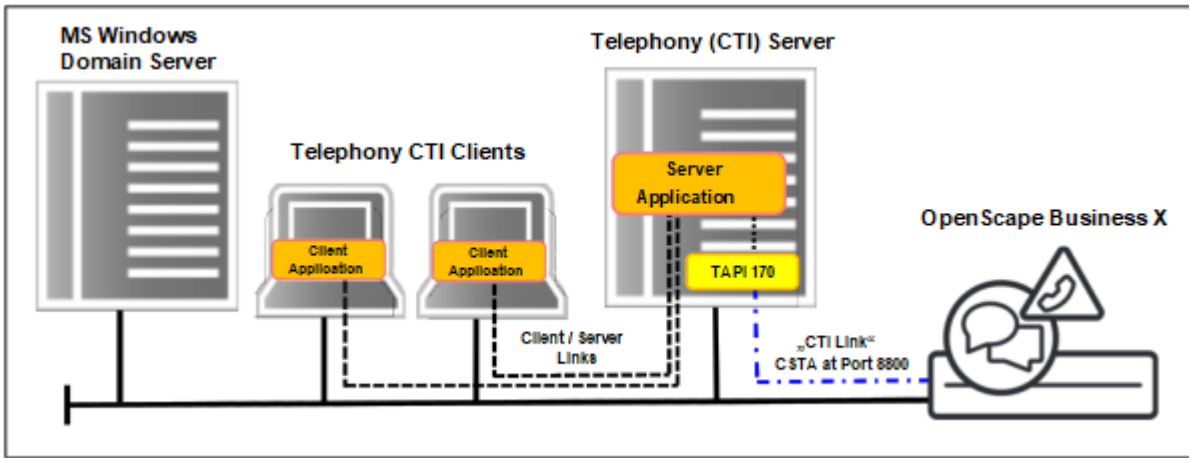


Illustration 12 : Application TAPI basée Server via TAPI 170 pour OpenScape Business

- **Connexion à OpenScape Business d'applications TAPI basées client, via TAPI 170 avec fonction "Remote TAPI"**

  Dans ce scénario, le logiciel OpenScape Business TAPI 170 est installé sur un serveur dans le réseau. Sur les PC Client avec applications TAPI, il est validé la fonction dite "Remote TAPI" à l'aide de laquelle l'application TAPI sur le client communique avec le logiciel TAPI 170 du serveur. Sur le client, il n'est pas nécessaire pour cela d'installer un logiciel TAPI 170. Le logiciel TAPI 170 est connecté via LAN à l'interface CSTA de OpenScape Business. Pour cette connexion, il est nécessaire d'avoir un lien CSTA de OpenScape Business ainsi qu'une licence TAPI pour chaque abonné TAPI configuré.

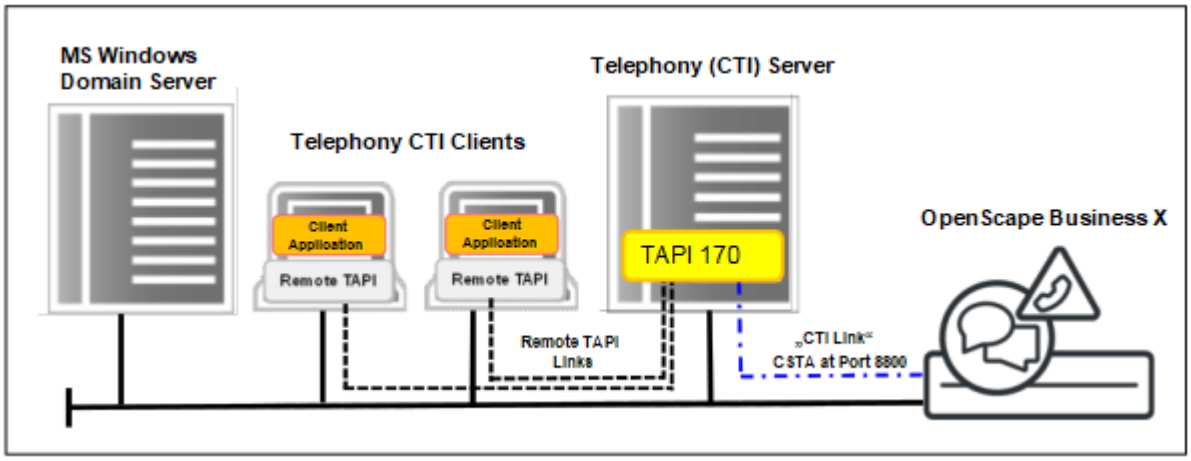


Illustration 13 : Application TAPI basée Client via "Remote TAPI" pour OpenScape Business

- **Connexion à OpenScape Business d'applications TAPI basées sur Terminal Server, via TAPI 170**

  Dans ce scénario, les applications TAPI basées client sont installées dans un ou plusieurs Terminal Servers. Dans ce cas, le logiciel TAPI 170 est également installé sur le Terminal-Server. Dans le cas d'un cluster comprenant plusieurs terminaux, il faut installer le logiciel TAPI 170 sur chaque Terminal-Server du cluster. Chaque logiciel TAPI 170 installé est

connecté via LAN à OpenScape Business. Pour chaque logiciel TAPI 170 installé sur un Terminal-Server, il est nécessaire d'avoir un lien CSTA de OpenScape Business. De plus, une licence TAPI est nécessaire pour chaque abonné TAPI configuré.

Le nombre maximum possible de serveurs OpenScape Business TAPI 170 en liaison avec OpenScape Business ne doit pas être dépassé.

Remarque : Dans le cluster, il est possible de gérer autant de Terminal-Servers qu'il y a de liens CSTA libres disponibles dans OpenScape Business pour la connexion du logiciel TAPI 170. La valeur maximale des connexions possibles est diminuée lorsque les liens CSTA de OpenScape Business sont occupés par d'autres applications CSTA.

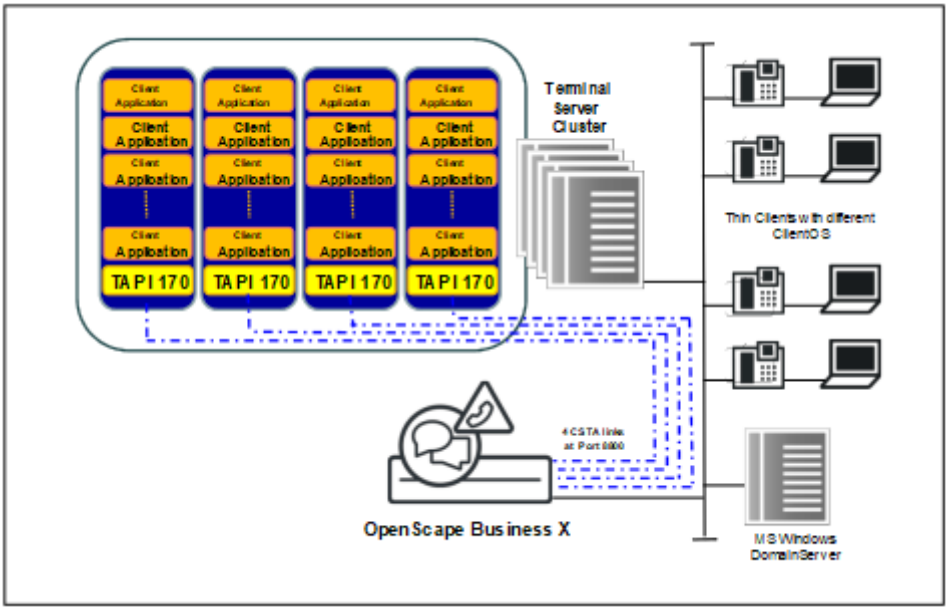


Illustration 14 : Application TAPI basée Client sur Terminal-Server pour OpenScape Business

- **Connexion de TAPI 170 aux systèmes OpenScape Business en réseau**

  Dans les systèmes OpenScape Business en réseau, le logiciel TAPI 170 est installé sur un serveur qui est raccordé via LAN à l'interface CSTA du noeud maître. Cette connexion dépend des modes d'exploitation mentionnés précédemment du TAPI 170 Service Provider (Remote TAPI ou connexion basée sur le serveur). Pour la réalisation, il est nécessaire d'avoir un lien CSTA de comptes maître OpenScape Business ainsi qu'une licence TAPI pour chaque abonné TAPI du réseau.

  Remarque : Via le noeud maître, TAPI 170 dispose d'un accès pour l'ensemble du réseau à tous les abonnés de ce réseau. Lors du raccordement de TAPI 170 à un noeud esclave au lieu d'un noeud maître, TAPI 170 accède uniquement aux abonnés du noeud esclave. Lors de l'utilisation de plusieurs TAPI 170 dans un cluster Terminal

Server, il faut pour chaque TAPI 170 un lien CSTA avec le noeud maître.

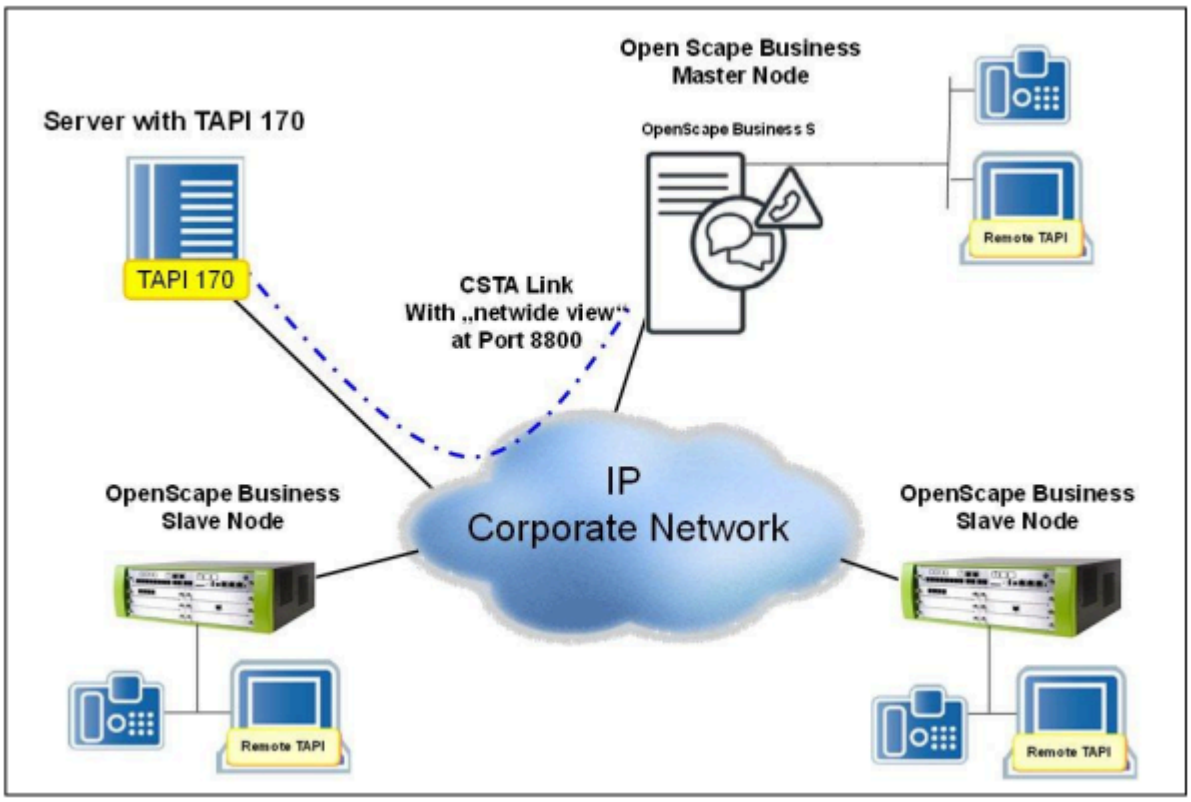


Illustration 15 : Connexion de TAPI 170 aux systèmes OpenScape Business en réseau

Limites de configuration

Le nombre maximum des PC Client TAPI 170 pouvant être raccordé à OpenScape Business dépend du modèle. Informations supplémentaires à ce sujet, voir Chapitre 1.3.9.4

Systèmes d'exploitation homologués

Les systèmes d'exploitation actuellement homologués pour le Microsoft Windows Server, le Terminal-Server et le Remote Client PC figurent dans les informations actuelles sur la distribution.

Seuls les systèmes d'exploitation Microsoft Windows sont utilisables en liaison avec TAPI 170.

Le modèle de licence de Microsoft nécessite, en plus de la licence pour le système d'exploitation du serveur, des Microsoft Devices ou User CAL correspondants, dans la quantité nécessaire pour réaliser l'extension prévue. Ces CAL ne font pas partie de la livraison de OpenScape Business TAPI 170 et doivent être acquis séparément. Dans certaines conditions, indiquées préalablement par Microsoft, il est possible d'utiliser pour OpenScape Business TAPI 170 un "Windows Server for embedded systems" avec la "Embedded Telco Licence".

Procédure de licence

L'utilisation de OpenScape Business TAPI 170 fait l'objet de licence sur la base de l'abonné. Les licences sont gérées à l'intérieur du système OpenScape Business. En cas d'utilisation de la fonctionnalité MULAP, il faut une licence TAPI pour chaque abonné du groupe MULAP.

Fourniture du logiciel

Le logiciel OpenScape Business TAPI 170 est fourni sur son propre support de données. Il ne fait pas partie du logiciel OpenScape Business System.

Exigences matérielles

Pour la connexion de OpenScape Business TAPI 170, il est nécessaire d'avoir un lien CSTA de OpenScape Office, indépendamment des clients TAPI 170 raccordés. C'est également vrai pour les systèmes OpenScape Business en réseau.

Le PC doit répondre au moins aux exigences système définies par Microsoft pour le système d'exploitation utilisé, à condition qu'aucune autre application logicielle que TAPI 170 ne soit exploitée. En plus, il faut une interface LAN Ethernet.

Terminaux supportés

Les terminaux supportés ainsi que les fonctionnalités supportées pour ces terminaux dépendent de l'étendue des fonctions CSTA ou WSI du système OpenScape Business utilisé. Ces informations figurent dans les informations de distribution de OpenScape Business.

22.3 Interface des services Web

L'interface de services Web intégrée permet la surveillance et le contrôle des ressources téléphoniques dans un système comportant des utilisateurs de communications unifiées.

Caractéristiques

L'interface des services Web offre les fonctionnalités suivantes :

- Accès via réseau local Ethernet (TCP/IP)
- Prise en charge des protocoles HTTP et HTTPS
- Assistance pour les systèmes individuels
- Des fonctions orientées utilisateur et clairement structurées pour :
  - Contrôle des appels
  - Contrôle de l'appareil
  - Dispositifs de surveillance
  - Annuaires
  - Journaux des utilisateurs
  - Statut de présence des utilisateurs

Remarque : Selon le type de client WSI (Web Services Interface), l'indicateur de station Services associés doit être

activé afin de permettre l'exécution de certaines commandes WSI.

Serveur Web Sessions Web

Le nombre de sessions de serveur Web disponibles est commun à toutes les applications concernées (par exemple, Application Launcher, optiClient Attendant (Server) et optiClient BLF).

Points de contrôle internes

Les points de contrôle internes sont indépendants des points de contrôle de l'interface CSTA. Si plusieurs applications surveillent le même utilisateur UC via l'interface des services Web, un seul point de surveillance interne est utilisé par le serveur Web à cette fin.

Ports

Les numéros de port suivants sont disponibles :

Port	Protocole
8801	HTTP (non chiffré)
8802	HTTPS (chiffré)

22.4 Open Directory Service

L'Open Directory Service (ODS) est un service d'annuaire ouvert, intégré et basé sur LDAP. Il agit comme un service de méta-annuaire, regroupant les résultats provenant de différentes sources d'annuaires internes et externes via une interface unique. L'Open Directory Service est accessible à différents types de clients, d'applications et d'appareils de communication au sein d'une entreprise.

L'Open Directory Service remplit deux fonctions :

1) Il permet d'accéder à des données de contact supplémentaires provenant de sources externes via un accès SQL ou ODBC aux bases de données du réseau client qui contiennent des données d'annuaire
2) Il expose les annuaires internes et externes aux clients, aux périphériques de communication et aux applications.

L'Open Directory Service est désactivé par défaut. Lorsque vous l'activez, veillez également à ce que les pare-feu soient ouverts pour le protocole LDAP sur le port TCP/389.

Open Directory Service sur différentes variantes d'OpenScape Business

Open Directory Service est proposé avec différentes fonctionnalités en fonction de la plate-forme OpenScape Business :

- OpenScape Business S, cartes mères OpenScape Business X V3 Advanced, Booster Server ou carte Booster :

  Toutes les fonctionnalités sont proposées, de sorte que les sources de données internes et externes peuvent être utilisées
- Cartes mères OpenScape Business X V3 Basic :

  La fonctionnalité est limitée aux sources de données internes par défaut.

- Cartes mères OpenScape Business X V2 :

  Une carte Booster ou un Booster Server est nécessaire pour utiliser l'Open Directory Service.

Pour vous connecter à l'Open Directory Service via le protocole LDAP, veuillez utiliser l'adresse IP indiquée dans le portail d'administration :

- À droite de la page d'accueil d'OpenScape Business Assistant, sous **Applications**.
- Sur la page **Sélection d'application** de l'assistant d'**installation initiale**, sous **Configuration** > **de l'installation de base**.

Sources de données internes

Les sources de données internes suivantes sont disponibles par défaut dans l'Open Directory Service :

- Annuaire externe
- Répertoire interne
- Numéros d'appel abrégé centraux

Pour ces sources de données internes, les noms de champs sont mappés de manière permanente au schéma de données d'Open Directory Service.

Ces sources de données internes ne peuvent être ni supprimées ni modifiées. Pour exposer les sources de données internes via ODS, une licence « OpenScape Business OpenDirectory Base » est nécessaire.

Sources de données externes

En tant qu'administrateur, vous pouvez intégrer les informations de contact provenant des types de bases de données suivants en tant que sources de données pour un accès en lecture seule via SQL ou ODBC.

- Sources de données avec pilotes intégrés (Microsoft SQL Server, PostgreSQL, Sybase SQL).
- Les sources de données sans pilotes intégrés nécessitent l'installation et la configuration d'un serveur ODBC Bridge sur le client ODS (téléchargeable via le WBM sous **Service Center** > **Software**).

Remarque : Pour une connectivité réussie, il est nécessaire de définir une valeur (la valeur peut être différente du nom de la source de données, mais le champ ne peut pas être vide) dans le champ **Description**. Dans le cas d'une source de données ODBC Bridge pour Access, Firebird, Excel et Oracle, veuillez ajouter le nom de la source de données, respectivement « access », « firebird », « excel » et « oracle », comme valeur du champ **Description**.

Remarque : Pour l'intégration de la base de données ODS à Microsoft Excel, seul le format de fichier *.xs*l (et non *.x*l*sx*) est pris en charge. Dans les versions récentes de MS Office, évitez de modifier/enregistrer les fichiers Excel afin de ne pas altérer leur encodage. De plus, un pilote ODBC Bridge spécifique pour Microsoft Excel est nécessaire.

Pour accéder à des sources de données externes à partir d'ODS, une licence « OpenScape Business OpenDirectory Connector » est requise pour chaque source de données connectée.

Nombre maximal de types de bases de données différents : 3

Nombre maximal de sources de données externes : 4

Assurez-vous que l'Open Directory Service est autorisé à accéder à la source de données externe. Contactez à l'avance l'administrateur de base de données responsable pour vous en assurer. Il peut être nécessaire d'ajouter un utilisateur distinct dans la source de données externe pour permettre l'accès au système.

Les sources de données externes peuvent être utilisées dans le cadre de recherches dans l'annuaire et de la résolution des numéros d'appel en noms.

Vous pouvez configurer l'accès direct à une table de base de données à partir d'une source de données externe ou d'une requête SQL personnalisée pour la source de données.

Toute colonne servant d'identifiant doit contenir des valeurs uniques et non nulles/non vides. Utilisez la propriété UNIQUE ou PRIMARY KEY pour vous assurer que c'est le cas.

Dans les cas où des bases de données externes sont intégrées, les restrictions suivantes s'appliquent :

- Les caractères spéciaux ´ [] ' " ne sont pas pris en charge par l'ODS dans les noms de tables et de colonnes.
- Les types de colonnes « nchar » et « nvarchar » ne sont pas pris en charge par l'ODS.
- Les espaces intermédiaires (au moins dans les 4-5 derniers chiffres) ne sont pas pris en charge par l'ODS pour les données téléphoniques.

Requêtes SQL personnalisées pour les sources de données externes

Les requêtes SQL personnalisées prennent également en charge les tables associées, par exemple :

```
SELECT * FROM users LEFT OUTER JOIN phonenumbers ON
users.id = phonenumbers.uid;
```

La structure des données doit être de type 1:1 ou n:1, c'est-à-dire que chaque enregistrement ne peut avoir qu'une seule ligne.

L'accès via des requêtes SQL personnalisées peut parfois être beaucoup plus lent que l'accès direct à un tableau de base de données.

Les requêtes SQL personnalisées présentant des risques potentiels pour la sécurité ne sont pas exécutées, par exemple :

- Modification des données
- Arrêt du serveur SQL
- Exécution de programmes via le serveur SQL
- Modification des droits d'utilisateur

Les requêtes SQL personnalisées contenant les commandes SQL suivantes ne sont donc pas exécutées :

- `POINT DE CONTRÔLE`
- `FERMER`
- `GROUPER`

- ENGAGER
- COPIER
- CRÉER
- DÉATTRIBUER
- DÉCLARER
- SUPPRIMER
- REJETER
- FAIRE
- ABANDONNER
- END
- EXÉCUTER
- EXPLIQUER
- RÉCUPÉRER
- ACCORDER
- INSÉRER
- CHARGER
- VERROUILLER
- DÉPLACER
- PRÉPARER
- RÉATTRIBUER PROPRIÉTÉ
- REINDEXER
- LIBÉRER POINT DE SAUVEGARDE
- RÉINITIALISER
- RÉVOQUER
- POINT DE SAUVEGARDE
- ÉTIQUETTE DE SÉCURITÉ
- SÉLECTIONNER DANS
- DÉFINIR
- AFFICHER
- DÉMARRER TRANSACTION
- TRONQUER
- DÉSACTIVER ÉCOUTE
- METTRE À JOUR
- DÉPRESSION
- VALEURS

Mappage des champs pour les sources de données

Pour ces sources de données, vous pouvez personnaliser le mappage des noms de champs au schéma de données d'Open Directory Service. Vous pouvez attribuer chaque champ du schéma de données d'Open Directory Service à un seul champ de la source de données externe. Cependant, vous pouvez attribuer un champ de la source de données externe à plusieurs champs du schéma de données d'Open Directory Service.

Mappages de sortie de données LDAP

Un mappage de sortie de données LDAP détermine quels champs du schéma de données d'Open Directory Service doivent être exportés via LDAP, par exemple pour des clients LDAP spécifiques ou pour différents groupes d'abonnés qui ne souhaitent pas voir tous les détails, mais seulement un sous-ensemble défini.

Le mappage de sortie de données LDAP **web** est disponible par défaut et ne peut être ni supprimé ni modifié. Tous les champs du schéma de données dans l'Open Directory Service sont attribués de manière permanente à la sortie LDAP qui s'y trouve. Vous pouvez également configurer d'autres mappages de sortie de données LDAP.

Les clients LDAP peuvent accéder à un mappage de sortie de données LDAP spécifique via le paramètre dc dans la connexion LDAP, par exemple : `dc=web`.

Normalisation des numéros de téléphone au format canonique

Pour chaque source de données, vous pouvez configurer la normalisation des numéros de téléphone au format canonique. Au cours de ce processus, les espaces, les parenthèses, les tirets et les virgules sont supprimés. Ceci est nécessaire pour identifier correctement le nom de l'appelant et pour la numérotation depuis le Desktop. Vous ne devez pas ignorer la normalisation, sauf si les numéros de téléphone utilisés dans la source de données sont déjà au format canonique. Vous pouvez faire en sorte que les valeurs liées à la normalisation, telles que l'indicatif régional, etc., soient saisies automatiquement par le système. Si la source de données externe se trouve sur un site différent de celui du système, vous devrez peut-être ajuster ces valeurs.

Statut des sources de données

L'affichage du statut sous **OpenDirectory** > **Sources de données** a la signification suivante :

Couleur	Statut
vert	actif(ve)
rouge	ODBC et LDAP ne fonctionnent pas correctement, configuration incorrecte ou source de données indisponible
jaune	LDAP ne fonctionne pas correctement : redémarrez l'Open Directory Service
gris	Configuration incomplète

Fourniture d'annuaires

Les types de clients, de périphériques de communication et d'applications suivants peuvent utiliser les annuaires fournis par l'Open Directory Service :

- Clients UC
- Application Launcher
- Répertoire système
- OpenStage avec prise en charge LDAP locale
- Téléphones IP DECT (via LDAP)
- Téléphones SIP (via LDAP)
- Applications, par exemple suites CRM telles que Microsoft Dynamics CRM (via LDAP, ODBC ou export CSV OpenLDAP)

L'Open Directory Service peut identifier dans les résultats de recherche la source de données à partir de laquelle une correspondance a été obtenue.

Concepts associés

Conditions nécessaires pour Application Launcher à la page 1127

22.4.1 Comment activer ou désactiver Open Directory Service

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **Open Directory Service**.
3) Dans l'arborescence du menu, cliquez sur **Open Directory** > **Configuration de base**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer Open Directory Service, cochez la case **Activé**.
   - Si vous souhaitez désactiver Open Directory Service, décochez la case **Activé**.
5) Cliquez sur **Sauvegarder**.
6) Cliquez sur **OK**.
7) Cliquez sur **OK**.

22.4.2 Comment démarrer de nouveau Open Directory Service

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Open Directory Service est activé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **Open Directory Service**.
3) Dans l'arborescence du menu, cliquez sur **Open Directory** > **Maintenance**.
4) Cliquez sur **Nouveau démarrage**.
5) Cliquez sur **OK**.

22.4.3 Comment configurer le mot de passe pour l'accès à Open Directory Service

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Effectuez les opérations suivantes pour définir le mot de passe permettant aux clients, appareils de communication et applications d'accéder à Open Directory Service.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **Open Directory Service**.
3) Dans l'arborescence du menu, cliquez sur **Open Directory** > **Configuration de base**.
4) Entrez le **Mot de passe LDAP** souhaité.
5) Cliquez sur **Sauvegarder**.
6) Cliquez sur **OK**.

22.4.4 Comment configurer le serveur ODBC en serveur ODBC Bridge

Conditions préalables

Le serveur ODBC Bridge a été téléchargé depuis WBM, dans **Centre de service** > **Logiciel** et installé sur un PC Windows (32 bits ou 64 bits) avec des sources de données pouvant accéder à des bases de données relationnelles ou non relationnelles. Le serveur ODBC Bridge est nécessaire pour que les pilotes ODBC puissent accéder à la source de données.

Remarque :

En raison des récentes mises à jour de Windows 10 / Windows Server par Microsoft, l'interface ODBC du système d'exploitation a été modifiée et, par conséquent, seuls les pilotes 32 bits sont pris en charge par ODBC vers OBDC Bridge. Il est fortement recommandé d'utiliser des pilotes ODBC 32 bits pour se connecter aux sources de données ODBC.

Il s'agit d'une restriction temporaire.

La source de données doit être configurée en tant que DSN sur ODS client, via l'administration de la source de données ODBC.

Le nom de l'utilisateur et le mot de passe de la source de données sont connus.

La configuration du serveur ODBC Bridge est décrite pour l'interface en anglais. Bien entendu, la configuration peut aussi être effectuées dans une autre langue d'interface (**Gestion des serveurs** > **Langue**).

Étape par étape

1) Avec le bouton droit de la souris, cliquez sur l'icône du serveur ODBC Bridge dans la barre d'état et sélectionnez l'option de menu **Paramètres**.

2) Définissez les paramètres généraux du serveur :

a) Cliquez sur l'onglet **Paramètres serveur**.

b) Dans **Paramètres de connexion**, sélectionnez dans la liste déroulante **Interface réseau** l'adresse IP sous laquelle doit pouvoir être joint le serveur ODBC Bridge pour le client ODBC (OpenScape Business).

Cette adresse IP doit être entrée dans la WBM par OpenScape Business lors de la configuration ODS.

c) Dans **Port**, entrez le port par lequel les demandes du client ODBC (OpenScape Business) doivent passer.

Cette port doit être entré dans la WBM par OpenScape Business lors de la configuration ODS.

d) Si le service est arrêté, vous pouvez activer l'**État du service** en le réglant sur **Activé** dans **Contrôle du service** ou en sélectionnant **Démarrer le service** dans la barre d'état.

e) Si le service est connecté, vous pouvez désactiver l'**État du service** en le réglant sur **Désactivé** ou en sélectionnant **Arrêter le service** dans la barre d'état.

f) Dans **Paramètres réseau**, vous pouvez activer le chiffrement en le réglant sur **Activé**.

g) Sous **Paramètres réseau**, indiquez le nombre maximum de connexions simultanées aux clients ODBC (minimum : 1, maximum : 20) dans le champ **Connexions maximales**.

h) Cliquez sur **Sauvegarder les paramètres**.

Remarque : Après l'enregistrement des paramètres, un redémarrage du service est nécessaire.

---

3) Créez un utilisateur pour l'accès client ODBC à la source de données :

a) Cliquez sur l'onglet **Gestion de rôle**.

b) Cliquez sur **Ajouter un utilisateur**.

c) Dans le champ **Nom utilisateur**, attribuez un nom d'utilisateur au client ODBC.

d) Entrez un mot de passe pour le client ODBC dans les champs **Mot de passe** et **Entrer de nouveau le mot de passe**.

Les mêmes détails d'utilisateur doivent être entrés dans la WBM par OpenScape Business lors de la configuration ODS.

e) Sélectionnez le DSN auquel le client ODBC doit pouvoir accéder en cochant la case appropriée dans la colonne **Accès**.

f) Entrez le **Nom utilisateur DB** et le **Mot de passe** si nécessaire.

g) Cliquez sur **Sauvegarder les paramètres**.

4) Cliquez sur l'onglet **Surveillance** pour surveiller les connexions. Les détails suivants sont affichées :

- Noms et versions des pilotes ODBC installés
- Nom et adresse IP de ODS Client, dernier temps de connexion active et temps total de connexion active.
- Sources de données ODBC disponibles (via le lien **Open Windows Datasource Administrator**).

5) Cliquez sur l'onglet **Journaux** pour activer la création des fichiers journaux et définir les niveaux de suivi devant être enregistrés :
   a) Activer l'enregistrement en réglant sur **Activé**.
   b) Sélectionnez le **Niveau de journalisation** : **Tout** pour tous les journaux, **Normal** pour les journaux de service ou seulement **Avertissements et erreurs**.
   c) Sélectionnez le type de journal dans la liste déroulante. Vous pouvez choisir de visualiser le dossier des journaux ou la console de journal.
6) Cliquez sur l'onglet **Apparence** pour modifier l'apparence :
   a) Sélectionnez un thème (sombre ou clair).
   b) Sélectionnez un style.
   c) Sélectionnez la langue souhaitée.
   d) Indiquez si le service doit être automatiquement mis en marche lors du démarrage.
   e) Indiquez si le service peut être réduit à l'intérieur de la barre d'état.
7) Cliquez sur l'onglet **#À propos de** afin de visualiser les détails du service et les mises à jour disponibles.

   Remarque : Si une nouvelle version est disponible, cliquez sur **Installer** pour effectuer la mise à jour.

8) Sélectionnez **Quitter** dans la barre d'état pour fermer la configuration du service.

22.4.5 Comment ajouter une source de données externe pour Open Directory Service

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Les données d'accès de la base de données externe sont disponibles.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **Open Directory Service**.
3) Dans l'arborescence du menu, cliquez sur **Sources de données**.
4) Cliquez sur **Ajouter** .
5) Cliquez sur l'onglet **Base de données**.
6) Indiquez le **Nom** de la source de données.
7) Donnez une **Description** de la source de données.

8) Si vous souhaitez ajouter une base de données SQL :

a) Sélectionnez le type **PostgreSQL** ou **Microsoft SQL Server, Sybase SQL** ou **ODBC Bridge** dans la liste déroulante du **pilote ODBC**.

b) Dans **Adresse du serveur de la base de données**, indiquez l'adresse IPv4 de la base de données.

c) Indiquer le **Port serveur de la base de données**.

d) Indiquez le **Nom de la base de données** sous forme correcte (majuscules/minuscules).

e) Indiquez la **Connexion à la base de données** sous forme correcte (majuscules/minuscules).

f) Indiquez le **Mot de passe de la base de données** sous forme correcte (majuscules/minuscules).

g) Si vous avez sélectionné le type **Microsoft SQL Server, Sybase SQL** dans la liste déroulante du **pilote ODBC**, saisissez également la **version du protocole TDS**.

9) Si vous souhaitez ajouter une base de données non SQL :

a) Dans la liste déroulante **Pilote ODBC**, sélectionnez le type **ODBC Bridge**.

b) Dans **Adresse du serveur ODBC Bridge**, indiquez l'adresse IPv4 de la base de données.

c) Indiquez le **OBDC Bridge Server port**.

d) Entrez le **ODBC Bridge Remote DSN**

e) Entrez le **nom d'utilisateur ODBC Bridge** correct et sensible à la casse.

f) Entrez le **mot de passer ODBC Bridge** correct et sensible à la casse.

10) Cliquez sur **Contrôler Accès à la base de données** pour tester l'accès.

11) Cliquez sur **Enregistrer**.

12) Cliquez sur l'onglet **Accès données**.

13) Si vous souhaitez utiliser une table de bases de données :

a) Cliquez sur **Sélection simple - Accès à une table**.

b) Cliquez sur **Interroger les tables de bases de données** et sélectionnez dans la liste **Tables de bases de données** la table souhaitée.

Remarque : Cette fonctionnalité n'est pas prise en charge pour certaines sources de données (par ex. Oracle). Si oui, veuillez indiquer le nom de la table manuellement.

---

c) Cliquez sur **Aperçu de la table de base de données** et naviguez dans l'aperçu, dans les articles de données, à l'aide des boutons correspondants.

14) Si vous souhaitez utiliser une requête SQL définie par l'utilisateur :

a) Cliquez sur **Requête SQL définie par l'utilisateur**.

b) Entrez-le dans la **Requête SQL**.

Remarque : Lorsque vous définissez une nouvelle source de données à l'aide d'une instruction SQL, vous devez formuler la requête de manière à ce que les identifiants des enregistrements soient constants. Vous devez utiliser les attributs d'identification inclus dans

les tables respectives au lieu de calculer les identifiants lors de l'exécution de la requête. Évitez toute instruction telle que « SELECT ROW_NUMBER() OVER As ID » qui crée des identifiants lors de l'exécution de la requête et qui fournira des identifiants différents en fonction du tri et du nombre d'enregistrements. En cas d'unification de tables dont les plages d'ID se chevauchent avec UNION ALL, atténuez le risque de duplication des ID en incrémentant les ID des tables existantes d'un nombre différent pour chaque table à unir (par exemple, « SELECT (table2.ID+1000) AS ID »).

c) Cliquez sur **Aperçu des résultats de la requête** et naviguez dans l'aperçu, dans les articles de données, à l'aide des boutons correspondants.

15) Cliquez sur l'onglet **Mappages de champ**.

Remarque : Toutes les colonnes de la tableau sélectionnée ou toutes les colonnes qui fournissent la requête SQL définie par l'utilisateur sont disponibles pour les mappages de champ.

16) Cliquez sur **Ajouter mappage de champ**.

17) Sélectionnez dans la liste déroulante de gauche le champ de la source de données externe et dans la liste déroulante de droite, sur la même ligne, le champ correspondant souhaité dans le schéma de données de Open Directory Service. Pour contrôle, il est affiché à droite un aperçu des articles de données concernés grâce auquel vous pouvez naviguer à l'aide des boutons correspondants.

Remarque : Le champ **Identifiant unique** doit être affecté à un champ de la source de données externe, qui doit être unique.

18) Si vous souhaitez supprimer une ligne d'affectations de champs, cliquez sur l'icône de la corbeille à gauche.

19) Cliquez sur l'onglet **Conversion des numéros d'appel**.

a) Cochez la case **Actif(ve)**.

b) Cliquez sur **Lire les paramètres système**.

c) Si la base de données externe se trouve à un autre emplacement que le système, saisir le **Code du pays**, le **Préfixe du réseau local**, l'**Indicatif réseau**, le **Préfixe national** et la **Longueur maximale du numéro interne**

d) Sélectionnez l'une des options suivantes :

- Si vous souhaitez supprimer un indicatif réseau qui figure éventuellement dans la source de données externe, cochez la case **Supprimer l'indicatif réseau**.

- Si vous ne souhaitez pas supprimer l'indicatif réseau, décochez la case **Supprimer l'indicatif réseau**.

20) Cliquez sur **Enregistrer**.

21) Cliquez sur **OK**.

Étapes suivantes

Démarrez de nouveau Open Directory Service afin que la modification soit opérationnelle.

Réaliser un aperçu des résultats de la recherche LDAP.

22.4.6 Comment réaliser un aperçu des résultats de la recherche LDAP pour Open Directory Service

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Effectuez les opérations suivantes pour vérifier sur le résultat de la recherche LDAP de Open Directory Service comprend des articles de données sous la forme souhaitée et au format de numéro d'appel correct.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **Open Directory Service**.
3) Dans l'arborescence du menu, cliquez sur la source de données souhaitée dans **Open Directory** > **Utilisateurs OpenScape Business** > **Sources de données**.
4) Cliquez sur l'onglet **Test LDAP**.
5) Cliquez sur **Démarrer le test**. Dans **Résultat de la recherche LDAP**, l'aperçu du résultat de la recherche est présenté.

Remarque : La limite de réponse par défaut d'OpenLDAP est de 500 entrées. Le moteur du système principal du Service de répertoire ouvert (ODS) impose aussi une limite de 500 entrées pour chaque source de données.

Le test LDAP du Service de répertoire ouvert (ODS) lance une requête de recherche jusqu'à la limite de 500 entrées. L'option du test LDAP n'a pas pour objectif de récupérer les résultats, mais de vérifier que la connectivité LDAP est correcte.

Par conséquent, s'il y a plus de 500 enregistrements, les ajouts et modifications aux données LDAP peuvent ne pas être répercutés sur le WBM après exécution du test LDAP.

22.4.7 Comment effacer une source de données externe pour Open Directory Service

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **Open Directory Service**.
3) Dans l'arborescence du menu, cliquez sur **Open Directory** > **Sources de donnée**.
4) Dans l'espace de travail, cliquez sur la source de données correspondante.
5) Cliquez sur **Effacer**.
6) Cliquez sur **OK**.

Étapes suivantes

Démarrez de nouveau Open Directory Service afin que la modification soit opérationnelle.

22.5 Intégration d'Active Directory Service

Active Directory est un service de répertoire de Microsoft pour les réseaux de domaines. Avec l'intégration offerte d'Active Directory Service, OpenScape Business peut lire la base de données d'Active Directory et synchroniser les utilisateurs avec sa propre base de données afin de simplifier l'administration et réduire les efforts de configuration.

Conditions requises

Pour que la synchronisation de l'intégration d'Active Directory Service ait lieu, les conditions requises suivantes doivent être satisfaites :

- Un serveur Active Directory Microsoft est déployé par le client
- Active Directory est utilisé comme seul point de configuration des données des employés et, notamment, des données utilisateur. Les champs suivants seront mappés entre Active Directory et OpenScape Business :
  - prénom
  - nom
  - nom de l'écran
- Seul cet Active Directory est utilisé pour ajouter, modifier ou supprimer des données des employés.
- Toutes les modifications d'Active Directory devraient également prendre automatiquement effet au niveau du système de communication.

Synchronisation

L'identifiant unique des utilisateurs d'OpenScape Business utilisé pour la synchronisation est le numéro SDA. Ce numéro est synchronisé avec le champ telephoneNumber d'AD (Active Directory).

Chaque modification apportée dans Active Directory de la société est immédiatement synchronisée dans OpenScape Business. Cela signifie que chaque nouvel utilisateur ajouté à AD sera également ajouté dans OpenScape Business et qu'une licence d'utilisateur IP sera attribuée à cet utilisateur.

Toute modification apportée dans AD à des utilisateurs déjà synchronisés se retrouve immédiatement chez les utilisateurs d'OpenScape Business.

Si un utilisateur synchronisé est supprimé d'AD, les firstName, sn et displayName de l'utilisateur seront également effacés dans OpenScape Business et la licence d'utilisateur IP sera libérée. Le numéro SDA et le numéro d'appel interne ne sont pas supprimés d'OpenScape Business et restent disponibles pour une attribution à un autre utilisateur.

Remarque : L'accès à Active Directory Service est en lecture seule. Cela signifie que la synchronisation des données utilisateur se fait uniquement depuis Active Directory vers OpenScape Business. Les modifications apportées aux informations de l'utilisateur d'OpenScape Business ne sont pas synchronisées dans Active Directory et seront écrasées par les données d'Active Directory lors de la prochaine synchronisation.

Mappage de champs

Vous pouvez adapter le mappage des noms de champ au schéma de données d'Active Directory Service. De cette manière, vous pouvez contrôler la manière dont les champs d'OpenScape Business sont mis à jour à partir des données d'Active Directory.

Le mappage par défaut des champs est donné dans le tableau suivant :

Champ OpenScape Business	Champ Active Directory
prénom	Prénom
nom	sn
nom de l'écran	displayName
SDA	telephoneNumber

Normalisation des numéros SDA

Les données du site de passerelle du système OpenScape Business sont utilisées pour convertir le numéro SDA d'un utilisateur au format de numéro canonique.

Le format de telephoneNumber dans Active Directory doit également être au format canonique, de sorte que la synchronisation automatique est possible.

22.5.1 Comment configurer Active Directory Service

Conditions préalables

Vous êtes connecté à la WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'assistant **Intégration d'Active Directory Service**.
4) Cochez la case **Activer** pour activer l'intégration d'Active Directory Service.

5) Configurez l'**Adresse IP** du serveur Active Directory, le **Nom utilisateur** et le **Mot de passe** pour un utilisateur valide.

   Le **Nom utilisateur** demandé ici n'est pas un nom utilisateur OpenScape Business, mais un nom utilisateur ActiveDirectory qui doit être au format de spécifications d'annuaire X.500. Dans ce format, les utilisateurs sont définis avec les nœuds suivants :

CN	Nom commun
OU	Unité organisationnelle
DC	Composant de domaine

   Le nom utilisateur est décrit avec les informations les plus spécifiques sur la gauche et les informations les plus générales sur la droite. Chaque élément d'informations est donné sous la forme de paires séparées par un signe égal (**=**).

   Voici un exemple de nom utilisateur `CN=John.doe,OU=Administrators,DC=SomeCompany`.

6) Cliquez sur **Extraire les ND** pour extraire les ND disponibles et sélectionnez-en un comme namingContext de base.

   En cas de problème avec les identifiants de l'utilisateur, vous verrez s'afficher `Erreur d'identification ! Veuillez vérifier vos identifiants`.

7) Modifiez les champs **Conteneur** et **Filtre** si nécessaire.

   La valeur du conteneur par défaut est `cn=Users`, et `(&(objectCategory=person)(objectClass=user))` pour le filtre

8) Cliquez sur **Extraire les données**.

   Les 1 000 premières entrées d'AD s'afficheront, dans l'ordre des lastname(sn).

9) Cliquez sur un utilisateur pour vérifier les détails.

10) Cliquez sur **OK et suivant** pour vous rendre à l'écran **Mappage de champs**.

11) Apportez les modifications nécessaires dans les valeurs de mappage des champs.

    Les valeurs de la colonne de gauche correspondent au schéma de la base de données d'OpenScape Business, et celles de la colonne de droite aux attributs d'Active Directory.

    Numéro de téléphone sera utilisé pour être assorti au numéro SDA d'OpenScape Business.

12) Cliquez sur **Terminer** pour compléter l'intégration d'Active Directory

22.6 Application Launcher

Application Launcher est une application Windows basée sur Java pour la gestion en fonction de l'appel des applications sur le PC Client des utilisateurs de l'UC Suite et de myAgent. Application Launcher peut par exemple servir à ouvrir automatiquement le formulaire de contact de l'appelant dans un système CRM.

Application Launcher offre les fonctionnalités suivantes :

- Recherche d'informations relatives à l'appel sur le numéro de téléphone (par ex. numéro d'appel, nom du correspondant, ID du client) soit dans Open Directory Service, soit dans les répertoires du système
- Appel d'applications Windows ou d'applications Web avec les appels sortants et entrants
- Transmission aux applications Windows ou aux applications Web d'informations relatives à l'appel
- exploitation automatique en arrière plan lors de la réception des appels
- Fenêtres contextuelles facultatives configurables pour les appels entrants avec informations relatives aux appels et boutons pour les actions utilisateur
- Liste des appelants avec fonction d'appel
- Fonction pré-affichage pour les tests durant la configuration
- simple reprise de la configuration du premier client configuré dans tous les autres du système à l'aide du profil de configuration

22.6.1 Conditions nécessaires pour Application Launcher

Pour utiliser Application Launcher, le PC client de l’utilisateur doit disposer des matériels et logiciels appropriés.

L’installation nécessite des droits d’administrateur locaux sur le PC client, mais pas de mise à jour automatique.

Système d’exploitation

Application Launcher peut être utilisé en association avec les systèmes d’exploitation suivants :

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bits ou 64 bits)
- Microsoft Windows Vista (32 bits)

Conseil : Le système d’exploitation utilisé a toujours besoin de la version la plus actuelle de toutes les mises à jour disponibles (Service Packs et Patches).

Mise à jour de Windows

Les PC doivent toujours disposer de l’état actuel de l’ensemble des mises à jour disponibles, Service Packs compris.

Logiciels supplémentaires

Oracle Java 8 ou version ultérieure, ou bien OpenJDK 8 (voir **Centre de service** > **Logiciel**)

Web Services pour téléphones mobiles

Web Services pour téléphones mobiles a été activé dans le système pour la liaison avec le système. Les ports configurés dans le système doivent être ouverts sur les pare-feu du LAN et les PC client.

Open Directory Service (option)

Si Application Launcher souhaite utiliser des données de Open Directory Service, ce dernier doit être configuré dans le système. Le port

configuré à cette fin dans le système doit être ouvert sur les pare-feu du LAN et les PC client.

Concepts associés

Configuration de l'entrée de mobilité à la page 894
Open Directory Service à la page 1112

22.6.2 Profil avec les données de configuration de Application Launcher

Un profil avec les données de configuration d'Application Launcher permet de configurer de manière simple et rapide Application Launcher sur tous les PC client.

Le profil comprend toutes les données de configuration y compris la connexion système et les données utilisateur. Une fois que Application Launcher a été entièrement configuré pour le premier utilisateur, vous pouvez, en tant qu'administrateur, mettre à disposition le profil avec les données de configuration de Application Launcher dans le système de communication. Ensuite, tous les utilisateurs peuvent effectuer la configuration de Application Launcher en important ce profil.

22.6.2.1 Comment fournir le profil avec les données de configuration de Application Launcher

Conditions préalables

Application Launcher est configuré entièrement pour un utilisateur.

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Applications** > **OpenScape Application Launcher**.
3) Cliquez sur **Parcourir** et sélectionnez le fichier suivant : `C:\Documents and Settings\<Windows User Name>\Application Data\Tray_Tool\profile.xml`.
4) Cliquez sur **Ouvrir**.
5) Cliquez sur **Charger**.

Étapes suivantes

Tous les utilisateurs peuvent importer ce profil dans Application Launcher et ainsi effectuer la configuration.

22.7 Présentation de myPortal for Teams

Le plugin myPortal for Teams permet d'intégrer l'application Microsoft Teams à OpenScape Business.

myPortal for Teams nécessite une nouvelle carte mère OpenScape Business V3 ou un système OpenScape Business S, et est compatible avec la version logicielle V3R1 FR2 et les versions ultérieures.

Avec myPortal for Teams, vous pouvez :

- Filtrer et gérer l'historique de vos appels
- Afficher et rechercher des contacts
- Organiser les contacts dans des groupes de favoris
- Envoyer des e-mails à vos contacts
- Sélectionner un appareil contrôlé (uniquement pour les utilisateurs MULAP)
- Lancer un appel
- Répondre, rejeter ou dévier un appel
- Mettre un appel en attente
- Transférer un appel
- Passer un double appel
- Passer d'un appel à l'autre
- Effectuer un transfert supervisé

Remarque : La recherche de contacts dans des répertoires externes comme LDAP n'est pas disponible.

Remarque : La fonctionnalité VoIP n'est pas prise en charge pour myPortal for Teams.

22.7.1 Comment configurer MyPortal for Teams

Conditions préalables

- Certificat Microsoft officiel et approuvé à importer dans OpenScape Business WBM
- ID d'application Microsoft qui doit être généré avant de configurer myPortal for Teams

Étape par étape

1) Accédez à **Configuration > Services Cloud**.
2) Cliquez sur Modifier en regard de **Plugin du client Microsoft Teams**.
3) Le nom de domaine et le numéro de port sont déjà remplis dans le champ **URL**.

   Le nom de domaine correspond au domaine de votre système OpenScape Business.

   La valeur par défaut pour le numéro de port est 8805. Vous pouvez changer l'ID de domaine et le numéro de port si vous le souhaitez.
4) Saisissez l'**ID d'application**.

   L'ID d'application est généré par l'administrateur sur le portail Microsoft Azure.

5) Cliquez sur **OK et Télécharger**.
   Le plugin est téléchargé sous forme de fichier zip. Le fichier téléchargé est un plugin personnalisé en fonction de votre configuration système.

Remarque :

L'onglet Microsoft Teams empêche le chargement du contenu Web à partir d'un serveur utilisant des certificats autosignés. Il s'agit d'un aspect de sécurité, et l'utilisation de certificats autosignés constitue pour l'essentiel une pratique dangereuse car cette interface est exposée à Internet.

Par conséquent, il convient d'installer un certificat Microsoft approuvé dans le système. Pour en savoir plus, consultez le chapitre Comment importer le certificat de serveur (PKCS#12) à la page 973.

22.7.2 Comment importer myPortal for Teams dans le magasin d’applications Teams

Conditions préalables

Vous devez disposer de droits d’administrateur pour l’application Microsoft Teams.

Étape par étape

1) Cliquez sur **Applications** dans le volet de navigation gauche de l’application Microsoft Teams.
2) Cliquez sur **Importer une application personnalisée** et sélectionnez **Importer pour mon organisation**.
   Sélectionnez le fichier WBM que vous avez téléchargé et importez-le.

Étapes suivantes

Une fois importé, le plugin myPortal for Teams peut être ajouté à l’application Microsoft Teams par les utilisateurs.

22.8 Unify Phone

Les utilisateurs d'OpenScape Business peuvent passer des appels téléphoniques via le client Unify Phone. Cette fonctionnalité est disponible à la fois à partir du client Unify Phone et à travers le périphérique. Pour ce faire, vous devez configurer la connectivité Unify Phone avec OpenScape Business et ajouter les utilisateurs Unify Phone.

La fonctionnalité Unify Phone disponible comprend :

- Passer/répondre à des appels
- Effacer/rejeter des appels
- Mettre en garde/récupérer des appels
- Transfert d’appel vers logiciel/appareil
- Prise en charge DTMF

- Swap d'appel (variante)
- Renvoi d’appel
- Numéro alternatif
- Routage de l'appel
- Accès au répertoire et au journal
- Contrôle d'appel tiers à l'aide des clients de communications unifiées (UC) embarqués suivants : myPortal @work, myPortal for Desktop, myPortal for Outlook, myAttendant, my Agent et myPortal for Teams.

Outre les fonctionnalités mentionnées ci-dessus, aucune autre fonctionnalité n'est disponible, en particulier les codes de fonctionnalités.

Remarque : Le contrôle des appels par des tiers (contrôle CTI) n'est actuellement possible que pour le client Unify Phone Desktop. Le contrôle s'effectue toujours via le client Unify Phone Desktop (Web/PWA) et n'est pas prévu pour le client Unify Phone mobile. Il est possible de déplacer un appel vers le client mobile Unify Phone après avoir accepté l'appel. De plus, le contrôle d'appel tiers n'est pas destiné à être utilisé en conjonction avec une fonction active de "numéro alternatif" du Unify Phone.

22.8.1 Comment configurer la connectivité du Unify Phone

Conditions préalables

Vous avez saisi la valeur **Amont jusqu'à (Kbps)** sous **Configuration** > **Assistants** > **Installation de base** > **Installation de base** > **Amont de votre connexion internet**, afin de pouvoir effectuer des appels simultanés. Par exemple, entrez '256' pour 2 appels simultanés.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.

2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Services cloud** .

3) Cliquez sur **Modifier** à côté de **Connectivité Unify Phone** pour configurer les paramètres de connectivité de base.

4) Cochez la case **Activer Unify Phone** pour activer la connectivité Unify Phone.

5) Dans **Informations d'identification du Unify Phone**, entrez les détails suivants :

a) Sélectionnez le **Domaine** dans la liste déroulante disponible.

Les possibilités suivantes sont disponibles :

- phoneapp.unify.com
- Personnalisé

Remarque : Si vous avez sélectionné Personnalisé, remplissez le champ **Domaine personnalisé**.

---

b) Entrez la clé API générée pour votre locataire dans le champ **Clé API du téléphone Unify**.

6) Dans **Appels Unify Phone simultanés**, sélectionnez le nombre d'appels Unify Phone simultanés à partir de la liste déroulante disponible. Ce nombre dépend de la valeur de transmission configurée précédemment.

   Remarque : Si la qualité d'appel se détériore, il faut réduire le nombre de communications simultanées.

7) Cliquez sur **OK & Suivant**.
8) Dans la fenêtre **Numéro de localisation du Unify Phone**, sélectionnez le schéma de numérotation que vous souhaitez utiliser. Cette sélection affecte le format des numéros SIP et WSI.
   - Pour utiliser des numéros internationaux, cochez la case **Utiliser la numérotation internationale**.

     Si vous choisissez les numéros internationaux, l'assistant vous invite à configurer les numéros de localisation manquants de la route téléphonique Unify, qui seront utilisés pour former le numéro international. De plus, les paramètres de l'itinéraire Unify Phone pour le type de numéro sont mis à jour en fonction de la sélection.
   - Numéros internes
9) Cliquez sur **OK & Suivant**.
10) Cliquez sur **Exécuter la fonction** dans la fenêtre pop-up pour créer un trunk SIP pour Unify Phone.
11) Cliquez sur **OK & Suivant** puis sur **Terminer**.

    Remarque : Il est conseillé de sauvegarder les données de configuration en sélectionnant **Sauvegarde de données** > **Sauvegarde - immédiate** dans le menu principal.

Étapes suivantes

Si vous souhaitez désactiver la connectivité du Unify Phone, vous devez d'abord supprimer tous les utilisateurs du Unify Phone, comme décrit dans Comment retirer ou supprimer des utilisateurs d'Unify Phone à la page 1135.

Remarque : Il est essentiel de supprimer les utilisateurs Unify Phone actifs avant, par exemple, les migrations de système, afin d'éviter des divergences critiques entre la base de données OpenScape Business et la base de données dans le cloud.

22.8.2 Comment configurer l'instance utilisateur de Unify Phone

Conditions préalables

La connectivité du Unify Phone est configurée.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Services cloud** .
3) Cliquez sur **Modifier** à côté de **instance d'utilisateur d'Unify Phone**.

4) Cliquez sur **OK et Suivant** et puis **Terminer**.

22.8.3 Comment gérer les utilisateurs Phone Unify

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Services Cloud**.
3) Cliquez sur **Modifier** à côté de **Instance utilisateur Unify Phone**.

   Une liste des utilisateur Unify Phone configurés s'affiche pour le système spécifique.

Remarque : Si des utilisateurs Unify Phone sont déjà enregistrés, vous serez invité à exécuter l'assistant de connectivité de Unify Phone sans modifier la configuration.

22.8.3.1 Comment créer de nouveaux utilisateurs de téléphone Unify

Conditions préalables

La connectivité du Unify Phone est configurée.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Services cloud** .
3) Cliquez sur **Modifier** à côté de **instance d'utilisateur d'Unify Phone**.
   Les utilisateurs Unify Phone disponibles sont affichés.
4) Cliquez sur **Créer** à côté de **Créer un nouvel utilisateur pour Unify Phone**.
5) Sur la page **création d'un utilisateur Unify Phone**, procédez comme suit :
   a) Le **Code d'accès au tronc + le numéro d'appel de l'utilisateur du Unify Phone** est en lecture seule et est généré automatiquement selon le schéma de numérotation sélectionné (international ou interne).
   b) Entrez le **No. d'appel de l'utilisateur du Unify Phone**.
   c) Entrez le **SDA de l'utilisateur du Unify Phone**.
   d) Entrez le **Prénom**.
   e) Entrez le **Nom de famille**.
   f) Entez l'**Adresse e-mail** de l'utilisateur du Unify Phone.
6) Cliquez sur **OK & Suivant**.
7) Cliquez sur **Terminer**.
   Une fois ce processus terminé avec succès, un courriel est envoyé à l'adresse e-mail saisie, ce qui permet à l'utilisateur du Unify Phone de terminer la configuration.
8) Répétez les étapes 4 à 6 pour ajouter d'autres utilisateurs Unify Phone.

22.8.3.2 Comment ajouter des utilisateurs existants d'Unify Phone

Conditions préalables

La connectivité du Unify Phone est configurée.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Services cloud** .
3) Cliquez sur **Modifier** à côté de **instance d'utilisateur d'Unify Phone**. Les utilisateurs Unify Phone disponibles sont affichés.
4) Cliquez sur **Ajouter** à côté de **Ajouter un utilisateur existant à Unify Phone**.
5) Sur la page **Unify Phone User Allocation**, les utilisateurs disponibles sont affichés sous forme d'icônes. Pour ajouter un utilisateur existant, procédez comme suit :
   a) Le **Code d'accès au tronc + le numéro d'appel de l'utilisateur du Unify Phone** est en lecture seule et est généré automatiquement selon le schéma de numérotation sélectionné (international ou interne).
   b) Entrez le **No. d'appel de l'utilisateur du Unify Phone**.
   c) Entrez le **SDA de l'utilisateur du Unify Phone**.
   d) Vous pouvez rechercher un utilisateur par **Nom** ou **E-mail**.
   e) Sélectionnez un utilisateur d'Unify Phone à l'aide des icônes disponibles.

      Il existe trois types d'icônes pour les utilisateurs du téléphone Unify :

      - Icônes vertes : Les utilisateurs disponibles qui sont actifs.
      - Icônes vertes grisées : Utilisateurs non disponibles qui ne sont pas actifs.
      - Icône verte grisée dans un cadre rouge : Utilisateurs non disponibles qui ne sont pas actifs, déjà configurés avec un numéro dans Unify Phone.

      Les champs **Prénom** et **Nom de famille** de l'utilisateur Unify Phone sont remplis automatiquement.
6) Cliquez sur **OK & Suivant**.
7) Répétez les étapes 4 à 6 pour ajouter d'autres utilisateurs Unify Phone.

Étapes suivantes

Attribuez des licences aux utilisateurs d'Unify Phone comme décrit dans Comment obtenir des licences d’abonné (autonome) à la page 268 ou Comment effectuer la procédure de licence pour les abonnés (interconnexion de réseaux) à la page 279.

Lors de l'intégration d'un utilisateur d'Unify Phone dans une équipe (MULAP), notez les points suivants :

- Un seul téléphone de bureau IP ou TDM peut être inclus dans l'équipe avec l'utilisateur du Unify Phone. La fonction de routage dans Unify Phone est utilisée pour déterminer quel appareil final doit être utilisé pour signaler un appel entrant.
- Le téléphone de bureau dans l'équipe avec Unify Phone peut toujours être contrôlé par des applications externes via TAPI, WSI ou CSTA. Ceci s'applique également lorsque le Unify Phone est contrôlé par des applications tierces.

- Les abonnés sans fil ne sont pas autorisés à utiliser le Unify Phone.

22.8.3.3 Comment modifier les détails des utilisateurs de Unify Phone

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Services Cloud**.
3) Cliquez sur **Modifier** à côté de l'utilisateur Unify Phone correspondant.
4) Vous pouvez modifier les détails suivants.
   a) Le **Code d'accès de la ligne + Numéro d'appel de l'utilisateur Unify Phone** est en lecture seule et est généré automatiquement selon le plan de numérotation sélectionné (international ou interne).
   b) Le **Numéro d'appel de l'utilisateur Unify Phone**.
   c) Le **DID de l'utilisateur Unify Phone**.
   d) Le **Prénom** de l'utilisateur Unify Phone.
   e) Le **Nom de famille** de l'utilisateur Unify Phone.

   Remarque : Le champ Utilisateur Unify Phone sélectionné contenant l'adresse e-mail de l'utilisateur n'est pas modifiable.
5) Cliquez sur **OK & Suivant**.

22.8.3.4 Comment retirer ou supprimer des utilisateurs d'Unify Phone

Dans certains cas, il est absolument nécessaire de supprimer les utilisateurs d'Unify Phone de votre système OpenScape Business. Par exemple :

- Par exemple, lors de la migration d'un système de laboratoire de test vers un système réel.
- Lors du remplacement d'une carte mère de V2 H/W à V3 H/W ou en cas de défaillance de la H/W.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Services cloud** .
3) Cliquez sur **Modifier** à côté de **instance d'utilisateur d'Unify Phone**.
4) Cliquez sur **Modifier** à côté de l'utilisateur Unify Phone correspondant.
5) Cliquez sur **Retirer** ou **Supprimer**.
6) Répétez les étapes 1 à 5 pour supprimer d'autres utilisateurs Unify Phone.

   Gardez à l'esprit que la suppression d'utilisateurs administrateurs est différente de la suppression d'utilisateurs Unify Phone non administrateurs :

   Lorsque des utilisateurs d'Unify Phone, qu'ils aient ou non un rôle d'administrateur, sont supprimés du système, ils ne sont pas supprimés du

locataire d'Unify Phone auquel ils appartiennent. Ces utilisateurs existent toujours, mais aucun numéro de téléphone ne leur est plus attribué.

Lorsque des utilisateurs d'Unify Phone sans rôle d'administrateur sont supprimés du système, ils sont également supprimés du locataire auquel ils appartiennent.

Lorsque des utilisateurs d'Unify Phone avec un rôle d'administrateur sont supprimés du système, ils ne sont pas supprimés du locataire auquel ils appartiennent. Ces utilisateurs existent toujours, mais aucun numéro de téléphone ne leur est plus attribué.

Remarque : Si un nouveau système est mis en place par clonage ou restauration de données (migration), alors que le système d'origine avait un accès au connecteur Unify Phone configuré, il faut s'assurer que toute divergence entre l'état du cloud UP et celui de la base de données OSBiz sera évitée. Pour cette raison, il est essentiel de supprimer tous les utilisateurs UP si nécessaire et de désactiver le connecteur Unify Phone avant de cloner/sauvegarder le système d'origine.

22.8.3.5 Comment préparer un numéro alternatif et un routage des appels pour une interopérabilité des téléphones Unify

Pour que les fonctionnalités de numéro alternatif et de routage des appels de téléphones unify soient prises en charge par OpenScape Business, vous devez effectuer le réglage suivant depuis le mode Expert.

Étape par étape

1) Dans **Mode Expert**, cliquez sur **Serveur de téléphonie** > **Appels entrants** > **Renvois d'appel**.
2) Cliquez sur l'onglet **Table d'acheminement - Définition**.
3) Sous **Modifier le renvoi temporisé**, faites les réglages suivants :
   a) Comme **Dest 1** sélectionnez `* Abonné appelé`.
   b) Comme **Dest 2** sélectionnez `** Utilisateur défini`.
   c) Comme **Dest 3** sélectionnez `Nombre de messages vocaux` (optionnel).

22.9 Mitel WX

OpenScape Business prend en charge l'intégration avec l'application Mitel WX, permettant aux utilisateurs de bénéficier de fonctionnalités de collaboration avancées tout en continuant à exploiter leur environnement PBX existant. En configurant la connectivité Mitel WX dans OpenScape Business et en provisionnant les utilisateurs Mitel WX correspondants, vous pouvez étendre de manière transparente les services de communication unifiée aux abonnés OpenScape Business.

L'intégration est prise en charge dans :

- OpenScape Business S (minimum 3 Go de RAM)
- Systèmes OpenScape Business X fonctionnant sur du matériel V3 (minimum 4 Go de RAM)

Les fonctionnalités disponibles de Mitel WX comprennent :

- Passer/répondre à des appels
- Terminer/rejeter des appels
- Mettre des appels en garde/reprendre des appels
- Prise en charge du DTMF
- Transférer un appel
- Couper/rétablir le son
- Prise en charge de MULAP dans OpenScape Business
- Transférer un appel depuis/vers le téléphone de bureau
- Passer ou répondre à un second appel
- Permuter les appels (alternance)
- Fusionner deux appels en conférence
- Renvoi d’appel
- Contrôle à distance des appels du téléphone de bureau
- Numéro alternatif
- Messagerie vocale
- Afficher le profil d'un contact/les détails de mon profil
- Contacts personnels
- Groupement
- Présence (visibilité de l'état du poste)
- Routage basé sur la présence
- Chat (via CloudLink)
- Clients localisés
- Tonalités nationales localisées
- Accessibilité WCAG 2.2 AA
- Contrôle d'appels tiers à l'aide des clients de communications unifiées (UC) intégrés suivants : myPortal @work, myPortal for Desktop, myPortal for Outlook, myAttendant, my Agent et myPortal for Team.

Remarque : Le contrôle d'appels tiers (contrôle CTI) est actuellement possible avec le client Mitel WX Desktop. Le contrôle s'effectue toujours via le client Mitel WX Desktop (Web/PWA) et n'est pas prévu pour le client mobile Mitel WX. Il est possible de transférer un appel vers le client mobile Mitel WX après avoir accepté l'appel. De plus, le contrôle d'appels tiers n'est pas destiné à être utilisé conjointement avec la fonctionnalité active « Numéro alternatif » de Mitel WX.

22.9.1 Comment configurer la connectivité Mitel WX

Configurez la connexion entre OpenScape Business et Mitel WX pour activer les services de communications unifiées (UC). Configurez les paramètres système requis et créez des comptes utilisateur Mitel WX afin de permettre un accès client sécurisé et fiable.

Conditions préalables

- Générez une licence incluant les **fonctionnalités Mitel WX**.

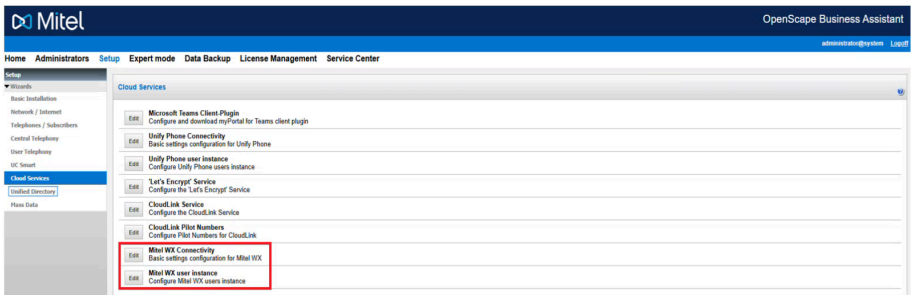
  La licence est générée sur le portail de services CLS / SLS.
- Activez sur le système la **licence incluant les fonctionnalités Mitel WX**.

  La licence est activée sur le PBX OpenScape Business.
- Un compte **Mitel CloudLink Platform**.
- Configurez **Mitel WX** dans **CloudLink Service**.
- Activer le **service de synchronisation CloudLink**

  Également utilisé par les applications CloudLink.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Services Cloud**.



3) Cliquez sur **Modifier** à côté de **Connectivité Mitel WX** pour configurer les paramètres de connectivité de base.
4) Cochez la case **Activer Mitel WX** pour activer la connectivité Mitel WX.
5) Sous **Appels Mitel WX simultanés**, sélectionnez le nombre d'appels Mitel WX simultanés dans la liste déroulante.
   - Pour utiliser des numéros internationaux, cochez la case **Utiliser la numérotation** internationale.
6) Cliquez sur **OK et suivant**, puis sur **Terminer**.

Remarque : Il est recommandé de sauvegarder les données de configuration en sélectionnant **Sauvegarde des données** > **Sauvegarde immédiate** dans le menu principal.

22.9.2 Migration d'Unify Phone vers Mitel WX

La procédure suivante décrit les étapes nécessaires pour migrer les utilisateurs Unify Phone existants vers Mitel WX.

Conditions préalables

- Générez une licence incluant les fonctionnalités Mitel WX
- Activez sur le système la licence incluant les fonctionnalités Mitel WX
- Une **plateforme Mitel CloudLink**
- OpenScape Business doit être connecté à CloudLink

- Activer le **service de synchronisation CloudLink**

  Également utilisé par les applications CloudLink.
- Activez la **prise en charge du conteneur CAS**

Étape par étape

1) Dans **CloudLink Administration Portal**, accédez à **Integration & Apps**.
2) Activez le **connecteur de téléphonie Mitel** et cliquez sur le bouton **Terminer la configuration**.
3) Activez la case à cocher **« Êtes-vous en train d'intégrer un locataire existant ? »**.
4) Ajoutez la **clé API** du compte Unify Phone.
5) Cochez la case **Migrer les utilisateurs vers CloudLink**.
6) Cliquez sur le bouton « **Terminé** ».

   Le locataire sera automatiquement migré vers CloudLink et tous les utilisateurs Unify Phone seront ajoutés à CloudLink.
7) Dans **OpenScape Business Assistant**, cliquez sur les assistants **Connectivité Mitel WX** ou **Instance utilisateur Mitel WX**.
8) Une fenêtre contextuelle apparaît pour indiquer qu'une intégration Unify Phone a été détectée.
9) Cliquez sur **OK & Suivant**.

   La procédure de migration va démarrer.
10) Dans **Migration Mitel WX**, attribuez aux utilisateurs le niveau de licence (Essential, Premier ou Elite).
11) Cliquez sur **OK & Suivant**.

    La migration sera effectuée automatiquement. Les utilisateurs seront provisionnés à la fois dans les bases de données OpenScape Business et CloudLink.
12) Dans l'**assistant Connectivité Mitel WX**, configurez les éléments suivants :

    a) Nombre d'appels Mitel WX simultanés
    b) Si nécessaire, activez l'option **Utiliser la numérotation internationale**.
13) Cliquez sur **Terminer**

    La migration est terminée.

22.9.3 Comment configurer Mitel WX dans le service CloudLink

Pour configurer la connectivité Mitel WX et l’instance utilisateur, vous devez configurer Mitel WX dans le service CloudLink

Conditions préalables

- Compte CloudLink

  Un compte actif Mitel CloudLink Platform est requis
- Activer le **service de synchronisation CloudLink**

  Également utilisé par les applications CloudLink.
- Connecter le service CloudLink avec OpenScape Business WBM
- Activer la **prise en charge des conteneurs cas**

Étape par étape

1) Dans le site d'**administration Mitel**, dans l'arborescence de navigation, sélectionnez « **Navigation et applications** ».
2) Activez le **connecteur de téléphonie Mitel** et cliquez sur le bouton **Terminer la configuration**.
3) Dans la **Configuration du connecteur de téléphonie Mitel**, renseignez les informations requises.
4) Cliquez sur le bouton « **Terminé** ».

   Le tenant Mitel WX sera créé sur CloudLink.

22.10 Service Let's Encrypt

Let's Encrypt est une autorité de certification automatisée qui propose des certificats TLS/SSL gratuits via le protocole Automatic Certificate Management Environment (ACME). Le service vérifie la propriété du domaine à l'aide de jetons et de défis uniques, tels que le défi HTTPS. Après vérification, les serveurs de Let's Encrypt fournissent des certificats signés pour une communication sécurisée entre les serveurs et les utilisateurs.

22.10.1 Comment configurer le service Let's Encrypt

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Services cloud** .
3) Cliquez sur **Modifier** à côté du **Service Let's Encrypt**.
4) Dans **Configuration du nom de domaine**, entrez les détails suivants :
   - Saisissez le nom de domaine dans le champ **Nom de domaine primaire**.
   - En option, saisissez un deuxième domaine dans le champ **Nom de domaine secondaire (optionnel)**.
5) Sous **Configuration de la mise à jour automatique des certificats**, définissez l'heure à laquelle la mise à jour automatique doit avoir lieu dans le champ **Heure de mise à jour automatique**.

   Remarque : Les systèmes redémarrent lors d'une mise à jour automatique.
6) Cliquez sur **Activer** pour activer ou **Désactiver** pour désactiver le service.

7) Sous **Statut du service Let's Encrypt** vous trouverez des informations détaillées sur le service et son statut :

   - **L'état du service** indique si le service est actuellement `Actif` ou `Inactif`.
   - **La date d'activation du certificat** indique la date à laquelle le certificat a été activé.
   - **La date de renouvellement** indique la date d'échéance du renouvellement automatique du certificat.
   - **L'état du renouvellement** indique l'état du processus de renouvellement automatique.

   Remarque : Le protocole Let's Encrypt utilise le port HTTP TCP/80 pour le défi HTTP, pendant la création initiale du certificat ou la mise à jour du certificat.

   Sur la page d'accueil du WBM, un message s'affiche pour informer les administrateurs du système de l'expiration du certificat (X jours) et de l'échec de la tentative de mise à jour du certificat.

22.11 Service CloudLink

CloudLink permet la communication entre les systèmes OpenScape Business sur site et les applications Mitel basées sur le cloud.

Connexion SIP

La fonctionnalité de connexion SIP est utilisée pour connecter OpenScape Business à des services cloud tels que Workflow Studio.

Remarque : Une licence Workflow Studio est requise.

Pour activer cette fonctionnalité, consultez le chapitre Comment configurer le connecteur SIP.

Conseil : Avant cela, assurez-vous que le Flux ascendant de votre connexion Internet est configuré (voir Comment configurer l'accès Internet via un routeur Internet externe).

Prise en charge des conteneurs dans OpenScape Business

Un environnement d'exécution de conteneurs est disponible dans OpenScape Business pour prendre en charge le conteneur CAS (Cloudlink Gateway). En raison de contraintes de performance/capacité, il n'est disponible que dans les versions OpenScape Business suivantes :

- Cartes mères V3 avec disque NVMe intégré (systèmes embarqués)
- Systèmes OpenScape Business S (variantes serveur)

Sur les systèmes embarqués, l'environnement d'exécution du conteneur est préinstallé dans le cadre de l'image logicielle OpenScape Business pour matériel V3. Il n'est pas lancé par défaut au démarrage afin d'économiser les ressources système. Elle n'est activée que lorsque l'administrateur active la prise en charge des conteneurs dans l'interface utilisateur Web de Cloudlink.

Sur les variantes serveur, l'environnement d'exécution de conteneurs (package Docker) doit être installé par l'administrateur lors de l'installation du système d'exploitation SLES15.

Pour configurer le service de prise en charge des conteneurs, consultez le chapitre Comment configurer l'interface Web CloudLink Daemon.

22.11.1 Comment configurer le service CloudLink

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Services cloud**.
3) Cliquez sur **Modifier** en regard de **Service CloudLink**.
4) Cliquez sur la case à cocher située à coté de **Activer le service CloudLink**.
5) Si nécessaire, cochez la case située à côté de **Utiliser un proxy**.
6) Saisissez respectivement l'adresse IP et le port du proxy dans les champs **HTTP-Proxy** et **HTTP-Proxy Port**.
7) Pour activer le service de **synchronisation CloudLink**, cochez la case située à côté de **Activer le service de synchronisation**.

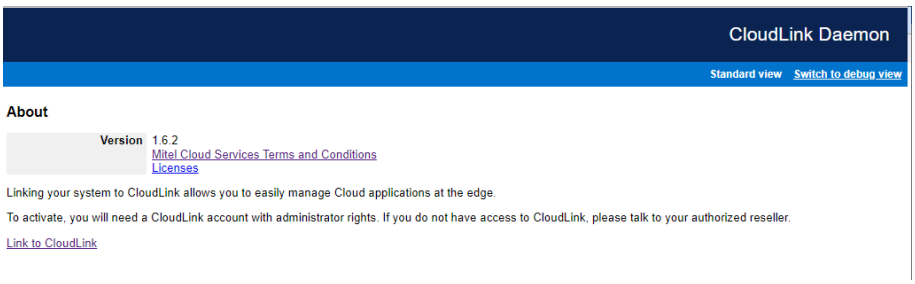
   Le service de **synchronisation CloudLink** synchronise les utilisateurs d'OpenScape Business avec CloudLink. Une fois activées, les applications cloud Mitel, telles que Mitel WX ou Workflow Studio, peuvent s'intégrer étroitement à OpenScape Business en accédant à la liste des utilisateurs pour le suivi des statuts, la numérotation par nom et d'autres cas d'utilisation similaires.
8) Cliquez sur **Appliquer** pour enregistrer vos paramètres.
9) Cliquez sur le bouton **CloudLink** pour ouvrir la fenêtre de l'interface Web de CloudLink Daemon.

22.11.2 Comment ouvrir l'interface web de CloudLink Daemon

L'interface web CloudLink Daemon permet de configurer et d'intégrer des systèmes en nuage et sur site, améliorant ainsi les capacités des applications de communication d'OpenScape Business.

Étape par étape

1) Cliquez sur **Lien vers CloudLink**.



   Vous serez transféré vers le portail CloudLink.
2) Indiquez votre **nom d'utilisateur** et **mot de passe** pour vous connecter au portail CloudLink.
3) Commencez une connexion.

22.11.3 Comment configurer l'interface web de CloudLink Daemon

Vous pouvez effectuer les actions suivantes en utilisant l'affichage standard ou l'affichage de débogage. Pour passer d'un affichage à l'autre, cliquez sur **Basculer vers l'affichage de débogage** ou **Basculer vers l'affichage standard**.

Étape par étape

1) Cliquez sur **Conditions générales de Mitel Cloud Services** pour afficher les conditions générales.
2) Cliquez sur **Licences** pour afficher les licences correspondantes.
3) Cliquez sur **Portail CloudLink**.

   Vous serez transféré vers le portail CloudLink.
4) Cliquez sur **Déconnecter de CloudLink** pour vous déconnecter du service.
5) Modifiez le jour et l'heure des mises à jour automatiques et cliquez sur **Replanifier**.
6) Cliquez sur **Pause** pour mettre en pause la prochaine mise à jour.
7) Cliquez sur **Démarrer tous les tunnels** et **Arrêter tous les tunnels** pour démarrer ou arrêter les tunnels configurés.
8) Cliquez sur **Démarrer** ou **Arrêter** pour démarrer ou arrêter l'accès à distance via le portail CloudLink Gateway.
9) Pour les cartes mères V3 OCCe avec NVMe et les systèmes OpenScape Business S, vous pouvez configurer la fonctionnalité de prise en charge des conteneurs en procédant comme suit :
   a) Cliquez sur **Activer la prise en charge des conteneurs**.
   b) Dans la fenêtre de confirmation qui s'affiche, cliquez sur **Oui**.
   c) Si nécessaire, cliquez sur **Redémarrer** ou **Désactiver la prise en charge des conteneurs** pour respectivement redémarrer ou arrêter le service.

22.11.4 Comment activer/configurer SIP Connector pour se connecter à Workflow Studio

Conditions préalables

La connexion Internet en amont est configurée (voir Comment configurer l'accès Internet via un routeur Internet externe).

Un compte CloudLink est requis et une connexion à CloudLink doit être établie (voir Comment configurer l'interface Web CloudLink Daemon).

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Services cloud** .
3) Cliquez sur **Modifier** à côté de **CloudLink Service**.
4) Cliquez sur la case à cocher à côté de **Activer le CloudLink Service**.
5) Si nécessaire, cochez la case située à côté de **Utiliser un proxy**.
6) Saisissez l'adresse IP et le port du proxy dans les champs **HTTP-Proxy** et **HTTP-Proxy Port** respectivement.
7) Saisissez vos identifiants dans les champs **Nom d'utilisateur** et **Mot de passe**.
8) Si nécessaire, cochez la case à côté de **Activer le connecteur SIP**.
   a) Sélectionnez une valeur dans la liste déroulante du champ **Nombre d'appels CloudLink simultanés**.
9) Cliquez sur **OK & Suivant**.
   Les jonctions sont ajoutées (aucune licence n'est nécessaire pour les jonctions). CloudLink est configuré et une connexion est établie.
10) Dans la fenêtre contextuelle, vous pouvez voir le statut de la connectivité. Cliquez sur **Terminer**.

22.12 Numéros de pilote CloudLink

Tout appel vers un numéro pilote CloudLink configuré est acheminé vers Wokflow Studio pour un traitement ultérieur.

Les numéros pilotes pour les services Cloudlink par système OpenScape Business seront limités à 60 par système OpenScape Business.

Les lignes réseau par système OpenScape Business sont limitées à une capacité totale de 250 lignes réseau.

De plus, les lignes réseau sont limitées par la bande passante amont définie dans l'assistant d'installation de base (128 Kbps par ligne).

L'interconnexion des lignes réseau Cloudlink occupera 1 des 10 routes ITSP/ Native-SIP dédiées dans un système OpenScape Business.

22.12.1 Comment configurer les numéros pilotes CloudLink

Conditions préalables

L'assistant CloudLink est configuré.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Services cloud** .
3) Cliquez sur **Modifier** à côté de **Numéros pilotes CloudLink**.
4) Cliquez sur **Ajouter** .
5) Dans la colonne **Numéros pilotes CloudLink**, saisissez les numéros nécessaires.
6) Pour chaque numéro, saisissez un nom dans la colonne **Nom d'affichage**.
7) Cliquez sur **OK & Suivant**.
8) Si nécessaire, cliquez sur **Supprimer** ou **Supprimer tout** pour supprimer une ou toutes les entrées, puis sur **OK** pour confirmer la suppression.
9) Cliquez sur **OK & Suivant** puis sur **Terminer**.

23 Taxation

La taxation englobe la collecte des données de connexion, des codes affaire,la transmission et l'affichage des données de connexion ainsi que le contrôle des coûts et les outils de taxation.

23.1 Données de connexion

Les données de connexion englobent la saisie des données de connexion ainsi que les codes affaire.

23.1.1 Saisie des données de connexion

Le système peut consigner les données de connexion des lignes utilisées.

Pour chaque communication terminée ou pour chaque communication entrante, un ticket de taxation est enregistré. Pour une nouvelle séquence temporelle d'une communication (par ex. due à un transfert ou renvoi à un autre abonné), un ticket de taxation propre est enregistré. Les connexions internes ne sont pas consignées.

Pour la saisie des données de connexion, l'administrateur peut activer les options suivantes :

- Saisie activée ou désactivée
- Durée de la connexion
- Montants en devise ou unités de tarification :

  La conversion des unités de tarification en montant en devise est réalisée à l'aide du facteur tarifaire configurable (monten en devise par unité de tarification).
- Format décimal

  Divise le montant en devise par 100 afin par ex. de représenter 6 Cent sous la forme 0,06
- Supprimer les quatre derniers chiffres des numéros de destination
- Consigner les connexions entrantes
- Appels sortants sans connexion :

  L'abonné reçoit ainsi par ex. la preuve de la non-réception de l'appel par l'abonné de destination (caractérisée dans le journal par la durée de communication 00:00:00). L'option vaut uniquement pour les liaisons RNIS et pour tous les abonnés.
- Protocole de connexion

  Protocole dès le début de l'appel
- Consigner MSN
- Edition du numéro LCR sortant ou du numéro composé entrant
  - sortant:

    numéro réellement envoyé au RTC par LCR
  - entrant :

    numéro interne composé à l'origine

Si des coûts de connexion sont générés déjà avant l'établissement de la connexion (comme en Autriche)ceux-ci sont consignés, indépendamment de l'activation de la consignation des appels sortants sans connexion.

Le système ne prend en compte les communications par lignes QSIG que si un indicatif de ligne est configuré pour celles-ci.

Il n'y a pas de consignation dans les cas suivants :

- annulation prématurée de la tentative d'appel
- connexions non autorisées (LCR, listes des numéros interdits).

Concepts associés

Codes affaire à la page 1151

23.1.1.1 Comment activer ou désactiver la saisie des données de connexion

Avec l'assistant **Enregistrement des données de taxation** vous pouvez activer la saisie des données de connexion.

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Enregistrement des données de taxation**.
4) Sélectionnez une des possibilités suivantes :
   - Pour activer la saisie des données de connexion, cochez la case **Activer la taxation**.
   - Pour désactiver la saisie des données de connexion, décochez la case **Activer la taxation**.
5) Cliquez sur **OK&Suivant** puis sur **Terminer**.

23.1.1.2 Comment activer ou désactiver l'enregistrement des communications

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.

4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Durée de la sonnerie**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Durée de la sonnerie**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.1.3 Comment configurer la création de journal pour les montants en devise ou les unités de tarification

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous voulez que le système consigne les montants en argent, cochez la case **Editer montant à la place des unités**.
   - Si vous voulez que le système consigne les montants en argent, cochez la case **Editer montant à la place des unités**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.1.4 Comment configurer le facteur de taxation, la devise et la précision

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxation** > **Taxes - Facteurs**.
4) Entrez pour chaque faisceau souhaité dans les champs **Prix de l'unité** et **Multipl. RNIS** les valeurs correspondantes.
5) Dans **Devise** sur la partie inférieure du formulaire la valeur correspondante.

6) Pour chaque faisceau concerné avec protocole QSIG, en accord avec le système de communication associé, sélectionnez une des trois possibilités suivantes :
   - Si des montants en devise doivent être reçus et envoyés, cochez la case **Montant devise**.
   - Si des unités de tarification doivent être reçues et envoyées, décochez la case **Montant devise**.
7) Dans chaque avec faisceau, avec protocole QSIG, qui reçoit et envoie des unités de tarification, entrez un espace dans **Devise**.
8) Dans la liste déroulante **Précision**, sélectionnez l'entrée **Rien après la virgule**, **1 chiffre après la virgule**, **2 chiffres après la virgule**, **3 chiffres après la virgule** ou **Via impulsion taxation**.
9) Cliquez sur **Appliquer** puis sur **OK**.

23.1.1.5 Comment activer ou désactiver la consignation des quatre derniers chiffres

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Masquage des 4 derniers chiffres**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Masquage des 4 derniers chiffres**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.1.6 Comment activer ou désactiver l'enregistrement des appels sortants sans connexion

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.

4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Appels sortants sans connexion**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Appels sortants sans connexion**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.1.7 Comment activer ou désactiver l'enregistrement des communications entrantes

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Appels entrants**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Appels entrants**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.1.8 Comment activer ou désactiver le protocole de communication

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Impression d'un ticket arrivé**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Impression d'un ticket arrivé**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.1.9 Comment activer ou désactiver l'édition des MSN

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Edition des MSN/SDA**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Edition des MSN/SDA**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.1.10 Comment activer ou désactiver le format décimal

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Format décimal**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Format décimal**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.2 Codes affaire

Les codes Affaire (PKZ) permettent d'affecter les données et les coûts de communication en fonction des projets. Pour cela, le système consigne dans les données de connexion correspondantes les codes Affaire entrés au téléphone par les abonnés.

Le code affaire est utilisé en association avec l'enregistrement des données de taxation et il est disponible pour chaque abonné.

L'abonné peut entrer un code affaire sur le téléphone, avant le début de la numérotation ou après la fin de la numérotation. La numérotation à partir d'un client n'est pas possible lorsque le code affaire (CA) est activé.

Un CA entré au cours d'une conférence avec des abonnés externes est attribué à toutes les communications/lignes participantes.

L'administrateur peut indiquer si un code affaire peut être enregistré pour la répétition de la numérotation.

L'annuaire personnel peut enregistrer en commun dans une entrée l'indicatif pour la fonctionnalité Code affaire + un code affaire + un numéro.

Procédure d'entrée du code affaire

L'administrateur définit la procédure d'entrée du code affaire dans le plan de numérotation LCR :

- Forcée

  Le code affaire doit être entré avant le début de la communication (avant ou après la prise d'un faisceau).
- volontaire

  Le code affaire peut être entré librement avant le début de la communication. Sur les téléphones client IP, l'entrée est également possible en cours de communication, même entrante.

Procédure de contrôle du code affaire

Le système peut vérifier la validité d'un code d'affaire entré selon les modalités suivantes.

- Contrôle de liste

  Seuls les codes affaire prédéfinis sont valides. Après l'entrée d'un code affaire valide, l'abonné peut continuer à numéroter immédiatement. Le système présente un CA non valide. Sur l'écran apparaît "Entrée erronée" et une tonalité d'acquittement négative retentit.
- contrôle du nombre de digits

  Sont valides tous les codes affaire en théorie possibles avec le nombre de caractères paramétré. Après l'entrée d'un code affaire valide par l'abonné, il est possible de continuer à numéroter immédiatement.
- sans contrôle

  La validité du code affaire n'est pas contrôlée. L'abonné doit séparer les codes affaire de moins de 11 caractères des autres chiffres composés en tant "#". Avec les terminaux RNIS, cette variante nécessite toujours des codes affaire de 11 caractères, sinon la numérotation n'est pas effectuée.

Si l'abonné constate pendant une communication que le code affaire affecté à la communication n'est pas correct, il peut en entrer un autre. Le système remplace alors le code affaire actuellement paramétré. La saisie des données de connexion crée après chaque segement un jeu de données de connexion. Donc, les parties de communication déjà terminées sont identifiées par l'ancien code affaire.

Concepts associés

Saisie des données de connexion à la page 1146

23.1.2.1 Comment configurer le code Affaire

L'Assistant **Enregistrement des données de taxation** permet de configurer les codes affaire.

Conditions préalables

Vous êtes connecté à WBM.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour démarrer l'Assistant **Enregistrement des données de taxation**.
4) Entrez dans la page **Codes affaires**, dans les champs de saisie, les codes affaire de la façon décrite dans l'Assistant.
5) Cliquez sur **OK&Suivant** puis sur **Terminer**.

23.1.2.2 Comment configurer la procédure de contrôle des codes affaire

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Codes affaire**.
4) Sélectionnez dans la ligne de la liste de codes affaire, dans la liste déroulante **Procédure de contrôle**, l'entrée voulue : **aucun contrôle**, **contrôle par rapport à la liste** ou **contrôle du nombre de positions**.
   a) Sélectionnez éventuellement dans la liste déroulante **Nb de digits à contrôler** la valeur souhaitée.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.1.2.3 Comment activer ou désactiver la répétition de la numérotation avec code affaire

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.

3) Dans l'arborescence de menu, cliquez sur **Configur. de base** > **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Rép. auto avec code affaire**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Rép. auto avec code affaire**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.2 Affichage et tranmission des données de connexion

L'affichage et la tranmission des données de connexion englobe différentes possibilités d'affichage à l'écran des téléphones système et de transmission des données.

23.2.1 Transfert des montants (non disponible aux Etats-Unis)

Le système de communication peut afficher sur l'écran du téléphone le montant transmis par l'opérateur du réseau pour la liaison externe actuelle.

L'opérateur du réseau doit supporter la transmission des montants pour la fonctionnalité Advice Of Charge (AOC-D ou AOC-S). Le système cumule les montants des unités de tarification correspondantes.

Le montant peut en général être transmis aux périodes suivantes :

- au début de la communication et le cas échéant en cours de communication (AOC-S)
- En cours de communication (AOC-D)

Par le paramètre Précision, l'administrateur peut éviter les inexactitudes dans l'enregistrement des données de connexion. La précision de calcul détermine

- le nombre de chiffres après la virgule pour l'analyse des données de communication (montant le plus faible)
- le total maximum des montants en argent cumulés.

La précision de calcul réglée doit au moins être celle de RNIS. Si les trois chiffres après la virgule maximum possibles ne suffisent pas, il y arrondissement automatique. La précision de calcul peut accepter les valeurs suivantes :

Précision de calcul	Montant le plus faible	Montant le plus élevé
Rien après la virgule	1	environ 4,3 milliards
1 après la virgule	0,1	environ 430 millions
2 chiffres après la virgule (par ex. pour Euro)	0,01	environ 43 millions
3 chiffres après la virgule (par ex. pour livre sterling anglaise)	0,001	environ 4,3 millions

23.2.1.1 Comment configurer la transmission des montants

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxation** > **Taxes - Facteurs**.
4) Par faisceau souhaité, sélectionnez dans la liste déroulante **Avis de taxation** l'entrée **Pendant la connexion**, **A la fin de la connexion**, **durant / à la fin de la connexion** ou **Aucune taxation**.
5) Sélectionnez dans la liste déroulante **Précision** sur la partie inférieure du formulaire le nombre de chiffres après la virgule à prendre en compte.
6) Cliquez sur **Appliquer** puis sur **OK**.

23.2.2 Affichage des coûts de connexion sur le téléphone

Le système peut afficher à l'écran du téléphone le montant en argent correspondant au coût d'une connexion externe en cours.

Le système cumule les montants des unités de tarification correspondantes. Le montant en argent est calculé à partir des unités de tarification et du facteur tarifaire configuré. Le fournisseur de services doit supporter la fonctionnalité Advice Of Charge (AOC).

L'information concernant les coûts de connexion peut être tranmise aux moments indiqués ci-après.

- Au début de la communication et le cas échéant en cours de communication (AOC-S)
- En cours de communication (AOC-D)
- A la fin de la communication (AOC-E)

A la fin de la communication, l'écran affiche les taxes définitives pour cette communication pendant environ 5 secondes dans la mesure où l'abonné ne démarre pas une autre action.

Lors du Va-et-vient, il est toujours indiqué les coûts de connexion de la connexion actuelle.

Si le transfert avant réponse ne réussit pas, le montant total est affiche et calculé.

Un abonné auquel une communication est transférée reçoit pendant la communication uniquement les taxes à partir de cet instant.

23.2.3 Affichage de la durée de connexion sur le téléphone

Le système peut afficher la durée des communications externes sortantes et entrantes sur l'écran du téléphone.

Le format est HH:MM:SS.

Si l'affichage de la durée de la connexion est désactivé, l'écran du téléphone affiche à la place l'information concernant les coûts de connexion du RTC. Si aucune information de taxation n'est disponible, l'écran affiche le numéro de l'interlocuteur, dans la mesure où il est connu.

23.2.3.1 Comment activer ou désactiver l'affichage de durée de la communication

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Système** > **Ecran**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la fonction, cochez la case **Affichage de la durée de communication**.
   - Si vous souhaitez désactiver la fonction, décochez la case **Affichage de la durée de communication**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.2.4 Transmission des données de connexion

Le système peut transmettre les données de connexion dans un fichier avec HTTPS.

Vous pouvez évaluer le fichier transmis avec un programme adapté.

L'édition en continu des données de connexion est exclusivement possible via CSTA.

Pour les données de connexion, l'administrateur peut choisir parmi les formats ci-après (ASCII 8-bits).

- Format comprimé
- Format non comprimé

Format comprimé, par défaut

Un jeu de données de connexion au format comprimé contient les champs suivants, séparés par | ; CRLF termine chaque jeu de données de connexion :

Position du champ	Longueu	Description
1	8	Date à la fin de la communication
2	8	Heure à la fin de la communication
3	3	Numéro de ligne réseau occupé

Position du champ	Longueu	Description
4	16	Numéro interne de l'abonné
5	8	Durée de sonnerie de la connexion entrante
6	8	Durée de la connexion
7	25 maxi.	numéro externe sélectionné ou reçu
8	11	Unité de tarification/Montant
9	2	Information supplémentaire, (par ex. entrant, sortant, connexion transférée, conférence, DISA, coûts pour l'établissement de la liaison)
10	11 maxi.	Code affaire
11	11 maxi.	uniquement pour un raccordement multiposte : MSN utilisé
12	6	Code d'accès LCR, indicatif réseau
13	2	Route LCR utilisée (règle de numérotation, 2 caractères)
14	25	Numéro d'appel sélectionné ou reçu (option)

Exemples de données de connexion :

- connexion sortante :

```
13.02.13|14:18:02|201|33388|00:02|00:00:07|0123456789||
1||||||
```

- Connexion entrante :

```
13.02.13|14:28:02|202|33388|00:05|00:00:12|0123456789||
1|||||
```

Format comprimé, spécifique des Etats-Unis

Un jeu de données de connexion au format comprimé contient les champs suivants, séparés par | ; CRLF termine chaque jeu de données de connexion :

Position du champ	Longueu	Description
1	8	Date à la fin de la communication
2	8	Heure à la fin de la communication
3	3	Numéro de ligne réseau occupé
4	16	Numéro interne de l'abonné
5	8	Durée de sonnerie de la connexion entrante
6	8	Durée de la connexion
7	25 maxi.	numéro externe sélectionné ou reçu
8	11	Unité de tarification/Montant

Position du champ	Longueu	Description
9	2	Information supplémentaire, (par ex. entrant, sortant, connexion transférée, conférence, DISA, coûts pour l'établissement de la liaison)
10	11 maxi.	Code affaire
11	11 maxi.	uniquement pour un raccordement multiposte : MSN utilisé
12	6	Code d'accès LCR, indicatif réseau
13	2	Route LCR utilisée (règle de numérotation, 2 caractères)
14	2	PRI Nodal Service
15	1	PRI WATS band
16	3	PRI CIC
17	25	Numéro d'appel sélectionné ou reçu (option)

Remarque : Dans les clés de registre *HKEY_LOCAL_MACHINE\SOFTWARE* pour *Outil comptable*, la valeur de **DateFormat DWORD** doit être réglée sur 1 pour le format de date Amérique du Nord (MM.DD.YY). La valeur par défaut est 0 et correspond au format de date Europe/Amérique latine (DD.MM.YY).

Remarque : Les enregistrements de données du gestionnaire de comptabilité au format compressé sont séparés par le délimiteur |. Cela ne peut être configuré que par Manager E.

Format non comprimé

Le format non comprimé convient aux impressions. De plus, il est édité une ligne d'en-tête et un saut de page. Un jeu de données de connexion au format comprimé comprend les champs suivants, séparés par | :

Position du champ	Position du caractère, longueur	Description
1	1-8 (8)	Date à la fin de la communication: TT.MM.JJ (JJ = jour : plage de valeurs 01 ... 31, MM = mois : plage de valeurs 01 ... 12, AA = année : plage de valeurs 00 ... 99)
2	9-16 (8)	Heure de fin du tronçon de communication ou d'un appel entrant non répondu : hh:mm:ss (hh = heures : plage de valeurs 00 ... 23, mm = minutes : plage de valeurs 00 ... 59, ss = secondes : plage de valeurs 00 ... 59)

Position du champ	Position du caractère, longueur	Description
3	17-19 (3)	Ligne : numéro de ligne Plage de valeurs 1 ... 250
4	20-35 (16)	Abonnés : numéro interne de l'abonné Lorsque les appels ne sont pas interrogés, il est toujours indiqué le dernier abonné appelé (par ex. groupe de recherche, renvoi d'appel, renvoi temporisé). Dans un appel de groupe, il s'agit du dernier abonné inscrit. Lorsque les appels sont interrogés, il est indiqué l'abonné qui a accepté l'appel. Un préfixe RNR programmé (seulement en cas de mise en réseau) n'est pas édité. Si la numérotation interne a été convertie en plan de numérotation de 7 positions maxi., il est alors édité le numéro de téléphone converti. Le numéro interne d'abonné peut être précédé par un numéro de noeud de 7 positions maxi. Si la somme Numéro de noeud plus Numéro d'abonné est supérieure à 7, seuls les 7 derniers chiffres du numéro sont édités.
5	36-40 (5)	Donnée d'appel d'une connexion entrante : mm:ss (mm = minutes: plage de valeurs 00 ... 59, ss = secondes: plage de valeurs 00 ... 59) L'affichage se produit pour tous les appels entrants si l'édition de la "durée d'appel" est configurée dans le système. En cas de débordement du compteur (durée > 59:59), il est édité "59:59". Cela peut par ex. se produire à un changement de date ou d'heure durant le fonctionnement de l'installation. En cas d'appel entrant adressé à un abonné occupé, la durée de l'appel a pour valeur "00:00".
6	41-48 (8)	Durée de la connexion ou de la section de connexion : hh:mm:ss (hh = heures : plage de valeurs 00 ... 23, mm = minutes : plage de valeurs 00 ... 59, ss = secondes : plage de valeurs 00 ... 59) Si aucune communication n'a été établie à la fin d'un appel entrant, des espace vides sont édités. En cas de débordement du compteur (durée > 23:59:59), il est édité "23:59:59".
7	49-73 (25)	Numéros sélectionnée ou, si disponible, numéros externes reçus : nnnnnnnnnnnnnnnnnnnnnnnnn (n = caractère sélectionné ou reçu : plage de valeurs 0 ... 9, *, #, ?) L'édition se produit pour les appels entrants et sortants, si existants. Pour les appels sortants, il est affiché le numéro composé ou, si disponible, le numéro transmis par COLP. Lorsque la fonction protection des données est activée, les 4 derniers caractères composés sont remplacés par ""????". S'il n'y a aucune information sur le numéro de téléphone, des espaces vides sont édités.

Position du champ	Position du caractère, longueur	Description
8	74-84 (11)	Unités de tarification pour une section de connexion : zzzzzzzzzzz (z = Chiffre : plage de valeurs 0 ... 9) Il peut être opéré une sélection entre unités de taxation et montants de taxation. La conversion des unités de taxation en montants se fait avec le facteur de taxation qui est défini comme montant (y compris une majoration nécessaire) par unité de tarification. Pour le paramétrage du facteur de taxation, on applique les règles ci-après. • avec précision de calcul : facteur de taxation = 100% majoration nécessaire évent. • sans précision de calcul : facteur de taxation = montant/unité + majoration nécessaire évent. En fonction de la précision de calcul, la saisie des coûts de communication est effectuée avec ou sans majoration. L'édition se produit toujours lorsque des taxes sont dues pour le tronçon de communication (par ex. également pour les communications transférées).

Position du champ	Position du caractère, longueur	Description
9	85-86 (2)	Elément d'information : information supplémentaire Plage de valeurs 0 ... 9 Signification : • 1 = liaison entrante (Voix / appel audio 3.1 kHz) • 2 = liaison sortante (Voix / appel audio 3.1 kHz) • 3 = liaison entrante (autres services) • 4 = liaison sortante (autres services) • 5 = liaison entrante, transférée • 6 = liaison sortante, transférée • 7 = conférence int/ext/ext avec liaison entrante / transit par transfert vers l'extérieur • 8 = conférence avec liaison sortante / transit par transfert vers l'extérieur • 9 = liaison sortante via renvoi d'appel vers destination externe • 0 = Info Appel (liste des appelants), est sorti immédiatement lors de la réception d'un appel entrant (il est possible de verrouiller cette sortie). Ceci peut servir, par exemple, pour une recherche de base de données d'un PC. Lorsque plusieurs postes sont appelés, une ligne distincte est éditée pour chacun des participants (sans informations sur la durée d'appel, la durée de la communication ou le coût de l'appel). • +10 = écart comme code pour les appels sur la liste noire • +20 = écart en tant qu'identification pour les coûts de l'établissement de la connexion (sans durée de la connexion) • +30 = écart en tant qu'identification pour un article de données consécutif pour – Durée de la connexion > 24 h. – sections de communication associées avec même numéro de ligne / d'abonné (par ex. après transfert d'une communication, après annulation d'une conférence). • +40 = écart pour un article de données avec identification de transit (par un poste de sous-installation). Peut se produire en combinaison avec écart +30. • +50 = écart identifiant les connexions DISA • +70 = combinaison des écarts +30 et +40
10	87-97 (11)	Code affaire CA entré pour cette communication par l'utilisateur : pppppppppp (a = chiffre ACCT : plage de valeur 0 ... 9) Les chiffres manquants sont remplacés par des espacements.
11	98-108 (11)	MSN utilisé : mmmmmmmmmm (m = chiffres du MSN : plage de valeurs 0 ... 9) L'affichage a lieu si l'abonné a programmé une touche MSN. Pour les communications sortantes d'un abonné MULAP, il est fourni le numéro du MULAP occupé. Les chiffres manquants sont remplacés par des espacements.

Position du champ	Position du caractère, longueur	Description
12	109-113 (5)	Indicatif de prise de ligne utilisé, code d'accès : bbbbb (b = chiffre de l'indicatif de prise de ligne : plage de valeurs 0 ... 9)
13	114-115 (2)	Route LCR utilisée : rr (r = chiffres de la route sélectionnée : plage de valeurs 0 ... 9)

Déroulement de la communication

La transmission des données de connexion peut être demandé (Download Request), à cela le système répond en conséquence éléchargement (Download Response).

Ensuite, il est possible de demander l'effacement des données de connexion (Delete Request) ; le système réagit en conséquence (Download Response).

Download Request - Définition

Elément	Sommaire
En-tête HTTP	Request method = GET
URL	https://<adresse IP du système>/management/portlet
Paramètres	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=get
	username=<nom de l'utilisateur>
	password=<mot de passe>

Remarque : Lorsque vous accédez aux données de taxation par l'interface référencée, les restrictions de requête HTTP GET s'appliquent. Les caractères spéciaux suivants ne sont pas autorisés comme mots de passe, lorsque que l'on essaie d'obtenir des données via une demande URL :

:/?#[]@ !$&'()*+,;=

Exemple:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Download Response - Definition

Elément	Sommaire
En-tête HTTP	ContentType = "text/plain"
Paramètres	attachment filename = "<charging file>"
	data=<content of the charging file>

Response-Code	Signification
sc_OK(200)	Succès
sc_BAD_REQUEST(400)	paramètres manquants in Request
sc_UNAUTHORIZED(401)	Echec de la connexion ou nom de l'utilisateur ou mot de passe erroné
SC_INTERNAL_SERVER_ERROR(500)	Erreur interne

Delete Request - Definition

Elément	Sommaire
En-tête HTTP	Request method = POST
URL	https://<adresse IP du système>/management/portlet
Paramètres	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=delete
	username=<nom de l'utilisateur>
	password=<mot de passe>

Exemple:

```
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	Signification
sc_OK(200)	Succès
sc_BAD_REQUEST(400)	paramètres manquants in Request
sc_UNAUTHORIZED(401)	Echec de la connexion ou nom de l'utilisateur ou mot de passe erroné
SC_INTERNAL_SERVER_ERROR(500)	Erreur interne

Concepts associés

Outils de taxation à la page 1166

23.2.4.1 Comment sélectionner le format

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez le format comprimé, cochez la case **Format d'édition comprimé**.
   - Si vous souhaitez le format non comprimé, décochez la case **Format d'édition comprimé**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.2.4.2 Comment activer ou désactiver la transmission de données de taxation via HTTPS

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Taxes** > **Taxes - Format d'édition**.
4) Dans la liste déroulante **Sortie**, sélectionner l'une des possibilités suivantes :
   - Si vous souhaitez activer la fonctionnalité, sélectionnez l'entrée **HTTPS**.
   - Si vous voulez désactiver la fonctionnalité, sélectionnez l'entrée **None**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.3 Contrôle des coûts

Le contrôle des coûts propose les fonctionnalités Remarque sur les voies de communication onéreuses et Protection contre une falsification des taxes.

23.3.1 Remarque sur les voies de communication onéreuses

Si une destination d'appel n'est pas actuellement joignable par la voie de communication la plus économique, le téléphone peut indiquer à l'abonné une voie de communication onéreuse.

L'abonné peut alors décider s'il souhaite passer la communication malgré la voie de communication onéreuse à ce moment-là. L'indication peut se faire de deux façons :

- Texte affiché
- Tonalité
- Texte affiché et tonalité

Le système signale la voie de communication à prix élevé si l'avertissement correspondant est configuré dans la table de routage et s'il n'utilise pas le faisceau de l'index 1 de la table de routage.

La remarque sur l'écran s'affiche uniquement si aucun nom n'est configuré pour la règle de numérotation correspondante. Si un nom est configuré, celui-ci s'affiche.

23.3.1.1 Comment configurer l'avertissement relatif à une voie de communication onéreuse

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **LCR**.
3) Dans l'arborescence du menu, cliquez sur **Routage** > **LCR** > **Tables de routage** et sur la table de routage concernée.
4) Sélectionnez pour chaque itinéraire coûteux (Colonne **Faisceau**) dans la liste déroulante **Avertissement** l'entrée désirée : **Son**, **Ecran** ou **Ecran + Son**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.3.2 Protection contre les fraudes de taxation

Le système peut surveiller les communication pour identifier une falsification des taxes (Toll Fraud Monitoring). Cela concerne les communications qui arrivent par une ligne réseau et repartent par une ligne réseau.

Le premier abonné signale le dépassement de la durée de communication paramétrée et permet ainsi de couper la communication en cas de besoin. En tant qu'administrateur, vous pouvez indiquer si une telle connexion doit être signalée et si c'est le cas au bout de combien de temps.

23.3.2.1 Comment activer ou désactiver la Protection contre une falsification des taxes

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configuration de base** > **Système** > **Temporisations**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la Protection contre une falsification des taxes, sélectionnez dans **Compteur pour contrôle d'abus de taxation**, liste déroulante **Base**, l'entrée souhaitée et entrez dans le champ **Facteur** une valeur différente de 255. **Base** * **Facteur** indique la durée de connexion à l'issue de laquelle une connexion potentiellement frauduleuse est signalée.
   - Si vous souhaitez désactiver la Protection contre une falsification des taxes entrez 255 dans **Compteur pour contrôle d'abus de taxation**, champ **Facteur**.
5) Cliquez sur **Appliquer** puis sur **OK**.

23.4 Outils de taxation

Les outils de taxation (accounting tools) sont proposés par le gestionnaire de taxation et par Teledata Office.

Concepts associés

Centre de service – Documents à la page 99
Transmission des données de connexion à la page 1156

23.4.1 Accounting Manager

Accounting Manager est une application Windows permettant d'interroger les données de connexion via HTTPS en vue d'une évaluation sous forme de tableaux et de graphiques.

Accounting Manager contient sa propre documentation. Accounting Manager appelle les données de connexion des différents noeuds de réseau. Vous pouvez aussi utiliser Accounting Manager pour tester l'interface des données de connexion. Vous pouvez télécharger le gestionnaire de taxation (Accounting Manager) dans le **Centre de service** de la WBM. Le gestionnaire de taxation nécessite des droits d'administration locaux et l'activation de TLS 1.2 dans Microsoft Internet Explorateur.

23.4.2 Teledata Office

Teledata Office est une application Windows pour l'évaluation des données de connexion.

24 Entretien

Le système offre plusieurs options de maintenance. Cela comprend la modification des paramètres de téléphonie, la sauvegarde et la restauration des données de configuration, la mise à jour du logiciel avec des mises à jour et des mises à niveau, ainsi que le redémarrage/rechargement des fonctions. De plus, des fonctions appropriées pour l'identification, la surveillance et la maintenance de l'état sont disponibles. L'accès à distance au système est possible via différents services d'accès à distance.

24.1 Configuration téléphonique

Le système de communication offre différentes possibilités de configuration pour la téléphonie, par ex. date et heure, SNTP, affichage écran et musique d'attente individualisés pour chaque client.

24.1.1 Date et heure

Le système de communication comprend une horloge système, avec date et heure. myPortal for Desktop ainsi que chaque écran d'un terminal affiche l'heure système.

Vous pouvez définir ou actualiser l'heure système de la manière suivante.

- A l'aide d'un serveur de temps via SNTP
- A l'aide d'une ligne réseau RNIS par un appel sortant
- Par un réglage manuel

Une fois le serveur SNTP activé, aucun réglage individuel de l'heure système n'est plus possible.

Si le serveur SNTP est non joignable et que les téléphones HFA utilisent une autre source de temps que le système, l'heure affichée peut différer de l'heure système.

L'heure système paramétrée manuellement après la mise en route de l'installation est toujours remplacée par l'information de temps RNIS lors de la première communication sortante RNIS, à condition que l'opérateur du réseau fournisse cette information. Lorsque l'installation fonctionne, si la différence entre l'heure système paramétrée manuellement et l'information de temps RNIS est située entre 2 et 70 minutes, l'information de temps RNIS est reprise. Sinon, l'heure système réglée manuellement est conservée.

Pour la représentation de la date sur l'écran du téléphone, l'administrateur peut sélectionner un des formats suivants. Le format dépend également du type de téléphone :

Format de date	OpenStage	optiPoint 410, optiPoint 420
Europe	Ma 20.11.07	20. NOV 07
Etats-Unis	Ma 11/20/07	Ma NOV 20.07
International1	Ma 20.11.07	MA 20 NOV 07
International2	Ma 20.11.07	MA 20.11.07

Si vous paramétrez par erreur une date avant 2007, vous ne pouvez pas ensuite recourir à WBM. Cela n'est possible qu'après un redémarrage qui a replacé la date sur 01.01.2007.

24.1.1.1 Comment paramétrer manuellement la date et l'heure

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Effectuez les étapes suivantes lorsquele système n'a pas la date et l'heure et ne peut pas les obenir via une ligne réseau numérique ou SNTP.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configur. de base**.
3) Dans l'arborescence de menu, cliquez sur **Configuration de base** > **Date et heure** > **Date et heure**.
4) Entrez la **Date et l'heure**.
5) Cliquez sur **Appliquer**.
6) Cliquez sur **Déconnexion**
7) Déconnectez-vous de la WBM et reconnectez-vous.

24.1.1.2 Comment paramétrer le fuseau horaire

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configur. de base**.
3) Dans l'arborescence de menu, cliquez sur **Configuration de base** > **Date et heure** > **Paramètres de fuseau horaire**.
4) Dans la liste déroulante **Fuseau horaire**, sélectionnez le fuseau horaire.
5) Cliquez sur **Appliquer**.
6) Déconnectez-vous de la WBM et reconnectez-vous.

24.1.1.3 Comment configurer le format de la date

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie** > **Configur. de base**.
3) Cliquez dans l'arborescence de menu sur **Configur. de base** > **Système** > **Ecran**.
4) Dans la liste déroulante **Format de la date**, sélectionnez le format de la date.
5) Cliquez sur **Appliquer**.

24.1.2 SNTP

À l'aide de SNTP, vous pouvez synchroniser la date et l'heure de vos systèmes sur l'ensemble du réseau avec les serveurs de temps NTP.

SNTP (Simple Network Time Protocol) est une version simplifiée de NTP (Network Time Protocol), une norme de synchronisation de la date et de l'heure via des réseaux de communication de type paquets. Pour synchroniser la date et l'heure, votre système a besoin d'une liaison avec un serveur NTP. Celui-ci peut se trouver sur votre réseau local ou sur Internet. Sur Internet, il existe des serveurs NTP d'accès libre ; vous pouvez sélectionner l'un d'entre eux se trouvant dans votre fuseau horaire. Tenez compte des conditions d'utilisation du serveur correspondant et demandez les autorisations lorsque cela est nécessaire.

24.1.2.1 Comment reprendre la date et l'heure d'un serveur SNTP

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence de menu, cliquez sur **Configuration de base** > **Date et heure** > **Paramètres SNTP**.
4) Entrez **Adresse IP/Nom DNS du serveur temporel externe**, par ex. `0.fr.pool.ntp.org`.
5) Sélectionnez dans la liste déroulante **Etat de fonctionnement actuel du serveur SNTP** l'entrée **Activé**.
6) Dans la liste déroulante **Intervalle d'interrogation pour le serveur temporel externe**, sélectionnez l'intervalle de temps souhaité pour la récupération de la date de l'heure à partir du serveur SNTP.
7) Cliquez sur **Appliquer**.
8) Déconnectez-vous de la WBM et reconnectez-vous.

24.1.3 Logos Téléphone

Les téléphones système avec écran peuvent afficher un logo individualisé pour le client en arrière plan de l'interface téléphonie.

En tant qu'administrateur, vous pouvez importer, attribuer ou supprimer dans le système des logos téléphone pour les téléphones système avec écran. Les différents types de téléphones système peuvent utiliser des logos de téléphone différents.

Concepts associés

Mise à jour des téléphones système à la page 1199

24.1.3.1 Comment charger un logo téléphone dans le système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Le fichier image avec le logo du téléphone remplit les conditions suivantes.

Téléphone	Format	Couleur
OpenStage 40	112 x 32, BMP	monochrome
OpenStage 60 OpenStage 80	240 x 71, JPEG	monochrome ou couleur
OpenScape Desk Phone CP 400 OpenScape Desk Phone CP 400T/405T	112 x 32, BMP	monochrome
OpenScape Desk Phone CP 600/700/700X OpenScape Desk Phone CP 710	220 x 70, PNG	24 bits avec alpha (transparence)
OpenScape Desk Phone CP 600E	220 x 70, PNG	24 bits avec alpha (transparence) ou 256 niveaux de gris avec alpha

Vous avez accès au fichier image avec le logo téléphone dans le système de fichiers du PC d'administration.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Cliquez sur **Maintenance** > **Image logicielle** dans l'arbre de navigation.
3) Dans l'arborescence du menu, double-cliquez sur **Image du téléphone** > **Charger**.
4) Cliquez sur **Parcourir** pour sélectionner le fichier image correspondant.
5) Cliquez sur **Charger**.

24.1.3.2 Comment distribuer un logo téléphone aux téléphones système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Image logicielle**.
3) Dans l'arborescence du menu, double-cliquez sur **Image du téléphone** > **Distribuer**.
4) Dans la ligne du logo de téléphone à distribuer, cochez **Distribuer**.
5) Dans la liste déroulante **Distribuer aux points de travail des types suivants**, sélectionnez le type de téléphone système souhaité.
6) Cliquez sur **Appliquer**.

24.1.3.3 Comment effacer le logo Téléphone

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Vous avez accès au fichier image avec le logo téléphone dans le système de fichiers du PC d'administration.

Pour effacer un logo téléphone du système de communication, effectuez les opérations suivantes.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Image logicielle**.
3) Dans l'arborescence du menu, double-cliquez sur **Image du téléphone** > **Charger**.
4) Dans la ligne du logo téléphone à effacer, cochez **Effacer**.
5) Si vous souhaitez effacer d'autres logos téléphone, répétez l'opération précédente.
6) Cliquez sur **Effacer**. Tous les logos téléphone sélectionnés sont effacés du système de communication.

24.1.4 Affichage spécifique du client

L'affichage spécifique du client permet d'afficher par ex. le nom de la société à l'écran des téléphones système lorsqu'ils sont au repos.

La seule partie modifiable est la partie droite (18 caractères maximum) de la deuxième ligne de l'afficheur, dans laquelle "OpenScape" s'affiche par défaut.

Le texte est aligné à gauche avec la date, dans la mesure où la longueur du texte l'autorise.

```
16:30       VE 29 FÉV 08         123456 Hôtel de la Poste >
```

24.1.4.1 Comment modifier l'affichage du client (nom du système)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configur. de base** > **Passerelle**.
4) Dans le champ **Nom du système**, entrez la valeur souhaitée.

   Remarque : Utilisez uniquement les caractères A-Z, a-Z et 0-9.

5) Cliquez sur **Appliquer** puis sur **OK**.

24.1.5 Texte en plusieurs langues

Il est possible de choisir pour l'ensemble du système comme individuellement la langue des affichages écran.

Langues disponibles : Chinois, Danois, Français, Anglais, Estonien, Finlandais, Français, Grec, Italien, Catalan, Letton, Lituanien, Néerlandais, Norvégien, Polonais, Portugais, Russe, Suédois, Serbocroate, Slovaque, Slovène, Espagnol, Allemand (Telekom), Tchèque, Turc, Hongrois, Anglais (US), Serbe, Bulgare, Roumain et Macédonien.

Le paramétrage de la langue en général est effectué lors de la mise en route du système avec l'initialisation du pays.

Concepts associés

Configuration des abonnés à la page 403

Tâches associées

Comment configurer les abonnés IP et SIP à la page 169

24.1.6 Menus flexibles

Les menus flexibles permettent l'adaptation spécifique pour chaque client des options de menu sur l'écran des téléphones système.

En tant qu'administrateur vous pouvez afficher ou masquer individuellement les options de menu.

24.1.6.1 Comment modifier les menus flexibles

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, cliquez sur **Configur. de base** > **Système** > **Menus flexibles**.
4) Pour modifier la **Liste de désactivation**, procédez comme indiqué ci-après :
   - Pour masquer une option de menu, activez sa case à cocher.
   - Pour afficher une option de menu, désactivez sa case à cocher.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.1.7 Musique en attente

Le système de communication peut diffuser de la musique d'attente (MOH) aux abonnés en attente pendant les opérations de commutation. Les appelants entendent le message d'attente pendant que leur téléphone est en attente, en stationnement ou en transfert. Cela s'applique également aux appelants placés dans la file d'attente de distribution des appels.

Le système peut importer la musique d'attente à partir des sources suivantes :

- Musique en attente
- EXMR

  Consultez la documentation relative à l'installation d'OpenScape Business X1 ou la documentation relative à l'installation d'OpenScape Business X5/X8.
- Module plugin MUSIQUE

  Consultez la documentation relative à l'installation d'OpenScape Business X1 ou la documentation relative à l'installation d'OpenScape Business X5/X8.
- Module MPPI USB EXM (uniquement pour OpenScape Business X5)

  Consultez la documentation relative à l'installation d'OpenScape Business X5/X8.

Fichiers audio

L'administrateur peut transférer les fichiers audio de la musique d'attente interne du PC vers le système de communication pour les utiliser comme musique d'attente interne alternative.

Remarque : Avant d'utiliser des annonces ou de la musique provenant d'autres sources, assurez-vous de ne pas enfreindre les droits d'auteur.

Important : Si le poste en attente est un client de poste de travail IP ou une ligne IP, la mémoire d'attente interne est utilisée. Le MOH externe n'est pas destiné à la propriété intellectuelle.

Les fichiers audio doivent être disponibles au format `Wave` et présenter les propriétés suivantes :

- PCM 16 bits
- Mono ou stéréo
- Fréquences d'échantillonnage possibles : 8 / 22,05 / 24 / 32 / 40 / 44,1 ou 48 kHz.
- Longueur maximale du nom du fichier audio : 30 caractères

Recommandé : **16 bits PCM - Mono - 8 kHz, longueur env. 2 min**

Musique en attente

Il est possible de configurer différentes musiques d'attente pour le service de jour et de nuit.

Remarque : Pour UC Suite, il n'y a pas de distinction entre les fichiers de jour et de nuit. Le **fichier journalier du ministère de la Santé** est utilisé.

L'administrateur peut configurer les fonctions suivantes :

- Musique d'attente avec sonnerie (retour d'appel) :

  L'abonné en attente entend d'abord la mélodie du ministère de la Santé pendant la consultation. Une fois l'appel transféré vers sa destination, la sonnerie retentit à la place de la musique d'attente.
- Musique d'attente sans sonnerie (retour automatique) :

  La personne retenue entendra le message du ministre jusqu'à ce que la personne appelée réponde.
- Pas de musique d'attente :

  La partie retenue n'entend rien (silence). L'appelant entend la tonalité de retour d'appel en cas de transfert non filtré pour un appel externe.

24.1.7.1 Comment importer la musique d’attente

L’assistant **Musique d’attente / Annonces** vous permet d’importer dans le système de communication des fichiers audio comme musique d’attente interne.

Conditions préalables

Vous êtes connecté à WBM.

Les fichiers audio à importer sont disponibles en tant que fichiers sons au format nécessaire.

Remarque : Assurez-vous que vous ne violez aucun copyright avant d'utiliser les annonces ou la musique.

Remarque : Aucune distinction n'est faite entre les fichiers de jour et de nuit avec UC Suite. Le **Fichier musique d'attente journée** est utilisé.

Étape par étape

1) Dans la barre de navigation, cliquez sur**Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Musique d'attente / Annonces**.
4) Cliquez sur **Fichier musique d'attente journée** pour le mode Jour ou sur **Fichier musique d'attente nuit** pour le mode Nuit, puis sur **Parcourir**.
5) Sélectionnez un fichier audio et cliquez sur **Ouvrir**. Le chemin d'accès au fichier audio sélectionné est indiqué dans **Fichier musique d'attente journée** et/ou **Fichier musique d'attente nuit**.
6) Cliquez sur **Charger**.
7) Confirmez avec **OK** et cliquez sur **OK & Suivant**.
8) Cliquez sur **Terminer**.

24.1.7.2 Comment configurer la fonction Musique d'attente interne

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

La longueur du nom du fichier de musique d'attente est de 30 caractères au maximum.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Connexion**.
3) Dans l'arborescence du menu, cliquez sur **Connexions** > **Annonce / Musique d'attente interne**.
4) Dans la zone **Musique d'attente interne** dans la liste déroulante **Type de MoH**, sélectionnez l'entrée **Pas de musique d'attente**, **Sans retour d'appel** ou **Avec retour d'appel**.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.1.7.3 Comment modifier la musique d'attente pour chaque groupe de restriction de tarif

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie > Connexions**.

3) Dans l'arborescence du menu, cliquez sur **Connexions > Annonce / Musique d'attente interne**.
4) Cliquez sur l'onglet **Modifier la musique d´attente**.
5) Dans la ligne du groupe de restriction de trafic correspondant, dans la liste déroulante Fichier audio sélectionnez la musique d'attente souhaitée.
6) Si aucune musique d'attente n'est affectée à un groupe de restriction de trafic, la musique d'attente interne est utilisée.
7) Dans la ligne du groupe de restriction de trafic correspondant, entrez une Description.
8) Cliquez sur **Appliquer**.
9) Cliquez sur **OK**.

Remarque : Cette fonctionnalité est uniquement applicable aux systèmes OpenScape Buisness S et n'est pas supportée dans OpenScape Business X.

24.1.8 Annonces

Le système de communication permet de diffuser des annonces d'attente pour les appelants avant de répondre à un appel, ainsi que lors de l'utilisation de la distribution d'appels et de la numérotation directe DTMF. Dans certaines situations, vous pouvez également remplacer la mélodie MOH par une communication d’interphone, par exemple lorsqu'un correspondant est mis en attente ou lorsqu'un abonné est occupé ou en cours d'acheminement.

Le système peut importer des communication d’interphone à partir des sources suivantes :

- Communications d’interphone internes
- Périphérique de communication d’interphone analogique

  Voir la zone Équipement auxiliaire - Dispositif d'annonce analogique dans la *documentation Unify OpenScape Business Administrateur*.
- Module MPPI-USB EXM (uniquement pour OpenScape Business X3/X5)

  Pour plus d'informations, voir *Installation d'Unify OpenScape Business X5/ X8, Documentation de service*.

L'administrateur peut configurer les communications d’interphone pour une lecture unique (démarrage/arrêt) ou continue.

Un périphérique de communication d’interphone externe doit se comporter comme une station, c'est-à-dire s'annoncer, diffuser la communication d’interphone et commuter l'appel (entrer en consultation, mettre en attente, composer et raccrocher).

Fichiers audio

L'administrateur peut transférer des fichiers audio contenant des communication d’interphone du PC vers le système de communication.

Remarque : Veuillez vous assurer préalablement qu'en utilisant des annonces ou une musique d'attente, vous ne violez pas un copyright.

Les fichiers audio doivent être disponibles sous forme de fichiers `Wave` avec les propriétés suivantes :

- 16 bits PCM
- Mono ou stéréo
- 8 / 22,05/ 24 / 32 / 40 / 44,1 ou 48 kHz.
- Longueur maximale du nom du fichier audio : 30 caractères

Recommandé : **16 bits PCM - Mono - 8 kHz, longueur env. 2 min**

24.1.8.1 Comment configurer les communications d'interphone (UC Smart)

L'assistant **Musique d'attente / Annonces** peut être utilisé pour configurer les annonces.

Conditions préalables

- Dans **Mode expert > Middleware > Lecteur d'annonces**, cochez la case **Le service sera démarré automatiquement** pour activer le lecteur d'annonces.
- Un numéro d'appel du lecteur d'annonces doit être défini dans **Mode expert > Paramètres de base > Messagerie vocale / Lecteur d'annonces**.
- Vérifiez que le numéro est correctement configuré dans **Mode expert > LCR > Plan de numérotation**, sous le champ **Lecteur d'annonces**.
- La **table de routage** associée est définie sur **12**, **UC Suite** est défini pour **Route** et **MEB** est défini pour **Règle de numérotation**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration**.

2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.

3) Cliquez sur **Modifier** pour lancer l'assistant **Musique d'attente / Annonces**.

4) Ignorez la sélection **Charger les fichiers de musique d'attente via les fichiers HTTP** en cliquant sur **OK & Suivant**.

> **Remarque :** Avant d'utiliser des annonces ou de la musique, assurez-vous de ne pas enfreindre les droits d'auteur.

5) Pour transférer un fichier audio vers le système de communication, procédez comme suit :

a) Cliquez sur **Choisir un fichier**.
b) Sélectionnez un fichier audio.
c) Cliquez sur **Ouvrir**.
d) Cliquez sur **Charger**.
e) Confirmez la remarque avec **OK**.
f) Si vous souhaitez charger d'autres fichiers audio dans le système, répétez ces étapes.

6) Cliquez sur **OK & Suivant**.

> **Conseil :** Les paramètres de configuration des **Annonces** sont également décrits et peuvent être configurés via **Mode expert > Équipement auxiliaire > Annonces**.

7) Sélectionnez le type d'annonce à lire dans la colonne **Type**.
8) Sélectionnez le port auquel le périphérique est connecté dans la colonne **Accès**. Les destinations externes peuvent être utilisées pour adresser des appareils d'annonce dans un autre nœud du système.
9) Sélectionnez un fichier d'annonce dans la liste déroulante de la colonne **Fichier Wave** (uniquement pour le type **Lecteur d'annonces** et en mode UC Suite).
10) Sélectionnez le type de lecture dans la liste déroulante de la colonne **Mode**.
11) Cliquez sur **OK & Suivant**, puis sur **Terminer**.

24.1.8.2 Comment configurer les communications d'interphone (UC Smart)

L'assistant **Musique d'attente / Annonces** peut également être utilisé pour configurer les Annonces.

Conditions préalables

Les ports analogiques qui sont configurés comme ports de communication d'interphone doivent se voir attribuer la valeur **Répondeur automatique** sous **Type de poste**.

Les ports EVM qui sont configurés comme ports de communication d'interphone doivent :

- se voir attribuer la valeur **Standard** sous **Type de poste**.
- supprimés du groupe de recherche de la boîte vocale.
- attribuer une boîte vocale au numéro d'appel du port en mode Expert**Mode Expert > Connexion > Smart VM**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arbre de navigation, cliquez sur **Assistants** > **Téléphonie centrale**.
3) Cliquez sur **Modifier** pour lancer l'assistant **Musique d'attente / Communication d'interphone**.
4) Ignorez la sélection **Charger les fichiers de musique d'attente via les fichiers HTTP** en cliquant sur **OK & Suivant**.

> **Conseil :** Les paramètres de configuration des **Communications d'interphone** sont décrits et peuvent être configurés via Mode expert > Connexion > Communications d'interphone.

5) Sélectionnez le type d'annonce à lire dans la colonne **Type**.
6) Sélectionnez le port auquel le périphérique est connecté dans la colonne **Accès**. Les destinations externes peuvent être utilisées pour adresser des appareils d'annonce dans un autre nœud du système.

7) Sélectionnez un fichier d'annonce dans la liste déroulante de la colonne **Fichier Wave** (uniquement pour le type **Lecteur d'annonces** et en mode UC Suite).
8) Sélectionnez le type de lecture dans la liste déroulante de la colonne **Mode**.
9) Cliquez sur **OK & Suivant**, puis sur **Terminer**.

24.1.9 Signalisation d'abonné à abonné

Le système de communication permet la transmission transparente de messages entre les terminaux (signalisation d'abonné à abonné - UUS) La variante UUS1 est supportée pour l'échange d'informations dans les messages de commande servant à l'établissement et à la coupure de la liaison.

Dans un raccordement multiple, il faut veiller à ce qu'au maximum un terminal transmette un message lors d'un appel entrant.

24.1.10 Protection de la signalisation sur le canal vocal

Le système de communication est doté d'une protection contre la falsification des données par l'insertion de tonalités non souhaitées dans le canal voix ; cette protection peut être paramétrée par l'administrateur. L'entrée en tiers dans une liaison ainsi protégée n'est pas possible. Chaque abonné configuré comme fax bénéficie automatiquement de cette protection contre la signalisation.

Les retours d'appel sont inhibés jusqu'à ce que le poste redevienne libre.

Un abonné mis en garde bénéficie toujours de la protection contre les intrusions.

24.1.11 Temporisations

Le système de communication offre à l'administrateur des possibilités de réglage de différents paramètres de temps, par ex. la durée du double appel ou l'intervalle de répétition automatique de la numérotation.

Les paramètres de temps sont préréglés dans le système de communication et n'ont généralement pas besoin d'être modifiés.

24.1.12 Gestion des fonctionnalités Centrex

Pour la gestion des fonctionnalités Centrex les caractère de sélection * et # doivent être transmis dans le RNIS et au ITSP.

En tant qu'administrateur, vous pouvez activer ou désactiver cette fonctionnalité.

La saisie de l'indicatif doit être effectuée en cours de numérotation (par exemple après l'entrée de l'indicatif de ligne). L'entrée débute toujours par * ou #, suivi d'un chiffre ou d'une combinaison de chiffres et se termine par #.

24.1.12.1 Comment activer ou désactiver la gestion des fonctionnalités Centrex

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Configuration de base**.
3) Dans l'arborescence du menu, allez à **Système** > **Flags système**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez activer la gestion des fonctionnalités Centrex, cochez la case **Sélection de * et # sur les interfaces de ligne**.
   - Si vous souhaitez désactiver la gestion des fonctionnalités Centrex, décochez la case **Sélection de * et # sur les interfaces de ligne**.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.2 Sauvegarde et restauration

Les données de configuration du système de communication peuvent être sauvegardées et restaurées.

Les données de configuration sont enregistrées dans un ensemble de sauvegarde. Chaque sauvegarde crée un ensemble de sauvegarde distinct. Les sauvegardes peuvent être créées manuellement et immédiatement, ou programmées pour une exécution automatique à des moments précis.

Remarque : Il est fortement recommandé de sauvegarder régulièrement les données de configuration sous forme de jeux de sauvegarde. Lors de la mise à jour vers une nouvelle version mineure, il est nécessaire de créer un nouveau jeu de sauvegarde. Chaque sauvegarde est chiffrée à l'aide d'une clé spécifique au système. Un ensemble de sauvegarde chiffré ne peut être utilisé que pour la restauration du système qui a chiffré la sauvegarde.

Remarque : Lors de la restauration des données des systèmes OpenScape Business utilisant Unify Phone, veuillez noter qu'il n'est pas possible de réactiver le service Unify Phone / la connexion au cloud ni de réactiver les utilisateurs Unify Phone via la restauration des données. Cela est dû à des problèmes de synchronisation avec le cloud Unify Phone. Lors de la restauration des données, assurez-vous que le service Unify Phone / la connexion au cloud est activé et configuré, et que les utilisateurs Unify Phone sont les mêmes que dans l'ensemble de sauvegarde.

Différents supports de sauvegarde peuvent être utilisés pour stocker les ensembles de sauvegarde (tels que des supports USB ou des lecteurs réseau, par exemple).

En fonction de la configuration du système, de l'utilisation du système de communication et du type de support de sauvegarde utilisé, une sauvegarde ou une restauration peut prendre beaucoup de temps – dans certains cas pour les systèmes dotés de la suite UC, jusqu'à trois heures. Ce processus ne doit pas être interrompu manuellement ni par un redémarrage du système.

L'interruption d'une récupération de données peut entraîner une configuration système incohérente, dans laquelle un fonctionnement sans erreur du système n'est pas garanti. Une procédure de récupération interrompue doit toujours être répétée jusqu'à ce qu'elle soit menée à bien. Autrement, une reconfiguration complète du système pourrait s'avérer nécessaire. Si la récupération échoue à plusieurs reprises, veuillez contacter le service d'assistance et assurez-vous entre-temps que votre sauvegarde n'est pas écrasée par de nouvelles sauvegardes. Pour ce faire, la sauvegarde automatique des données doit être temporairement désactivée.

Jeux de sauvegarde à des fins de diagnostic

Des ensembles de sauvegarde « plus petits » contenant des données de diagnostic pour le support technique peuvent être créés à des fins de diagnostic. Contrairement aux ensembles de sauvegarde classiques, des quantités de données nettement inférieures sont produites à cet effet et peuvent donc être facilement envoyées par courrier électronique, par exemple. Les ensembles de sauvegarde de diagnostic comprennent, entre autres, les données de configuration du système de communication et de la solution UC installée. Les messages vocaux, les fax et les annonces ne sont pas inclus.

24.2.1 Jeux de sauvegarde

Les données de configuration du système de communication sont enregistrées dans un jeu de sauvegarde.

En plus du jeu de sauvegarde, il faut enregistrer le fichier texte correspondant au jeu de sauvegarde. Il contient des informations sur la date et l'heure de la sauvegarde et sur la version du logiciel qui a servi à effectuer la sauvegarde. Le fichier texte est nécessaire pour rétablir les jeux de sauvegarde.

Si le nombre des jeux de sauvegarde enregistré dépasse la valeur paramétrée pour l'archive, les jeux de sauvegarde les plus anciens sont effacés.

Données du jeu de sauvegarde

Les données suivantes correspondant à un jeu de sauvegarde sont affichées :

- **Nom d'archive** : Nom du jeu de sauvegarde
- **Taille** : Taille du jeu de sauvegarde en octets
- **Date** : date à laquelle le jeu de sauvegarde a été créé.
- **Commentaire** : commentaire qui a été indiqué lors de la création du jeu de sauvegarde (en option).

Les jeux de sauvegarde affichés en grisé ne peuvent pas être rétablis.

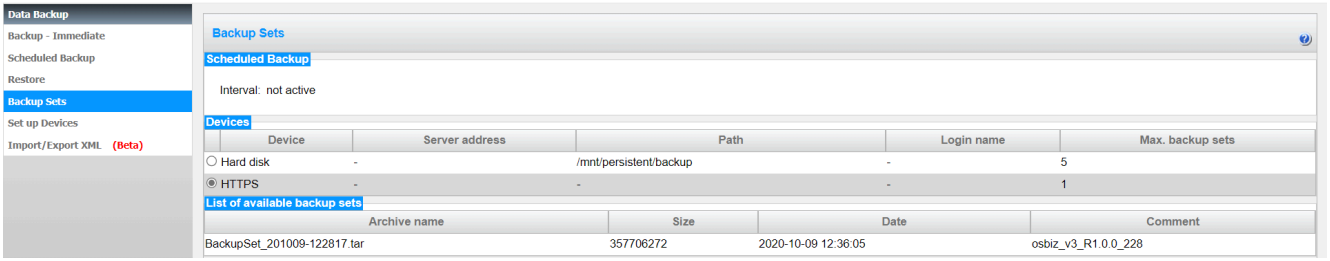
24.2.1.1 Comment afficher les jeux de sauvegarde

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Sauvegarde des données**.
2) Dans l'arborescence de navigation, cliquez sur **Jeux de sauvegarde**.
3) Dans la zone **Équipements**, sélectionnez le moyen de sauvegarde contenant le jeu de sauvegarde que vous voulez afficher. Vous recevez une liste de tous les jeux de sauvegarde disponibles sur ce support.



24.2.1.2 Comment effacer les jeux de sauvegarde

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Sauvegarde et restauration**.
2) Dans l'arborescence de navigation, cliquez sur **Jeux de sauvegarde**.
3) Dans la plage **Equipement** sélectionnez le moyen de sauvegarde dont vous voulez afficher le jeu de sauvegarde. Vous recevez une liste de tous les jeux de sauvegarde disponibles sur ce support.
4) Cochez la case du jeu de sauvegarde que vous souhaitez supprimer et cliquez sur **Effacer**. Le jeu de sauvegarde est supprimé.

24.2.2 Supports de sauvegarde

Les ensembles de sauvegarde sont stockés sur le support de sauvegarde sélectionné.

Les supports de sauvegarde suivants peuvent être utilisés :

- périphérique de stockage USB inséré
- lecteur réseau
- PC client utilisant HTTP (possible uniquement avec sauvegarde immédiate)
- Serveurs FTP/FTPS

Pour chaque support de sauvegarde, le nombre maximal d'ensembles de sauvegarde à stocker dans le répertoire peut être spécifié.

périphérique de stockage USB

Pour utiliser un périphérique de stockage USB (par exemple, un disque dur USB ou une clé USB) pour la sauvegarde, le périphérique USB doit être branché sur le port serveur USB du système de communication. De plus, le périphérique USB doit être formaté en FAT-32. En raison des limitations du système de fichiers, la taille maximale de la sauvegarde ne peut pas dépasser 4 Go. Dans de tels cas, il convient de sélectionner un autre support de sauvegarde. Les supports USB formatés en NTFS sont en lecture seule. Notez que s'il existe plusieurs partitions, seule la première partition peut être utilisée pour la sauvegarde !

Les périphériques USB amorçables ne sont pas pris en charge.

Avec OpenScape Business S, le périphérique USB est branché sur le port USB du serveur Linux.

Serveurs FTP/FTPS et lecteurs réseau

Les serveurs FTP/FTPS et les lecteurs réseau peuvent être ajoutés, modifiés ou supprimés en tant que nouveaux médias. Les serveurs FTP/FTPS et les lecteurs réseau peuvent également être spécifiés plusieurs fois si différents répertoires y sont utilisés. Le protocole TLS 1.2 est pris en charge en tant que protocole de transfert de fichiers chiffré (FTPS).

Pour sauvegarder les données de configuration, l'utilisateur doit disposer des droits d'écriture sur le répertoire racine d'un serveur FTP/FTPS. Pour effectuer une sauvegarde sur un lecteur réseau, les utilisateurs ont uniquement besoin des droits d'écriture pour le répertoire souhaité.

Si la vitesse de transmission vers le serveur FTPS est trop faible, il peut y avoir un dysfonctionnement au niveau de la sauvegarde. Si cela se produit, la sauvegarde doit être redémarrée.

Pour FTPS, les certificats jusqu'à 2048 bits sont pris en charge. Ces certificats sont nécessaires pour l'authentification auprès du serveur FTPS.

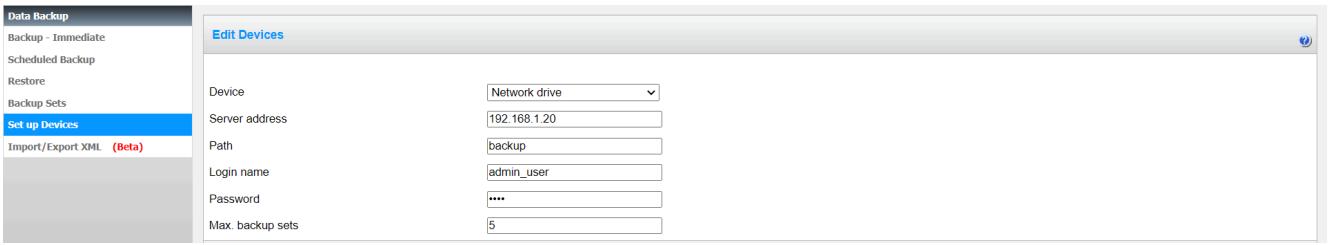
24.2.2.1 Comment ajouter un moyen de sauvegarde

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Sauvegarde des données**.
2) Dans l'arborescence de navigation, cliquez sur **Configuration**.
3) Cliquez sur **Ajouter**.



4) Dans la liste déroulante, colonne **Système** sélectionner le moyen de sauvegarde souhaité.
   - Si vous souhaitez enregistrer sur un serveur FTP/FTPS, sélectionnez **(S)FTP**.
   - Si vous souhaitez effectuer l'enregistrement sur un lecteur réseau, sélectionnez **Lecteur réseau**.

   Remarque : La version de Samba prise en charge est SMB2.

5) Dans **Adresse du serveur**, indiquez le nom d'hôte ou l'adresse IP du média.
6) Dans **Répertoire**, indiquez le chemin d'accès où le jeu de sauvegarde doit être enregistré.
7) Si vous souhaitez effectuer l'enregistrement sur un serveur FTP/FTPS, entrez **Nom d'utilisateur** et **Mot de passe** pour l'accès au serveur FTP/FRPS.

   Remarque : Les caractères suivants sont acceptés dans le champ Mot de passe : `0-9 A-Z a-z ~ ! @ # $ % ^ _ - + = ? / , . :`

   La longueur maximale d'un mot de passe est de 64 caractères.

8) Si vous voulez procéder à la sauvegarde sur un lecteur réseau qui est sécurisé, entrez le **Nom d'utilisateur** et le **Mot de passe** pour l'accès au lecteur réseau.

   Remarque : Par défaut, un domaine vide sert à l'authentification. Si vous voulez fournir le domaine, utilisez alors une barre oblique (/) comme séparateur dans le champ **Nom de connexion**. Par exemple : `domaine/utilisateur`.

9) Dans **Jeux de sauvegarde maxi.** entrez le nombre de jeux de sauvegarde pouvant être enregistrés au maximum dans le répertoire.
10) Cliquez sur **OK & Suivant**. Le moyen de sauvegarde nouvellement créé apparaît dans la liste des moyens de sauvegarde disponibles.
11) Dans l'arborescence de navigation, cliquez sur **Jeux de sauvegarde**.
12) Dans la zone **Équipements**, activez le moyen de sauvegarde que vous venez d'ajouter. S'il ne figure aucune ligne rouge avec message d'erreur dans la liste des jeux de sauvegarde disponibles, cela signifie que le support de sauvegarde est paramétré correctement.
13) Si un message d'erreur s'affiche, vous devez de nouveau vérifier vos entrées (voir Comment modifier le moyen de sauvegarde à la page 1185

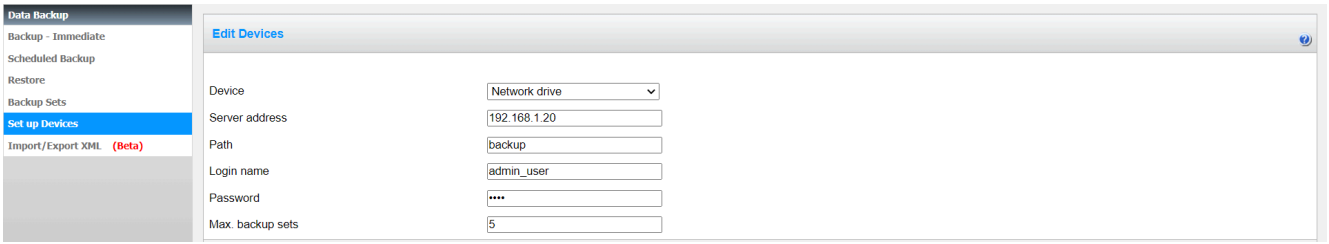
24.2.2.2 Comment modifier le moyen de sauvegarde

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Sauvegarde des données**.
2) Dans l'arborescence de navigation, cliquez sur **Configuration**.
3) Activez le moyen de sauvegarde à modifier, puis cliquez sur **Modifier**.



4) Modifiez les valeurs souhaitées.
5) Cliquez sur **OK & Suivant**.

24.2.2.3 Comment effacer le moyen de sauvegarde

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Sauvegarde des données**.
2) Dans l'arborescence de navigation, cliquez sur **Configuration**.
3) Activez le moyen de sauvegarde à supprimer, puis cliquez sur **Supprimer**.

   Il est possible de sélectionner plusieurs supports de sauvegarde à effacer.
4) Confirmez cette demande avec **OK**. Le moyen de sauvegarde est effacé dans la liste des moyens de sauvegarde disponibles.

24.2.3 Sauvegarde immédiate

Les données de configuration peuvent être sauvegardées manuellement immédiatement.

Divers supports de sauvegarde peuvent être utilisés pour la sauvegarde des données ; par défaut, le support de sauvegarde est configuré en **HTTPS** . Vous pouvez ainsi stocker la sauvegarde dans tous les emplacements de stockage accessibles depuis le PC client avec lequel vous vous êtes connecté au WBM. L'emplacement de stockage choisi doit également être accessible lors de la restauration de la sauvegarde. Si un périphérique USB est connecté au système de communication, **le périphérique USB** est affiché comme un support de sauvegarde supplémentaire.

Le nom du jeu de sauvegarde est attribué automatiquement lors de la sauvegarde. Il comprend notamment la date à laquelle la sauvegarde a été effectuée. De plus, ces données sont également incluses dans un fichier texte qui doit également être stocké. Si vous le souhaitez, un commentaire peut être ajouté afin d'identifier plus facilement un ensemble de sauvegarde avant une restauration ultérieure.

Concepts associés

Sauvegarde planifiée à la page 1188

Tâches associées

Comment modifier le propre mot de passe d'administrateur à la page 92

24.2.3.1 Comment sauvegarder immédiatement un jeu de sauvegarde

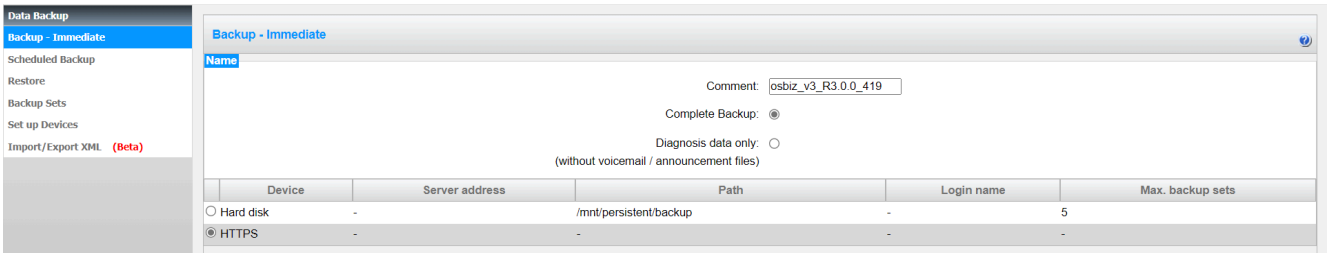
Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Uniquement en cas d'utilisation d'UC Suite : UC Suite a démarré correctement.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Sauvegarde des données**.
2) Dans l'arborescence de navigation, cliquez sur **Sauvegarde - immédiate**.



3) Dans le champ **Commentaire**, saisissez un commentaire afin de pouvoir identifier plus facilement le jeu de sauvegarde à utiliser plus tard lors d'une éventuelle restauration. Lors de la saisie, évitez les inflexions et les caractères spéciaux.
4) Si vous voulez créer un jeu de sauvegarde incluant les messages Voix et les annonces, sélectionnez l'option **Sauvegarde complète**.
5) Si vous voulez créer un jeu de sauvegarde sans messages Voix et annonces, sélectionnez l'option **Uniquement données de diagnostic**.
6) Dans la zone **Équipements**, activez le lecteur de destination sur lequel le jeu de sauvegarde doit être enregistré.
7) Cliquez sur **OK & Suivant**. Dans une autre fenêtre, le système affiche la progression de la sauvegarde.

Remarque : Si le bouton **OK&Suite** est affiché en grisé, cela signifie que toutes applications dont les données doivent être sauvegardées n'ont pas démarré correctement (par ex. UC Suite).

Si vous n'avez pas d'autorisation pour le répertoire d'archive sélectionné, vous recevez un message d'erreur. Sélectionnez un autre lecteur de destination ou modifiez le chemin d'accès pour l'archive.

S'il n'y a pas suffisamment de capacité mémoire disponible pour le jeu de sauvegarde sur le lecteur de destination, vous voyez un message d'erreur. Sélectionnez un autre

lecteur de destination ou effacez un jeu de sauvegarde et démarrez la sauvegarde des données de nouveau.

8) La sauvegarde a été effectuée si le message **Sauvegarde terminée ! 100 %** s'affiche.

9) Si vous avez choisi **HTTPS** comme support de sauvegarde, vous devez enregistrer le jeu de sauvegarde de diagnostic et le fichier texte correspondant à un emplacement de votre choix. Avec les autres moyens de sauvegarde, cela se fait automatiquement. La fenêtre de navigation doit rester ouverte tant que se déroule l'opération d'enregistrement du jeu de sauvegarde et du fichier texte.

Remarque : Si vous utilisez une clé USB comme moyen de sauvegarde, attendez que la LED de la clé USB ait fini de clignoter. C'est seulement alors que la sauvegarde est terminée sur la clé USB. Ensuite retirez la clé USB.

10) Cliquez sur **Terminer**.

24.2.4 Sauvegarde planifiée

Une commande temporelle permet de sauvegarder automatiquement les données de configuration. L'heure, l'intervalle et le lieu de la sauvegarde automatique sont paramétrables.

La sauvegarde des données en fonction du temps peut être planifiée de manière quotidienne ou hebdomadaire, pour une heure définie ; elle démarre alors automatiquement. Cette "tâche de sauvegarde" peut être paramétrée pour un support de sauvegarde interne ou externe. La configuration de plusieurs tâches de sauvegarde n'est pas possible.

Concepts associés

Sauvegarde immédiate à la page 1186

24.2.4.1 Comment sauvegarder un jeu de sauvegarde de façon planifiée

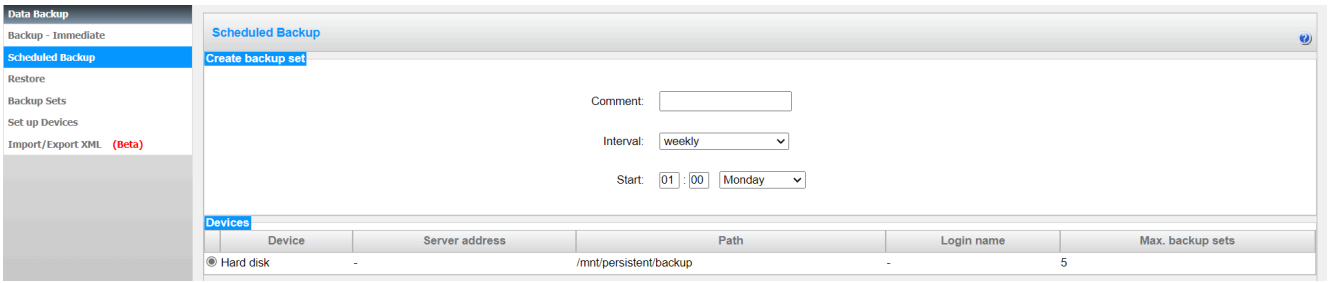
Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Sauvegarde des données**.

2) Dans l'arborescence de navigation, cliquez sur **Sauvegarde planifiée**.



3) Dans la zone **Créer un jeu de sauvegarde** du champ **Commentaire**, saisissez un commentaire afin de pouvoir identifier plus facilement le jeu de sauvegarde à utiliser plus tard lors d'une éventuelle restauration. Lors de la saisie, évitez les inflexions et les caractères spéciaux.
4) Définissez l'intervalle de sauvegarde :
   - Sauvegarde quotidienne : Dans la liste déroulante **Fréquence**, sélectionnez l'option **Quotidien(ne)**, puis, sous **Heure de sauvegarde**, saisissez l'heure où la sauvegarde doit débuter chaque jour.
   - Sauvegarde hebdomadaire : Dans la liste déroulante **Intervalle**, sélectionnez **Hebdomadaire**, puis, sous **Heure de sauvegarde**, saisissez le jour de la semaine et l'heure auxquels la sauvegarde doit débuter.
5) Dans la zone **Équipements**, activez le lecteur de destination sur lequel le jeu de sauvegarde doit être enregistré.
6) Cliquez sur **OK & Suivant**. La sauvegarde des données est lancée quotidiennement ou hebdomadairement au moment indiqué.

24.2.5 Rétablir

Le rétablissement des données de configuration est effectué manuellement à l'aide des jeux de sauvegarde.

Le rétablissement peut être effectué à partir de tous les moyens de sauvegarde supportés.

24.2.5.1 Comment rétablir un jeu de sauvegarde

Conditions préalables

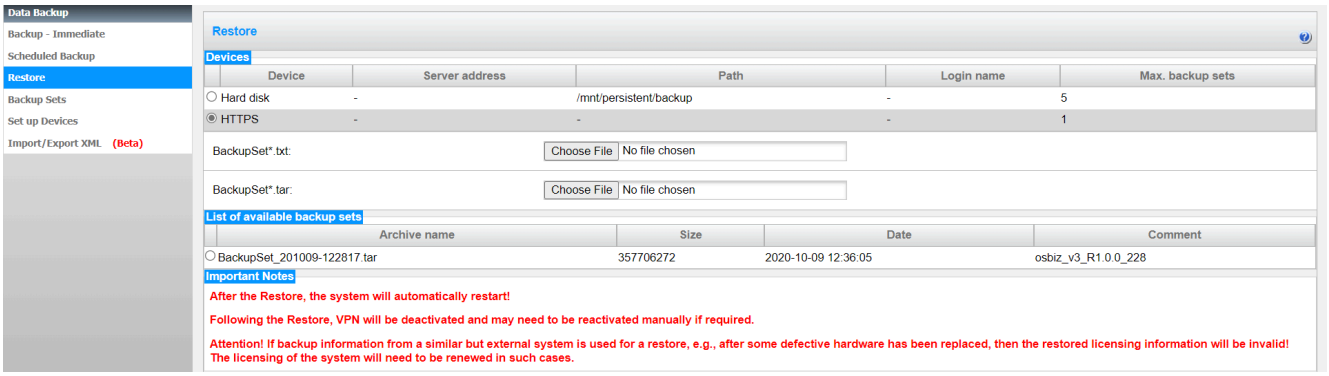
Vous êtes connecté à WBM avec le profil **Advanced**.

Uniquement en cas d'utilisation d'UC Suite : UC Suite a démarré correctement.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Sauvegarde des données**.

2) Dans l'arborescence de navigation, cliquez sur **Restaurer**.



3) Dans la zone **Équipements**, activez le support qui contient le jeu de sauvegarde à restaurer.
4) Si vous avez activé **HTTPS** comme moyen de sauvegarde, allez à l'endroit où le jeu de sauvegarde est enregistré et sélectionnez-le. Allez ensuite à l'endroit où le fichier texte est enregistré et sélectionnez-le.
5) Si vous avez activé un support de sauvegarde autre que **HTTPS**, dans la zone **Liste des jeux de sauvegarde disponibles**, sélectionnez le jeu de sauvegarde qui contient les données de configuration à restaurer.
6) Attendez que les fichiers soient chargés sur le système et cliquez ensuite sur **OK. & Suivant**. Le rétablissement des données de configuration est lancé. Le système vous indique la progression du rétablissement.
7) Une fois que le message **Restauration terminée !** s'est affiché, le système effectue automatiquement un redémarrage. Le rétablissement est achevé avec succès lorsque le système est de nouveau en service.

24.3 Mises à jour

Les mises à jour fournissent les logiciels les plus récents disponibles pour les composants du système au sein d'une version.

Pour installer les mises à jour, vous aurez besoin du support logiciel de 3 ans.

La version du logiciel installé et la date d'expiration du support logiciel sont affichées sur la page d'accueil du WBM. Si des mises à jour logicielles plus récentes sont disponibles, cela est également indiqué.

Remarque : Lors de la mise à jour vers une nouvelle version mineure, il est nécessaire de créer un nouveau jeu de sauvegarde.

La mise à jour du logiciel s'effectue via WBM. Sur un modèle matériel, la mise à jour peut également être effectuée directement depuis un périphérique USB, sans passer par WBM.

Grâce au WBM, le logiciel peut être mis à jour via un serveur web Internet, un serveur web local ou directement via des fichiers image.

Les composants système suivants sont mis à jour :

- Logiciel du système de communication
- Logiciel des clients UC

- Logiciel pour téléphones système (les mises à jour peuvent également être effectuées individuellement)
- Documentation

Le logiciel des clients UC est mis à jour en même temps que celui du système de communication. Si une version logicielle plus récente est disponible, les utilisateurs des clients UC sont avertis par un message de mise à jour automatique qu'une mise à jour est disponible et peut être installée.

La mise à jour logicielle des téléphones du système IP s'effectue automatiquement lors de la mise à jour du système de communication, mais peut également être effectuée manuellement. Pour les téléphones du système UP0, la mise à jour est effectuée manuellement à l'aide de Manager E.

La mise à jour du logiciel peut être lancée immédiatement ou en définissant indépendamment les horaires de transfert et d'activation du logiciel. La mise à jour doit être effectuée en dehors des heures ouvrables du client, car le système de communication et/ou les téléphones du système sont redémarrés, les appels en cours sont interrompus et l'utilisation des clients UC est temporairement interrompue.

Une fois le logiciel transféré vers le système de communication, il est activé à l'heure sélectionnée. La dernière image du téléphone est alors automatiquement chargée sur les téléphones du système IP. Après un redémarrage du système de communication et des téléphones du système IP, le logiciel nouvellement chargé sera actif.

Remarque : La mise à jour du logiciel ne doit pas être effectuée simultanément sur tous les systèmes et sur différentes versions du logiciel.

Fichiers image

Pour mettre à jour les composants du système, des fichiers image compressés contenant le logiciel de ces composants sont nécessaires. Ces fichiers image peuvent être téléchargés depuis le serveur logiciel (serveur web Internet) et stockés indépendamment sur un serveur web local, sur le réseau interne ou sur une clé USB, par exemple. Il existe également un fichier image distinct pour chaque type de téléphone système, au cas où les téléphones système devraient être mis à jour séparément.

Les types de fichiers image suivants sont disponibles :

- **tgz** : pour le logiciel du système de communication. Le fichier tgz contient un fichier tar. Le fichier tar doit être décompressé à partir du fichier tgz avec un décompresseur tel que WinZip ou 7-zip, par exemple. Le fichier tgz est proposé au téléchargement car une vérification peut être effectuée pour déterminer si le fichier est corrompu ou non lors du téléchargement du logiciel depuis le serveur.
- **tar** : pour le logiciel du système de communication. Il contient les fichiers compressés pour chaque composant du système.
- **app** : pour le logiciel du téléphone système.

Serveur Web local

Lors de l'exécution d'une mise à jour logicielle via un serveur web, c'est le serveur logiciel (serveur web Internet) qui est accédé par défaut.

Toutefois, il est également possible d'utiliser un serveur web local pour les mises à jour. Pour ce faire, le fichier image doit être stocké sur le serveur web local, et le chemin d'accès à ce serveur web local doit être configuré dans le WBM.

Mise à niveau de vitesse

Une mise à niveau de la vitesse comme avec le HiPath 3000 n'est pas possible.

Important : Retirer la carte SDHC pendant son fonctionnement entraînera une perte de données !

Réseau - Licences

Lors de la mise à niveau ou de la migration de systèmes dans un réseau où le nœud maître est utilisé pour l'octroi de licences aux nœuds esclaves, veuillez commencer par les nœuds esclaves avant le nœud maître.

24.3.1 Utilisation d'un serveur Web local

Le logiciel peut être actualisé via un serveur Web local.

Les fichiers image actuels doivent être enregistrés sur le serveur Web local. Il faut en plus inscrire dans WBM les données d'accès du serveur Web local. Cette modification ne peut être effectuée que par un administrateur de profil **Expert**. Si les données d'accès du serveur Web local sont inscrites, elles deviennent les données par défaut ; pour toutes les autres mises à jour ultérieures du système de communication, il sera utilisé à la place du serveur web Internet le serveur Web local.

24.3.1.1 Comment configurer l'accès au serveur web local

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Il existe une liaison avec le serveur web local.

Vous avez besoin de l'adresse web (URL) et de l'identifiant d'accès du serveur Web local ainsi que du nom du fichier Image.

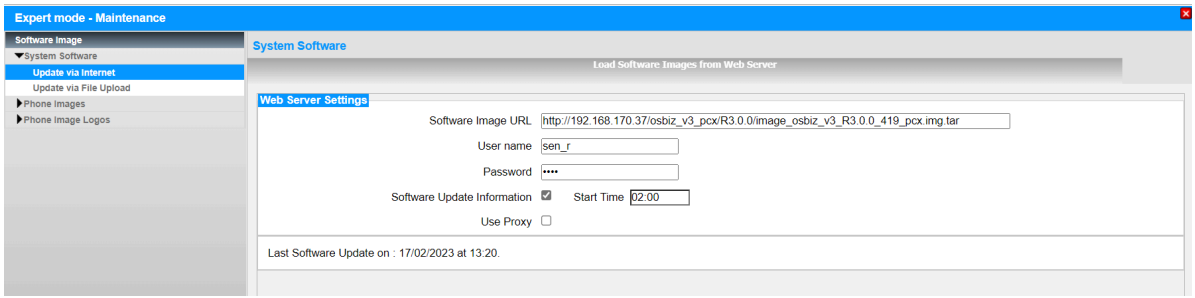
Le fichier Image est enregistré comme fichier tar dans le serveur Web local et l'emplacement d'enregistrement est connu. Il est éventuellement nécessaire de décomprimer le fichier tar à partir du fichier tgz enregistré.

Si vous utilisez un serveur proxy pour la mise à jour, vous devez disposer de ses données (éventuellement également du nom d'utilisateur et du mot de passe).

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Image logicielle**.
3) Dans l'arborescence du menu, cliquez sur **Logiciel système**.

4) Cliquez sur **Mise à jour via Internet**.



5) Paramétrez l'accès au serveur web local :
   a) Dans **Image logicielle URL** indiquez l'adresse du serveur Web local ainsi que le nom du fichier Image.

      Remarque : Le bouton **Paramétrage par défaut** vous permet de ramener les valeurs entrées aux valeurs par défaut.

   b) Dans le champ **Nom utilisateur**, entrez le nom de l'utilisateur et dans le champ **Mot de passe**, entrez le mot de passe pour l'accès au serveur Web local.
   c) Cochez la case **Informations sur la mise à jour logicielle** et entrez dans Heure de début l'**heure** à laquelle il doit être recherché un logiciel plus récent dans le serveur indiqué ci-dessus.
   d) Si vous utilisez pour le transfert un serveur proxy, cochez la case **Utiliser le proxy** et entrez les données pour le serveur proxy.
6) Cliquez sur **Appliquer**. Les données d'accès du serveur web interne sont reprises par défaut.

   Si un nouveau fichier image figure dans le serveur Web local, l'actualisation du logiciel est lancée et l'accord de licence est affiché (voir Comment actualiser le système à partir d'un serveur Web). Le démarrage de l'actualisation du logiciel peut toutefois être empêché si nécessaire.

24.3.2 Mise à jour du système de communication

La mise à jour du système de communication comprend la mise à jour non seulement du logiciel du système de communication lui-même, mais aussi des images logicielles des téléphones du système, qui sont stockées sur le système de communication. Une mise à jour complète de tous les composants du système peut ainsi être effectuée rapidement et facilement.

Avant chaque mise à jour logicielle, les données de configuration du système de communication doivent être sauvegardées (Sauvegarde et restauration).

Mise à jour via un serveur Web

Lors de l'exécution d'une mise à jour logicielle via un serveur web, c'est le serveur logiciel (serveur web Internet) qui est accédé par défaut.

Si un serveur web local est utilisé, le fichier image doit être stocké sur ce serveur.

Le système vérifie la présence de nouvelles mises à jour logicielles après avoir établi automatiquement une connexion au serveur web. Seuls les paquets

ayant subi des modifications par rapport à la version du logiciel installé sont transférés. Il est possible de sélectionner l'heure de début du transfert et de l'activation du logiciel. Si le délai d'activation du logiciel est atteint avant que la mise à jour logicielle n'ait été entièrement transférée au système, l'activation n'est pas exécutée automatiquement. Il faut alors définir manuellement une nouvelle heure d'activation.

Mise à jour via périphérique de stockage USB

Le fichier image est stocké sur un périphérique USB. Le périphérique de stockage USB doit être inséré dans le port serveur USB du système de communication. Ce type de mise à jour ne peut être effectué que par un administrateur de profil **Expert** et n'est pas possible pour Unify OpenScape Business S.

Mise à jour par téléchargement de fichier

Le fichier image se trouve dans un répertoire du réseau interne ou sur le PC de l'administrateur.

Mise à jour via un périphérique USB sans accès WBM

Le système de communication peut être mis à jour directement sans accès WBM via un périphérique USB. Cela nécessite que le périphérique USB soit branché sur le port serveur USB du système et que le fichier image soit situé à la racine du périphérique USB. Si une réinitialisation du système de communication est effectuée avec le périphérique USB inséré, la mise à jour du logiciel démarre automatiquement. Ce type de mise à jour n'est pas possible avec OpenScape Business S.

24.3.2.1 Comment actualiser le système à partir d'un serveur Web

Conditions préalables

Vous êtes connecté à WBM avec le profil **Avancé**.

Sur la page d´accueil de la WBM, il est indiqué qu'une nouvelle version logicielle est disponible.

Il existe un accès au serveur Web. Par défaut, la connexion avec le serveur Web local est établie. A la place, il est possible de configurer un serveur Web interne. (voir Utilisation d'un serveur Web local).

Si la mise à jour est réalisée via un serveur web local, il faut disposer sur le serveur web local du fichier Image le plus récent.

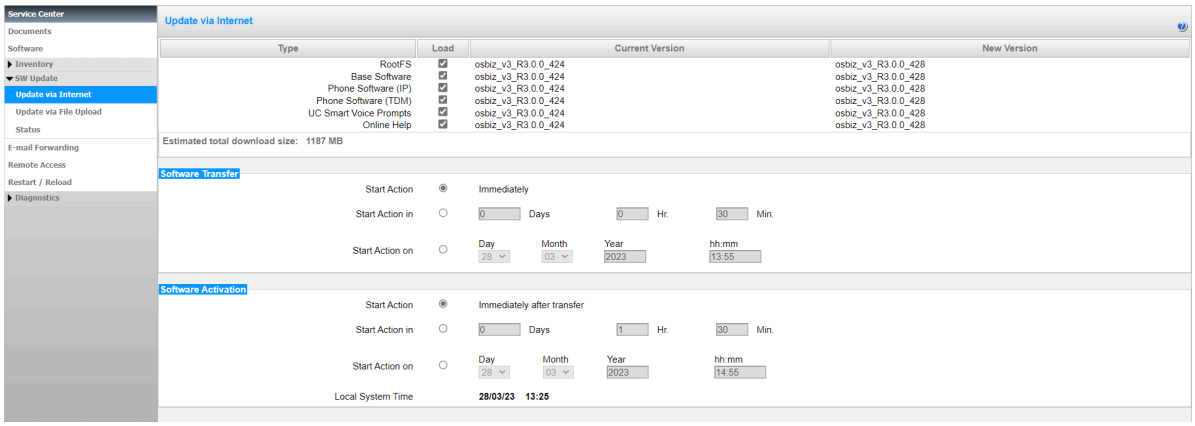
Étape par étape

1) Dans la barre de navigation, cliquez sur **Page d´accueil** puis tout d'abord sur le lien **Vous trouverez de plus amples détails à l'adresse suivante : Lien** Le système ouvre un fichier PDF avec des informations sur la nouvelle version de logiciel. Lisez les informations et tenez compte des indications sur la mise en route du système. Fermez la fenêtre pour terminer.
2) Cliquez dans la barre de navigation sur **Centre de service**.
3) Dans l'arborescence de navigation, cliquez sur **Mise à jour logicielle** > **Mise à jour via Internet**. Le système affiche la version de logiciel installée actuellement.

4) Cliquez sur **OK & Suivant**.

5) Lisez l'accord de licence (EULA) puis cliquez ensuite sur la case **J'accepte l'accord de licence**.

6) Cliquez sur **OK & Suivant**.



7) Désactivez si nécessaire les paquets qui ne doivent pas être actualisés dans la colonne **Charger**. Cela est par ex. utile sur les liaison Internet lentes ou lors de l'actualisation de logiciel via RNIS.

8) Sélectionnez les moments pour la transmission du logiciel et pour son activation :

- **Démarrage de l'action - Immédiat/immédiatement après la transmission** : Le logicel sera transféré immédiatement et activé juste après le transfert. La mise à jour logicielle est chargée en arrière-plan dans le système de communication. Après deux redémarrages, le logiciel est actualisé.
- **Démarrage de l'action le** : le logiciel est transmis ou activé une fois un certain délai écoulé. Indiquez la période en jours, heures et minutes.
- **Démarrage de l'action le** : le logiciel est transmis ou activé à un certain moment. Pour cela, indiquez la date et l'heure de ce moment.

Remarque : Lorsque le moment de l'activation du logiciel est atteint alors que la mise à jour logicielle n'est pas entièrement chargée sur le système, l'activation n'est pas effectuée automatiquement. Il faut définir manuellement une nouvelle heure d'activation.

---

9) Cliquez sur **OK & Suivant**. La mise à jour du logiciel est chargée dans le système et activée au moment fixé par vous. Pour l'activation du logiciel, il est effectué successivement deux redémarrages automatiques.

Remarque : Vous pouvez fermer la fenêtre du navigateur à tout moment.

---

10) Vous pouvez interroger l'état actuel de la mise à jour avec WBM dans **Centre de services** > **Mise à jour du logiciel** > **Etat**.

24.3.2.2 Comment actualiser le système à partir d'un support USB

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

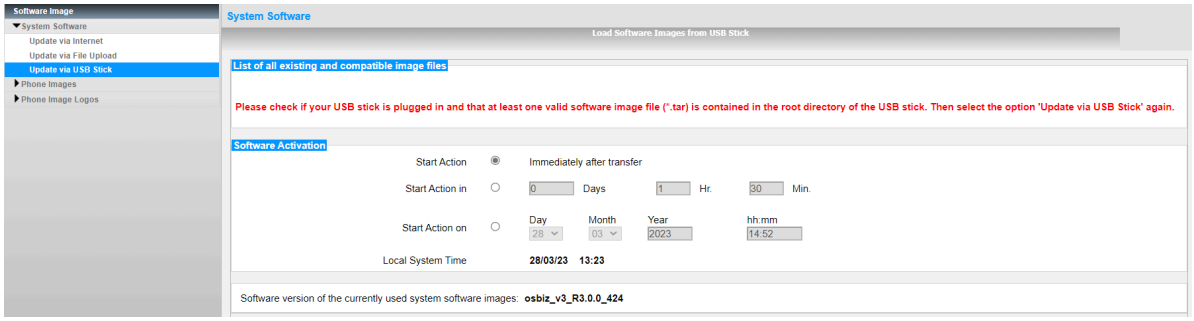
Le support USB doit être formaté avec FAT32.

Un fichier Image actuel est enregistré comme fichier tar sur le support USB. Il est également possible de déposer plusieurs fichiers Image dans des répertoires différents.

Si le support USB dispose de plusieurs partitions, le fichier Image doit être déposé dans la première partition.

Étape par étape

1) Insérez le support USB dans le port du serveur USB de la carte mère.
2) Dans la barre de navigation, cliquez sur **Mode Expert**.
3) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Image logicielle**.
4) Dans l'arborescence du menu, cliquez sur **Logiciel système**.
5) Cliquez sur **Mise à jour via clé USB**. Il vous est indiqué tous les fichiers Image valides, enregistrés sur le support USB, avec numéro de version et nom de fichier.



6) Si plusieurs fichiers Image sont enregistrés, sélectionnez le fichier Image souhaité, sinon le fichier Image fait l'objet d'une sélection automatique.
7) Sélectionnez le moment de l'activation du logiciel :
   - **Démarrage de l'action immédiatement après la transmission** : le logiciel est immédiatement activé après la transmission au système de communication.
   - **Démarrage de l'action le** : Le logiciel est immédiatement transmis au système de communication. Après un certain temps, le logiciel est activé. Indiquez la période en jours, heures et minutes.
   - **Démarrage de l'action le** : Le logiciel est immédiatement transmis au système de communication. Le logiciel est activé à un moment défini. Pour cela, indiquez la date et l'heure de ce moment.
8) Cliquez sur **Charger**. Le fichier Image est transmis dans le système de communication et sa cohérence est vérifiée. Pour ces deux opérations, plusieurs minutes sont nécessaires. Pendant ce temps, le support USB doit rester enfiché.
9) Retirez le support USB dès que WBM vous l'indique et cliquez sur **Quitter**. Au moment indiqué de l'activation du logiciel, il est effectué automatiquement deux redémarrages successifs.

10) Vous pouvez interroger l'état actuel de la mise à jour avec WBM dans **Centre de services** > **Mise à jour du logiciel** > **Etat**.

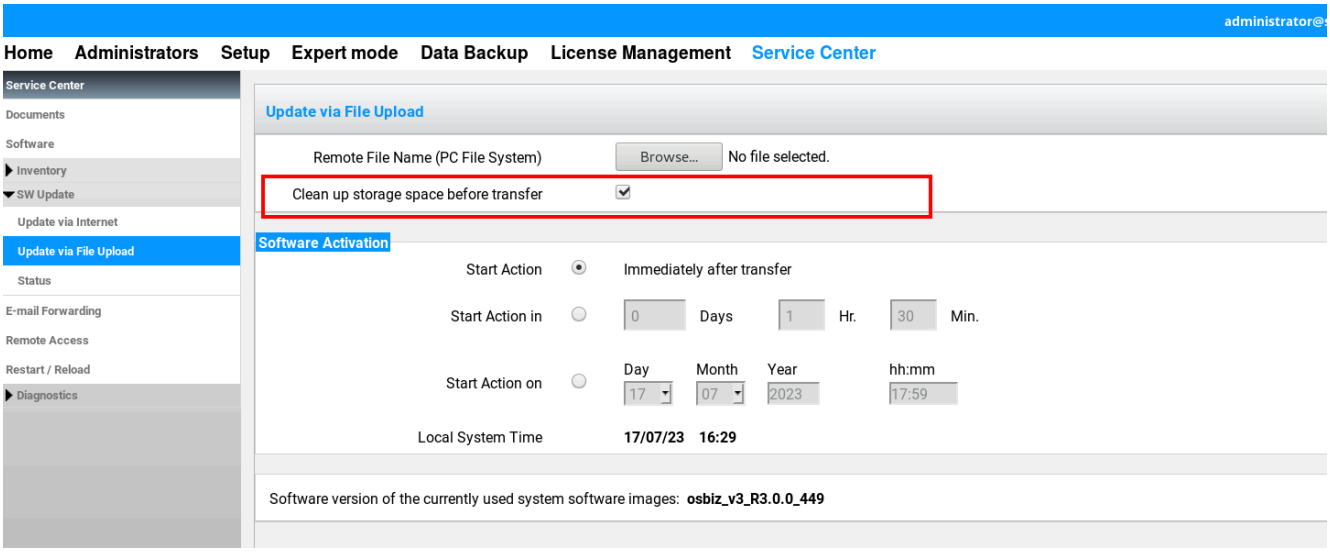
24.3.2.3 Comment actualiser le système à partir d'un chargement de fichier

Conditions préalables

Le fichier Image est enregistré comme fichier tar dans le réseau interne ou directement sur le PC Admin, et l'emplacement d'enregistrement est connu. Si un fichier tgz est enregistré, le fichier tar doit être extrait du fichier tgz.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Mise à jour logicielle** > **Mise à jour via chargement du fichier**. Le système affiche la version de logiciel installée actuellement.
3) Cliquez sur **OK & Suivant**.



4) A l'aide du bouton **Parcourir** allez à l'endroit où est stocké le fichier image (`*.tar`).
5) L'option **Nettoyer l'espace de stockage avant le transfert** est activée par défaut. Les actions suivantes sont déclenchées pour libérer de la mémoire de stockage en vue du téléchargement du fichier logiciel.
   - Tous les journaux et traces sont supprimés.
   - Toutes les images logicielles du téléphone sont supprimées.
   - Les éventuels vidages TCP sont supprimés.

6) Sélectionnez le moment de l'activation du logiciel :
   - **Démarrage de l'action immédiatement après la transmission** : Le logiciel est immédiatement transmis au système de communication, en arrière-plan. Après deux redémarrages, le logiciel est actualisé.
   - **Démarrage de l'action le** : Le logiciel est immédiatement transmis au système de communication, en arrière-plan. Après un certain temps, le logiciel est activé. Indiquez la période en jours, heures et minutes.
   - **Démarrage de l'action le** : Le logiciel est immédiatement transmis au système de communication, en arrière-plan. Le logiciel est activé à un moment défini. Pour cela, indiquez la date et l'heure de ce moment.
7) Cliquez sur **OK & Suivant**.
8) Le fichier Image est transmis dans le système de communication et sa cohérence est vérifiée. Pour ces deux opérations, plusieurs minutes sont nécessaires.

   Remarque : Si vous fermez la fenêtre du navigateur durant le transfert de logiciel, l'opération est interrompue. Durant le contrôle de cohérence, vous pouvez continuer à utiliser la WBM ou la fermer.
9) Si le logiciel doit être activé immédiatement, il est effectué deux redémarrages successif à l'issue du contrôle de cohérence réussi.
10) Si le logiciel n'est pas immédiatement activé, cliquez sur **Quitter** une fois la transmission effectuée. Pour l'activation du logiciel, il est effectué successivement deux redémarrages automatiques.
11) Vous pouvez interroger l'état actuel de la mise à jour avec WBM dans **Centre de services** > **Mise à jour du logiciel** > **Etat**.

24.3.2.4 Comment actualiser le système à partir d'un support USB sans accès WBM

Conditions préalables

Le support USB doit être formaté avec FAT32.

Un fichier Image actuel est enregistré comme fichier tar dans le niveau de répertoire supérieur du support USB. Un seul fichier Image peut être déposé à ce niveau.

Si le support USB dispose de plusieurs partitions, le fichier Image doit être déposé dans la première partition.

La version logicielle du fichier Image doit être plus récente que la version logicielle du système. Attention : l'actualisation se fait également sur des versions logicielles plus anciennes.

Le système de communication est démarré.

Étape par étape

1) Insérez le support USB dans le port du serveur USB de la carte mère.
2) Appuyer sur le bouton de réinitialisation durant 1 à 4 secondes. Le système d'arrêt et lance un redémarrage.

   Le logiciel est contrôlé durant la montée en puissance. Si le support USB contient un fichier Image adapté, le fichier est chargé dans le système de communication. La LED rouge clignote à un rythme de 1Hz (0,5 s allumée /

0,5 s éteinte). Une fois la copie terminée, le logiciel est décompressé et les données client sont automatiquement reprises. La LED rouge clignote au rythme de 5Hz (100 ms allumée / 100 ms éteinte).

3) Retirez le support USB lorsque la LED rouge clignote à un rythme de 5 Hz.
4) Pour terminer, le système effectue automatiquement deux nouveaux démarrages successifs. Si die LED verte clignote à un rythme de 1 Hz (0,5 s allumée / 0,5 s éteinte), le système est de nouveau en service.

24.3.3 Mise à jour des téléphones système

Le logiciel des téléphones système est actualisé à partir d'un fichier Image. Il existe un fichier Image spécifique pour chaque type de téléphone système ; ce fichier contient le logiciel de téléphonie correspondant à ce type. Ces fichiers Image sont contenus dans le logiciel du système de communication Inclus et sont chargés automatiquement dans le système de communication lors de la mise à jour.

Par défaut, les téléphones système IP reçoivent automatiquement le logiciel le plus actuel. Si un téléphone système IP est reconfiguré dans la WBM (d'un **Client TFA** en **Client SIP** ou inversement), il est automatiquement chargé sur le téléphone système IP, via DLI, le logiciel correspondant, enregistré dans le système de communication. Sur les téléphones système IP, déjà en service dans le système ou dans un autre système, il faut tout d'abord rétablir les paramètres usine (Factory Reset) avant que ne puisse être effectuée l'actualisation du logiciel.

L'administrateur peut, à l'aide de WBM, transmettre manuellement à tous les téléphones système IP d'un même type un logiciel de téléphonie différent du logiciel par défaut. La mise à jour du logiciel pour les téléphones système UP0 est effectuée avec Manager E.

Si un logiciel téléphonique (fichier image) est sélectionné par défaut dans WBM, cette image est automatiquement transférée à chaque téléphone système appartenant à ce type, lors de la première connexion au système.

Lors d'une mise à jour manuelle, veillez à ce que le logiciel des téléphones système soit compatible avec la version de logiciel du système de communication (voir Release Note).

Concepts associés

Logos Téléphone à la page 1170

24.3.3.1 Comment charger le logiciel de téléphonie dans le système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Les fichiers Image sont enregistrés dans le réseau local et l'emplacement d'enregistrement est connu. Un fichier Image propre est nécessaire pour chaque type de téléphone système.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Image logicielle**.
3) Dans l'arborescence du menu, double-cliquez sur **Images du téléphone**.
4) Cliquez sur **Charger**. Une liste des fichiers Images actuellement présents dans le système de communication s'affiche.
5) Avec **Nom de fichier distant (système de fichiers PC)**, **Parcourir** aller à l'emplacement de stockage du fichier image (`*.app`).
6) Cliquez sur **Charger**. Le fichier Image est chargé et l'absence d'erreur contrôlée.

Remarque : En cas d'erreur, vous voyez un message d'erreur. Vérifiez vos entrées et répétez les étapes 5 à 6.

---

7) Si les résultats du contrôle sont positifs, validez avec **OK**. Le fichier Image est repris dans la liste des fichiers Image actuellement présents dans le système de communication.
8) Si vous souhaitez charger d'autres fichiers Image pour d'autres types de téléphones système, répétez les étapes 5 à 7.

24.3.3.2 Comment distribuer le logiciel téléphone aux téléphones système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Image logicielle**.
3) Dans l'arborescence du menu, double-cliquez sur **Images du téléphone**.
4) Si vous souhaitez distribuer une image téléphone à tous les téléphones système d'un type :
   a) Cliquez sur **Distribuer**. Une liste des fichiers Images actuellement présents dans le système de communication s'affiche.
   b) Cocher **Distribuer** sur l'image ou les images du téléphone souhaitées.
5) Si vous souhaitez distribuer une image téléphone à un téléphone système défini :
   a) Cliquez sur **Distribuer par terminal**. Le système affiche une liste des téléphones système.
   b) Dans la liste déroulante **Logiciel distribuable**, sélectionnez l'image téléphone pour le ou les téléphones système souhaités.
6) Cliquez sur **Appliquer**.

24.3.3.3 Comment effacer le logiciel de téléphonie

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Image logicielle**.
3) Dans l'arborescence du menu, double-cliquez sur **Images du téléphone**.
4) Cliquez sur **Charger**. Une liste des fichiers Images actuellement présents dans le système de communication s'affiche.
5) Dans la ligne de l'image téléphone à effacer, cochez la case **Effacer**.
6) Si vous souhaitez effacer d'autres images téléphone, répétez l'opération précédente.
7) Cliquez sur **Effacer**. Toutes les images téléphone sélectionnées sont effacées du système de communication.

24.3.3.4 Comment activer ou désactiver la diffusion automatique du logiciel de téléphonie

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Image logicielle**.
3) Dans l'arborescence du menu, double-cliquez sur **Images du téléphone**.
4) Cliquez sur **Distribuer**. Une liste des fichiers Images actuellement présents dans le système de communication s'affiche.
5) Si le logiciel de téléphonie doit être automatiquement transmis aux téléphones système, cochez dans la ligne du fichier Image souhaité la case **Par défaut** (réglage par défaut).
6) Si le logiciel de téléphonie ne doit pas être automatiquement transmis aux téléphones système, décochez dans la ligne du fichier Image souhaité la case **Par défaut**.
7) Cliquez sur **Appliquer**.

24.3.3.5 Comment configurer le reflashing automatique

Le reflashing automatique est un moyen simple de flasher les logiciels HFA uniquement pour les téléphones de bureau OpenScape IP 35G Eco et OpenScape CP 100/110/200/205/210/400/600/600E/700/700X/710 neufs ou réinitialisés aux paramètres d'usine, à l'aide du serveur DLI du système.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Remarque : Le reflashing automatique fonctionne uniquement pour les appareils neufs (sortis de l'usine). De plus, les paramètres d'usine doivent être restaurés sur l'appareil

("Rétablir les paramètres d'usine") avant d'effectuer le reflashing automatique.

Étape par étape

1) Configurez l'appareil en attribuant un numéro et en le définissant en tant que client système :
   a) Dans la barre de navigation, cliquez sur **Mode Expert**.
   b) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie > Abonnés > Clients IP**.
   c) Saisissez le numéro d'appel interne dans le champ **N° d'appel**.
   d) Saisissez le numéro public dans le champ **SDA**.
   e) Saisissez un nom pour l'appareil.
   f) Sélectionnez **Client système** à partir du menu déroulant **Type**.
   g) Cliquez sur **Appliquer**.

2) Configurez le serveur DHCP pour qu'il envoie l'adresse IP de DLI via l'option DHCP :
   a) Dans la barre de navigation, cliquez sur **Mode Expert**.
   b) Dans l'arborescence de navigation, cliquez sur **Serveur de téléphonie > Interfaces réseau > DHCP > Serveur DHCP > Modifier les paramètres généraux**.
   c) Cochez l'option **Utiliser le DLI interne** dans la section **Serveur DNS**.

3) Branchez l'appareil et spécifiez le numéro du terminal une fois que le téléphone est démarré.

4) Le téléphone est également enregistré dans la base de données DLI. Pour vérifier l'enregistrement de l'appareil :
   a) Cliquez sur **Mode Expert** dans la barre de navigation.
   b) Dans l'arborescence de navigation, cliquez sur **Maintenance > Image logicielle** .
   c) Dans l'arborescence du menu, cliquez sur **Images du téléphone**.
   d) Cliquez sur **Déployer sur l'appareil**.

5) Le reflashing automatique démarre et charge le logiciel HFA enregistré dans le système de communication sur l'appareil.

Remarque : Ne débranchez pas l'appareil pendant cette opération.

L'appareil est maintenant configuré.

Remarque : Si l'appareil est réglé sur SIP (sous **Serveur de téléphonie > Abonné > Clients IP**), une mise à jour vers le logiciel SIP le plus récent sera effectuée, uniquement

si la mise à jour est disponible dans la version logicielle correspondante.

Lorsqu'un client SIP est remplacé par un client système, un redémarrage manuel du téléphone est nécessaire pour charger le logiciel HFA.

Remarque : En cas d'échec du reflashing, les paramètres d'usine doivent être rétablis ("Rétablir les paramètres d'usine") sur l'appareil.

24.3.4 Etat du logiciel

L'état du logiciel (software-status) indique la version et l'actualisation du logiciel.

Les états suivants peuvent être affichés :

- version actuelle du logiciel
- version plus actuelle disponible pour mise à jour
- moment où aura lieu l'actualisation du logiciel
- nouveau logiciel actuellement en cours de chargement dans le système
- chargement réussi ou échec du chargement

24.3.4.1 Comment interroger l'état du logiciel

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

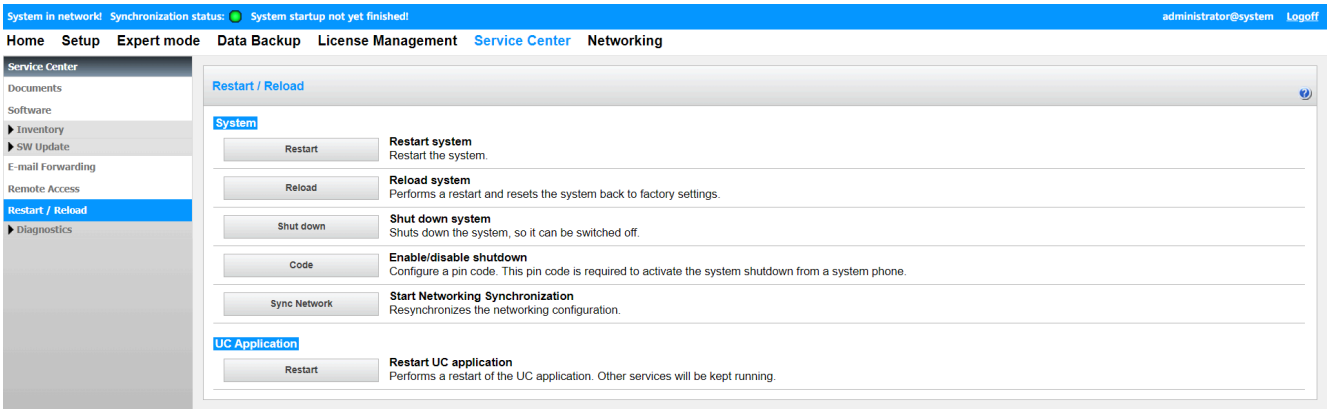
1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Mise à jour logicielle** > **Etat**. La version actuelle du logiciel s'affiche. Cette information est affichée sur la page d'accueil de la WBM.

   Si une mise à jour du logiciel se déroule en arrière-plan, cela vous est indiqué ici.

   Si une nouvelle mise à jour du logiciel est disponible sur le serveur web, cela vous est indiqué ici. Cette information est affichée sur la page d'accueil de la WBM.

24.4 Redémarrer, recharger, éteindre

Vous pouvez utiliser les fonctionnalités associées pour lancer un redémarrage ou un rechargement des systèmes de communication OpenScape Business et pour un arrêt contrôlé d'OpenScape Business X. De plus, un redémarrage (redémarrage) de l'application UC (UC Smart ou UC Suite) est déclenché. Pour permettre l'arrêt contrôlé d'OpenScape Business X via un téléphone système, un code PIN peut être défini.



24.4.1 Redémarrage d'OpenScape Business

La fonction **Redémarrer le système** peut être utilisée pour lancer un redémarrage contrôlé d'Unify OpenScape Business.

Les différences suivantes doivent être observées :

- OpenScape Business S et OpenScape Business X

  Un redémarrage contrôlé du système de communication a lieu. Le système de communication sera de nouveau opérationnel après le redémarrage.

  Le temps de démarrage dépend de la configuration du système et du scénario de réseau OpenScape Business.

Lors d'un redémarrage, toutes les applications actives telles que myPortal pour ordinateur et myPortal pour Outlook, par exemple, sont déconnectées. Après le redémarrage, toutes les connexions sont automatiquement rétablies.

24.4.1.1 Comment lancer un redémarrage d'OpenScape Business

La fonction **Redémarrer le système** peut être utilisée pour lancer un redémarrage d'Unify OpenScape Business.

Conditions préalables

Vous êtes connecté au WBM avec le profil **Avancé** .

Conseil : Lors d'un redémarrage, toutes les applications actives telles que myPortal pour ordinateur et myPortal pour Outlook, par exemple, sont déconnectées. Après le démarrage, toutes les connexions sont automatiquement rétablies.

Étape par étape

1) Cliquez sur **Centre de services** dans la barre de navigation.
2) Cliquez sur **Redémarrer / Recharger** dans l'arborescence de navigation.

3) Cliquez sur **Redémarrer le système**, puis sur **OK**. OpenScape Business effectue un redémarrage (redémarrage).

   OpenScape Business S et OpenScape Business X : Le système de communication sera de nouveau opérationnel après le redémarrage.

24.4.2 Rechargement d'OpenScape Business

La fonction **Reload system** peut être utilisée pour lancer un rechargement d'Unify OpenScape Business.

Les différences suivantes doivent être observées :

- OpenScape Business S et OpenScape Business X

  Le système de communication est rechargé. Après le redémarrage suivant, le système de communication sera dans son état par défaut.

  – Tous les paramètres spécifiques au pays et au client ont été supprimés (code pays du système = Allemagne).
  – Le système de communication a l'adresse IP par défaut 192.168.1.2 et la plage d'adresses IP internes 192.168.3.xxx.
  – La licence est conservée.

  Le temps de démarrage dépend de la configuration du système.

24.4.2.1 Comment lancer un rechargement d'OpenScape Business

La fonction **Reload system** peut être utilisée pour lancer un rechargement d'Unify OpenScape Business.

Conditions préalables

Vous êtes connecté au WBM avec le profil **Avancé** .

OpenScape Business S et OpenScape Business X : Les données de configuration du système de communication ont été enregistrées dans un ensemble de sauvegarde.

Remarque :

Le rechargement rétablit le système de communication à son état par défaut. Tous les paramètres spécifiques au pays et au client sont supprimés (code pays du système = Allemagne). L'adresse IP par défaut (192.168.1.2) du système de communication est réinitialisée.

Étape par étape

1) Cliquez sur **Centre de services** dans la barre de navigation.
2) Cliquez sur **Redémarrer / Recharger** dans l'arborescence de navigation.
3) Cliquez sur **Appliquer**, puis sur **OK**. OpenScape Business se recharge.

Conseil : OpenScape Business S et OpenScape Business X : après le redémarrage suivant, le système de communication sera dans son état par défaut. Une

fois les paramètres Basic configurés à l'aide de l'assistant de **Première Installation**, les sauvegardes de données spécifiques au pays et au client peuvent être rechargées. Pour des informations plus détaillées sur la procédure, voir Restaurer.

24.4.3 Arrêt (shutdown) d'OpenScape Business X

À l'aide de la fonction **Arrêter le système**, il est possible d'effectuer un arrêt contrôlé des systèmes de communication OpenScape Business X.

24.4.3.1 Comment arrêter OpenScape Business X

La fonction **Arrêter le système** peut être utilisée pour arrêter gracieusement les systèmes de communication Unify OpenScape Business X, c'est-à-dire pour effectuer un arrêt contrôlé.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Redémarrer/Recharger**.
3) Cliquez sur **Arrêter le système**, puis sur **OK**. Un arrêt contrôlé du système de communication est effectué.

Conseil : la montée en puissance du système de communication est uniquement possible en retirant puis en insérant de nouveau la fiche secteur.

OpenScape Business X8 : la montée en puissance ultérieure du système de communication est uniquement possible en désactivant puis en réactivant toutes les alimentations électriques LUNA2.

24.4.4 PIN pour l'arrêt contrôlé (Shutdown) de OpenScape Business X

L'activation de l'arrêt (shutdown) par le téléphone système est protégée par un PIN.

Lors de l'activation à l'aide d'un téléphone système, il faut toujours entrer le PIN configuré dans le système de communication. La configuration de ce PIN est assurée par un administrateur de profil **Advanced**.

24.4.4.1 Comment configurer un PIN pour l'arrêt contrôlé (Shutdown) d'OpenScape Business X

Le PIN sert à l'activation d'un arrêt (shutdown) à l'aide d'un téléphone système.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Avancé**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Redémarrer/Recharger**.
3) Cliquez sur **Activer/désactiver l'arrêt**.
4) Dans le champ **PIN** entrez le PIN à six caractères.
5) Cliquez sur **Enregistrer** puis sur OK.

Étapes suivantes

L'activation d'un arrêt à l'aide d'un téléphone système est réalisé par l'entrée de l'indicatif correspondant (indicatif par défaut = *997) suivie de la saisie du PIN à six positions.

- Pour les téléphones IP : vous pouvez exécuter l’arrêt contrôlé depuis les deux premiers terminaux configurés.
- Pour les téléphones UP0 : vous pouvez exécuter l’arrêt contrôlé depuis chacun de ces téléphones. Dans ce cas, les clients IP ne disposent pas des droits d’exécution d’un arrêt.

24.4.5 Redémarrage (restart) de l'application UC

A l'aide de la fonction **Redémarrer l'application UC** vous pouvez, en tant qu'administrateur, lancer un redémarrage (restart) contrôlé de l'application UC (UC Smart ou UC Suite).

Lors du redémarrage de l'application UC, les liaisons avec toutes les applications actives comme myPortal for Desktop, myPortal Smart et myAttendant sont coupées. Après la remise en route, toutes les liaisons sont automatiquement rétablies.

24.4.5.1 Comment lancer le redémarrage (restart) de l'application UC

La fonction **Redémarrer l'application UC** vous permet d'effectuer un redémarrage (restart) de l'application UC (UC Smart ou UC Suite).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Conseil : Lors du redémarrage, les liaisons avec toutes les applications actives comme myPortal for Desktop, myPortal Smart et myAttendant sont coupées. Après la remise en route, toutes les liaisons sont automatiquement rétablies.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Redémarrer/Recharger**.
3) Cliquez sur **Redémarrer l'application UC** puis sur **OK**. L'application UC effectue un Restart (redémarrage).

24.5 Gestion Inventory

Gestion Inventory (Inventory-Management) correspond à la détermination de l'état actuel des systèmes de communication OpenScape Business X et OpenScape Business S ainsi que de la configuration matérielle des systèmes de communication OpenScape Business X.

24.5.1 Etat du système

Un administrateur est en mesure de déterminer avec la WMB l'état actuel des systèmes de communication OpenScape Business X et OpenScape Business S. Il peut être récupéré des informations sur l'état des abonnés, de l'établissement de la connexion, des ITSP et des VPN ainsi que la liste des adresses IP configurées.

Etat de l'abonné

L'état de l'abonné permet d'interroger les informations suivantes via les abonnés paramétrés :

- Numéro de l'abonné
- Nom
- Type d’équipement
- Adresse IP (il est affiché en plus pour les téléphones système une lien permettant d'ouvrir la WBM du téléphone.)
- Adresse MAC
- Version actuelle du logiciel
- Version matérielle
- Etat (Activé/Désactivé)

Etat de l'établissement de la liaison

L'état d'établissement de la liaison permet d'interroger les informations via les connexions établie avec les partenaires du RTC (réseau téléphonique commuté, par exemple les réseaux de télécommunications publics ou privés) du système de communication OpenScape Business X.

Etat ITSP

L'état du ITSP permet d'interroger les informations concernant l'état actuel des fournisseurs de service de téléphonie sur Internet (ITSP) préconfigurés et éventuellement ajoutés. Il est également affiché les correspondances entre abonnés et ITSP.

L'état de chaque ITSP actif est indiqué par la couleur du carré correspondant (vert = OK, orange = au moins un abonné a été paramétré de manière non exempte d'erreur).

Etat VPN

L'état VPN permet d'interroger les informations via les tunnels VPN configurés du système de communication OpenScape Business X.

Aperçu des adresses IP

Les adresses IP configurées dans le système de communication OpenScape Business X sont affichées.

Il est également indiqué l'assistant et les menus en mode Expert permettant de configurer les adresses IP.

De plus, un aperçu de l'état de la Carte Booster et des interfaces Ethernet de la carte mère est affiché.

24.5.1.1 Comment consulter l'état de l'abonné

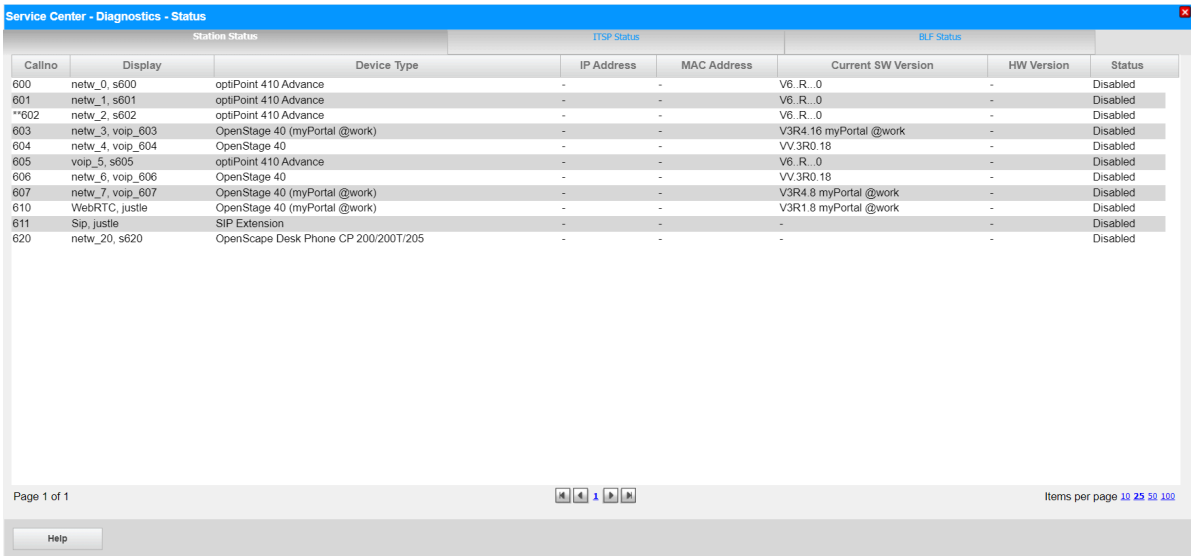
L'Assistant **Etat** permet d'identifier l'état actuel de tous les abonnés paramétrés.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Etat**.
3) Cliquez sur l'onglet **Etat de l'abonné**. Le système affiche l'état de tous les abonnés paramétrés.



4) Cliquez sur **Terminer**.

24.5.1.2 Comment interroger l'état d'établissement de la liaison

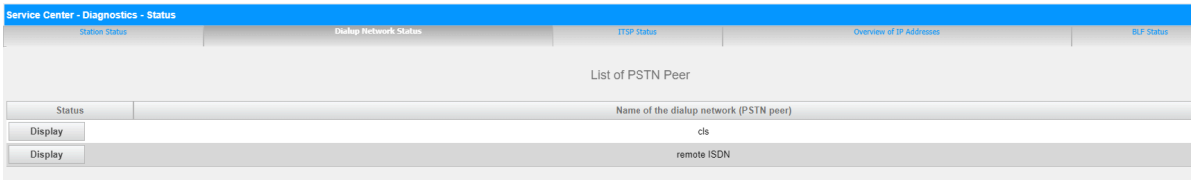
Avec l'assistant **Etat**, vous pouvez déterminer l'état actuel des partenaires RTC d'un système de communication OpenScape Business X.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Etat**.
3) Cliquez sur l'onglet **Etat Etablissement de la liaison**. Le système affiche la liste des partenaires RTC.
4) Sur la ligne de la connexion souhaitée (partenaires RTC) cliquez sur **Afficher**. L'état actuel de cette connexion (partenaire RTC) est affiché.



5) Si vous voulez afficher les informations d'état d'une autre connexion (partenaires RTC), procédez comme indiqué à l'étape 3.
6) Cliquez sur **OK** puis sur **Quitter**.

24.5.1.3 Comment interroger l'état ITSP

L'assistant **Etat** vous permet de déterminer l'état actuel du fournisseur de service de téléphonie Internet (ITSP).

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Etat**.
3) Cliquez sur l'onglet **Etat ITSP**. Il est affiché l'état actuel du fournisseur de service de téléphonie sur Internet (ITSP) préconfiguré à l'état actif et de tout autre fournisseur éventuellement ajouté.
4) Cliquer sur **Diagnostiquer** pour obtenir des informations supplémentaires sur la connexion SIP.
5) Cliquez sur **Terminer**.

24.5.1.4 Comment afficher les adresses IP

Avec l'assistant **Etat** vous pouvez appeler un aperçu des adresses IP configurées dans un système de communication OpenScape Business X. Il

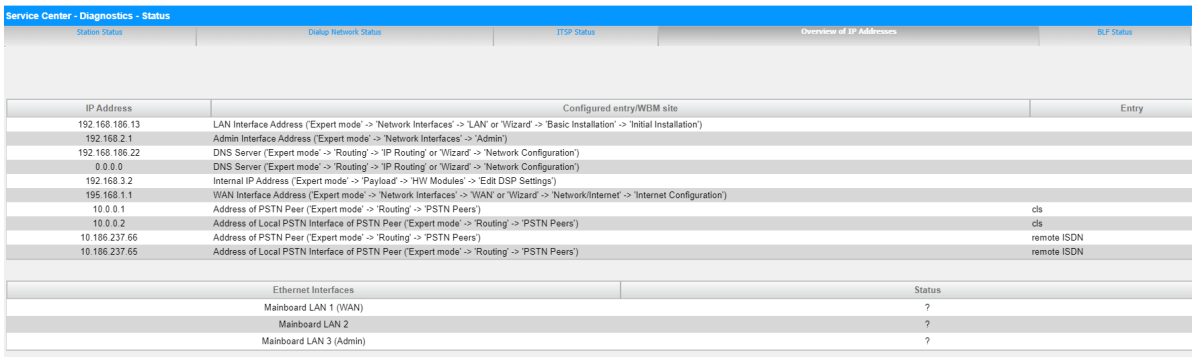
est également indiqué l'assistant et les menus en mode Expert permettant de configurer les adresses IP.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Etat**.
3) Cliquez sur l'onglet **Aperçu adresses IP**. Une liste des adresses IP configurées dans le système de communication s'affiche.



4) Cliquez sur **Quitter**.

24.5.2 Inventaire

L'inventaire permet à un administrateur de récupérer des informations sur le matériel et les logiciels d'OpenScape Business X et les logiciels d'OpenScape Business S.

OpenScape Business X

Les informations suivantes peuvent être récupérées :

- Système de communication

  Les informations suivantes sont notamment affichées :

  – Représentation graphique du système de communication et des cartes
  – Référence de la carte mère, adresse MAC, adresse IP, nom d'hôte et version du logiciel
  – Type d'UCT et RAM (en Go) du système
  – Détails sur la quantité de mémoire, y compris l'espace disponible et utilisé sur la carte SDHC
  – Statut de toutes les applications
- Cartes

  Les informations affichées comprennent les éléments suivants : emplacement, type, numéro de pièce et état de toutes les cartes installées.

OpenScape Business S

Les informations suivantes peuvent être récupérées :

- Logiciel

  Entre autres, les informations suivantes sont affichées : adresse MAC, adresse IP, nom d'hôte et version du logiciel.
- Informations sur le disque dur

  Détails sur la quantité de mémoire, y compris la mémoire disponible et utilisée.
- Applications

  Toutes les applications et leur statut respectif sont affichés.

24.5.2.1 Comment interroger Inventory d'OpenScape Business X

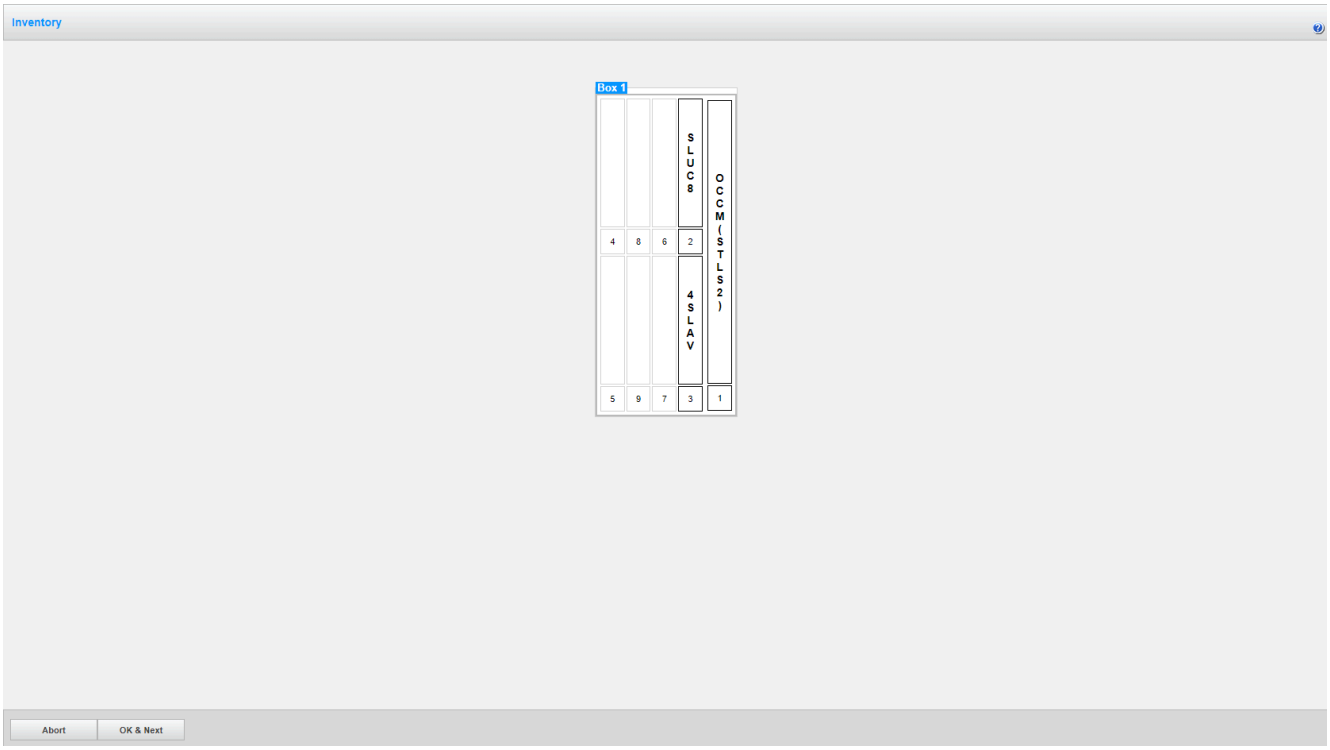
L'assistant **Inventaire** permet de connaître l'état actuel du matériel et des logiciels des systèmes de communication Unify OpenScape Business X.

Conditions préalables

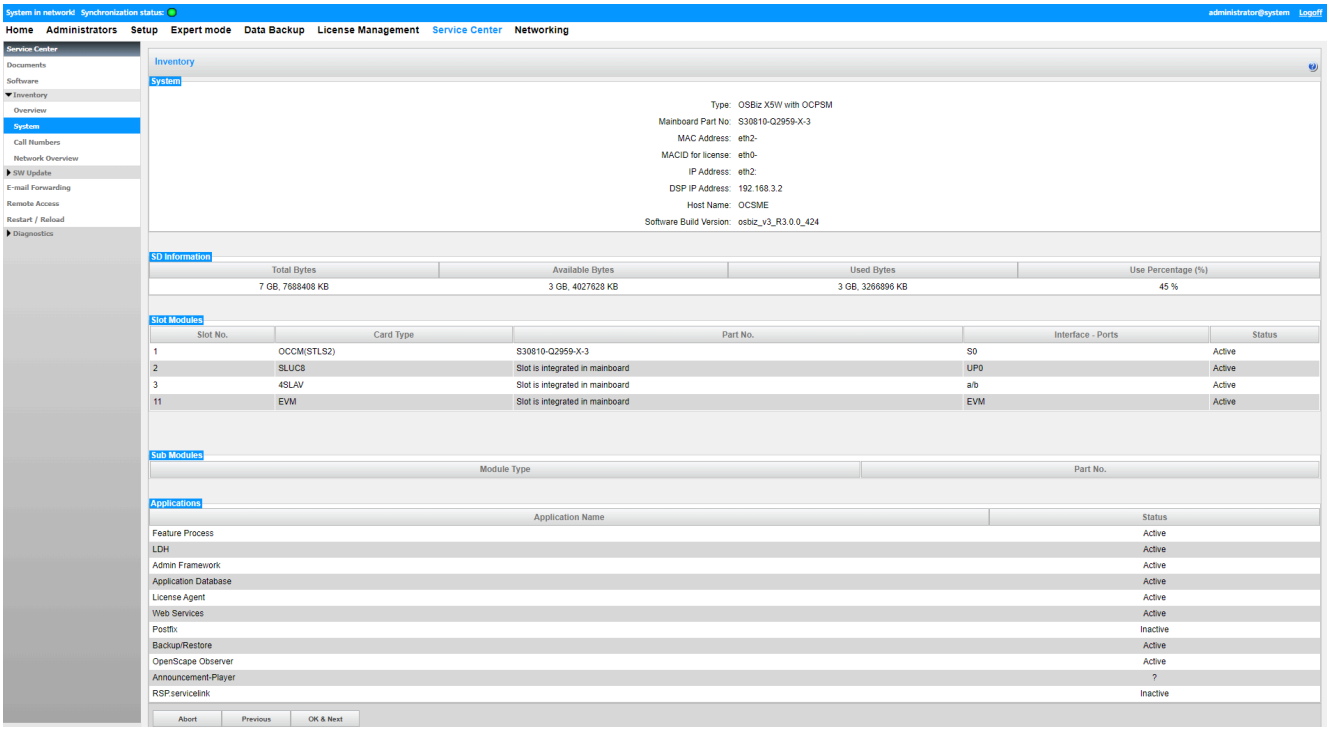
Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Inventaire** > **Vue d'ensemble**. Il vous est présenté une représentation graphique du système de communication et des modules.



3) Cliquez sur **OK & Suivant**. Il vous est fourni des informations sur le système de communication, sur la mémoire disponible et occupée de la carte SDHC, sur les modules et sur l'état de l'application.



4) Cliquez sur **OK & Suivant**.
5) Cliquez sur **Terminer**.

24.5.2.2 Comment interroger Inventory d'OpenScape Business S

L'Assistant **Inventory** permet de connaître l'état actuel des logiciels d'OpenScape Business S.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Inventory**. Il est affiché des informations sur le logiciel du système de communication, sur la capacité mémoire disponible et occupée sur les disques dur et sur l'état de l'application.

24.6 Actions automatiques

Cette fonction permet de définir des actions à effectuer une fois ou plusieurs fois. Ces actions sont alors effectuées automatiquement par le système de communication au moment paramétré.

24.6.1 Action automatique Regroupement des positions non utilisées

L'action automatique Regroupement des positions non utilisées permet d'effectuer régulièrement un nettoyage périodique automatique de la mémoire sur le système de communication. Une fois terminé le nettoyage automatique de la mémoire, le système de communication effectue un redémarrage (Restart).

Lors de la représentation dans l'arborescence du menu, la couleur du point dans la liste indique l'état de l'action (vert = action activée, rouge = action non activée).

En sélectionnant **Démarrer/Arrêter l'action**, il est possible d'activer/démarrer une action non active (point rouge) ou de désactiver/arrêter une action active (point vert).

Par défaut, l'action automatique Regroupement des positions non utilisées n'est pas activée.

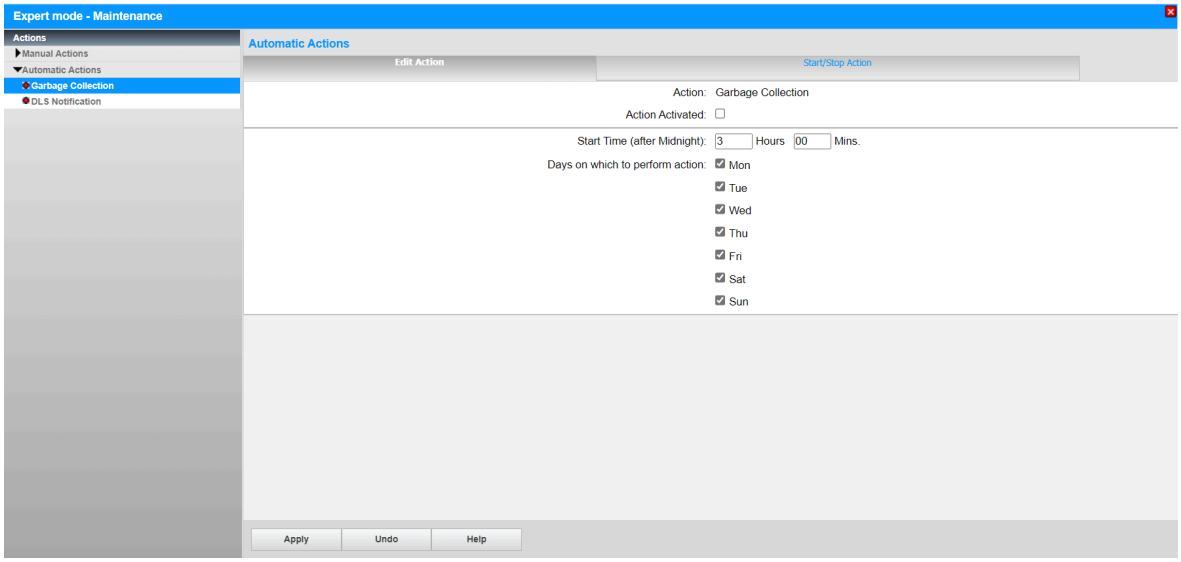
24.6.1.1 Comment modifier l'action automatique Regroupement des positions non utilisées

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Actions**.
3) Dans l'arborescence du menu, allez à **Actions** > **Actions automatiques** > **Regroupement des positions non utilisées**.
4) Cliquez sur l'onglet **Modifier l'action**.



5) Sélectionnez le paramètre souhaité :
   - Si l'action Regroupement des positions non utilisées doit être effectuée, cochez la case **Action activée**.
   - Si l'action Regroupement des positions non utilisées ne doit pas être effectuée, décochez la case **Action activée**.
6) Si nécessaire, modifiez le **Point de démarrage après minuit**.

   Dans le champ **Heure** entrez les heures et dans le champ **Min.** les minutes à l'issue desquelles l'action doit être lancée.

   Exemple : Dans le champ **h.** il a été inscrit `3` et dans le champ **min.** `30`. Cela signifie que l'action Regroupement des positions non utilisées sera lancée le matin, à 3h30.
7) Si nécessaire, modifiez les jours de la semaine par **Exécuter l'action les jours de semaine suivants**.

   Cochez les cases correspondant aux jours de la semaine où l'action doit être effectuée. Décochez les cases correspondant aux jours de la semaine où l'action ne doit pas être effectuée.
8) Cliquez sur **Appliquer** puis sur **OK**.

24.6.1.2 Comment lancer (activer) l'action automatique Regroupement des positions non utilisées

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Actions**.
3) Dans l'arborescence du menu, double-cliquez sur **Actions** > **Actions automatiques**. Dans l'arborescence du menu, il est affiché le nom de toutes les actions automatiques. Les actions activées sont identifiées par un point vert sur la liste. Les actions activées sont identifiées par un point vert sur la liste.
4) Dans l'arborescence du menu, cliquez sur **Regroupement des positions non utilisées**.
5) Cliquez sur l'onglet **Démarrer/Arrêter l'action**.
6) Cliquez sur **Démarrer** et ensuite sur **OK**.

24.6.1.3 Comment arrêter (désactiver) l'action automatique Regroupement des positions non utilisées

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Actions**.

3) Dans l'arborescence du menu, double-cliquez sur **Actions** > **Actions automatiques**. Dans l'arborescence du menu, il est affiché le nom de toutes les actions automatiques. Les actions activées sont identifiées par un point vert sur la liste. Les actions activées sont identifiées par un point vert sur la liste.
4) Dans l'arborescence du menu, cliquez sur **Regroupement des positions non utilisées**.
5) Cliquez sur l'onglet **Démarrer/Arrêter l'action**.
6) Cliquez sur **Arrêter** et ensuite sur **OK**.

24.6.2 Action automatique Notification DLS

L'action automatique Notification DLS peut lancer la connexion automatique à un serveur DLS externe lors de la mise en route du système de communication.

Lors de la représentation dans l'arborescence du menu, la couleur du point dans la liste indique l'état de l'action (vert = action activée, rouge = action non activée).

En sélectionnant **Démarrer/Arrêter l'action**, il est possible d'activer/démarrer une action non active (point rouge) ou de désactiver/arrêter une action active (point vert).

Par défaut, l'action automatique Notification DLS n'est pas activée.

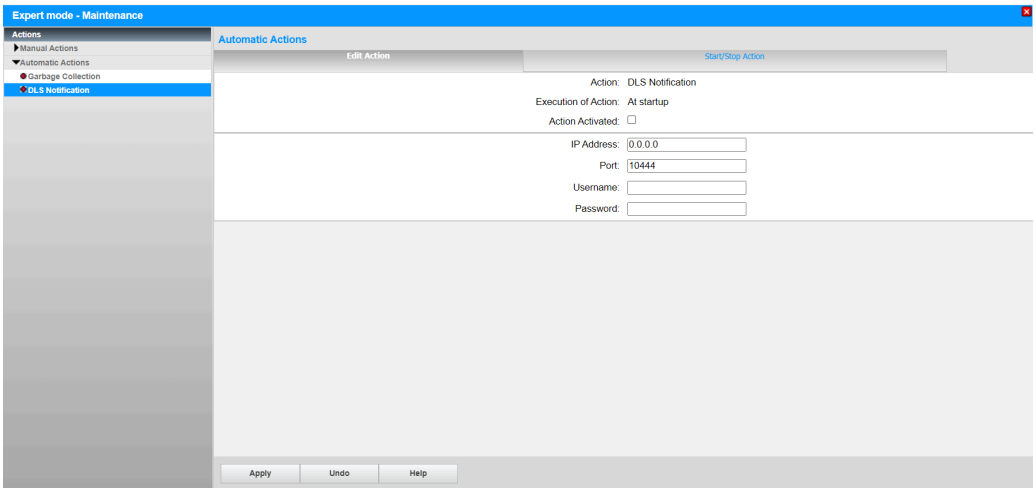
24.6.2.1 Comment modifier l'action automatique Notification DLS

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Actions**.
3) Dans l'arborescence du menu, allez à **Actions** > **Actions automatiques** > **DLS Notification**.
4) Cliquez sur l'onglet **Modifier l'action**.



5) Sélectionnez le paramètre souhaité :
   - Si l'action Notification DLS doit être effectuée, cochez la case **Action activée**.
   - Si l'action Notification DLS ne doit pas être effectuée, décochez la case **Action activée**.
6) Si nécessaire, modifiez dans le champ **Adresse de destination** l'adresse IP du serveur DLS externe.
7) Si nécessaire, modifiez dans le champ **Port** le port du serveur DLS externe.
8) Si nécessaire, modifiez dans le champ **Nom utilisateur** le nom d'utilisateur servant à ouvrir une session sur un serveur DLS externe.
9) Si nécessaire, modifiez dans le champ **Mot de passe** le mot de passe servant à ouvrir une session sur un serveur DLS externe.
10) Cliquez sur **Appliquer** puis sur **OK**.

24.6.2.2 Comment lancer l'action automatique Démarrer la notification DLS (activer)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Actions**.
3) Dans l'arborescence du menu, double-cliquez sur **Actions** > **Actions automatiques**. Dans l'arborescence du menu, il est affiché le nom de toutes les actions automatiques. Les actions activées sont identifiées par un point vert sur la liste. Les actions activées sont identifiées par un point vert sur la liste.
4) Dans l'arborescence du menu, cliquez sur **Notification DLS**.
5) Cliquez sur l'onglet **Démarrer/Arrêter l'action**.
6) Cliquez sur **Démarrer** et ensuite sur **OK**.

24.6.2.3 Comment arrêter l'action automatique Arrêter la notification DLS (désactiver)

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Actions**.
3) Dans l'arborescence du menu, double-cliquez sur **Actions** > **Actions automatiques**. Dans l'arborescence du menu, il est affiché le nom de toutes les actions automatiques. Les actions activées sont identifiées par un point vert sur la liste. Les actions activées sont identifiées par un point vert sur la liste.
4) Dans l'arborescence du menu, cliquez sur **Notification DLS**.
5) Cliquez sur l'onglet **Démarrer/Arrêter l'action**.

6) Cliquez sur **Arrêter** et ensuite sur **OK**.

24.6.3 Mécanisme d'alerte pour la durée de vie de la carte SDHC

Le mécanisme d'alerte pour la durée de vie de la SDHC à action automatique est une manière d'obtenir des informations sur l'état d'intégrité des cartes SDHC avec un contrôle du système de fichiers lors du démarrage. Un assistant WBM démarre et guide le technicien à travers le processus de définition du moment où le système devrait redémarrer et effectuer le contrôle.

Remarque : Dans le cas où aucune erreur de système de fichiers n'est détectée par la vérification, **Etat d'intégrité de la carte** repassera en vert ou jaune, même si des erreurs ont été signalées auparavant.

Toutes les informations sont enregistrées dans la trace client. Le mécanisme d'alerte à action automatique pour la SDHC est désactivé par défaut.

Remarque : Cette option déclenche un redémarrage du système et affiche un message d'alerte : "`Remarque : le système va redémarrer peu après que vous ayez appuyé sur OK`".

L'écran d'accueil WBM reconnaît deux états :

- Si l'information du système est disponible, un texte sera présenté sur l'écran d'accueil, indiquant l'état général de la carte, **Etat d'intégrité de la carte** (vert, jaune ou gris rouge).

  La durée de vie générale de la carte est calculée en fonction des spécifications du fabricant et des cycles d'écriture moyens du système. Différentes valeurs pour la durée de vie de la carte sont possibles. Cette information est présentée avec d'autres informations sur la page de vérification d'intégrité SDHC dans le WBM.

  Une durée de vie estimée de 4 ans pour les cartes standard et de 10 ans pour les cartes haute résistance est stockée dans le système.

  Remarque : Les valeurs estimées pour la durée de vie ne sont que la base du mécanisme d'avertissement d'état d'intégrité de la carte intégré. Ces valeurs n'impliquent

pas automatiquement qu'une carte est défectueuse après l'expiration de ce délai.

L'état d'intégrité vert signifie que la carte n'a pas atteint sa durée de vie estimée et qu'il n'y a aucun problème avec le système de fichiers.

L'état d'intégrité jaune signifie que la carte a atteint sa durée de vie estimée.

L'état d'intégrité rouge signifie que plus de 50 erreurs de système de fichiers ont été détectées.

L'état d'intégrité gris signifie que la carte n'est pas prise en charge ou qu'il n'est pas possible de récupérer les informations de la carte. La carte SDHC doit être remplacée par un type de carte pris en charge.

Le mécanisme d'avertissement pour l'état d'intégrité jaune est basé sur la date de fabrication et la durée de vie estimée de la carte. Etant donné les cartes peuvent être stockées plus longtemps avant d'être utilisées dans OpenScape Business, la date de création du système de fichiers est également prise en compte dans l'algorithme de calcul.

Vous trouverez ci-dessous une table de calcul pour l'état d'intégrité de la carte avec une durée de vie estimée de 4 ans.

Facteur	**Années et pondération**									
Date de fabrication	< 4 ans	< 5 ans		< 6 ans		< 7 ans		< 8 ans		> 8 ans
Système de fichiers créé	< 4 ans	< 4 ans	4-5 ans	< 4 ans	4-6 ans	< 3 ans	3-7 ans	< 2 ans	2-8 ans	-
Etat d'intégrité	Vert	Vert	Jaune	Vert	Jaune	Vert	Jaune	Vert	Jaune	Jaune

- Si l'information n'est pas disponible, il est indiqué à l'utilisateur **Etat d'intégrité de la carte** inconnu.

Remarque : Si le système de fichiers est corrompu, l'image du logiciel système appropriée doit être téléchargée à partir de SWS et copiée sur la carte SDHC à l'aide de l'outil Card Manager. Après le démarrage du système avec la nouvelle carte SDHC, la configuration peut être restaurée en utilisant la dernière sauvegarde.

Le texte "**Etat d'intégrité de la carte**" fournit également un lien qui mène à la "page Actions"

24.6.3.1 Comment définir une notification en cas d'erreur sur la carte SDHC

Si la fonction de contrôle de fichier d'intégrée signale un nombre d'erreurs dépassant le seuil donné (50 erreurs) ou si le système ne peut plus lire/écrire depuis/sur la carte SDHC en fonctionnement normal, le système avertit l'utilisateur par e-mail ou via un événement SNMP.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Tableau de réactions**. Dans l'arborescence du menu, le nom du tableau de réactions s'affiche.
4) Sélectionnez **FP_EVT_HW_067** dans l'arborescence du menu.
5) Sélectionnez l'une des possibilités suivantes :
   a) Envoyer un trap SNMP
   b) Envoyer un e-mail
6) Cliquez sur **Appliquer** puis sur **OK**.

Remarque :

L'adresse e-mail doit être configurée dans **Mode expert > Maintenance > Événements > E-mail.**

24.6.3.2 Comment démarrer le mécanisme d'alerte pour l'action automatique sur la durée de vie de SDHC

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Enregistrez le système sur un support externe via la fonction de sauvegarde.
2) Dans la barre de navigation, cliquez sur **Mode Expert**.
3) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Actions**.
4) Dans l'arborescence du menu, double-cliquez sur **Actions** > **Actions automatiques**. Dans l'arborescence du menu, il est affiché le nom de toutes les actions automatiques.
5) Cliquer sur**Contrôle d'intégrité SDHC** dans l'arborescence de menu.

   La date et l'heure des éléments **Heure du système local** et **Dernier contrôle d'intégrité** s'affichent. Le contenu du **fichier journal** s'affiche également.
6) Sélectionnez l'une des possibilités suivantes :
   a) Démarrer immédiatement le contrôle d'intégrité.
   b) Démarrer le contrôle d'intégrité à une date spécifique
7) Cliquez sur **Appliquer** puis sur **OK**.

24.6.3.3 Comment cloner et changer une carte SDHC

Les cartes SDHC ont une durée de vie limitée en général. La durée de vie dépend principalement du nombre de cycles d'écriture de la carte SDHC. OpenScape Business prend en charge un mécanisme de détection intégré « Statut de santé SDHC » pour la durée de vie de la carte SDHC et une

fonction intégrée « Sauvegarde des données SDHC », décrite ci-dessous pour le remplacement de la carte SDHC à remplacer et la création d'une nouvelle carte.

Remarque : La fonction de sauvegarde de données SDHC est capable de copier le contenu de la carte SDHC actuellement insérée dans le système sans arrêter le système Voir aussi Comment retirer ou supprimer des utilisateurs d'Unify Phone à la page 1135.

Les données pertinentes peuvent être sauvegardées dans différents emplacements de stockage et supports de stockage comme :

- Clé USB connectée au système.
- Lecteur de carte SDHC USB connecté au système.
- Lecteur NFS (Network File System).
- Lecteur NFS (Network File System) via USB.

Remarque : Les options de clé USB ou de lecteur de carte SDHC USB ne sont pas disponibles pour OpenScape Business X1. Dans ce cas, la sauvegarde de données SDHC doit être stockée sur un lecteur NFS.

Dans le cas où un lecteur de carte USB est utilisé, il est possible que l'accès à la carte SDHC ou son formatage soit impossible. Dans ce cas, un autre lecteur de carte USB ou une clé USB doivent être utilisés.

Dans le cas où un lecteur de carte USB avec la nouvelle carte SDHC insérée est utilisé et directement connecté au système, la fonction de sauvegarde de données SDHC intégrée crée une carte SDHC fonctionnelle complète. Dans tous les autres cas, il crée un « fichier tar » qui contient toutes les données du système et de la configuration.

Remarque : Le fichier tar ne peut pas être utilisé par la fonction de restauration du système.

La taille de la sauvegarde de données SDHC (fichier tar) dépend des données spécifiques du système et peut atteindre plusieurs Go si des fichiers multimédias (messages vocaux, enregistrements d'appels, etc.) sont stockés.

Pour cloner et modifier une carte SDHC dans un système actif, la procédure suivante est requise :

1) Créez un fichier de sauvegarde de données SDHC avec un support approprié (voir Comment créer un fichier de sauvegarde de données SDHC)
2) Créez une nouvelle carte SDHC opérationnelle comprenant toutes les données du système (voir Comment utiliser le gestionnaire de cartes pour écrire le logiciel de communication sur la carte SDHC à la page 1284).
3) Mettez le système hors tension, changez la carte SDHC et remettez-le sous tension (voir Comment utiliser le gestionnaire de cartes pour écrire le logiciel de communication sur la carte SDHC à la page 1284).

24.6.3.4 Comment créer un fichier de sauvegarde de données SDHC

Conditions préalables

Une clé USB ayant au moins la même capacité que la carte SDHC du système ou un lecteur de carte USB avec une nouvelle carte SDHC insérée ayant au moins la même taille que la carte du système ou un lecteur NFS (Network File System) qui est accessible depuis le système.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Sauvegarde de données**.

2) Cliquez sur **Sauvegarde des données SDHC** > **Sauvegarde des données** dans l'arborescence de navigation.

3) Sélectionnez l'une des options disponibles suivantes en fonction de l'emplacement de stockage et du support disponible :

a) NFS

Une adresse de serveur valide, le chemin d'accès approprié et des informations d'identification de connexion valides doivent être configurés.

Cliquez sur **Enregistrer et vérifier**

Remarque : Une sauvegarde planifiée est disponible. Une seule action peut être planifiée à la fois et l'utilisateur pourra la modifier ou l'annuler.

---

b) Lecteur de carte

Cette option crée une copie fonctionnelle complète de la carte SDHC sans trace ni fichier journal.

Un lecteur de carte SDHC USB avec une carte SDHC insérée doit être connecté au système avant le début du processus de copie.

Une fois le processus commencé, la carte SDHC insérée est formatée et tous les fichiers pertinents sont transférés vers la carte SDHC insérée.

Remarque : Ne retirez pas le lecteur de carte SDHC USB ou la carte SDHC insérée avant la fin du processus.

Remarque : La nouvelle carte SDHC est pleinement fonctionnelle pour une utilisation immédiate dans le système OpenScape Business. La nouvelle carte contient

tous les fichiers et données, à l'exception des fichiers journaux et des fichiers de trace.

Remarque : Une sauvegarde planifiée est disponible. Une seule action peut être planifiée à la fois et l'utilisateur pourra la modifier ou l'annuler.

c) NFS via USB.

Une adresse de serveur valide, le chemin d'accès approprié et des informations d'identification de connexion valides doivent être configurés.

Cliquez sur **Enregistrer et vérifier**

Remarque : Une sauvegarde planifiée est disponible. Une seule action peut être planifiée à la fois et l'utilisateur pourra la modifier ou l'annuler.

d) USB.

Un périphérique USB vierge au format FAT32 doit être connecté au système.

Remarque : Ne retirez pas la clé USB avant la fin du processus.

Remarque : Le fichier de données de sauvegarde SDHC copié (fichier tar) peut être utilisé dans l'outil Card Manager afin de créer une carte SDHC fonctionnelle complète pour le système.

Remarque : Une sauvegarde planifiée est disponible. Une seule action peut être planifiée à la fois et l'utilisateur pourra la modifier ou l'annuler.

4) Cliquez sur **OK & Suivant**. Dans une autre fenêtre, le système affiche la progression de la sauvegarde.

Remarque : Un message d'erreur s'affiche si le partage NFS ou le périphérique USB ne peut pas être monté ou si le support de stockage ne peut pas être formaté.

5) Le message **Tâche de sauvegarde terminée avec succès** s'affiche après la copie du fichier de sauvegarde.

6) Cliquez sur **Terminer**.

Remarque : La procédure à suivre ensuite diffère selon l'emplacement de stockage et le support choisis.

En cas d'utilisation du lecteur de carte SDHC avec une carte SDHC, la nouvelle carte SDHC peut immédiatement être utilisée.

Dans tous les autres cas, le fichier de sauvegarde de carte SDHC généré doit être utilisé en combinaison avec l'outil Card Manager pour générer une nouvelle carte SDHC.

Étapes suivantes

Suivez les étapes pour créer une nouvelle carte SDHC opérationnelle et la modifier dans le système actif (voir Comment utiliser Card Manager pour inscrire le logiciel de communication sur la carte SDHC)

24.6.3.5 Comment remplacer une carte SDHC

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Uniquement en cas d'utilisation d'UC Suite : UC Suite a démarré correctement.

Le passage à une version antérieure du logiciel n'est pas autorisé. Si une carte équipée du logiciel V2 est installée, seules les versions mineures précédant V2 peuvent être restaurées.

La version actuelle de logiciel doit être utilisée afin d'éviter tout effet secondaire.

Remarque : Lorsque la carte SDHC est brisée et que le système est en panne, une sauvegarde antérieure doit être utilisée et les 10 premières étapes de la procédure suivante doit être ignorées. Voir aussi Comment retirer ou supprimer des utilisateurs d'Unify Phone à la page 1135.

Étape par étape

1) Cliquez dans la barre de navigation sur **Sauvegarde et restauration**.
2) Dans l'arborescence de navigation, cliquez sur **Sauvegarde - immédiate**.
3) Dans le champ **Commentaire**, entrez un commentaire pour le jeu de sauvegarde afin de pouvoir plus facilement identifier le jeu de sauvegarde lors d'une éventuelle restauration. Lors de la saisie, évitez les inflexions et les caractères spéciaux.
4) Si vous voulez créer un jeu de sauvegarde y compris messages vocaux et annonces, activez l'option **Sauvegarde complète**.
5) Dans la zone **Equipements**, activez le lecteur de destination sur lequel le jeu de sauvegarde doit être enregistré.

6) Cliquez sur **OK & Suivant**. Dans une autre fenêtre, le système affiche la progression de la sauvegarde.

Remarque : Si le bouton **OK&Suite** est affiché en grisé, cela signifie que toutes applications dont les données doivent être sauvegardées n'ont pas démarré correctement (par ex. UC Suite).

Si vous n'avez pas d'autorisation pour le répertoire d'archive sélectionné, vous recevez un message d'erreur. Sélectionnez un autre lecteur de destination ou modifiez le chemin d'accès pour l'archive.

S'il n'y a pas suffisamment de capacité mémoire disponible pour le jeu de sauvegarde sur le lecteur de destination, vous voyez un message d'erreur. Sélectionnez un autre lecteur de destination ou effacez un jeu de sauvegarde et démarrez la sauvegarde des données de nouveau.

Remarque : Si vous utilisez une clé USB comme moyen de sauvegarde, attendez que la LED de la clé USB ait fini de clignoter. C'est seulement alors que la sauvegarde est terminée sur la clé USB. Ensuite retirez la clé USB.

Remarque : En plus du jeu de sauvegarde, il faut enregistrer le fichier texte correspondant au jeu de sauvegarde. Il contient des informations sur la date et l'heure de la sauvegarde et sur la version du logiciel qui a servi à effectuer la sauvegarde.

---

7) La sauvegarde a été effectuée si le message **Sauvegarde terminée ! 100 %** s'affiche.

8) Si vous avez choisi **HTTPS** comme support de sauvegarde, vous devez enregistrer le jeu de sauvegarde de diagnostic et le fichier texte correspondant à un emplacement de votre choix. Avec les autres moyens de sauvegarde, cela se fait automatiquement. La fenêtre de navigation doit rester ouverte tant que se déroule l'opération d'enregistrement du jeu de sauvegarde et du fichier texte.

9) Cliquez sur **Terminer**.

10) Eteindre le système.

11) Retirer la carte SDHC existante.

12) Installer le nouvelle carte SDHC.

13) Allumer le système.

Lorsqu'une nouvelle carte SDHC est installée, la version de logiciel équipant la carte avec la configuration par défaut est automatiquement installée dans le système. Après le démarrage, le système aura son adresse IP par défaut.

14) Cliquez dans la barre de navigation sur **Sauvegarde et restauration**.

15) Dans l'arborescence de navigation, cliquez sur **Restaurer**.

16) Dans la plage **Système** activez le média qui contient le jeu de sauvegarde à rétablir.

17) Si vous avez activé **HTTPS** comme moyen de sauvegarde, allez à l'endroit où le jeu de sauvegarde est enregistré et sélectionnez-le. Allez ensuite à l'endroit où le fichier texte est enregistré et sélectionnez-le.

18) Si vous avez activé un autre moyen de sauvegarde que **HTTPS**, activez dans la Liste des jeux de sauvegarde disponibles le jeu de sauvegarde qui contient les données de configuration à rétablir.

19) Attendez que les fichiers soient chargés sur le système et cliquez ensuite sur **OK. & Suivant**. Le rétablissement des données de configuration est lancé. Le système vous indique la progression du rétablissement.

20) Une fois que le message **Restauration terminée !** s'est affiché, le système effectue automatiquement un redémarrage. Le rétablissement est achevé avec succès lorsque le système est de nouveau en service.

Remarque : Après la restauration, l'équipement doit être supprimé du serveur RSP pour ensuite être reconfiguré.

24.7 Gestion de l'alimentation

La gestion de l'alimentation place automatiquement le système de communication en mode Economie d'énergie, en fonction de la charge du système. Cela réduit la consommation d'énergie du système et constitue une contribution à la protection de l'environnement. L'intervalle de temps où le système peut être placé en mode Economie d'énergie est configurable (par ex. la nuit).

La gestion de l'alimentation ne peut être activée que si les interfaces LAN du système sont en mode liaison Ethernet **Auto**. En mode Economie d'énergie, les interfaces LAN du système passent automatiquement en mode duplex intégral 100 Mbit/s. Les interfaces LAN de l'infrastructure connectée doivent également se trouver en mode Autosense.

Etats d'exploitation

- Etat Actif (Active Mode)

  En mode Actif, les fonctions du système de communication sont utilisées et il existe des échanges de données importants entre le système et l'infrastructure connectée.
- Mode Veille (Idle Mode)

  En mode Veille, les fonctions du système de communication ne sont pratiquement pas utilisées, il n'y pratiquement pas d'échange de données entre le système et l'infrastructure connectée. Si une fonction est activée, le système passe du mode Veille au mode Actif.
- Mode Economie d'énergie (Low Power Mode)

  Le mode Economie d'énergie présente une consommation d'énergie encore plus réduite que le mode Veille. Le système se trouve en mode duplex intégral 100 Mbit/s.

Il est également possible d'exploiter le système de manière permanente en mode liaison Ethernet Duplex intégral 100 Mbit/s ou Semi-duplex 100 Mbit/s.

24.7.1 Comment activer ou désactiver la gestion de l'alimentation

Conditions préalables

L'interface LAN de la carte mère, via laquelle le système est connecté à l'infrastructure LAN, est définie sur le mode de liaison Ethernet **Auto**.

Les interfaces LAN de l'infrastructure connectée (par exemple, les téléphones IP) sont configurées en mode de détection automatique.

Vous êtes connecté au WBM avec le profil **Avancé** .

Étape par étape

1) Dans la barre de navigation, cliquez sur **Configuration** .
2) Dans l'arborescence de navigation, cliquez sur **Installation de base** > **des assistants** .
3) Cliquez sur **Modifier** pour lancer l'Assistant **Gestion d'alimentation**.
4) Si vous souhaitez activer la gestion de l'alimentation :
   a) Cochez la case **Marche/Arrêt de la gestion d'alimentation**.
   b) Sous **Start of LowPowerMode** et **End of LowPowerMode**, entrez la période pendant laquelle le système de communication doit passer en mode basse puissance.
5) Si vous souhaitez désactiver la gestion d'alimentation, désactivez la case à cocher **Marche/Arrêt de la gestion d'alimentation**.
6) Cliquez sur **OK et Suivant** . Vos paramètres ont été appliqués.
7) Cliquez sur **Terminer** .

24.7.2 Comment modifier le mode de liaison Ethernet des interfaces LAN

Conditions préalables

Vous êtes connecté au WBM avec le profil **Expert** .

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert** .
2) Dans l'arborescence de navigation, cliquez sur **Téléphonie** > **Interfaces réseau**.

3) Sélectionnez le mode de liaison Ethernet pour l'interface LAN de la carte mère :
   a) Dans l'arborescence du menu, cliquez sur **Carte mère** > **LAN 2**. Le système de communication est intégré à l'infrastructure LAN via le port LAN 2.
   b) Si vous souhaitez activer la gestion d'alimentation, sélectionnez l'élément de liste **Auto** dans la liste déroulante **Mode liaison Ethernet**.
   c) Si vous souhaitez régler le système en mode basse consommation de manière permanente, sélectionnez l'élément de liste **100HDX** ou **100FDX** dans la liste déroulante **Mode liaison Ethernet**.

      Remarque :

      La gestion d'alimentation ne peut pas être activée pour les modes de liaison Ethernet **100HDX**, **100FDX** et **1000FDX**.

   d) Cliquez sur **Appliquer** .

24.8 Surveillance et maintenance d'OpenScape Business

OpenScape Business propose différentes fonctions permettant de surveiller l'état actuel du système et de trouver et éliminer les erreurs.

24.8.1 Contrôler une connexion réseau d'OpenScape Business X

Grâce à une demande ICMP (Internet Control Message Protocol), il est possible de tester la liaison réseau entre le système de communication OpenScape Business X et l'adresse de destination, à l'aide de paquets de demande d'écho.

Les paquets de demande d'écho peuvent être envoyés à l'aide de la fonction **Ping** comme à l'aide de la fonction **Itinéraire de trace**. Les acquittement de réponse sont affichés avec les temps de parcours.

La fonction **Itinéraire de trace** envoie les paquets de demande d'écho avec différentes valeurs TTL croissantes (Time-To-Live).

24.8.1.1 Comment envoyer un Ping

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Diagnostic IP**.
3) Dans l'arborescence du menu, allez à **Routage IP** > **Demande ICMP** > **Ping**.
4) Dans le champ **Adresse de destination**, entrez l'adresse IP de la destination souhaitée.

5) Entrez dans le champ **Nombre de demandes d'écho à envoyer** le nombre souhaité (valeur par défaut = 3).
6) Cliquez sur **Envoyer**.

   Ensuite, les acquittements de réponse sont affichés avec les temps de parcours.

24.8.1.2 Comment tester l'itinéraire de trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Diagnostic IP**.
3) Dans l'arborescence du menu, allez à **Carte mère** > **Exigence ICMP** > **Itinéraire de trace**.
4) Dans le champ **Adresse de destination**, entrez l'adresse IP de la destination souhaitée.
5) Dans le champ **Octet TOS** entrez la valeur souhaitée (valeur par défaut = 0).
6) Cliquez sur **Envoyer**.

   Ensuite, les acquittements de réponse sont affichés avec les temps de parcours.

24.8.2 SNMP (Simple Network Management Protocol)

Le Simple Network Management Protocol (SNMP - protocole simple de gestion de réseau) est un protocole réseau permettant de surveiller et de gérer les composantes du réseau (par ex. routeurs, serveurs, commutateurs, imprimantes, PC) à partir d'une station centrale. Le protocole règle la communication entre les composantes surveillées et la station de surveillance.

SNMP décrit la configuration des paquets de données pouvant être envoyées ainsi que le déroulement de la communication. SNMP est configuré de manière à ce que chaque appareil susceptible de fonctionner en réseau puisse être surveillé. Parmi les tâches de gestion du réseau via SNMP figurent les suivantes :

- surveillance des composantes du réseau,
- commande et configuration à distance des composantes du réseau,
- détection des erreurs et information sur les erreurs.

Pour la surveillance, on utilise ce que l'on appelle des agents. Il s'agit de programmes qui tournent directement sur les composantes surveillées. Ces programmes sont en mesure de consigner l'état de la composante et d'effectuer eux-mêmes des paramétrages ou bien de lancer des actions. A l'aide de SNMP, il est possible de faire communiquer la console de gestion centrale avec les agents, via un réseau.

Remarque : OpenScape Business supporte SNMPv2c, et réagit aussi aux demandes SNMPv1 snmpget.

Bases de données d'informations de gestion MIB

L'étendue des données qui peuvent être gérées par SNMP peut être définie par les MIB (bases de données des informations de gestion). Les MIB sont des modèles de données qui décrivent d'une manière indiquée les composantes du réseau à gérer. La MIB des systèmes de communication OpenScape Business X peut être téléchargée avec WBM (Centre de service).

Les systèmes de communication disposent d'un agent SNMP qui permet d'accéder à toute une série de données système enregistrées dans la sa base de données d'informations de gestion MIB. MIB fournit des informations fondamentales sur les systèmes, des informations d'état, des données relatives à un événement ainsi que des informations sur le matériel installé (emplacements) et les liaisons paramétrées (ports).

SNMP permet la surveillance et l'administration centrales des composantes du réseau y compris celles des systèmes de communication. Cela rend possible :

- le contact avec un système de communication via TCP/IP.
- l'accès aux données via des applications de gestion externes,
- la réalisation de tâches de télémaintenance,
- la visualisation de l'état de fonctionnement du système de communication,
- la transmission des erreurs concernant l'exploitation (traps).

Communautés

L'accès aux données SNMP (MIB) est réglé par les Communautés. Il est fait la distinction entre les communautés de lecture, les communautés d'écriture et les communautés Trap. Derrière une communauté se cache une adresse IP.

Pour permettre par exemple à un PC d'accéder en lecture aux données SNMP (MIB), il faut inscrire l'adresse IP de ce PC dans la liste des communautés de lecture. Pour disposer d'un accès en lecture et en écriture, il faut que l'adresse IP soit inscrite dans la liste des communautés d'écriture.

Les communautés Trap gèrent les destinataires des messages d'erreur (traps).

Traps

En cas de problème du système de communication, des traps sont générés afin de donner des informations sur les erreurs et défaillances. Il existe les types de traps suivants :

- Traps système = erreurs système nécessitant des mesures immédiates pour leur élimination.
- Traps performances = informations à propos des problèmes de performances, ne nécessitant pas toutefois une élimination.

Les traps sont classés en fonction de leurs effets et peuvent être appelés par un administrateur avec le profil **Expert** à l'aide de la WBM. Il est affiché une lise de tous les traps reçus, avec les informations suivantes :

Colonne du tableau	Signification
VarBind1 (gravité)	Classe d'influence Traps Les entrées suivantes sont possibles : Critique : Message d'erreur L'erreur a des conséquences problématiques. Majeur : message d'erreur. L'erreur peut avoir des conséquences problématiques. Mineur : message d'erreur. L'erreur n'a pas de conséquences problématiques. Avertissement : message concernant un processus ou un état pouvant être problématique, n'est pas un message d'erreur. Supprimé(s) Information : pur message d'état, n'est pas un message d'erreur. Etat intermédiaire Autres traps
VarBind2 (Nom)	Nom du trap
Nom générique	Désignation générale comme Entreprise Specific
Nom spécifique	Type de trap (1 = Logiciel, 2 = Matériel)
Entreprise	–
Heure	Heure de survenance de l'erreur
Index	Numéro de liste

L'affichage des traps est actualisé toutes les 30 secondes. Le tri des traps est effectué dans l'ordre de leur apparition.

Cliquez sur le nom du trap pour afficher les données détaillées du trap.

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
Classe d'erreur 01 - Messages généraux				
	Redémarrage du système	Redémarrage à froid (réinitialisation) de l'ensemble du système avec la CDB actuelle.	Néant	
FP_EVT_ADM_002	rechargement de l'emplacement signé	rechargement de l'emplacement signé		
FP_EVT_ADM_003	redémarrage du système	redémarrage du système		
FP_EVT_ADM_010	Redémarrage du système SNMP	Redémarrage à froid de l'ensemble du système via SNMP	Néant	

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
FP_EVT_ADM_014	Changements dans la base de données locale SNMP	Modifications "sur place" de la base de données	Néant	
FP_EVT_ADM_015	Modifications à distance SNMP de la base de données	Modifications à distance de la base de données	Néant	
FP_EVT_ADM_016	Résultat du transfert APS SNMP	Message d'accusé de réception du transfert APS via SNMP	Néant	
FP_EVT_ADM_017	Échec de l'authentification SNMP	Tentative d'accès non autorisée.	Vérifiez les paramètres du pare-feu dans OpenScape Business/ Manager E (pare-feu du réseau).	
FP_EVT_ADM_019	Alarme du capteur	La température dans le boîtier OpenScape Business est trop élevée.	Vérifiez le ventilateur et la climatisation du boîtier 19 pouces. Notez la température ambiante.	
FP_EVT_ADM_020	Limite de la mémoire tampon du CDR atteinte	Débordement de la mémoire tampon du CDR (informations CDR).	Vérifiez que les interfaces (V.24, LAN), les ports et la connexion fonctionnent, ou lisez les données d'appel.	
FP_EVT_ADM_024	application non autorisée	Tentative d'accès via une application non autorisée.	Vérifiez les paramètres du pare-feu dans OpenScape Business/ Manager E (Réseau>Pare-feu).	
FP_EVT_ADM_025	commutation manuelle à partir d'HiPath Manager			
Classe d'erreur 02 - Messages de gestion des licences				
Classe d'erreur 09 - Messages du module matériel				
FP_EVT_HW_034	perte de trame activée (STMD)	perte de trame activée (STMD)		
FP_EVT_HW_035	perte de trame désactivée (STMD)	perte de trame désactivée (STMD)		
FP_EVT_HW_036	glissement détecté activé (STMD)	Un glissement de bit s'est produit sur une ligne RNIS.	Vérifier la ligne S0. Si nécessaire, rechargez la carte ou effectuez un redémarrage complet. Si l'erreur persiste, établissez une trace RNIS.	Le problème peut être causé par des fréquences d'horloge interne et externe asynchrones. Perte de données possible ; la connexion peut être interrompue.

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
FP_EVT_HW_039	erreur de signal d'indication d'alarme désactivée (TMS2M)	Affichage de l'alarme : L'erreur S2M a été corrigée.	Néant	
FP_EVT_HW_040	erreur de minute dégradée activée (TMS2M)	erreur de minute dégradée activée (TMS2M)		
FP_EVT_HW_041	erreur de minute dégradée désactivée (TMS2M)	erreur de minute dégradée désactivée (TMS2M)		
FP_EVT_HW_042	erreur de signal absent activée (TMS2M/ STMD)	Affichage de l'alarme : Une erreur S2M s'est produite. Aucune connexion physique disponible.	Vérifiez la ligne et la carte S2M. Si nécessaire, rechargez la carte ou effectuez un redémarrage complet. Si l'erreur persiste, établissez une trace RNIS.	
FP_EVT_HW_043	erreur de signal absent désactivée (TMS2M/ STMD)	Affichage de l'alarme : L'erreur S2M a été corrigée.	Néant	
FP_EVT_HW_046	erreur de secondes gravement erronées activée (TMS2M)	erreur de secondes gravement erronées activée (TMS2M)		
FP_EVT_HW_047	erreur de secondes gravement erronées désactivée (TMS2M)	erreur de secondes gravement erronées désactivée (TMS2M)		
FP_EVT_HW_052	possible d'utiliser l'horloge comme référence (TMS2M/ STMD)	possible d'utiliser l'horloge comme référence (TMS2M/ STMD)		
FP_EVT_HW_053	impossible d'utiliser l'horloge comme référence	impossible d'utiliser l'horloge comme référence		
FP_EVT_HW_060	Erreur d'alimentation d'accès activée (SLMO)	Erreur d'alimentation d'accès activée (SLMO)		
FP_EVT_HW_063	Erreur ELIC activée (SLMO/SLMC)	Erreur ELIC activée (SLMO/SLMC)		
FP_EVT_HW_064	Erreur ELIC désactivée (SLMO/SLMC)	Erreur ELIC désactivée (SLMO/SLMC)		
FP_EVT_HW_067	Erreur OCTAT activée (SLMC)	Erreur OCTAT activée (SLMC)		
FP_EVT_HW_096	erreur inconnue de LW	erreur inconnue de LW		

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
Classe d'erreur 11 - Messages généraux				
FP_EVT_DEV_041	couche 1 asynchrone activée	couche 1 asynchrone activée		
FP_EVT_DEV_042	couche 1 asynchrone désactivée	couche 1 asynchrone désactivée		
FP_EVT_DEV_043	Erreur de surcharge activée	Erreur de surcharge activée		
FP_EVT_DEV_044	Erreur de surcharge désactivée	Erreur de surcharge désactivée		
FP_EVT_DEV_045	Erreur de contrôle en temps réel activée	Erreur de contrôle en temps réel activée		
FP_EVT_DEV_046	info optiPoint	info optiPoint		
FP_EVT_DEV_048	Erreur de couche 2 détectée	Erreur de couche 2 détectée		
FP_EVT_DEV_049	Erreur de la couche 3 détectée	Erreur de la couche 3 détectée		
FP_EVT_DEV_052	Autres erreurs	Autres erreurs		
FP_EVT_DEV_057	Aucun TEI disponible	Aucun TEI disponible		
FP_EVT_DEV_058	Trop d'erreurs de la couche 1	Trop d'erreurs de la couche 1.	Vérifiez les lignes, le terminal et le port. Un court-circuit s'est peut-être produit.	
FP_EVT_DEV_059	Accès non configuré	Accès non configuré		
Classe d'erreur 16 - Messages du système d'exploitation				
FP_EVT_GEN_002	Erreur dans le pool de lancement	Erreur dans le pool de lancement	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_004	Erreur dans OSF-Send	Erreur dans OSF-Send	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
FP_EVT_GEN_005	Erreur dans OSF-Timer	Erreur dans OSF-Timer	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_010	REDÉMARRAGE : réinitialisation manuelle	REDÉMARRAGE : réinitialisation manuelle	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_011	REDÉMARRAGE : rechargement manuel	REDÉMARRAGE suite à un rechargement manuel	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_012	REDÉMARRAGE : Mise hors tension	Redémarrage suite à une mise hors tension	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_013	Le KDS n'a pas été sauvegardé	Le KDS n'a pas été sauvegardé	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
FP_EVT_GEN_014	REDÉMARRAGE : repos inconnu. Différence d'indication matérielle	REDÉMARRAGE pour cause de repos inconnu. Différence de matériel	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_015	journalisation des erreurs générales	journalisation des erreurs générales	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_020	CSTA : longueur hors plage	CSTA : longueur hors plage	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_024	inactivité après le redémarrage	inactivité après le redémarrage	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
FP_EVT_GEN_030	dépassement des points de surveillance CSTA	dépassement des points de surveillance CSTA	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
Classe d'erreur 19 - Messages des services réseau				
FP_EVT_NWS_011	Impossible d'activer le client SNTP sur PCS	Impossible d'activer le client SNTP sur PCS		

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
Classe d'erreur 20 - Messages relatifs au traitement des appels				
FP_EVT_CP_002	RS232 : DSR non prêt	L'interface RS232/V.24 est hors service.	Vérifiez l'interface, la ligne et l'application.	
FP_EVT_CP_013	voies non connectées	Le nombre maximum de chemins de connexion autorisés a été dépassé.	Utilisez l'outil de planification de projet pour tester la configuration du système. Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
Classe d'erreur 21 - Messages du gestionnaire d'équipements				
FP_EVT_DH_004	Port hors service	Port hors service		
FP_EVT_DH_005	Port en service	Port en service		
FP_EVT_DH_016	Nom dans rejet msg S0/S2M	Nom dans rejet msg S0/S2M		
FP_EVT_DH_017	msg trop long L3S int->ext	msg trop long L3S int->ext		
FP_EVT_DH_018	msg trop long L3S ext->int	msg trop long L3S ext->int		
FP_EVT_DH_022	Détec auto PRI prot DMS250	Détec auto PRI prot DMS250		
FP_EVT_DH_023	Détec auto PRI prot NI2		Détec auto PRI prot NI2	I
FP_EVT_DH_024	Détec auto PRI prot 4ESS		Détec auto PRI prot 4ESS	
FP_EVT_DH_026	débordement du module de touches	débordement du module de touches		
FP_EVT_DH_027	Limite du canal B atteinte	Limite du canal B atteinte		
Classe d'erreur 23 - Messages du gestionnaire d'équipements				

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
FP_EVT_NW_060	système en attente, pas de tampon disponible	Le système est en attente, il n'y a plus de tampon disponible.	Mettez en place un traçage en utilisant les informations du support de niveau 2. Créez un vidage de pile. Sauvegardez un instantané.	
Classe d'erreur 26 - Messages d'administration de la carte				
FP_EVT_PR_001	carte hors service	La carte spécifiée est hors service.	Néant	
FP_EVT_PR_003	type de carte différent détecté	Type de carte incompatible. L'emplacement est déjà pré-affecté à un autre type de carte.	Remplacez la carte ou utilisez l'Assistant T pour supprimer le type de carte préassigné afin que la nouvelle carte soit reconnue.	
FP_EVT_PR_004	carte en service	La carte spécifiée est opérationnelle.	Néant	
FP_EVT_PR_005	erreur lors de la lecture de la base de données	erreur lors de la lecture de la base de données		
Classe d'erreur 28 - Messages de récupération				
FP_EVT_RC_008	APS manquant dans journal événements B	APS manquant dans journal événements B	Néant	La version actuelle de l'APS est saisie lors de la copie de la mémoire B du journal d'événements. Cela facilite l'analyse.
Classe d'erreur 30 - Messages du logiciel de la carte				
FP_EVT_LW_095	pas de connexion USBS au système	pas de connexion USBS au système		
Messages concernant le gestionnaire de ressources				
FP_EVT_RM_001	Erreur de configuration du gestionnaire de ressources	Erreur de configuration du gestionnaire de ressources		
Messages concernant UPM				
FP_EVT_UPM_010	UPM : redémarrage	UPM : redémarrage		

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
MSG_DLSC_BOOTSTRAP_OK	Client DLS amorcé avec succès.	Client DLS amorcé avec succès.		

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
MSG_STRC_STOP	Trace sécurisée arrêtée.	Trace sécurisée arrêtée.		
MSG_STRC_START	Trace sécurisée démarrée pour les protocoles.	Des traces sécurisées ont été activées par l'utilisateur pour les protocoles mentionnés.		
MSG_SPE_CERT_MISSING	Certificat SPE manquant.	Aucun certificat SPE installé.	Importez le certificat SPE et la clé privée (fichier PKCS#12).	
MSG_SPE_CERT_AVAIL	Certificat SPE disponible.	Le certificat SPE est maintenant disponible.		
MSG_SPE_CERT_UPDATED	Certificat SPE mis à jour avec succès.	Certificat SPE mis à jour avec succès.		
MSG_SPE_CERT_EXPIRED	Certificat SPE expiré.	La période de validité du certificat SPE installé est dépassée.	Installez un nouveau certificat valide.	
MSG_SPE_CRL_EXPIRED	La CRL SPE d'une autorité de certification spécifique a expiré.	CDP inaccessible ou CRL récupérée expirée.	Importez un certificat d'une autorité de certification SPE avec des CRL valides configurées dans CDP.	
MSG_SPE_CRL_UPDATED	La CRL SPE de l'autorité de certification a été mise à jour avec succès.	La CRL SPE de l'autorité de certification a été mise à jour avec succès.		
MSG_SPE_ALL_CRLS_UPTODATE	Toutes les CRL SPE sont à nouveau à jour.	Toutes les CRL SPE sont à nouveau à jour.		
MSG_MIKEY_REBOOT	Pile Mikey : échec de l'assertion.	Pile Mikey : échec de l'assertion.		
MSG_IPSEC_REBOOT	Erreur fatale dans la pile IPSec.	Erreur fatale dans la pile IPSec.		
MSG_CAT_H323_REBOOT		Redémarrage avec H.323		
MSG_CAT_HSA_REBOOT		Redémarrage avec HAS		
MSG_GW_SUCCESSFULLY_STARTED				
MSG_IP_LINK_FAILURE				
MSG_IP_LINK2_FAILURE		1 lien IP haut/bas		
MSG_IP_LINK3_FAILURE				
MSG_NEW_SW_AVAILABLE				

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
MSG_ADMIN_REBOOT		Redémarrage avec la WBM/l'admin CLI, mise à niveau logicielle ou restauration des données		
MSG_SYSTEM_REBOOT		Redémarrage automatique, par exemple avec le récupérateur de mémoire		
MSG_EXCEPTION_REBOOT		Redémarrage avec l'exception logicielle		
MSG_GW_OBJ_MEMORY_EXHAUSTED		Mémoire insuffisante		
MSG_TLS_POOL_SIZE_EXCEEDED		Pas d'autres pools internes		
MSG_OAM_RAM_THRESHOLD_REACHED		Limite de RAM atteinte		
MSG_OAM_DMA_RAM_THRESHOLD_REACHED		Limite de DRAM atteinte		
MSG_OAM_THRESHOLD_REACHED		Limite atteinte, par exemple, pour la mémoire flash ou les pools IP		
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION		Limite de température atteinte (trop chaud)		
MSG_HACKER_ON_SNMP_PORT_TRAP		Accès non autorisé au port SNMP		
MSG_DVMGR_LAYER2_SERVICE_TRAP		Canal B haut/bas		
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	Plus de 2 tronçons d'appel : non pris en charge CSID : %x/%x	Il n'est pas permis d'avoir plus de deux tronçons d'appel par session. Cela a rendu le logiciel instable. Le redémarrage nécessaire est exécuté.		
MSG_SSM_SESSION_CREATION_FAILED	Échec de la création de session	La signalisation n'est plus possible, car une session n'a pas pu être créée. Le redémarrage nécessaire est exécuté. Un trap SNMP est généré.		
MSG_IPNCV_STARTUP_ERROR	Démarrage d'IPNCV : Échec de la création du gestionnaire IPNCV	Impossible de démarrer IPNCV. Un trap SNMP est généré.	Créez un TR/MR.	

Code SNMP	Entrée du journal d'événements	Signification	Mesures requises	Remarque
MSG_IPNCV_STARTUP_SHUTDOWN	Démarrage/arrêt d'IPNCV : Gestionnaire IPNCV créé avec succès ou démarrage/ arrêt d'IPNCV : Gestionnaire IPNCV arrêté avec succès	IPNCV a été démarré ou arrêté avec succès. Un trap SNMP est généré.		
MSG_IPNCV_INTERNAL_ERROR	Erreur interne d'IPNCV : %s	Erreur logicielle : données internes non valides trouvées. Un trap SNMP sera généré avec le profil IPNCV - Détaillé.		
MSG_IPNCV_MEMORY_ERROR	Mémoire IPNCV : %s	Débordement de la mémoire : un trap SNMP est généré.	Redémarrez la passerelle. Créez une TR/MR.	
MSG_IPNCV_SIGNALING_ERROR	Erreur de signalisation IPNCV : %s	Erreur logicielle : données internes non valides trouvées.		
MSG_CAR_ALIVE_IP_CONNECTION_LOST	CAR : Actif : connexion IP %d.%d. %d.%d perdue	CAR : Actif : Connexion IP perdue.		
MSG_LIC_DATA_ACCEPTED		Données de licence acceptées		
MSG_LIC_DATA_CORRUPTED		Données de licence incomplètes		
MSG_LIC_DATA_NOT_ACCEPTED		Données de licence acceptées		
MSG_SPE_CERT_MISSING	Aucun certificat SPE installé	Certificat SPE manquant.	Installez le certificat SPE.	

Remarque : Certains événements SNMP ne sont pas documentés dans ce guide.

24.8.2.1 Comment afficher toutes les communautés

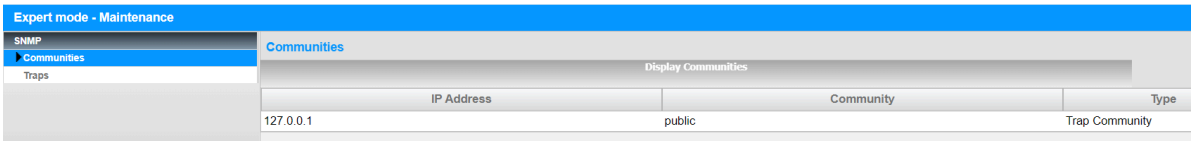
Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **SNMP**.

3) Dans l'arborescence du menu, cliquez sur **SNMP** > **Communautés**. Le système affiche une liste de toutes les communautés avec les données correspondantes (adresse IP, communauté, type).



24.8.2.2 Comment ajouter une communauté

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **SNMP**.
3) Sélectionnez la communauté souhaitée :
   - Si vous voulez ajouter une communauté de lecture, dans l'arborescence du menu cliquez sur **SNMP** > **Communautés** > **Communautés de lecture**. Cliquez sur l'onglet **Ajouter la communauté de lecture**.
   - Si vous voulez ajouter une communauté d'écriture, dans l'arborescence du menu cliquez sur **SNMP** > **Communautés** > **Communautés d'écriture**. Cliquez sur l'onglet **Ajouter la communauté d'écriture**.
   - Si vous voulez ajouter une communauté Trap, dans l'arborescence du menu cliquez sur **SNMP** > **Communautés** > **Communautés Trap**. Cliquez sur l'onglet **Ajouter la communauté Trap**.
4) Dans le champ **Adresse IP** indiquez l'adresse IP de la nouvelle communauté.
5) Dans le champ **Communauté** indiquez le nom de la nouvelle communauté.
6) Cliquez sur **Appliquer** puis sur **OK**.

24.8.2.3 Comment modifier la communauté

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **SNMP**.
3) Naviguez dans l'arborescence menu sous **SNMP** > **Communautés** > **…** pour accéder à la communauté souhaitée.
4) Cliquez sur l'onglet **Modifier la communauté**.
5) Modifiez Communauté.
6) Cliquez sur **Appliquer** puis sur **OK**.

24.8.2.4 Comment effacer la communauté

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **SNMP**.
3) Naviguez dans l'arborescence menu sous **SNMP** > **Communautés** > **…** pour accéder à la communauté souhaitée.
4) Cliquez sur l'onglet **Effacer la communauté**.
5) Cliquez sur **Effacer** et ensuite sur **OK**.

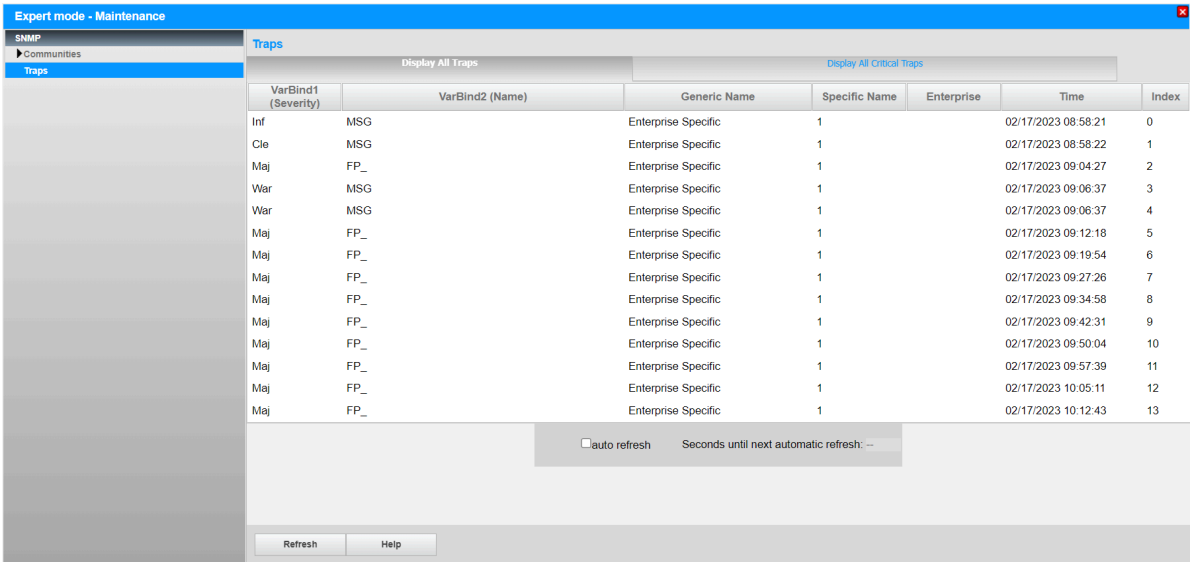
24.8.2.5 Comment afficher des traps

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **SNMP**.
3) Dans l'arborescence du menu, cliquez sur **SNMP** > **Traps**.
4) Sélectionnez une des possibilités suivantes :
   - Pour afficher une liste de tous les Traps, cliquez sur l'onglet **Afficher tous les Traps**.



   - Pour afficher une liste de tous les Traps critiques, cliquez sur l'onglet **Afficher tous les Traps critiques**.

24.8.2.6 Comment afficher les détails d'un trap

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **SNMP**.
3) Dans l'arborescence du menu, cliquez sur **SNMP** > **Traps**.
4) Cliquez sur l'onglet **Afficher tous les Traps**. Le système affiche une liste de tous les traps avec les données correspondantes.
5) Cliquez sur le nom de l'événement du trap souhaité. Le système affiche les données détaillées relatives à ce trap.
6) Cliquez sur l'onglet **Afficher tous les Traps** pour appeler de nouveau la liste de tous les traps.

24.8.3 Actions manuelles

De nombreux journaux différents (données de diagnostic et journaux de diagnostic) peuvent être chargés via des actions manuelles.

Les Administrateurs avec le profil **Advanced** peuvent charger des données de diagnostic (journaux de diagnostic) à l'aide de l'assistant de **suivi**.

Les administrateurs avec le profil **Expert** peuvent charger des données de diagnostic (journaux de diagnostic) en **mode Expert**.

Les journaux suivants peuvent être chargés :

Protocole	Explication	Application
Fichier-journal de trace	Fichier de trace standard, si des profils de trace ont été activés. Une sélection peut être faite parmi les options suivantes : • **Journal de trace complet** : la totalité des fichiers journal Trace sont téléchargés. • **Journal du jour** : Les fichiers journal de trace système du jour (à partir de 00h00) sont téléchargés. • **Propre sélection** : **De :** XXX **à :** YYY : Les fichiers journaux de suivi du système de la période sélectionnée sont téléchargés.	Pas d'application particulière
Journal des événements	Actions/événements du système de communication (Reset, On/Off, etc.)	Pas d'application particulière
Journal d'administration (également appelé protocole d'administration)	Messages sur les processus d'administration au niveau du système de communication (tentatives de connexion, etc.)	Pas d'application particulière

Protocole	Explication	Application
Protocoles de licence	Messages sur les composants du système de communication qui nécessitent des licences	Problèmes de licence (le fichier de licence ne peut pas être activé, etc.)
Trace des appels entrants d'un client	Les messages pour le suivi client sont fournis dans un format plus détaillé que dans le journal de suivi, par exemple (connexion à distance, connexion ITSP, etc.).	Problèmes avec la connexion ITSP (Internet Telephony Service Provider) ou la connexion à distance
Protocole Framework	Messages WBM	Problèmes de gestion des licences, de sauvegarde, de restauration ou avec le Web based Management (Web admin)
Protocole de diagnostic	Journaux de diagnostic du système de communication (FP/LDH)	Crash système ou arrêt incontrôlé du système de communication
Comptes rendus Suite UC	Messages de la suite UC du système de communication (logs UC Suite, CSP et Media Extension Bridge (MEB)) Une sélection peut être faite parmi les options suivantes : • **Journal de suivi complet** : Tous les fichiers-journaux Suite UC, CSP et Media Extension Bridge (MEB) sont téléchargés. • **Journal du jour** : les fichiers journal suite UC, CSP et Media Extension Bridge (MEB) du jour (à partir de 00h00) sont téléchargés. • **Propre sélection** : **De :** XXX **à :** YYY : les fichiers journal suite UC, CSP et Media Extension Bridge (MEB) de la période sélectionnée sont téléchargés. Tous les fichiers journaux sont archivés ensemble dans un fichier compressé. Les conventions de nommage de fichiers suivantes s'appliquent aux journaux Unify OpenScape Business : fichiers journaux UC Suite = `vs_yyy_mm_dd.log`, fichiers journaux CSP = `csptrace_yyyy_mm_dd.log`, fichiers journaux Media Extension Bridge (MEB) = `mebtrace_yyyy_mm_dd.log`. ***INFORMATIONS*** : lors de l'utilisation du serveur OpenScape UC Business Booster, les données de diagnostic doivent être téléchargées à partir du serveur lui-même.	Problèmes avec la suite UC et/ou le client (myPortal for Desktop, myAttendant, etc.)

Protocole	Explication	Application
Protocoles d'application	Messages du côté application du système de communication (par exemple, protocoles CSP) Un administrateur avec le profil **Expert** peut choisir parmi les options suivantes en **mode Expert** : • **Journal de suivi complet** : tous les fichiers journaux existants sont téléchargés • **Journal du jour** : Les fichiers journal de la journée d'aujourd'hui (à partir de 00h00) sont téléchargés. • **Propre sélection** : **De :** XXX **à :** YYY : Les fichiers journaux de la période sélectionnée sont téléchargés. Tous les fichiers journaux sont archivés ensemble dans un fichier compressé.	Problèmes avec le côté application du système de communication
Récupérer les journaux de diagnostic	Adresse IP du système de communication	Pas d'application particulière
Journaux PPP	Messages pour le protocole point à point	Problèmes avec les connexions d'entrée ou de sortie
Protocole CoreLog	Les CoreLogs sont créés pour les réinitialisations, etc. (par exemple, les vidages de mémoire sur un PC).	Crash système ou arrêt incontrôlé d'Unify OpenScape Business

Une fois les journaux souhaités sélectionnés, un fichier compressé est créé et stocké dans un répertoire spécifié.

24.8.3.1 Comment Télécharger les données de diagnostic / les journaux de diagnostic

L'assistant **Trace** vous permet de télécharger les données de diagnostic (Journaux de diagnostic) des systèmes de communication.

Conditions préalables

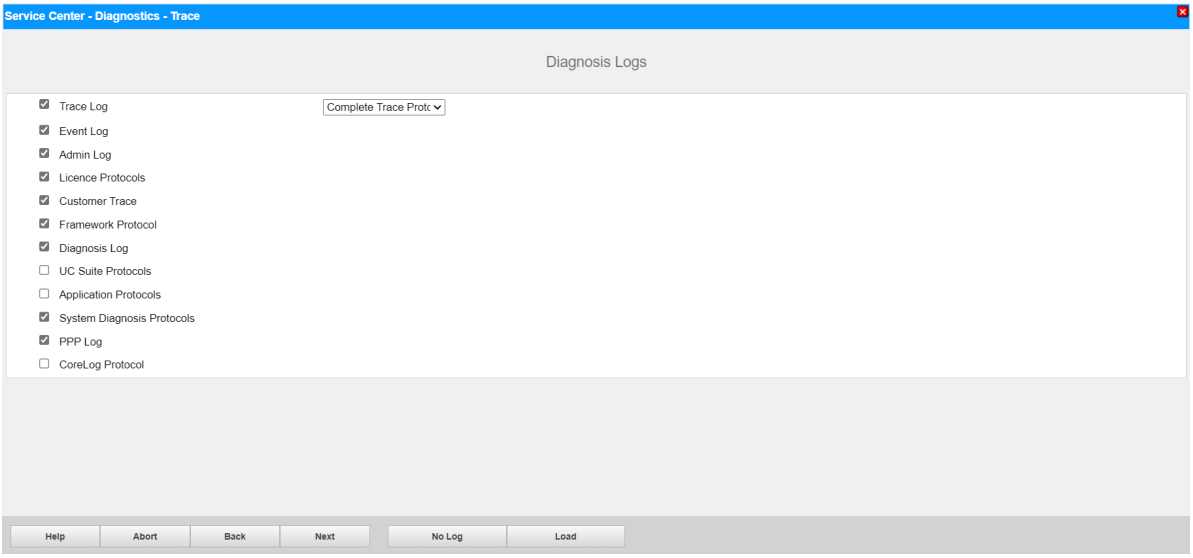
Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.

2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Trace**.

3) Cliquez sur **Données de diagnostic**.



4) Cochez les protocoles que vous souhaitez télécharger. Décochez les cases correspondant aux protocoles que vous ne voulez pas télécharger.
5) Cliquez sur **Charger** et ensuite sur **OK**. La fenêtre de téléchargement de fichiers s'affiche.
6) Sauvegardez le fichier dans le répertoire choisi. Fermez ensuite la fenêtre où vous avez confirmé le téléchargement.
7) Cliquez sur **Suivant** puis sur **Quitter**.

24.8.4 Traces

A l'aide des Traces, il est possible d'enregistrer les étapes d'un programme et leurs résultats lors du déroulement d'un programme. En liaison avec d'autres données de diagnostic, il ainsi possible de remonter jusqu'à la cause du défaut lorsqu'un programme est défectueux. A l'aide des profils Trace et des composantes Trace, il est possible de configurer quelles seront les traces enregistrées, et jusqu'à quel niveau de détails.

Conseil : L'activation des traces peut avoir un impact négatif sur les performances du système et ne doit donc être effectuée que par des administrateurs expérimentés et après consultation du service d'assistance compétent.

La Trace de console notamment occupe une part importante des ressources du système et nuit ainsi aux performances du système de communication.

Mise en réseau

Pour le diagnostic des systèmes de communication en réseau, il faut collecter séparément les données Trace de chacun des noeuds. Il n'est pas possible de collecter de manière centralisée les données Trace des systèmes de communication en réseau.

Configuration du format Trace

La fonction Configuration du format Trace permet à un administrateur avec le profil **Expert** de définir quelles données d'en-tête doivent figurer dans l'édition Trace et quel doit être le formatage des données Trace.

Données d'en-tête pour l'édition Trace (par défaut, toutes les options sont activées) :

- Paramètres de format d'en-tête de trace généraux

  Si cette option est activée, les options concernant les données d'en-tête suivantes peuvent être activées ou désactivées.
- ID de sous-système
- Nom de tâche
- ID de tâche
- Heure
- Nom du module
- Numéro de ligne

Préparation des données Trace (formatage)

- Formatage complet avec extension de paramètres (par défaut) = volume élevé de données, performances Trace normales. Paramètre par défaut
- Limité (types de messages binaires, spécialement pour X-Tracer) = volume de données moyen, performances Trace rapides.
- Limité (uniquement extension de types de données élémentaires) = faible volume de données, performances Trace très rapides.
- Trace avec optimisation de performances sans extension de paramètre = très faible volume de données, performances Trace extrêmement rapides.

Conseil :

Il faut savoir que des données supplémentaires d'en-tête Trace et un formatage plus complet des données Trace réduisent les performances globales de Trace.

Interfaces d'édition Trace

Cette fonction permet à un administrateur avec le profil **Expert** de définir les interfaces de l'édition Trace. Possibilités : activation du fichier Chiffrement de la trace, activation de Trace sur LAN ou désactivation des deux interfaces.

Interface d'édition Trace	Explication	Paramètre par défaut
Trace de fichier	**Activer la trace de fichier** Les messages Trace sont inscrits dans un fichier-journal, dans le système de communication. Lorsque l'option est activée, les paramètres suivants s'appliquent : **Quota de trace maximum (koctets)** : Affiche la taille maximale de la mémoire de trace **Police pour gérer l'atteinte du quota maximum**. Il est possible de choisir entre **Wrap Around (effacement du fichier le plus ancien)** et **Arrêt temporaire du fichier Trace**. **Délai entre la création de nouveaux fichiers Trace (s) :** 900 **Période de temps pendant laquelle les fichiers trace sont disponibles :** La période actuelle est indiquée.	Activé
Trace par LAN	**Activer la trace par LAN** Les messages Trace sont transmis via l'interface LAN. Lorsque l'option est activée, le paramètre suivant s'applique : **Valeur de temporisation** = 25 sec. (temporisation avant transmission de données.)	Non activé

Fichier-journal de trace

Si l'interface d'édition Trace Fichier Trace est activée, un administrateur avec le profil **Expert** peut, à l'aide de cette fonction, transmettre ou effacer les fichiers-journal sur un PC.

Bouclage numérique

Le bouclage numérique est utilisé pour contrôler la ligne des canaux B des interfaces S_0, S_{2M} et T1 d'éventuels modules disponibles. L'activation des boucles numériques de contrôle ne doit être effectuée qu'à la demande du fournisseur de services.

La configuration de boucles de contrôle numériques est exclusivement possible avec Manager E.

Observateur d’événements / Journal de trace client

Un administrateur avec profil **Advanced** peut, à l'aide de l'assistant **Observateur d’événements**, lancer l'affichage des événements (Trace client). De plus, le fichier journal Trace Client peut être transmis à un PC ou effacé.

Il est décrit la procédure d'interrogation des fonctions suivantes, qui est lancée à partir de l'Assistant :

- Comment afficher ou modifier le journal Observateur d’événements / Journal de trace client
- Comment télécharger et ouvrir le journal Observateur d’événements / le journal Trace client

- Comment effacer le journal Observateur d’événements / le journal Trace client

Un administrateur avec le profil **Expert** peut démarrer l'affichage du fichier journal Trace client via le **mode Expert**. De plus, le fichier journal Trace Client peut être transmis à un PC ou effacé.

Composante de trace M5T

Cette fonction sert à la surveillance de la pile SIP par un administrateur de profil **Expert**. Pour chaque Composante de Trace M5T, il est possible de définir le niveau de détails des enregistrements à l'aide du niveau de trace (0 = plus faible niveau de détails à 4 = plus fort niveau de détails).

Chiffrement de la trace

Cette fonction sert à enregistrer les flux de données de signalisation et de données de charge utile VoIP chiffrés par un administrateur de profil **Expert**.

Lorsque la fonctionnalité Signaling and Payload Encryption (cryptage de la signalisation et de la charge utile) (SPE) est activée, les flux VoIP de la charge utile et des données de signalisation sont cryptés en provenance et vers le système de communication ainsi qu'entre les téléphones IP.

Afin d'être en mesure de procéder à une analyse en cas de défaillance, il est possible, pendant une période de temps limitée, de transmettre au LAN des informations supplémentaires de trace (**Secure Trace** - Chiffrement de la trace). Il est généré des fichiers Secure-Trace à cryptage asymétrique ; leur décryptage et leur analyse ne sont possibles que par le service Développement.

Afin de limiter l'utilisation de la fonction Secure Trace, les caractéristiques de sécurité suivantes ont été mises en place :

- Un technicien de maintenance doit importer une clé publique (certificat) dans le système de communication concerné. Le certificat est une partie d'un fichier X.509 et c'est la condition pour générer Secure Trace. Le fichier X.509 est préparé par le service Développement. Le certificat fourni a une durée de validité d'un mois au maximum.
- Le démarrage et l'arrêt du chiffrement de la trace sont protégés par un mot de passe particulier (passphrase). Ce mot de passe est connu uniquement du client.

Le certificat est donc la clé du technicien et le mot de passe (passphrase) est la clé du client. Les deux clés sont nécessaires pour activer la fonction Secure Trace.

Déroulement pour la création du chiffrement de la trace :

1) Un technicien de maintenance trouve un problème dans le LAN du client. En raison de l'évolution permanente, on a pris conscience de la nécessité de générer un chiffrement de la trace (Secure Trace).
2) Le client est informé de cette nécessité et il doit confirmer qu'il a été informé. Ensuite, le client effectue une commande pour générer Secure Trace où la date et l'heure du début et de la fin de surveillance sont indiquées.

3) Un développeur crée une paire de clés composée d'une clé publique et d'une clé privée. Ces deux clés permettent de réaliser une seule Secure Trace. Les certificats sont utilisés de la manière suivante
   - Le certificat avec la clé privée est strictement confidentiel et ne doit être utilisé que par les développeurs autorisés.

     La clé privée est nécessaire au décryptage des fichiers Secure-Trace.
   - Le certificat avec la clé publique est transmis au technicien sous la forme d'un fichier X.509 au format PEM ou binaire.

     L'importation de ce certificat dans le système de communication concerné est la condition pour générer Secure Trace.
4) Le technicien de maintenance informe le client que la génération de le trace sécurisé va bientôt commencer. Le client doit informer les abonnés concernés.

   Remarque : L'enregistrement des communications et des données de connexion constitue un délit si les abonnés concernés n'ont pas été informés.
5) Le technicien de maintenance importe le certificat avec la clé publique dans le système de communication concerné.
6) Le client démarre Secure Trace en entrant le mot de passe (Passphrase). Les fichiers de chiffrement de la trace sont générés.

   Le démarrage et l'arrêt du chiffrement de la trace sont consignés par le système de communication.
7) Une fois le chiffrement de la trace terminé, le client est informé de la fin de l'activité de chiffrement de la trace. Le technicien retire le certificat du système de communication.
8) Les fichiers Trace sont mis à la disposition du service Développement.
9) Un développeur décrypte les fichiers de chiffrement de la trace à l'aide de la clé privée. Ensuite est effectuée l'analyse des données déchiffrées.

   Remarque : Une fois l'analyse terminée, toutes les données correspondantes doivent être détruites de manière sûre. Cela englobe aussi la destruction de la clé privée afin qu'une éventuelle copie non autorisée des fichiers de chiffrement de la trace ne puisse plus être décryptée.

Marqueur de test pour H.323

Via cette fonction, le paramétrage de la configuration Trace de pile H.323 est possible par un Administrateur avec le profil **Expert**. Le niveau de détail de l'enregistrement peut être défini à l'aide des niveaux Trace (0 = niveau de détails le plus faible, 4 = niveau de détails le plus élevé). Il est possible de sélectionner les réglages suivants pour l'édition Trace de la pile H.323 :

Interface d'édition Trace	Explication	Paramètre par défaut
Trace de console	**Activer la trace de console** Les messages Trace de la pile H.323 sont affichés sur la console.	Non activé

Interface d'édition Trace	Explication	Paramètre par défaut
Trace de fichier	**Activer la trace de fichier** Les messages Trace de la pile H.323 sont inscrits dans un fichier journal. Lorsque l'option est activée, les paramètres suivants s'appliquent : Taille maxi. du tampon de trace = 50000 octets (quantité de données conservées en mémoire tampon.) Taille maxi. du fichier Trace = 1000000 octets (taille maximum du fichier-journal) Temporisation de trace = 60 s (délai de temporisation avant que les données ne soient inscrites dans le fichier-journal.)	Non activé

L'activation et/ou la désactivation des modules H.323 permet de définir pour quelles composantes de la Trace de pile H.323 les informations de processus et d'état doivent être enregistrées. L'état de chaque module H.323 est indiqué par la couleur du point correspondant de la liste (vert = module H.323 activé, rouge = module H.323 non activé).

Le fichier-journal Trace de la pile H.323 peut être transféré sur un PC ou supprimé.

Trace des composants de la licence

Cette fonction sert serveiller l'agent de licence CLA (Customer License Agent) interne au système par un administrateur de profile Expert. Le niveau de détails de l'enregistrement peut être défini à l'aide des niveaux Trace (Bas = niveau de détails le plus faible (réglage par défaut), Standard = niveau de détails moyen, Tout = niveau de détails le plus élevé).

Dans le paramétrage par défaut la licence Composantes Trace est activée (niveau = bas).

La modification du niveau de suivi peut avoir un impact négatif sur les performances du système et ne doit donc être effectuée que par des administrateurs expérimentés et seulement après avoir consulté le service d'assistance compétent.

Profils de trace

Les profils Trace précisent le niveau de détail pour l'enregistrement des différentes données. Il est affecté des composantes Trace à chaque profil Trace. Il est précisé les composantes du système pour lesquelles le profil Trace doit enregistrer les informations de processus et d'état.

Il est proposé des profils Trace prédéfinis qui s'adressent à tous les scénarios standard. De plus, un administrateur avec le profil **Expert** est en mesure de créer ses propres profils de trace. Lorsque l'on démarre le profil Trace, l'enregistrement est activé par le biais de ce profil. Et il est désactivé à l'aide de la fonction Arrêter.

- Un administrateur avec profil **Advanced** peut, à l'aide de l'assistant **Trace** lancer et/arrêter des profils Trace. L'état de chaque profil Trace est indiqué par la couleur du point correspondant de la liste (vert = profil Trace activé,

rouge = profil Trace désactivé). Sélectionner **Démarrer/Arrêter** pour activer/démarrer un profil Trace non actif (point rouge) et désactiver/arrêter un profil Trace actif (point vert).

Utiliser **Charger la trace** pour transférer sur un PC les fichiers-journal obtenus ou pour les ouvrir.

A l'aide de **Supprimer la trace**, vous pouvez supprimer les fichiers-journal obtenus.

Il est décrit la procédure d'interrogation des fonctions suivantes, qui est lancée à partir de l'Assistant :

- Comment charger le fichier journal de trace système
- Comment effacer le fichier journal de trace système
- Comment afficher tous les profils de trace
- Comment démarrer ou arrêter un profil de trace
- Comment Télécharger les données de diagnostic / les journaux de diagnostic

- Un administrateur avec le profil **Expert** peut, à l'aide du **mode Expert** peut arrêter tous les profils Trace et redémarrer individuellement ces profils Trace puis redémarrer et/ou arrêter un profil Trace individuellement.

  Dans la représentation de l'arborescence des menus, la couleur du point identifie l'état du profil Trace (vert = profil Trace activé, rouge = profil Trace non activé). Sélectionner **Démarrer/Arrêter le profil Trace** pour activer/démarrer un profil Trace non actif (point rouge) et désactiver/arrêter un profil Trace actif (point vert).

  Sélectionner **Afficher le profil Trace** pour afficher les données détaillées du profil Trace souhaité : Celles-ci comprennent, en dehors du nom du profil, des indications sur la protection contre l'écriture et sur l'état du profil, ainsi que des informations précisant pour quels problèmes ce profil Trace doit être utilisé. Il est indiqué également les composantes Trace du profil Trace.

Profil de trace	Application
Acteurs / Capteurs / Ouvre-porte	Information non disponible !
Base	Information non disponible !
Calls_with_Analog_Subscriber_Trunks	Information non disponible !
Calls_with_ISDN_Subscriber_Trunks	Information non disponible !
Calls_with_System_Device_HFA	Information non disponible !
Calls_with_System_Device_Upn	Information non disponible !
CDR_Charging_data	Information non disponible !
CMI	Information non disponible !
Application CSTA	Information non disponible !
Display_problems	Information non disponible !
Gateway_Stream_detailed	Information non disponible !
Gateway_Stream_overview	Information non disponible !
IP_Interfaces	Information non disponible !
License_problem	Information non disponible !

Profil de trace	Application
Network_Call_Routing_LCR	Information non disponible !
Peripheral_cards	Information non disponible !
RAS_or_Internal_access	Information non disponible !
Resources_MOH_Conferencing	Information non disponible !
SIP_Interconnection_Subscriber_ITSP	Information non disponible !
SIP_Registration	Information non disponible !
Smart_VM	Information non disponible !
UC_Smart	Information non disponible !
Voice_fax_connection	Information non disponible !
VPN	Information non disponible !
Web_based_Assistant_Expert_Mode	Information non disponible !

Composantes de trace

Les composants Trace peuvent être utilisés pour enregistrer les informations de processus et d'état des différents composants du système de communication.

Toutes les composantes Trace peuvent être arrêtées ensemble et arrêtées et démarrées individuellement par un administrateur avec le profil **Expert**. Le lancement d'une composante Trace active l'enregistrement, l'arrêt désactive cet enregistrement. Le niveau de détail de l'enregistrement peut être défini à l'aide des niveaux Trace (0 = niveau de détails le plus faible, 9 = niveau de détails le plus élevé).

Lors de la représentation dans l'arborescence du menu, la couleur du point dans la liste indique l'état de la composante Trace (vert = composante Trace activée, rouge = composante Trace non activée). Sélectionner **Démarrer/ Arrêter la composante Trace** pour activer/démarrer un profil Trace non actif (point rouge) et désactiver/arrêter un profil Trace actif (point vert).

Lors de l'affichage d'une composante Trace, il est indiqué le nom du sous-système, l'indice de la composante Trace, le niveau Trace paramétré ainsi que l'information d'état, que la composante Trace soit démarrée ou non. Si une composante Trace doit être modifiée, il est possible, en plus de la modification du niveau Trace, d'effectuer le démarrage ou l'arrêt de la composante Trace.

24.8.4.1 Comment charger le fichier journal de trace système

L'assistant **Trace** vous permet de télécharger des fichiers journaux Trace.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Trace**.
3) Cliquez sur **Données de diagnostic**.

4) Cliquez sur **Aucun protocole** pour décocher tous les protocoles.
5) Cochez la case **Fichier-journal de trace**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez télécharger tout le journal Trace système existant, opérez une sélection dans la liste déroulante **Journal complet**.
   - Si vous souhaitez télécharger le fichier-journal de trace système du jour, sélectionnez dans la liste déroulante **Protocole d'aujourd'hui**.
   - Si vous souhaitez télécharger le fichier-journal de trace système d'une période précise, sélectionnez dans la liste déroulante **Propre sélection**. Dans la liste déroulante **De :** sélectionnez le début et dans la liste déroulante **A :** sélectionnez la fin de la période souhaitée.
7) Cliquez sur **Charger** et ensuite sur **OK**. La fenêtre de téléchargement de fichiers s'affiche.
8) Sauvegardez le fichier dans le répertoire choisi. Fermez ensuite la fenêtre où vous avez confirmé le téléchargement.
9) Cliquez sur **Suivant** puis sur **Quitter**.

24.8.4.2 Comment effacer le fichier journal de trace système

L'assistant **Trace** vous permet d'effacer des fichiers journaux Trace.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Trace**.
3) Cliquez sur **Effacer Trace** et ensuite sur **OK**.
4) Cliquez sur **Suivant** puis sur **Quitter**.

24.8.4.3 Comment définir les paramètres Trace sur des valeurs par défaut

L'assistant **Trace** vous permet de définir les fichiers journaux Trace du système sur l'état par défaut.

Conditions préalables

Vous êtes connecté à l'interface WBM avec le profil **Avancé** ou **Expert** .

Étape par étape

1) Cliquez sur **Centre de service** dans la barre de navigation.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Trace**.
3) Cliquez sur le bouton **Paramètres Trace par défaut** puis sur **OK** dans le message contextuel suivant qui vous indique que l'action est terminée.
4) Cliquez sur **Suivant** puis sur **Terminer**.

Remarque : Le traçage étendu augmente la charge générale du système et ne doit pas être activé en

permanence. Les paramètres Trace doivent être restaurés sur les paramètres par défaut en cliquant sur le bouton **Paramètres Trace par défaut** dès que les traçages requis ont été créés**.**

Remarque : Si les paramètres de traçage étendu sont activés, vous en serez averti sur la page d'accueil de l'interface WBM dans la zone **Notifications**. Un lien direct vers les paramètres Trace du centre de service est également disponible.

24.8.4.4 Comment afficher tous les profils de trace

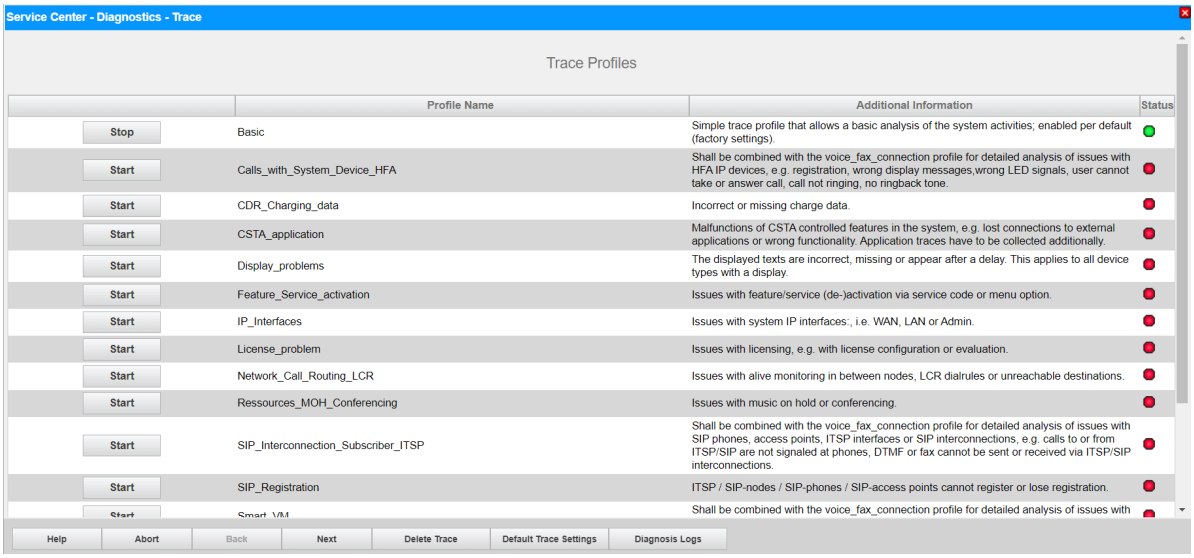
L'assistant **Trace** vous permet de vous informer de l'état actuel de tous les profils Trace.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Trace**. Le système affiche une liste de tous les profils de trace, avec indication des profils de trace démarrés et des profils de trace non démarrés.



3) Cliquez sur **Suivant** puis sur **Quitter**.

24.8.4.5 Comment démarrer ou arrêter un profil de trace

L'assistant **Trace** vous permet de lancer et arrêter des profils Trace.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Trace**. Le système affiche une liste de tous les profils de trace. Un point rouge identifie les profils de trace, qui doivent être lancés. Un point vert identifie les profils de trace, qui peuvent être arrêtées.
3) Sélectionnez une des possibilités suivantes :
   - Comment démarrer un profil de trace en cliquant sur **Démarrer**. La couleur du point de la liste, qui indique l'état du profil Trace, passe du rouge au vert.

     Remarque : Les profils de trace démarrés ont une incidence négative sur les performances du système. Vous devez donc arrêter tous les profils de trace une fois vos activités de diagnostic terminées, à l'exception du profil de trace **Par défaut**. Le profil de trace **Par défaut** doit demeurer actif.
   - Comment arrêter un profil de trace en cliquant sur **Arrêt**. La couleur du point de la liste, qui indique l'état du profil Trace, passe du vert au rouge.
4) Cliquez sur **Suivant** puis sur **Quitter**.

24.8.4.6 Comment afficher ou modifier la configuration du format Trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une demande émanant du support SAV correspondant et demandant de modifier la configuration du format Trace est disponible.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Trace** > **Configuration du format Trace**. Le système affiche les paramètres actuels de la configuration du format de trace.
4) Si nécessaire, modifiez les paramétrages souhaités.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.8.4.7 Comment afficher ou modifier les interfaces d'édition Trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Le support SAV correspondant a formulé une invitation à modifier les interfaces de sortie Trace.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Interfaces d'édition Trace**. Le Simple Network Management Protocol (SNMP - protocole simple de gestion de réseau) est un protocole réseau permettant de surveiller et de gérer les composantes du réseau (par ex. routeurs, serveurs, commutateurs, imprimantes, ordinateurs) à partir d'une station centrale.
4) Si nécessaire, modifiez les paramétrages souhaités.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.8.4.8 Comment afficher ou modifier le journal Observateur d'événements / Journal de trace client

L'assistant **Observateur d'événements** permet de lancer l'affichage des événements (trace client) et de modifier les paramètres d'actualisation.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Observateur d'événements**.
3) Cliquez sur l'onglet **Afficher**.
4) Sélectionnez le paramètre souhaité :
   - Si le protocole doit être actualisé automatiquement, cochez la case **Actualisation automatique**.
   - Si le protocole ne doit pas être actualisé automatiquement, décochez la case **Actualisation automatique**.
5) Cliquez si besoin est sur **Actualiser** pour actualiser manuellement le journal Trace client.
6) Cliquez sur **Terminer**.

24.8.4.9 Comment télécharger et ouvrir le journal Observateur d'événements / le journal Trace client

L'assistant **Observateur d'événements** permet de transférer sur un PC le fichier journal de trace client ou de l'ouvrir.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.

2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Observateur d'événements**.
3) Cliquez sur l'onglet **Charger par HTTP**.
4) Cliquez sur **Charger** et ensuite sur **OK**. La fenêtre de téléchargement de fichiers s'affiche.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez télécharger le fichier journal, cliquez sur **Enregistrer sous**. Sauvegardez le fichier dans le répertoire choisi. Fermez ensuite la fenêtre où vous avez confirmé le téléchargement du fichier.
   - Si vous souhaitez ouvrir le fichier journal, cliquez sur **Ouvrir**. Ensuite, le contenu du fichier-journal comprimé est affiché.
6) Cliquez sur **Terminer**.

24.8.4.10 Comment effacer le journal Observateur d'événements / le journal Trace client

L'assistant **Observateur d'événements** permet d'effacer le fichier journal de trace client.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Observateur d'événements**.
3) Cliquez sur l'onglet **Effacer le fichier-journal d'événements**.
4) Cliquez sur **Effacer le protocole** et ensuite sur **OK**.
5) Cliquez sur **Terminer**.

24.8.4.11 Comment afficher les composantes de trace M5T

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composantes de Trace M5T**. Le système affiche une liste de toutes les composantes de trace M5T avec les paramètres actuels. De plus, le nom de toutes les composantes de trace M5T est affiché dans l'arborescence du menu. Un point de couleur dans la liste indique l'état de chacune des composantes de trace M5T.

24.8.4.12 Comment démarrer ou arrêter une composante Trace M5T

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une invitation du support de service compétent pour démarrer ou arrêter une composante de trace M5T est présente.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composantes de Trace M5T**. Dans l'arborescence du menu, les noms de toutes les composantes de trace M5T sont affichés. Un point rouge identifie les composantes de trace M5T, qui doivent être lancés. Un point vert identifie les composantes de trace M5T, qui peuvent être arrêtées.
4) Dans l'arborescence du menu, cliquez sur la composante Trace M5T souhaitée.
5) Cliquez sur l'onglet **Démarrer/Arrêter la composante de trace**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez démarrer une composante de trace M5T, cliquez sur **Démarrer** et ensuite sur **OK**.
   - Si vous voulez arrêter une composante de trace M5T, cliquez sur **Stop** et ensuite sur **OK**.

24.8.4.13 Comment modifier la composante de trace M5T

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une demande émanant du support SAV correspondant et demandant de modifier les composantes Trace M5T a été reçue.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composantes de Trace M5T**. Le système affiche une liste de toutes les composantes de trace M5T avec les paramètres actuels.
4) Modifiez les paramètres souhaités.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.8.4.14 Comment démarrer ou arrêter le chiffrement de la trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Chiffrement de la trace**.
4) Cliquez sur l'onglet **Démarrer/arrêter le chiffrement de la trace**.
5) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez démarrer le chiffrement de la trace, procédez comme indiqué ci-après.

     Dans le champ **Phrase de passe d'activation du chiffrement de la trace**, entrez le mot de passe pour le chiffrement de la trace.

     Dans le champ **Durée du chiffrement de la trace (min)**, entrez la durée en minutes pendant laquelle le chiffrement de la trace sera activé.

     Cochez la case des protocoles pour lesquels un chiffrement de la trace doit être établi. Décochez la case des protocoles pour lesquels un chiffrement de la trace ne doit pas être établi.

     Cliquez sur **Activer SecureTrace** et ensuite sur **OK**.
   - Si vous souhaitez arrêter le chiffrement de la trace, cliquez sur **Quitter le chiffrement de la trace** et ensuite sur **OK**.

24.8.4.15 Comment interroger l'état Chiffrement de la trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Chiffrement de la trace**.
4) Cliquez sur l'onglet **Etat SecureTrace**. Ensuite, l'état actuel du Chiffrement de la trace est affiché.

24.8.4.16 Comment modifier le mot de passe pour le chiffrement de la trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Chiffrement de la trace**.
4) Cliquez sur l'onglet **Modifier le mot de passe du chiffrement de la trace**.

5) Dans le champ **Phrase de passe actuelle**, entrez le mot de passe actuel pour le chiffrement de la trace.
6) Dans les champs **Nouvelle phrase de passe** et **Confirmer nouvelle phrase de passe**, entrez le nouveau mot de passe pour le chiffrement ; il doit comporter au minimum cinq caractères et au maximum douze.
7) Cliquez sur **Appliquer**.

24.8.4.17 Comment importer le certificat pour le Chiffrement de la trace (Secure Trace) à partir d'un fichier X.509

Conditions préalables

Un fichier X.509 au format PEM ou binaire est disponible.

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Chiffrement de la trace**.
4) Cliquez sur l'onglet **Importer le fichier X.509 pour le chiffrement de la trace**.
5) Cliquez sur **Parcourir** pour sélectionner le fichier X.509 souhaité.
6) Cliquez sur **Ouvrir**.
7) Cliquez sur **Importer le certificat du fichier**.

24.8.4.18 Comment afficher ou modifier la configuration Trace de la pile H.323.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une demande émanant du support SAV correspondant et demandant de modifier la configuration de la pile H.323 Trace est disponible.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Trace de pile H.323**.
4) Cliquez sur l'onglet **Modifier la configuration de la trace de pile H.323**. Le système affiche les paramètres actuels de la configuration de la trace de pile H.323.
5) Si nécessaire, modifiez les paramétrages souhaités.
6) Cliquez sur **Appliquer** puis sur **OK**.

24.8.4.19 Comment modifier les modules H.323

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Une demande émanant du support SAV correspondant et demandant de modifier les modules H.323 est disponible.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Trace de pile H.323**.
4) Cliquez sur l'onglet **Modifier tous les modules H.323**.
5) Sélectionnez le paramètre souhaité pour **Trace activée** :
   - Si vous souhaitez activer la fonction Trace pour certains modules H.323, cochez les cases des modules H.323 correspondants. Décochez la case des modules H.323 pour lesquels la Trace doit être désactivée.
   - Si vous souhaitez désactiver Trace pour tous les modules H.323, cliquez sur **Néant**.
6) Cliquez sur **Appliquer** puis sur **OK**.

24.8.4.20 Comment télécharger ou ouvrir le fichier-journal Trace de la pile H.323

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Trace de pile H.323**.
4) Cliquez sur l'onglet **Charger le fichier-journal Trace de la pile H.323**.
5) Cliquez sur **Charger** et ensuite sur **OK**. La fenêtre de téléchargement de fichiers s'affiche.
6) Sélectionnez une des possibilités suivantes :
   - Si vous voulez enregistrer le fichier journal Trace de pile H.323, cliquez sur **Enregistrer sous**. Sauvegardez le fichier dans le répertoire choisi. Fermez ensuite la fenêtre où vous avez confirmé le téléchargement du fichier.
   - Si vous voulez ouvrir le fichier journal Trace de pile H.323, cliquez sur **Ouvrir**. Le fichier s'affiche ensuite dans l'éditeur de texte.

24.8.4.21 Comment effacer le fichier-journal Trace de la pile H.323

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Trace de pile H.323**.
4) Cliquez sur l'onglet **Effacer le fichier-journal Trace de la pile H.323**.
5) Cliquez sur **Effacer le protocole** et ensuite sur **OK**.

24.8.4.22 Comment modifier la composante de licence Trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Le support SAV correspondant a formulé une invitation à modifier la composante de licence Trace.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composante de licence** > **CLA**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez arrêter la composante de licence Trace, sélectionnez dans la liste déroulante **Niveau de trace** l'entrée **Désactiver**.
   - Si vous souhaitez un niveau de détails inférieur pour l'enregistrement Trace, sélectionnez dans la liste déroulante **Niveau de trace** l'entrée **Bas**.
   - Si vous souhaitez un niveau de détails moyen pour l'enregistrement Trace, sélectionnez dans la liste déroulante **Niveau de trace** l'entrée **Par défaut**.
   - Si vous souhaitez un niveau de détails élevé pour l'enregistrement Trace, sélectionnez dans la liste déroulante **Niveau de trace** l'entrée **Tout**.
5) Cliquez sur **Appliquer**.

24.8.4.23 Comment afficher les détails d'un profil de trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Profils Trace**. Le système affiche une liste de tous les profils de trace. De plus, le nom de tous les profils Trace est affiché dans l'arborescence du menu. Un point de couleur dans la liste indique l'état de chacun des profils de trace.
4) Dans l'arborescence du menu, cliquez sur le nom de l'événement souhaité. Le système affiche les données détaillées de ce profil de trace.

24.8.4.24 Comment arrêter tous les profils de trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Profils Trace**.
4) Cliquez sur l'onglet **Arrêter tous les profils de trace**.
5) Cliquez sur **Arrêter tout** et ensuite sur **OK**.

24.8.4.25 Comment ajouter un profil Trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Profils Trace**.
4) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez ajouter un profil Trace vide, cliquez dans le menu contextuel, sur **Ajouter un profil Trace (Profil vide)**.
   - Si vous souhaitez ajouter un profil Trace qui contient les composantes Trace de tous les profils Trace actuellement activés, cliquez sur l'onglet **Ajouter un profil Trace (avec les paramètres Trace actuels)**. Sélectionnez parmi les composantes de trace celles qui devront figurer dans le nouveau profil Trace et avec quel niveau.
5) Dans le champ **Nom du profil**, indiquez le nom du nouveau profil Trace.
6) Cliquez sur **Appliquer** puis sur **OK**.

24.8.4.26 Comment afficher les composantes de trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composantes de trace**.

4) Sélectionnez une des possibilités suivantes :
   - Pour afficher la liste de toutes les composantes de trace, cliquez sur l'onglet **Afficher toutes les composantes de trace**.
   - Pour afficher la liste de toutes les composantes de trace démarrées, cliquez sur l'onglet **Afficher toutes les composantes de trace démarrées**.
   - Pour afficher la liste de toutes les composantes de trace arrêtées, cliquez sur l'onglet **Afficher les composantes de trace arrêtées**.

24.8.4.27 Comment afficher les détails d'une composante de trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composantes de trace**. Le système affiche une liste de toutes les composantes de trace. De plus, le nom de toutes les composantes de trace est affiché dans l'arborescence du menu. Un point de couleur dans la liste indique l'état de chacune des composantes de trace.
4) Dans l'arborescence du menu, cliquez sur le nom des composantes de trace souhaitées. Le système affiche les données détaillées de ces composantes de trace.

24.8.4.28 Comment démarrer ou arrêter une composante Trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composantes de trace**. Dans l'arborescence du menu, les noms de toutes les composantes Trace sont affichés. Un point rouge identifie les composantes de trace, qui doivent être lancés. Un point vert identifie les composantes de trace, qui peuvent être arrêtées.
4) Dans l'arborescence du menu, cliquez sur la composante Trace souhaitée.
5) Cliquez sur l'onglet **Démarrer/Arrêter la composante de trace**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez démarrer une composante de trace, cliquez sur **Démarrer** et ensuite sur **OK**.
   - Si vous voulez arrêter une composante de trace, cliquez sur **Stop** et ensuite sur **OK**.

24.8.4.29 Comment arrêter toutes les composantes de trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composantes de trace**.
4) Cliquez sur l'onglet **Arrêter toutes les composantes de trace**.
5) Cliquez sur **Arrêter tout** et ensuite sur **OK**.

24.8.4.30 Comment définir les paramètres Trace sur des valeurs par défaut

Conditions préalables

Vous êtes connecté à l'interface WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composants Trace**.
4) Cliquez sur l'onglet **Paramètres Trace par défaut**.
5) Cliquez sur le bouton **Paramètres Trace par défaut** puis sur **OK** dans le message contextuel suivant qui vous indique que l'action est terminée.

Remarque : Le traçage étendu augmente la charge générale du système et ne doit pas être activé en permanence. Les paramètres Trace doivent être restaurés sur les paramètres par défaut en cliquant sur le bouton **Paramètres Trace par défaut** dès que les traçages requis ont été créés**.**

Remarque : Si les paramètres de traçage étendu sont activés, vous en serez averti sur la page d'accueil de l'interface WBM dans la zone **Notifications**. Un lien direct vers les paramètres Trace est également disponible.

24.8.4.31 Comment modifier la composante de trace

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.

2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Traces**.
3) Dans l'arborescence du menu, cliquez sur **Traces** > **Composantes de trace**.
4) Cliquez sur l'onglet **Modifier la composante de trace**. Le système affiche une liste de toutes les composantes de trace avec les paramètres actuels.
5) Modifiez les paramètres souhaités.
6) Cliquez sur **Appliquer** puis sur **OK**.

24.8.4.32 Comment transférer automatiquement les fichiers journaux système

Vous pouvez activer l'option permettant de transférer automatiquement les fichiers journaux système vers un serveur système/syslog de gestion externe.

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance > Traces > Transfert Syslog**.
3) Saisissez l'**Adresse IP** et le **Port** du système de gestion vers lequel le fichier syslog sera transféré.
4) Cliquez sur **Démarrer.** pour enregistrer les modifications de la configuration et lancer le processus.

   Si la connexion au portail de gestion/serveur syslog réussit, l'**Etat de la connexion** passe au vert.

   Si la connexion au portail de gestion/serveur syslog échoue, l'**Etat de la connexion** passe au rouge.
5) Cliquez sur **Arrêter** pour désactiver le processus.

   L'**Etat de la connexion** est défini sur Désactivé avec un indicateur gris.
6) Si vous modifiez les paramètres de configuration, cliquez sur **Appliquer** pour que les modifications aient lieu.

24.8.4.33 Comment démarrer le service des données de crash du noyau

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Votre système de communication est équipé d'une carte mère V3 OCC (OCCLA, OCCMA(R), OCCMB(R)).
Assurez-vous d'avoir suffisamment d'espace libre sur le disque de stockage pour que le service puisse s'exécuter correctement. Le service nécessite 200 Mo d'espace de stockage. Les disques affectés sont les suivants :

- SSS SATA 16 Go (si pas de SSD NVMe)
- SSD NVMe

Si vous souhaitez libérer de l'espace de stockage, il est recommandé de supprimer les traces avant de démarrer le service.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Suivis**.
3) Cliquez sur **Composantes de trace > Données de crash du noyau**.
4) Cliquez sur **Démarrer**.

Le service des données de crash du noyau démarre et un redémarrage du système est automatiquement lancé. Le service conserve l'état après redémarrage du système.

24.8.4.34 Comment arrêter le service des données de crash du noyau

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Votre système de communication est équipé d'une carte mère V3 OCC (OCCLA, OCCMA(R), OCCMB(R)).

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Suivis**.
3) Cliquez sur **Composantes de trace > Données de crash du noyau**.
4) Cliquez sur **Arrêter**.

Le service des données de crash du noyau s'arrête et un redémarrage du système est automatiquement lancé. Le service conserve l'état après redémarrage du système.

24.8.4.35 Comment démarrer la trace du serveur média

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Suivis**.
3) Cliquez sur **Trace du serveur média**.
4) Sélectionnez une option dans la liste déroulante **Niveau Trace** afin de définir le niveau de détail de la trace.
5) Cliquez sur **Démarrer**.

Remarque : Les traces actives augmentent la charge générale du système et peuvent avoir un impact négatif sur

ses performances. Il convient donc de désactiver la trace du serveur média dès que vous avez terminé vos activités de diagnostic.

24.8.4.36 Comment arrêter la trace du serveur média

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Suivis**.
3) Cliquez sur **Trace du serveur média**.
4) Cliquez sur **Arrêter**.

24.9 TCP-Dump

Un TCP-Dump sert à surveiller et analyser le trafic de données dans un réseau IP.

Conseil : L'activation d'un TCP-Dump a des répercussions négatives sur les performances du système et ne doit être effectuée que par des administrateurs expérimentés et uniquement en accord avec le support SAV compétent.

Les fichiers TCP-Dump sont enregistrés dans le système de communication. Pour le diagnostic des fichiers, une application correspondante est nécessaire.

Les TCP-Dumps sont fréquemment utilisés

- pour effectuer un suivi LAN durant une période courte (par ex en cas d'erreur reproductible).
- pour permettre aux techniciens de maintenance autorisés d'accès à un suivi LAN.

Avantages par rapport à Démon RPCAP : accès à distance possible, les fichiers de suivi n'ont pas besoin d'être envoyés par e-mail.

Désavantages par rapport à Démon RPCAP : suivi longue durée non judicieux, capacité d'enregistrement limitée, impossibilité de paramétrer des filtres Capture, manipulation plus lourde en cas de plusieurs suivis individuels.

24.9.1 Comment démarrer TCP-Dump

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Traces** > **TCP-Dump**.
3) Cliquez sur**Démarrer TCP-Dump**.
4) Modifiez les paramètres souhaités.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.9.2 Comment arrêter TCP-Dump

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Traces** > **TCP-Dump**.
3) Cliquez sur**Arrêter TCP-Dump**.
4) Cliquez sur **OK**.

24.9.3 Comment effacer TCP-Dump

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Traces** > **TCP-Dump**.
3) Cliquez sur**Mettre en ordre TCP-Dump**.
4) Cliquez sur **Appliquer** puis sur **OK**.

24.10 Démon RPCAP

Un Démon RPCAP (Remote Packet Capture) sert à surveiller et analyser le trafic de données dans un réseau IP.

Conseil : L'activation d'un démon RPCAP a des répercussions négatives sur les performances du système et ne doit être activée que par des administrateurs expérimentés et uniquement en accord avec le support SAV compétent.

Via le démon RPCAP, il est possible que des applications externes accèdent aux paquets TCP/IP des interfaces LAN du système de communication.

Un Démon RPCAP est souvent utilisé pour les suivis de longue durée parce que les fichiers trace sont enregistrés sur PC et non pas dans le système de communication.

Avantages par rapport à TCP-Dump : manipulation plus rapide et plus simple, suivis longue durée possible, nombre et/ou taille des fichiers trace librement sélectionnables, suivi du LAN interne possible.

Désavantages par rapport à TCP-Dump : double trafic de données sur le réseau et donc charge supérieure pour les interfaces LAN du système de communication, validation de port spéciale nécessaire (pare-feu)

24.10.1 Comment activer Démon RPCAP

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Le Démon RPCAP a été désactivé.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Traces** > **Démon RPCAP**.
3) Modifiez les paramètres souhaités.
4) Cliquez sur **Appliquer** puis sur **OK**.

24.10.2 Comment désactiver Démon RPCAP

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Le Démon RPCAP a été activé.

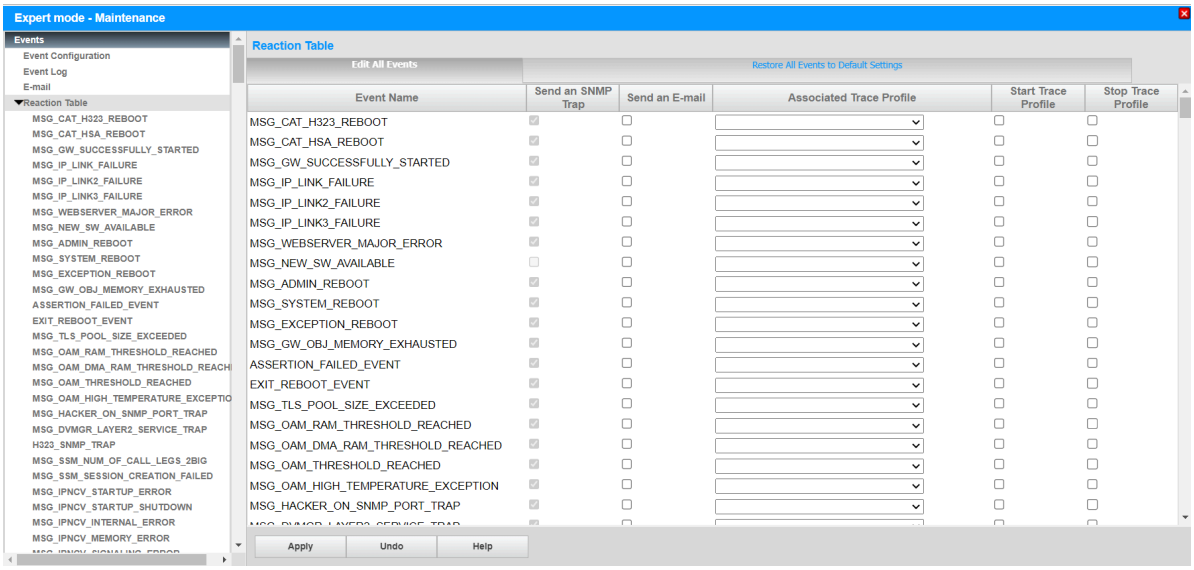
Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Traces** > **Démon RPCAP**.
3) Cliquez sur **Appliquer** puis sur **OK**.

24.11 Événements (events)

Les événements (events) informent sur les défaillances du système de communication. Tous les événements sont inscrits dans un fichier protocole de taille limitée. Lorsque la taille maximale du fichier est dépassée, un nouveau fichier est créé. Il est possible de créer jusqu'à sept fichiers.

En fonction du paramétrage du tableau de réactions et de la classe de problème, les événements peuvent générer une alarme SNMP, provoquer l'envoi d'un e-mail et/ou démarrer/arrêter une surveillance de suivi. L'évaluation, la configuration et l'enregistrement des journaux d'événements (de l'affichage des événements) sont possibles à l'aide de la WBM.



Pour qu'il soit possible d'interpréter le fichier du journal d'événements, il faut que le fichier ait été téléchargé et enregistré à l'aide de WBM. Ensuite il est possible d'ouvrir, de modifier ou d'imprimer le fichier avec un éditeur de texte quelconque. Une fois que le fichier du journal d'événements a été transmis, il est possible d'effacer le fichier dans la mémoire du système de communication.

Les événements qui provoquent des actions sont définis par les propriétés suivantes :

- Code d'événement :

  Identifie un Event (événement) comme `MSG_ADMIN_LOGGED_OUT` = information sur la fermeture de session (logout) d'un administrateur.
- Type d'événement

  Il existe les types suivants :

  – Information : pur message d'état, n'est pas un message d'erreur.
  – Avertissement : message concernant un processus ou un état pouvant être problématique, n'est pas un message d'erreur.
  – Mineur : message d'erreur. L'erreur n'a pas de conséquences problématiques.
  – Majeur : message d'erreur. L'erreur peut avoir des conséquences problématiques.
  – Critique : Message d'erreur L'erreur a des conséquences problématiques.
  – Réglée : message d'erreur. L'erreur a déjà été réglée par le Système de communication.
  – Indéterminée : message d'erreur. La cause de l'erreur ne peut pas être déterminée de manière précise.

- Evénements-Texte

  Certains textes d'événements contiennent des données variables. Elles sont identifiées de la manière suivante :

  – %s : chaîne de caractères
  – %u : nombre décimal positif ou négatif
  – %f : nombre à virgule flottante
  – %p : indicateur (adresse d'enregistrement)
  – %x : nombre hexadécimal (avec minuscules)
  – %x : nombre hexadécimal (avec majuscules)
  – %c : caractère individuel
  – %d et %i : nombre décimal positif

Tableau de réactions

À l'aide du tableau de réactions, un administrateur au profil **Expert** peut définir individuellement pour chaque événement comment réagir lorsque cet événement survient.

Il est possible de régler si un SNMP trap doit être envoyé ou non, si le système de communication doit être redémarré ou non, si un e-mail doit être envoyé ou non et si un profil de trace doit être démarré ou arrêté. Si un profil Trace est affecté à l'événement, son nom est affiché.

Paramètres e-mail

A partir de ces paramétrages, un administrateur au profil **Expert** peut fournir des indications sur l'envoi d'un e-mail lorsque survient un événement.

Journaux de diagnostic

Le système de communication consigne certaines actions des processus dans des journaux de diagnostic. Ces journaux peuvent être évalués par un administrateur avec le profil **Expert** en vue d'un diagnostic.

Signalisation d'alarme en cas de dépassement de température

Deux valeurs de température critiques sont enregistrées dans le système de communication. Si la température du système dépasse la première valeur, il se produit un message d'avertissement par SNMP trap ou E-mail, indiquant que la température du système est trop élevée. De plus, ce message est également affiché à l'écran de 3 téléphones système maxi. (UP0 & HFA), voir Comment définir les destinations de la signalisation d'alarme. Si la seconde valeur est dépassée, les modules responsables de la surchauffe sont arrêtés de manière contrôlée (par ex. OpenScape Business Booster Card) ou déconnectés (par ex. SLAV/SLAD). Pour effacer l'alarme et remettre en service les modules, il faut arrêter le système et le remettre en marche.

Il est possible d'indiquer les 3 destinations (téléphones système) à informer en cas de dépassement de la température.

24.11.1 Comment modifier la consignation des événements par LAN

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Configuration des événements**.
4) Sélectionnez le paramètre souhaité :
   - Si la consignation des événements doit être transmise via un LAN, cochez la case **Activer la consignation des événements par LAN**.
   - Si la consignation des événements ne doit pas être transmise via un LAN, décochez la case **Activer la consignation des événements par LAN**.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.11.2 Comment charger le fichier de journal d'événements

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Protocole des événement**.
4) Cliquez sur l'onglet **Charger par HTTP**.
5) Cliquez sur **Charger** et ensuite sur **OK**. La fenêtre de téléchargement de fichiers s'affiche.
6) Sauvegardez le fichier dans le répertoire choisi. Fermez ensuite la fenêtre où vous avez confirmé le téléchargement.

24.11.3 Comment effacer le fichier de journal d'événements

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Protocole des événement**.
4) Cliquez sur l'onglet **Effacer le fichier-journal d'événements**.
5) Cliquez sur **Effacer le protocole** et ensuite sur **OK**.

24.11.4 Comment modifier les paramètres e-mail des événements

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Renvoi E-Mail doit être configuré pour tous les systèmes pour pouvoir utiliser l'option **Destinataire des notifications d'urgence**. Informations supplémentaires, voir Comment configurer l'envoi d'e-mails à la page 175

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **E-mail**.
4) Sous **Objet**, saisissez ce qui sera affiché dans le champ Objet de l'e-mail.

   Conseil : L'objet doit indiquer de manière univoque qu'il s'agit d'un e-mail résultant d'un événement.

   ---

5) Dans les champs **Destinataire 1** à **Destinataire 5**, saisissez les adresses e-mail auxquelles l'e-mail doit être envoyé.
6) Dans le champ **Destinataire d'urgence**, saisissez l'adresse e-mail d'un agent de sécurité sur site à laquelle un e-mail est envoyé lorsqu'un numéro d'urgence est composé.

   L'objet de l'e-mail sera « Nouvel appel d'urgence ». Le numéro d'appel et le nom de l'appelant (s'ils sont configurés) sont inclus dans l'e-mail et récupérés auprès de la base de données du système.
7) Cliquez sur **Appliquer**, puis sur **OK**.

24.11.5 Comment afficher le tableau de réactions aux événements

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Tableau de réactions**. Le système affiche le tableau de réactions avec tous les événements possibles et leurs paramètres de réaction.

24.11.6 Comment modifier les paramètres de réaction d'un événement

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Tableau de réactions**. Le système affiche le tableau de réactions avec tous les événements possibles et leurs paramètres de réaction. L'arborescence des menus affiche également le nom de tous les événements possibles.
4) Cliquez dans l'arborescence du menu sur le nom de l'événement souhaité.
5) Cliquez sur l'onglet **Modifier l'événement**. Le système affiche les paramètres de réaction de l'événement souhaité

   Conseil : Vous ne pouvez pas modifier les paramètres de réaction **Redémarrer la passerelle** et **Avertir OpenScape**. Il n'est pas toujours possible de modifier le paramétrage **Envoyer un Trap SNMP** pour tous les événements.

6) Si nécessaire, définissez les paramètres de **Envoyer un Trap SNMP**:
   - Si un trap SNMP doit être envoyé lorsque survient un événement, cochez la case **Envoi de trap SNMP**.
   - Si aucun trap SNMP ne doit être envoyé lorsque survient un événement, décochez la case **Envoi de trap SNMP**.
7) Sélectionnez le paramètre pour **Envoyer un e-mail** :
   - Si un e-mail doit être envoyé lorsque survient un événement, cochez la case **Envoyer un e-mail**.
   - Si aucun e-mail ne doit être envoyé lorsque survient un événement, décochez la case **Envoyer un e-mail**.
8) Dans la liste déroulante **Profil de trace affecté**, sélectionnez le profil de trace souhaité.
9) Sélectionnez le paramètre pour le démarrage ou l'arrêt du profil Trace :
   - Si le profil Trace sélectionné doit être démarré lorsque survient un événement, cochez la case **Démarrer le profil Trace**.
   - Si le profil Trace sélectionné doit être arrêté lorsque survient un événement, cochez la case **Arrêter le profil Trace**.
10) Cliquez sur **Appliquer** puis sur **OK**.

24.11.7 Comment modifier les paramètres de réaction de plusieurs événements

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.

3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Tableau de réactions**. Le système affiche le tableau de réactions avec tous les événements possibles et leurs paramètres de réaction.

Conseil : Vous ne pouvez pas modifier les paramètres de réaction **Redémarrer la passerelle** et **Avertir OpenScape**. Il n'est pas toujours possible de modifier le paramétrage **Envoyer un Trap SNMP** pour tous les événements.

---

4) Modifier les paramètres de réaction des événements souhaités dans le tableau des réactions.
   - Si nécessaire, définissez les paramètres de **Envoyer un Trap SNMP**:

     Si un trap SNMP doit être envoyé lorsque survient un événement, cochez la case **Envoi de trap SNMP**.

     Si aucun trap SNMP ne doit être envoyé lorsque survient un événement, décochez la case **Envoi de trap SNMP**.
   - Sélectionnez le paramètre pour **Envoyer un e-mail** :

     Si un e-mail doit être envoyé lorsque survient un événement, cochez la case **Envoyer un e-mail**.

     Si aucun e-mail ne doit être envoyé lorsque survient un événement, décochez la case **Envoyer un e-mail**.
   - Dans la liste déroulante **Profil de trace affecté**, sélectionnez le profil de trace souhaité.
   - Sélectionnez le paramètre pour le démarrage ou l'arrêt du profil Trace :

     Si le profil Trace sélectionné doit être démarré lorsque survient un événement, cochez la case **Démarrer le profil Trace**.

     Si le profil Trace sélectionné doit être arrêté lorsque survient un événement, cochez la case **Arrêter le profil Trace**.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.11.8 Comment télécharger ou ouvrir les journaux de diagnostic

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Journaux de diagnostic**.
4) Cliquez sur l'onglet **Récupérer les journaux de diagnostic**. Le système affiche une liste de tous les fichiers-journal disponibles, avec les noms de fichier, la taille des fichiers en octets, l'heure de la dernière modification et les attributs du fichier.
5) Cliquez dans **Nom du fichier** sur le nom du journal de diagnostic souhaité. La fenêtre de téléchargement de fichiers s'affiche.

6) Sauvegardez le fichier dans le répertoire choisi. Fermez ensuite la fenêtre où vous avez confirmé le téléchargement.

24.11.9 Comment effacer les journaux de diagnostic

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Journaux de diagnostic**. Le système affiche une liste de tous les fichiers-journal disponibles, avec les noms de fichier, la taille des fichiers en octets, l'heure de la dernière modification et les attributs du fichier.
4) Cliquez sur l'onglet **Effacer les journaux de diagnostic**.
5) Cliquez sur **Effacer le protocole** et ensuite sur **OK**.

24.11.10 Comment définir les destinations de la signalisation d'alarme

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Evénements**.
3) Dans l'arborescence du menu, cliquez sur **Evénements** > **Signalisation d'alarme**.
4) Sélectionnez dans les listes déroulantes **Abonnés1-3** les trois destinations (téléphones système avec écran, UP0 & HFA) dont l'écran doit être informé lorsque la température du système dépasse une valeur critique fixe qui a été définie.
5) Cliquez sur **Appliquer** puis sur **OK**.

24.12 Données de configuration pour les diagnostics

Des ensembles de sauvegarde « plus petits » contenant des données de diagnostic pour le support technique peuvent être créés à des fins de diagnostic. Contrairement aux ensembles de sauvegarde classiques, des quantités de données nettement inférieures sont produites à cet effet et peuvent donc être facilement envoyées par courrier électronique, par exemple.

Les ensembles de sauvegarde de diagnostic comprennent, entre autres, les données de configuration du système de communication et de l'application UC (UC Smart ou UC Suite). Les messages vocaux, les fax et les annonces ne sont pas inclus.

Les supports suivants peuvent être utilisés pour sauvegarder les jeux de données à des fins de diagnostic :

- **périphérique USB**

  Les données peuvent être sauvegardées sur un disque dur USB ou une clé USB connectée, par exemple.

  Remarque : Si un disque dur USB, une partition de celui-ci ou une clé USB doit être utilisé pour la sauvegarde, il doit être formaté en FAT32. En raison des limitations du système de fichiers, la taille maximale de la sauvegarde ne peut pas dépasser 4 Go. Dans de tels cas, il convient de sélectionner un autre support de sauvegarde. Les supports USB formatés en NTFS sont en lecture seule. Notez que s'il existe plusieurs partitions, seule la première peut être utilisée pour la sauvegarde.

  Si une clé USB amorçable est utilisée pour la sauvegarde, cette clé USB doit être retirée en toute sécurité après la sauvegarde.

- **HTTPS**

  Les données peuvent être enregistrées via HTTPS sur le disque dur du PC client.

  Conseil : Il n'est pas possible de créer une sauvegarde sur le disque dur du système de communication.

24.12.1 Comment générer des données de configuration pour les diagnostics

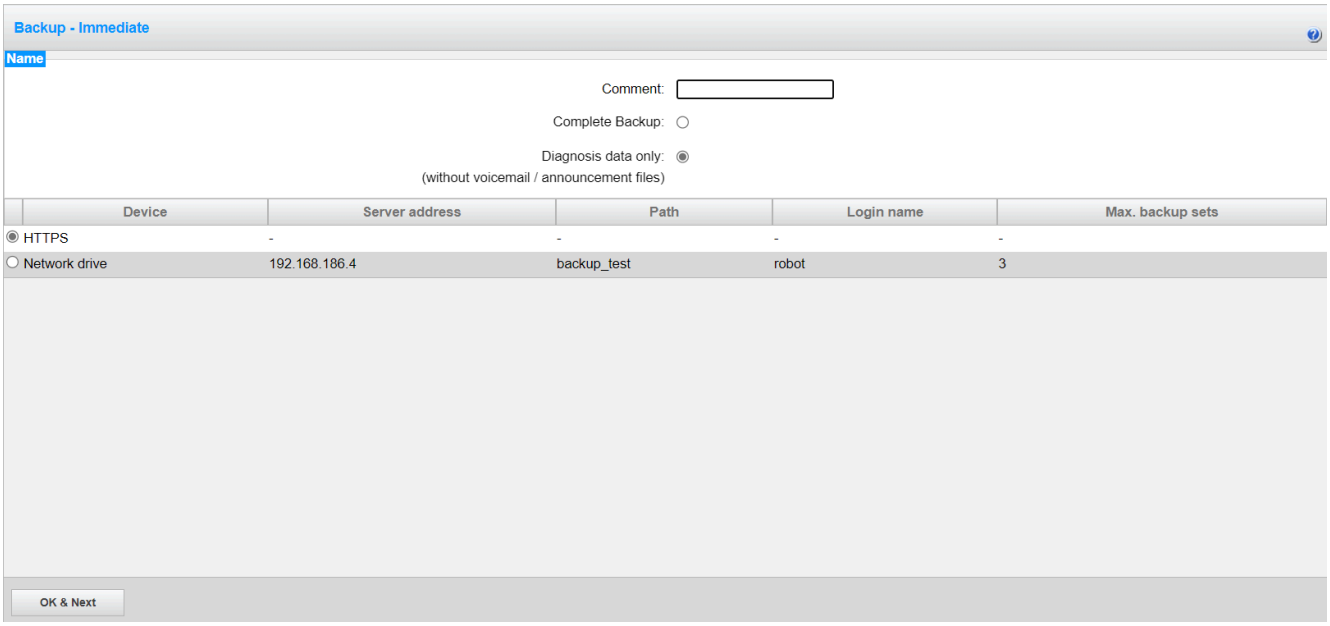
Conditions préalables

Vous êtes connecté au WBM avec le profil **Avancé** .

Étape par étape

1) Cliquez sur **Sauvegarde des données** dans la barre de navigation.

2) Dans l'arborescence de navigation, cliquez sur **Sauvegarde des données** > **Sauvegarde - immédiate**.



3) Activez la case à cocher **Diagnostics** .
4) Sélectionnez le périphérique sur lequel l'ensemble de sauvegarde des diagnostics doit être enregistré. Vous avez les options suivantes :
   - Si vous souhaitez enregistrer les données sur un disque dur ou une clé USB connectés, activez l'option « **Périphérique USB »** .
   - Si vous souhaitez sauvegarder les données en utilisant HTTPS sur le disque dur du PC client, activez l'option **HTTPS** .
5) Si nécessaire, veuillez saisir un commentaire pour votre ensemble de sauvegarde de diagnostic dans le champ **Commentaire** . Évitez d'utiliser des caractères diacritiques tels que les trémas et les caractères spéciaux dans votre saisie.
6) Cliquez sur **OK et Suivant** . La progression du processus de sauvegarde est affichée dans une fenêtre séparée.
7) La sauvegarde a réussi si le message « `Sauvegarde terminée !` » s'affiche.
8) Si vous avez sélectionné **HTTPS** comme support de sauvegarde, vous devez enregistrer l'ensemble de sauvegarde des diagnostics et le fichier texte associé à l'emplacement de votre choix. Cette opération est effectuée automatiquement pour les autres supports de sauvegarde. La fenêtre du navigateur doit rester ouverte jusqu'à ce que l'opération d'enregistrement du jeu de sauvegarde des diagnostics et du fichier texte soit terminée.

   Remarque : Si vous avez sélectionné **un périphérique USB** comme support de sauvegarde, attendez que la LED du périphérique USB cesse de clignoter. Ce n'est qu'à ce moment-là que l'ensemble de sauvegarde des diagnostics a été entièrement enregistré sur le périphérique USB. Vous pouvez ensuite retirer le périphérique USB.
9) Cliquez sur **Terminer** .

Étapes suivantes

Le jeu de sauvegarde des diagnostics peut désormais être envoyé par e-mail au service d'assistance compétent afin de faciliter le processus de dépannage, par exemple.

24.13 Gestionnaire de cartes

OpenScape Business est fourni avec des supports de démarrage contenant le logiciel système. Le Gestionnaire de cartes est un outil destiné au support technique pour créer un nouveau logiciel système sur une carte SDHC ou un SSD M.2 SATA vierge. Pour ce faire, le logiciel du système de communication doit être disponible sous forme de fichier image compatible.

Le logiciel présent sur la carte SDHC, le SSD M.2 SATA ou le disque dur est un logiciel système standard sans données client. Il ne peut pas être utilisé pour les mises à jour logicielles ni pour la sauvegarde des données client. Il est possible uniquement dans le cas d'une carte SDHC d'inclure un fichier de sauvegarde lors de sa création.

Le gestionnaire de cartes peut être lancé sous forme d'image ISO sur un DVD de démarrage Linux, une clé USB amorçable Linux ou dans un environnement virtuel.

Le logiciel Card Manager est disponible via le portail des partenaires.

Cas d'utilisation

- Avant la livraison du système, le logiciel doit être remplacé par la dernière version disponible.
- Le périphérique de stockage est défectueux et doit être remplacé par un neuf sur lequel aucun logiciel n'a encore été stocké.
- Le logiciel utilisé est corrompu et doit être réinstallé. Toutes les données client sont supprimées au cours de ce processus.

  Si un ensemble de sauvegarde existe pour la récupération des données client, le logiciel nouvellement installé doit correspondre à la version du logiciel avec laquelle l'ensemble de sauvegarde a été créé afin que les paramètres contenus dans l'ensemble de sauvegarde puissent également être pris en charge et traités par le logiciel installé.

24.13.1 Comment inscrire le logiciel de communication sur le disque SSD M.2 SATA à l’aide de Card Manager

Vous pouvez utiliser Card Manager pour écrire le logiciel de communication d’OpenScape Business V3 sur le disque SSD M.2 SATA.

Conditions préalables

La mémoire de travail du PC doit être d’au moins 3 Go.

Un PC avec un lecteur de DVD, un système d’exploitation Windows 10 et au moins 2 ports USB 2.0 ou version ultérieure sont disponibles.

L’outil Card Manager V3 ou version ultérieure est disponible et entièrement opérationnel sur un PC.

Un adaptateur USB SATA SSD est disponible. L'adaptateur doit prendre en charge les clés M et B.

Un disque SSD M.2 SATA qualifié est disponible.

Une image du système logiciel dans la version correcte est disponible en tant que fichier tar. La version du logiciel doit correspondre à la version du système cible. Elle doit être exactement la même que celle qui est utilisée dans le dispositif de stockage actuel du système.

Application Card Manager en tant que fichier ISO.

Le fichier ISO de Card Manager doit être gravé sur un DVD.

Étape par étape

1) Stockez le fichier image tar actuel sur une clé USB et démarrez l'application Card Manager à partir du fichier ISO du DVD.

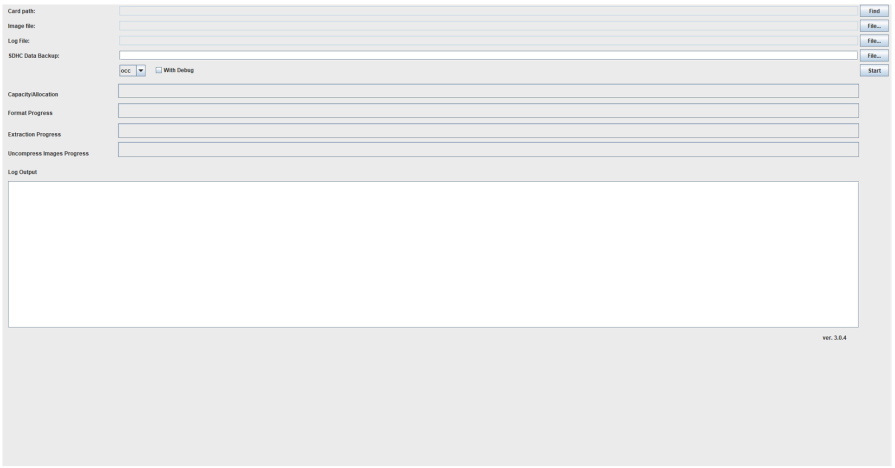
2) Branchez l'adaptateur USB SATA SSD dans un port USB du PC .

3) Insérez le disque SSD M.2 SATA dans l'adaptateur et cliquez sur **OK** dans la fenêtre contextuelle pour confirmer la sélection.

Toutes les données sur le SSD inséré seront supprimées par Card Manager.

N'insérez pas de périphérique USB supplémentaire dans le PC, car il sera reconnu comme un support de stockage OpenScape Business et toutes les données seront supprimées.

4) Sur l'application Card Manager, cliquez sur **Rechercher** à côté du champ **Emplacement de la carte**.



5) Insérez la clé USB avec le fichier image et cliquez sur **Fichier...** à côté du **Fichier image** et sélectionnez le fichier tar image stocké sur la clé USB.

6) Sélectionnez **OCCe** dans le menu déroulant pour créer le disque SSD M.2 SATA.

7) Vous pouvez aussi créer un fichier journal où sont enregistrées les éventuelles erreurs du programme : cliquez sur **Fichier...**, à côté de **Fichier journal** et allez à l'endroit où se trouve le fichier journal. Donnez un nom au fichier journal et cliquez sur **Enregistrer**.

8) Cliquez sur **Démarrer**.

Le processus d'écriture est lancé et la progression de chaque étape est affichée par une barre de progression.

9) Cliquez sur **OK** une fois l'installation terminée et retirez le disque SSD M.2 SATA de l'adaptateur.
10) Débranchez l'adaptateur du port USB.
11) Mettez le système de communication hors tension.
12) Insérez le nouveau disque SSD M.2 SATA dans le système de communication désactivé.
13) Mettez le système de communication en service. Le système se lance avec le nouveau disque SSD M.2 SATA dans la même version logicielle et configuration et est de nouveau en service si la LED verte clignote à une fréquence de 1 Hz (allumée pendant 0,5 s / éteinte pendant 0,5 s).

Remarque : Si le disque SSD M.2 SATA est inséré dans un système de communication OpenScape Business, le système est démarré dans l'état usine par défaut comprenant, entre autres, l'adresse IP par défaut `192.168.1.2`.

Restaurez une sauvegarde du système. La sauvegarde doit avoir la même version mineure avec le système installé.

24.13.2 Comment utiliser le gestionnaire de cartes pour écrire le logiciel de communication sur la carte SDHC

Vous pouvez utiliser le Gestionnaire de cartes pour écrire le logiciel de communication d'OpenScape Business V3 sur une carte SDHC.

Conditions préalables

Un PC équipé d'un système d'exploitation Windows 10, d'un lecteur DVD et d'au moins 2 ports USB 2.0 ou supérieurs est disponible.

Outil de gestion de cartes V3 ou supérieur, pleinement fonctionnel sur PC.

Un lecteur de cartes SDHC USB est disponible.

Une carte SDHC compatible est disponible.

En option : un fichier de sauvegarde de données SDHC (fichier tar) stocké sur une clé USB avec le système d'images.

La protection en écriture de la carte SDHC est désactivée.

Une image du logiciel système dans la version correcte est disponible sous forme de fichier tar, dans le petit fichier image (OCC). La version du logiciel doit correspondre à la version du système cible. Il doit s'agir exactement de la même version que celle utilisée sur la carte SDHC actuelle du système.

Application Gestionnaire de cartes sous forme de fichier ISO de DVD.

Le fichier ISO de Card Manager doit être gravé sur un DVD.

Étape par étape

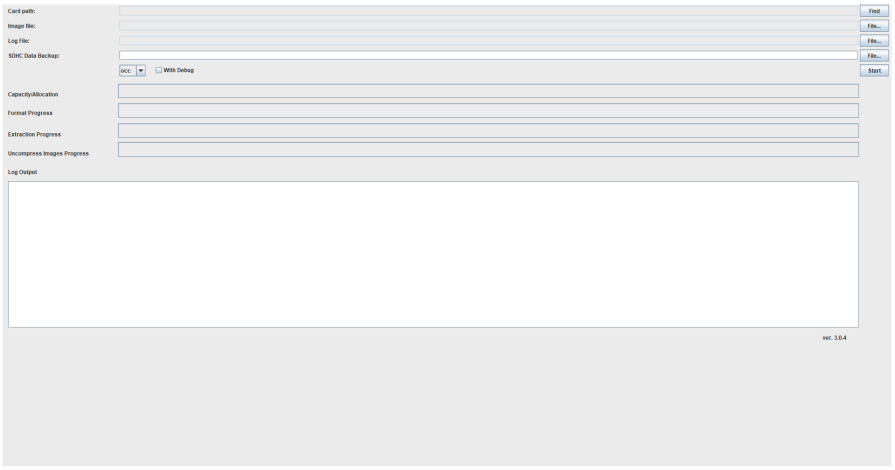
1) Stockez le fichier image tar actuel sur une clé USB et démarrez l'application Gestionnaire de cartes à partir du fichier ISO du DVD.
2) Connectez le lecteur de cartes SDHC USB à un port USB de l'ordinateur.

3) Débranchez le lecteur de cartes, insérez la carte SDHC, rebranchez le lecteur de cartes et cliquez sur **OK** dans la fenêtre contextuelle. Le chemin d'accès à la carte SDHC apparaît sous **Chemin d'accès à la carte** .

Toutes les données présentes sur le SSD inséré seront effacées par le Gestionnaire de cartes.

N'insérez aucun périphérique USB supplémentaire dans le PC, car il sera reconnu comme un support de stockage OpenScape Business et toutes les données seront supprimées.

4) Dans l'application Gestionnaire de cartes, cliquez sur **Rechercher** à côté de **Chemin de la carte** .



5) Insérez la clé USB contenant le fichier image, cliquez sur **Fichier...** à côté du **fichier image** et sélectionnez le fichier tar image stocké sur la clé USB.

6) Sélectionnez **OCC** dans le menu déroulant pour créer la carte SDHC.

7) Vous pouvez également, si vous le souhaitez, créer un fichier journal qui enregistre les éventuelles erreurs du programme. Pour ce faire, cliquez sur **« Fichier journal »** dans **le menu « Fichier… »** et accédez à l'emplacement de stockage du fichier journal. Donnez un nom au fichier journal et confirmez avec **Sauvegarder**.

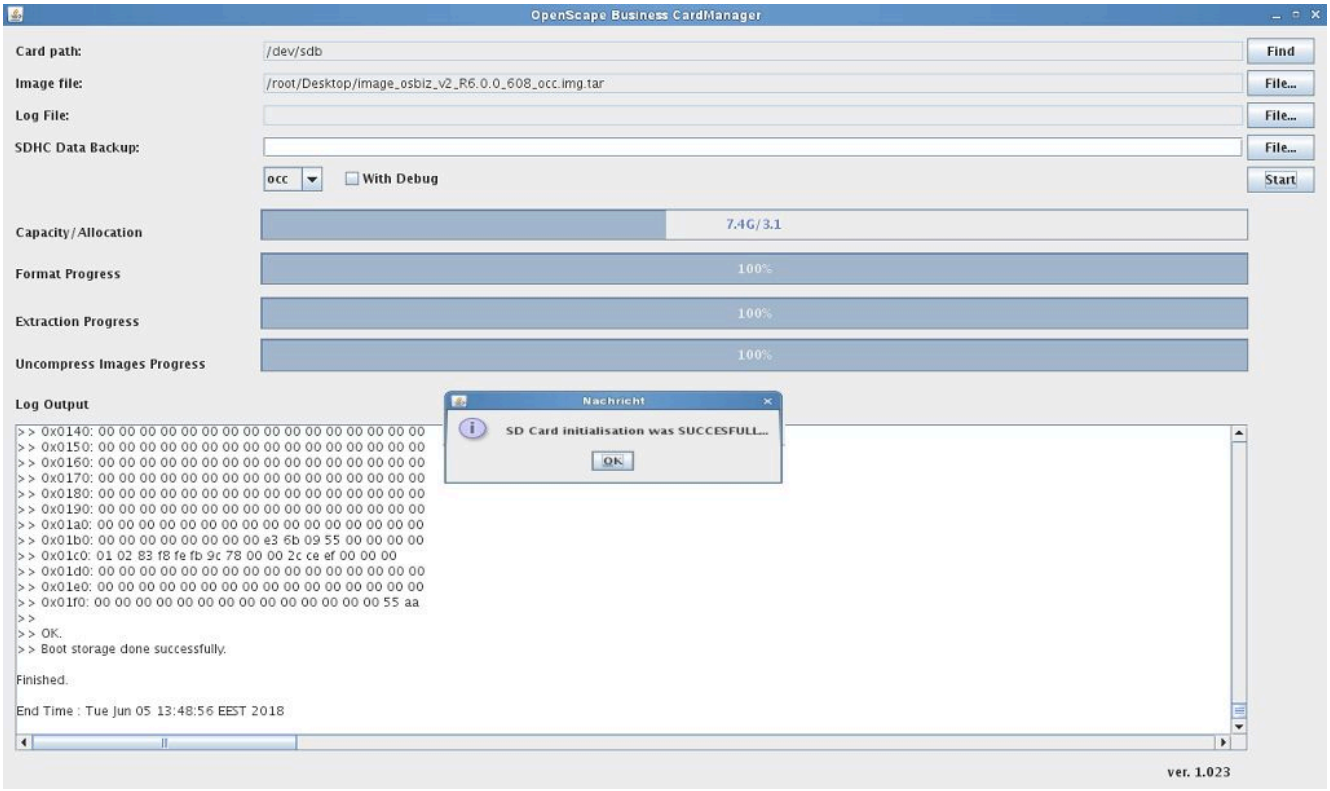
8) Vous pouvez également cliquer sous **Sauvegarde de données SDHC** dans **le fichier...** et sélectionner le fichier .tar contenant un fichier de sauvegarde de données de carte SDHC spécifique au client. Le chemin d'accès au fichier .tar apparaît sous **Sauvegarde de données SDHC.**

9) Cliquez sur **Démarrer** .

Le processus d'écriture démarre et la progression de chaque étape est affichée via une barre de progression.

Remarque : Si le champ de texte (**Sauvegarde de données SDHC**) est rempli, Card Manager comparera d'abord la version du fichier de sauvegarde de la carte SDHC avec la version du fichier image du logiciel système. En cas d'incompatibilité, un message d'erreur s'affiche et le processus est interrompu. En cas de correspondance, le gestionnaire de cartes écrit l'image sélectionnée puis extrait le fichier .tar spécifié dans la carte SDHC. Si aucune

sauvegarde de données SDHC n'est disponible, le champ de texte doit rester vide.



10) Cliquez sur **OK** une fois l'installation terminée et retirez la carte SDHC du lecteur de cartes.
11) Retirez le lecteur de cartes du port USB.
12) Mettez le système de communication hors tension.
13) Insérez la nouvelle carte SDHC dans l'emplacement SD du système de communication éteint.
14) Activez le système de communication. Le système démarre avec la nouvelle carte SDHC et avec la même version logicielle et la même configuration et est prêt à fonctionner lorsque la LED verte clignote à 1 Hz (0,5 sec allumée / 0,5 sec éteinte).

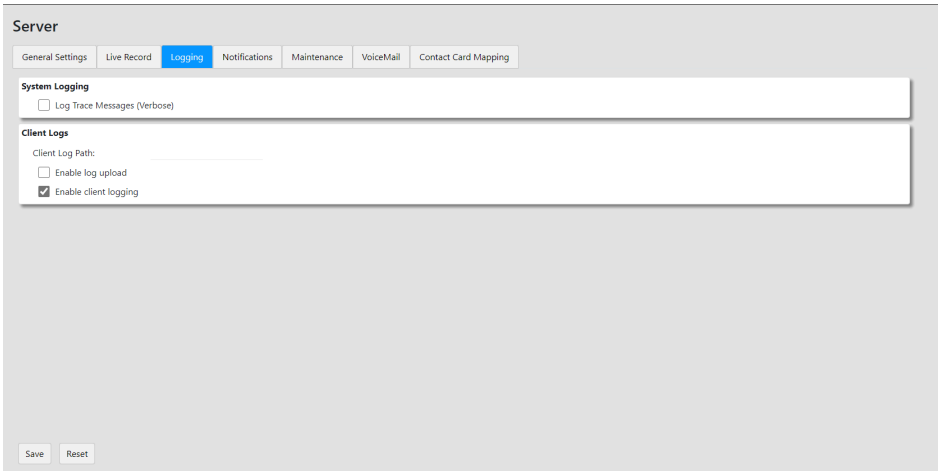
Remarque : Si la carte SDHC est insérée dans un système de communication OpenScape Business, le système démarre dans l'état par défaut d'usine, y compris, entre autres, l'adresse IP par défaut `192.168.1.2`.

24.14 Surveillance et Maintenance de la suite UC

WBM à l'administrateur de profil **Expert** différentes fonctions pour la surveillance et la maintenance de la suite UC.

24.14.1 Journalisation

L'exécution de la UC Suite est surveillée en interne par le système. La **journalisation système** peut être utilisée pour définir si des journaux doivent être créés. En outre, un journal des activités de la suite UC (par exemple, le démarrage d'un client UC Suite) est conservé dans les **journaux clients**.



Journalisation système

Les journaux système suivants peuvent être activés ou désactivés :

Journalisation système	Paramètre par défaut
Journaliser les messages de trace (en détail)	Non activé

Les résultats du journal système activé sont écrits quotidiennement dans un fichier journal avec la désignation `vs-yyyy-mm-dd.log` (par exemple, `vs-2013-01-222.log`) et stockés dans le système de communication sous `/var/system/trace_log/vsl/log`.

Conseil : L'analyse de ces fichiers journaux ne peut être effectuée que par Development.

Journaux Client

Les **journaux clients** sont les fichiers journaux de la suite UC. Pour chaque client UC Suite (myPortal for Desktop, myAttendant, etc.) et terminal (utilisateur), un répertoire distinct est créé et les fichiers journaux pertinents y sont stockés. Les journaux enregistrent les activités d'un abonné telles que le démarrage du client, les appels sortants et entrants, etc.

Conseil : Le stockage des journaux clients est pris en charge uniquement pour les clients UC Suite utilisés avec les systèmes d'exploitation Microsoft Windows.

Le chemin dans lequel le répertoire `CC-Logs` avec les sous-répertoires pour les clients UC Suite individuels doit être stocké peut être défini. Vous pouvez également sélectionner si le répertoire doit être stocké sur chaque PC client ou sur un PC central ou un serveur sur le réseau.

Par défaut, le répertoire `CC-Logs` est stocké dans le chemin suivant : `<Lecteur>:\Documents and Settings/<Nom d'utilisateur du poste>/CC-Logs`

La période de conservation des **journaux clients** est de 5 jours. Aucun changement n'est possible.

La journalisation des activités de la suite UC dans les **journaux clients** est activée par défaut. Les Administrateurs avec le profil **Advanced** peuvent désactiver la journalisation sur une base spécifique au terminal à l'aide de l'assistant **Répertoire utilisateur**. Un administrateur avec le profil **Expert** peut désactiver la journalisation sur une base spécifique au terminal en **mode Expert**.

Selon le scénario, les journaux clients sont également stockés par défaut sur le disque dur du système de communication Unify OpenScape Business S. Un administrateur avec le profil **Expert** peut désactiver l'enregistrement des journaux clients sur le disque dur du système en **mode Expert**.

Un Administrateur avec le profil **Advanced** peut utiliser l'assistant de **suivi** pour télécharger les journaux clients (fichiers journaux) des clients UC Suite (myPortal for Desktop, myAttendant, etc.) utilisés par les abonnés internes.

Un administrateur avec le profil **Expert** peut utiliser l'assistant de **mode Expert** pour télécharger les journaux clients (fichiers journaux) des clients UC Suite (myPortal for Desktop, myAttendant, etc.) utilisés par les abonnés internes.

24.14.1.1 Comment activer ou désactiver l'enregistrement de la journalisation système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur** puis sur **Journalisation**.
4) Dans la zone **Journalisation système**, sélectionnez l'une des options suivantes :
   - Si vous voulez enregistrer les messages de trace quotidiennement, cochez la case **Journaliser les messages de trace (en détail)**.
   - Si vous ne voulez pas enregistrer les messages de trace quotidiennement, décochez la case **Journaliser les messages de trace (en détail)**.
5) Cliquez sur **Enregistrer**.

24.14.1.2 Comment activer ou désactiver l'enregistrement de la journalisation client sur l'ensemble du système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur** puis sur **Journalisation**.
4) Dans la zone **Journalisation système**, sélectionnez l'une des options suivantes :
   - Si vous voulez enregistrer les journaux client, cochez la case **Activer la journalisation client**.
   - Si vous ne voulez pas enregistrer les journaux client, décochez la case **Activer la journalisation client**.

   Conseil : L'enregistrement des journaux Client est uniquement pris en charge pour les UC Suite Clients qui sont utilisés avec les systèmes d'exploitation Microsoft Windows.
5) Cliquez sur **Enregistrer**.

24.14.1.3 Comment activer ou désactiver l'enregistrement de la journalisation client, individuellement par abonné

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Configuration**.
2) Dans l'arborescence de navigation, cliquez sur **Assistants** > **Suite UC**.
3) Cliquez sur **Modifier** pour lancer l'Assistant **Répertoire utilisateur**.
4) Sélectionnez l'abonné souhaité dans le répertoire des utilisateurs et cliquez sur **Modifier**.
5) Dans l'arborescence des menus, cliquez sur **Mes Préférences** > **Divers**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous voulez enregistrer la journalisation client pour l'abonné souhaité, cochez la case **Journaliser les messages de trace (en détail))**.
   - Si vous ne voulez pas enregistrer la journalisation client pour l'abonné souhaité, décochez la case **Journaliser les messages de trace (en détail)**.

   Conseil : L'enregistrement des journaux Client est uniquement supporté pour les UC Suite Clients qui sont utilisés avec les systèmes d'exploitation Microsoft Windows.
7) Cliquez sur **Sauvegarder**.
8) Si vous voulez, pour un autre abonné, activer ou désactiver l'enregistrement de la journalisation client, répétez les points 4 à 7.

24.14.1.4 Comment configurer le chemin d'archivage pour fichiers journal Client

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur** puis sur **Journalisation**.
4) Dans le champ **Chemin journal client**, sous **Journaux client**, indiquez le chemin d'archivage pour le répertoire `CC-Logs` avec les sous-répertoires des différents clients UC Suite et leurs fichiers journaux client. Sélectionnez l'une des options suivantes :
   - Lorsque le répertoire `CC-Logs` doit être situé sur chaque PC client, entrez par exemple : `<lecteur>:\<chemin d'accès>`.
   - Lorsque le répertoire `CC-Logs` doit être situé dans une un PC ou un serveur central, se trouvant dans le réseau, indiquez par exemple : `\\<adresse IP>\<lecteur>\<chemin d'accès>`.

   Conseil : L'enregistrement des journaux Client est uniquement pris en charge pour les UC Suite Clients qui sont utilisés avec les systèmes d'exploitation Microsoft Windows.
5) Cliquez sur **Enregistrer**.

24.14.1.5 Comment activer ou désactiver le stockage centralisé des journaux clients sur le disque dur du système de communication

Conditions préalables

Vous êtes connecté au WBM avec le profil **Expert** .

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert** .
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite** .
3) Cliquez sur **Serveur**, puis sur **Journalisation**.
4) Sélectionnez l'une des options suivantes, dans la zone **Journaux clients** :
   - Si vous souhaitez que les journaux des clients soient enregistrés sur le disque dur du système de communication Unify OpenScape Business S, activez la case à cocher **Activer le téléchargement des journaux**.
   - Si vous ne souhaitez pas que les journaux des clients soient enregistrés sur le disque dur du système de communication Unify OpenScape

Business S, désactivez la case à cocher **Activer le téléchargement des journaux**.

Conseil : L'enregistrement des journaux clients est pris en charge uniquement pour les clients UC Suite utilisés avec les systèmes d'exploitation Microsoft Windows.

5) Cliquez sur **Enregistrer** .

24.14.1.6 Comment télécharger les journaux Client de tous les abonnées internes

A l'aide de l'assistant **Trace** vous pouvez télécharger les journaux Client (fichiers journal) des UC Suite Clients utilisées par les abonnés internes (myPortal for Desktop, myAttendant etc.). Les journaux Client sont uniquement supporté pour les UC Suite Clients qui sont utilisés avec les systèmes d'exploitation Microsoft Windows.

Conditions préalables

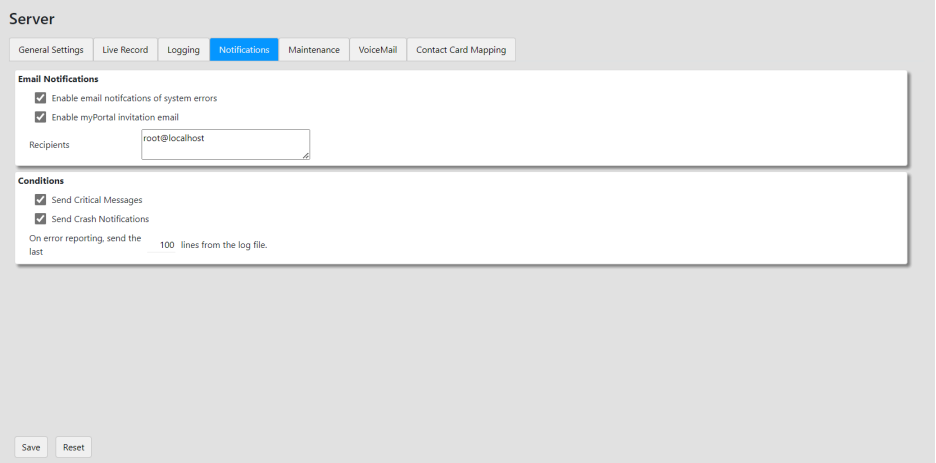
Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Diagnostics** > **Trace**.
3) Cliquez sur **Données de diagnostic**.
4) Cliquez sur **Aucun protocole** pour décocher tous les protocoles.
5) Cochez la case **Protocoles d'application**.
6) Sélectionnez une des possibilités suivantes :
   - Si vous souhaitez télécharger tout le journal existant, sélectionnez dans la liste déroulante **Journal complet**.
   - Si vous souhaitez télécharger le fichier-journal du jour, sélectionnez dans la liste déroulante **Protocole d'aujourd'hui**.
   - Si vous souhaitez télécharger le fichier-journal d'une période précise, sélectionnez dans la liste déroulante **Propre sélection**. Dans la liste déroulante **De :** sélectionnez le début et dans la liste déroulante **A :** sélectionnez la fin de la période souhaitée.
7) Cliquez sur **Charger** et ensuite sur **OK**. La fenêtre de téléchargement de fichiers s'affiche.
8) Sauvegardez le fichier dans le répertoire choisi. Fermez ensuite la fenêtre où vous avez confirmé le téléchargement.
9) Cliquez sur **Suivant** puis sur **Quitter**.

24.14.2 Notification

À l'aide de la **Notification par e-mail**, il est possible d'envoyer des e-mails afin d'informer notamment les **Destinataires** d'un niveau de remplissage critique du disque dur ou d'un défaut.



L'envoi d'e-mails peut être associé aux **Conditions** suivantes :

Conditions	Paramètre par défaut
Envoyer les messages critiques	Activé
Envoyer les notifications de panne système	Activés

Les notifications importantes et les notifications concernant les défaillances du système devraient être activées et envoyées. Ceux-ci avertissent le destinataire inscrit d'un problème possible, qui doit être signalé au service d'assistance compétent.

De plus, il est possible de définir le nombre des dernières lignes du fichier journal qui doivent être envoyées avec l'e-mail. Les erreurs système suivantes peuvent être signalées (en anglais exclusivement) :

Erreur système
NULL monitor
Could not notify CallHandler (notification au gestionnaire de l'appel impossible)
Terminate call failed (coupure après échec de l'appel)
Unable to load VM Structure from file (impossible de charger la structure VM depuis le fichier)
Alsa stuck
Alsa cancel failed
MEN CallID 0
NULL alsa handle
Database connection failed
Rules engine logic failure
Config schema format failure (défaut de format du schéma de config)
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!

Erreur système
Main: Could not read the settings from the configuration file!
A segmentation fault was detected (défaut de segmentation détecté).
Database logic error (erreur logique base de données)
Database schema error (erreur de schéma base de données)
ConnectionServer failed to start (échec du démarrage de ConnectionServer)
MultisiteSync failed to start (échec du démarrage MultisiteSync)
Multisite failed to start (échec du démarrage multisite)
TransferManager failed to start (échec du démarrage de TransferManager)
IPC failed to start (échec du démarrage IPC)
ConferenceManager failed to start (échec du démarrage de ConferenceManager)
CallManager failed to start (échec du démarrage de CallManager)
MediaProcessing failed to start (échec du démarrage de MediaProcessing)
Queues failed to start (échec du démarrage des files d'attente)
Import failed to start (échec du démarrage de l'importation)
DataClient failed to start (échec du démarrage de DataClient)
DirectoryClient failed to start (échec du démarrage de DirectoryClient)
DirectoryServer failed to start (échec du démarrage de DirectoryServer)
FV failed to start (échec du démarrage de FV)
IM failed to start (échec du démarrage de IM)
Switch failed to start (échec du démarrage du commutateur)
No Switches
Exchange Integration failed to start (échec du démarrage d'Exchange Integration)
Outbound Fax failed to start (échec du démarrage du fax sortie)
SQL connection pool failed to start (échec du démarrage du groupe de connexion SQL)
Task scheduler failed to start (échec du démarrage de Task scheduler)
Trunks failed to start (échec du démarrage des lignes)
Unknown switch type (type de commutateur inconnu)
Users failed to start (échec du démarrage des utilisateurs)
MEB has been disconnected (MEB a été déconnecté)
MEB ACK timeout (time de MEB ACK)
Switch Hearbeat timeout (temporisation pulsation du commutateur)

24.14.2.1 Comment configurer les notifications par e-mail des erreurs du système

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur**, puis sur **Notifications**.
4) Sélectionnez le paramètre souhaité pour la notification par e-mail, dans la zone **Notifications par e-mail** :
   - Si vous souhaitez recevoir des notifications par e-mail, cochez la case **Activer les notifications par e-mail des erreurs système**.
   - Si vous ne souhaitez pas recevoir de notifications par e-mail, décochez la case **Activer les notifications par e-mail des erreurs système**.
5) Saisissez les adresses e-mail des personnes auxquelles les notifications par courrier électronique doivent être envoyées dans le champ **Destinataires**. Les différentes adresses électroniques doivent être séparées par une virgule "," suivie d'un espace " ".
6) Sélectionnez le paramètre souhaité pour les messages critiques
   - Si vous souhaitez recevoir des notifications par e-mail pour les messages critiques, cochez la case **Envoyer les messages critiques**.
   - Si vous ne souhaitez pas recevoir de notifications par e-mail pour les messages critiques, décochez la case **Envoyer les messages critiques**.
7) Sélectionnez le paramètre souhaité pour les notifications de défaillance
   - Si vous souhaitez recevoir des notifications par e-mail en cas de défaillance du système, cochez la case **Envoyer des notifications de défaillance**.
   - Si vous ne souhaitez pas recevoir de notifications par e-mail en cas de défaillance du système, décochez la case **Envoyer des notifications de défaillance**.
8) Saisissez le nombre de lignes du fichier journal à envoyer avec un e-mail dans le champ **Envoyer les lignes du fichier journal**.
9) Cliquez sur **Sauvegarder**.

24.14.3 Maintenance

La maintenance permet de définir les périodes de conservation des messages, des informations sur les appels dans le journal des appels, des appels enregistrés avec myAgent, des fax et e-mails reçus et envoyés par le centre d'appels et des fichiers journal.

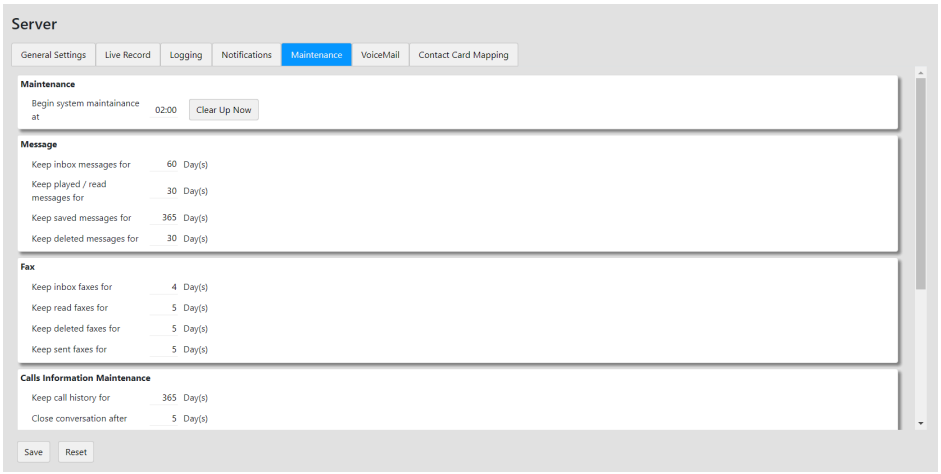
Il est également possible de définir à quelle heure a lieu quotidiennement l'effacement des données ci-après qui ont dépassé la période de conservation définie.

- Messages
- Informations d'appel dans le Journal des appels (historique des appels)
- Appels enregistrés avec myAgent (centre d'appels)

- Fax et e-mails reçus et envoyés par le centre d'appels
- Fichiers journal

Le réglage par défaut est 2h00.

De plus, il est possible de démarrer immédiatement la maintenance du système et donc de lancer l'effacement immédiat des données indiquées, qui ont dépassé la période de conservation définie. Cela peut par exemple être nécessaire lorsque le disque dur du système de communication a atteint un niveau de remplissage critique.



Pour plus d'informations sur la **Maintenance des messages**, voir Boîte vocale.

Pour plus d'informations sur la **Maintenance des messages Fax**, voir Boîte Fax.

Pour plus d'informations sur la **Maintenance des informations appels** : Historique des appels, voir Journal .

Lors de la **Maintenance des informations appels** : **Centre d'appels**, les appels enregistrés avec myAgent et les fax et e-mails reçus et envoyés par le centre d'appels sont supprimés, quand ils ont dépassé la période de conservation définie. Le réglage par défaut de la période de conservation des fichiers est de 60 jours.

Conseil : Les périodes de conservation pour la maintenance des informations d'appel sont indépendantes les unes des autres.

Les rapports du centre d'appels sont basés sur l'historique des appels. S'il a été défini pour l'historique des appels une période de conservation inférieure à celle des données du centre d'appels, certains rapports ne sont alors plus disponibles.

Pour la **Maintenance des fichiers journaux**, les fichiers journaux sont effacés lorsque la durée de conservation est dépassée. Le réglage par défaut de la période de conservation des fichiers est de 10 jours.

24.14.3.1 Comment configurer la période de la journée pour la maintenance

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur** puis sur **Maintenance**.
4) Sous **Maintenance**, entrez l'heure à laquelle la maintenance quotidienne doit être effectuée dans le champ **Commencer la maintenance système à**. A l'heure réglée ici commence l'effacement des messages, des informations d'appel dans le journal des appels et des fichiers qui ont dépassé la période de conservation.
5) Cliquez sur **Enregistrer**.

24.14.3.2 Comment configurer la durée de conservation des fichiers de protocole

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur** puis sur **Maintenance**.
4) Sous **Gestion du fichier journal**, entrez la période de conservation en jours dans le champ **Conserver les informations de journalisation pendant**. Les fichiers journal sont effacés lorsqu'il ont dépassé la période de conservation configurée ici.
5) Cliquez sur **Enregistrer**.

24.14.3.3 Comment effectuer une maintenance système instantanée

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur** puis sur **Maintenance**.

4) Dans la zone **Maintenance**, cliquez sur **Supprimer maintenant**.

Conseil : Sont supprimés les messages, les informations d'appel dans le journal des appel, les appels enregistrés par myAgent, les fax et e-mails pour le centre d'appels enregistrés et envoyés et les fichiers journal qui ont dépassé la durée de sauvegarde réglée.

---

5) Cliquez sur **OK** pour confirmer la suppression.

24.14.3.4 Comment configurer la durée de conservation des données de Centre d'appels

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Dans la barre de navigation, cliquez sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Applications** > **OpenScape Business UC Suite**.
3) Cliquez sur **Serveur** puis sur **Maintenance**.
4) Dans la zone **Maintenance des informations appels**, entrez la durée de conservation en jours dans le champ **Centre d'appels**. Les appels enregistrés avec myAgent et les fax et e-mais reçus et envoyés pour le centre d'appels contacts sont effacés lorsque le délai de conservation réglé ici est dépassé.
5) Cliquez sur **Enregistrer**.

24.15 Surveillance de UC Smart

Un administrateur de profil **Expert** est en mesure d'appeler avec WBM l'état actuel de UC Smart.

24.15.1 Comment appeler l'état actuel de UC Smart

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

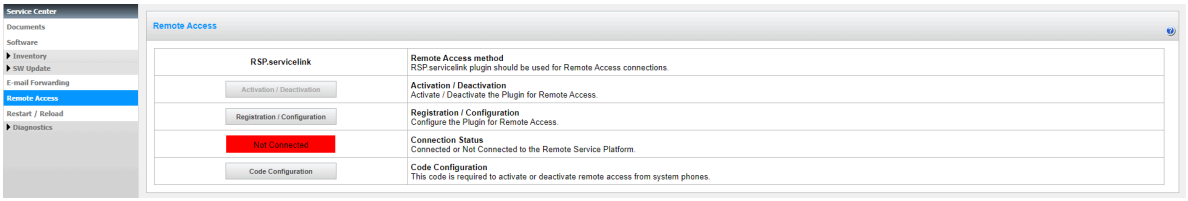
Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence du menu, cliquez sur **Applications** > **UC Smart**.
3) Cliquez sur **Etat**.

   Il est affiché l'état actuel du serveur d'application et le nombre de liaisons actives des différents clients UC.

24.16 Services à distance

Différents services à distance permettent d'accéder à distance au système de communication et aux composantes raccordées ; ces services sont assurés par des techniciens de maintenance autorisés. Ainsi, les tâches de maintenance sont effectuées de manière économique et les utilisateurs bénéficient d'un soutien sur place pour le solutionnement des problèmes.



En raison du très haut niveau de sécurité, le RSP.servicelink doit être préférer au service à distance. Informations supplémentaires voir RSP.servicelink.

24.16.1 RSP.servicelink

L'accès distant avec la connexion RSP.servicelink (**R**emote **S**ervice **P**latform) offre aux techniciens SAV autorisés d'un Remote Service Partner la possibilité d'administrer à distance, de manière pratique et sûre, le système de communication. Pour configurer RSP.servicelink, seuls une connexion Internet, un navigateur Web, l'identifiant partenaire et le mot de passe partenaire du partenaire de service distant sont nécessaires. RSP.servicelink garantit une connexion haut débit hautement sécurisée.

RSP.servicelink est basé sur la technologie OpenVPN. Il utilise le protocole et le chiffrement SSL/TLS et offre le plus haut niveau de sécurité grâce à un certificat client supplémentaire. Le terme RSP.servicelink est abrégé en RSP dans la documentation.

Remarque : Lorsque RSP est actif, il utilise la plage 100.64.0.1 - 100.127.255.254 pour l'interface tun0. Cela signifie que si une adresse IP externe appartenant à cette plage doit être accessible, une route statique doit être ajoutée dans le système Open Scape Business pour acheminer le trafic via l'interface souhaitée.

RSP offre les principaux avantages suivants en combinaison avec OpenScapeBusiness :

- Haute sécurité via la connexion Internet sortante

  L'ensemble de la configuration de la connexion à distance est toujours initié par le système de communication. Cela signifie que le pare-feu du réseau du client ne doit autoriser qu'une seule connexion HTTP vers une seule adresse du centre de services distant (port 443). Dans des circonstances normales, aucune modification n'est requise dans les politiques de sécurité des clients ou dans leurs pare-feu, car ce port est généralement déjà ouvert

pour les appels Internet sortants dans le pare-feu du client. La sécurité élevée du réseau client est ainsi garantie.

Avec RSP, l'administrateur du système de communication conserve le contrôle de la connexion à distance en activant et en désactivant simplement l'accès. Dans le cas de RSP.servicelink, un certificat client est également installé automatiquement.

- Bande passante élevée

  Grâce à la connexion Internet haut débit, les données de diagnostic peuvent être transmises beaucoup plus rapidement, améliorant ainsi la qualité du service.

- Installation simple et économique

  Le logiciel du système de communication comprend déjà un service appelé RSP.servicelink. Lors de l'activation du plugin de service, l'identifiant partenaire du partenaire de service à distance ainsi que le mot de passe partenaire doivent être saisis.

  Chaque partenaire de service à distance qui utilise RSP.servicelink possède un identifiant partenaire distinct.

  Le plugin RSP.servicelink doit être désactivé puis réactivé lors de la mise à jour du logiciel.

- À l'épreuve du temps

  RSP constitue la base de futurs services (à valeur ajoutée) tels que les sauvegardes automatisées, les rapports et la surveillance, par exemple.

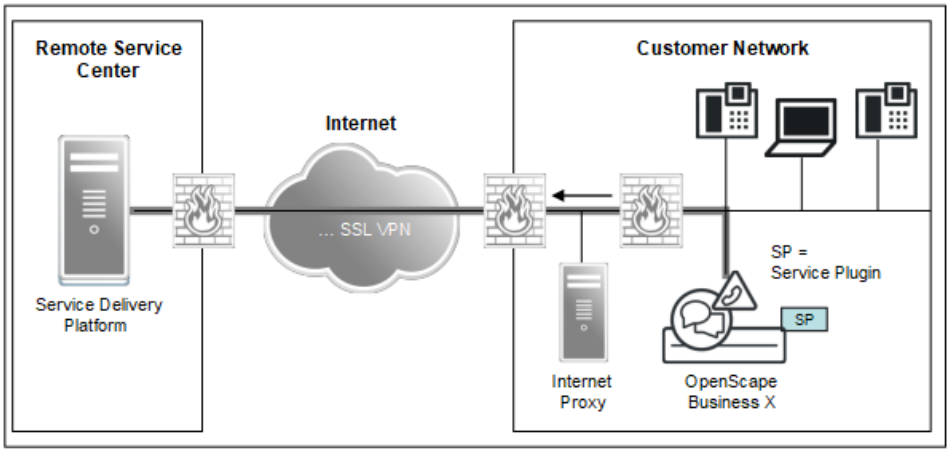


Illustration 16 : RSP - Présentation d'OpenScape Business X

RSP prend en charge toutes les normes habituelles des services Web, notamment le protocole de transfert hypertexte sécurisé (HTTPS), le protocole d'accès aux objets simples (SOAP) et le langage de balisage extensible (XML).

La communication entre le client et le centre de services distant est toujours sécurisée par un chiffrement AES-256-CBC pour RSP.servicelink.

Modules de service

Le plugin RSP.servicelink peut être activé ou désactivé individuellement.

Le plugin RSP.servicelink doit être réinitialisé après le remplacement de la carte mère, par exemple. La réinitialisation du plugin de service supprime l'intégralité de la configuration RSP et désactive le plugin.

Remarque : Si le système n'est pas en mode DTAG et que le plugin RSP.servicelink est actif, il n'est pas possible de modifier la configuration des paramètres du proxy. Le **bouton Inscription / Configuration est désactivé.**

En mode DTAG, si le plugin RSP.servicelink est actif, appuyer sur le bouton Enregistrement / Configuration affiche directement la page Paramètres du proxy avec les boutons Annuler/ Terminer. Ceci est également possible depuis le serveur distant.

Gestion des périphériques (périphériques gérés)

Dans les systèmes de communication, l'accès à distance à d'autres périphériques du réseau local du client peut être activé par une configuration côté SIRA. Les téléphones IP peuvent être configurés côté SIRA à l'aide de la fonction « Périphériques gérés ».

Conseil : L'accès à distance aux autres systèmes de communication OpenScape Business du réseau local du client n'est pas possible. Chaque entreprise OpenScape doit être configurée pour l'accès à distance.

Activation/Désactivation

Les options suivantes sont disponibles pour activer ou désactiver les plugins de service :

- Utilisation de l'assistant **d'activation/désactivation**

  Il existe un assistant d'activation/désactivation distinct pour les plugins du service RSP.
- En saisissant un code au téléphone du système (par défaut : activation via *996, désactivation via #996)

  Pour des raisons de sécurité, un code PIN à 4 chiffres doit être saisi en plus du code d'activation et de désactivation via un téléphone système. La configuration de ce code PIN est effectuée dans le WBM du système de communication avec le profil **Avancé** .

Sauvegarde et restauration

Les identifiants RSP sont stockés dans le jeu de sauvegarde du système.

Si un nouveau système OpenScape Business est mis en place par clonage ou par restauration de données (migration), et que le système d'origine disposait d'un accès RSP configuré, il faut s'assurer que le système cloné ou restauré dispose d'une configuration RSP différente.

Vous devez désactiver ou désinstaller le RSP avant de cloner ou de sauvegarder le système d'origine.

Si un certificat de connexion au service RSP est utilisé dans plusieurs systèmes, il sera révoqué et aucun des systèmes OpenScape ne pourra se connecter au service RSP.

Prérequis

- Accès Internet pour le système de communication ou le proxy HTTP sur le réseau local du client.

- Tout pare-feu existant sur le réseau local du client doit être ouvert pour le serveur d'enregistrement :
  - https://188.64.18.51
  - https://188.64.17.51
- Tout pare-feu existant sur le réseau local du client doit être ouvert pour le VPN :
  - https://188.64.18.50
  - https://188.64.17.50
- Un routeur par défaut doit être spécifié dans la configuration Internet.

Remarque : Si le système est en mode DTAG lors du démarrage et dispose d'un accès Internet sans que le plugin RSP.serviceplugin soit installé et configuré, un script installera, configurera et activera automatiquement RSP.serviceplugin en utilisant l'identifiant et le mot de passe du partenaire DTAG (le nom du périphérique sera l'adresse MAC du système). Le script sera également exécuté périodiquement toutes les 10 minutes (par exemple, dans le cas où il n'y a pas d'accès à Internet après l'installation initiale du système). Le script n'activera pas automatiquement RSP.serviceplugin si l'utilisateur l'a désactivé manuellement.

24.16.1.1 Comment installer, configurer et enregistrer le plugin RSP.servicelink

L'assistant **Enregistrement / Configuration** permet de installer, configurer et d'enregistrer le plugin RSP.servicelink pour l'accès à distance au système de communication via RSP.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.

2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.

3) Cliquez sur **Enregistrement / Configuration**.

4) Si le plugin RSP.servicelink n'est pas encore installé, cliquez sur **Installer** et ensuite sur **OK&Suivant**.

5) Si le plugin RSP.servicelink est déjà installé, cliquez sur **OK&Suivant**.

6) S'il n'est pas utilisé de serveur Proxy dans le réseau client, cliquez sur **OK&Suivant** puisqu'il n'est pas nécessaire de procéder à la configuration des **paramètres Proxy**. Sautez les deux étapes suivantes.

7) Si un serveur Proxy est utilisé dans le réseau client, vous devez sélectionner le réglage des **Paramètres Proxy** en fonction du réseau client :

- S'il existe dans le réseau de clients un proxy avec protocole HTTP, cochez la case **Utiliser le Proxy HTTP**. Dans le champ **Hôte HTTP Proxy** entrez le nom de l'hôte et dans le champ **Port HTTP Proxy** le numéro de port du serveur Proxy. Si nécessaire, entrez dans le champ

Nom utilisateur le nom de l'utilisateur et dans le champ**Mot de passe** le mot de passe pour l'authentification sur le serveur Proxy.

- S'il existe dans le réseau de clients un Proxy avec protocole SOCKS, cochez la case **Utiliser le Proxy SOCKS**. Dans le champ **Hôte SOCKS Proxy** entrez le nom de l'hôte et dans le champ **Port SOCKS Proxy** le numéro de port du serveur proxy. Si nécessaire, entrez dans le champ **Nom utilisateur** le nom de l'utilisateur et dans le champ**Mot de passe** le mot de passe pour l'authentification sur le serveur Proxy.

Conseil : Le fait qu'une authentification soit nécessaire ou non dépend du type et de la configuration du serveur Proxy.

---

8) Cliquez sur **OK&Suite**.
9) Uniquement si cela est nécessaire, modifiez l'ID partenaire prédéfini dans le champ **Partner ID**.
10) Dans le champ **Mot de passe**, entrez votre mot de passe.
11) Entrez le nom d'équipement. Vous trouverez l'équipement avec son nom d'équipement dans SIRA Equipment Explorer (EqE). L'adresse MAC d'OpenScape Business est l'entrée par défaut.
12) Cliquez sur **Quitter**.

Dans la colonne **RSP.servicelink** il est indiqué dans la ligne **Etat de la connexion** si l'enregistrement a bien été effectué ou non. En cas d'échec de l'enregistrement, il peut s'afficher les messages d'erreur ci-après.

- MAC already registered :

  Solution : effacer l'équipement (= système de communication OpenScape Business) sur SIRA Equipment Explorer et effectuer un nouvel enregistrement avec l'assistant **Enregistrement / Configuration**.

  Remarque : Vous pouvez trouver l'équipement sur SIRA Equipment Explorer à l'aide du nom de l'équipement ou de l'adresse MAC. Vous trouverez le nom d'équipement et l'adresse MAC du système de communication OpenScape Business dans **Centre de service**, **Accès distant**.

- Configuration Error :

  Solution : dans l'assistant **Enregistrement / Configuration**, entrez de nouveau l'ID partenaire et le mot de passe et quitter l'assistant de manière correcte.
- Wrong Credentials :

  Solution : dans l'assistant **Enregistrement / Configuration**, entrez de nouveau l'ID partenaire et le mot de passe et quitter l'assistant de manière correcte.

24.16.1.2 Comment activer le plugin RSP.servicelink

L'assistant **Activation / Désactivation** permet d'activer le plugin RSP.servicelink pour l'accès à distance au système de communication via SSDP.

Conditions préalables

Une configuration DNS opérationnelle est disponible.

Il existe dans le réseau client un routeur par défaut pour l'accès Internet ou un serveur proxy comme variante.

Le plugin RSP.servicelink a été désactivé.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.
3) Dans la colonne **RSP.servicelink**, cliquez sur **Activation / Désactivation**.
4) Cliquez sur **Activer**.

24.16.1.3 Comment désactiver le plugin RSP.servicelink

L'assistant **Activation/Désactivation** permet d'activer le plugin RSP.servicelink pour l'accès à distance au système de communication.

Conditions préalables

Le plugin RSP.servicelink est activé.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.
3) Cliquez sur **Activer / Désactiver dans la colonne RSP.servicelink**.
4) Cliquez sur **Désactiver**.

24.16.1.4 Comment réinitialiser le plugin Service RSP

L'assistant **Activation / Désactivation** permet de réinitialiser le RSP Service-Plugin. La configuration RSP entière est effacée et le plugin Service RSP est désactivé.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.
3) Dans la colonne **RSP.servicelink**, cliquez sur **Activation / Désactivation**.
4) Cliquez sur **Retour à la valeur par défaut** puis sur **OK**.
5) Dans la colonne **RSP.servicelink**, cliquez sur **Activation / Désactivation**.
6) Cliquez sur **Désactiver**.

7) Sur le serveur SIRA, effacez l'appareil (= système de communication OpenScape Business).

Remarque : A l'aide de l'adresse MAC, vous trouverez l'appareil sur le serveur SIRA. Vous trouverez l'adresse MAC du système de communication OpenScape Business dans **Centre de service**, **Inventory**.

24.16.1.5 Comment configurer un PIN pour l'activation et la désactivation du plugin RSP.servicelink

Le PIN sert à l'activation et la désactivation du plugin RSP.servicelink à l'aide d'un téléphone système.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.
3) Dans le champ **PIN** entrez le PIN à quatre caractères.
4) Cliquez sur **Enregistrer** puis sur **OK**.

Étapes suivantes

L'activation du plugin Service primaire à l'aide d'un téléphone système est réalisé par l'entrée de l'indicatif correspondant (indicatif par défaut = *996) suivie de la saisie du PIN à quatre positions.

La désactivation du plugin Service à l'aide d'un téléphone système est réalisée par l'entrée de l'indicatif correspondant (indicatif par défaut = #996) suivie de la saisie du PIN à quatre positions.

24.16.2 Accès distant

Grâce à l’accès distant, un technicien de maintenance autorisé est en mesure d’accéder aux systèmes de communication OpenScape Business X via Internet. Cela permet par exemple de fournir une assistance lors de la résolution des tâches d'administration ou lors de la recherche d'erreurs.

Afin de permettre l'accès distant au système de communication, l'accès distant doit être activé. Les méthodes d’accès suivantes sont disponibles :

Accès distant via liaison Internet

Conseil : L'accès distant via une connexion Internet représente un risque accru en matière de sécurité.

Pour effectuer une sélection via Internet, le technicien de maintenance a besoin d'un port spécial (**Numéro de port**) pour accéder au système de communication. Par défaut, le numéro de port 10099 est inscrit. En cas d'utilisation d'un routeur externe, il faut paramétrer sur le routeur externe un renvoi de port pour ce numéro de port.

Le numéro de port ne doit pas être bloqué par un pare-feu éventuellement en place sur le PC du technicien SAV. Il faut donc déterminer la sélection du numéro de port en accord avec le technicien de maintenance.

Les applications UC Booster (comme UC Suite, OpenDirectory Service, Gate View) ne peuvent pas être gérées via cet accès distant.

Afin de désactiver l'accès distant au système de communication, l'accès distant doit être désactivé.

Remarque : Pour éviter les accès non autorisés au système de communication, désactivez l'accès distant une fois l'administration à distance terminée.

24.16.2.1 Comment activer l'accès distant via RNIS

L'assistant **Accès distant** permet aux techniciens de maintenance autorisés d'accéder au système de communication via une liaison RNIS.

Conditions préalables

OpenScape Business X dispose d'une liaison réseau RNIS.

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.
3) Cliquez sur **Accès distant**, pour démarrer l'assistant **Accès distant**.
4) Cochez **Accès distant : activé** pour activer l'accès distant.
5) Activez le champ d'option **Accès distant par : RNIS** pour activer l'accès distant via RNIS.
6) Dans le champ **Numéro d'accès**, entrez le numéro interne via lequel l'accès distant doit avoir lieu.
7) Dans le champ **Numéro d'accès**, entrez le numéro de sélection via lequel l'accès distant doit avoir lieu.
8) Cliquez sur **OK&Suivant** puis sur **Terminer**.

24.16.2.2 Comment configurer les PC avec Microsoft Windows Vista pour l'accès à distance via RNIS

Conditions préalables

Le PC est équipé d'une carte RNIS et dispose d'une connexion réseau RNIS.

Un système de communication OpenScape Business X5/X8 avec une connexion point à point est accessible. L'indicatif régional local et le numéro PABX du système de communication sont connus.

L'accès à distance via le RNIS a été activé. Le numéro d'accès à distance au système de communication est disponible.

Le nom d'utilisateur et le mot de passe pour accéder au système de communication sont connus.

Conseil : La description suivante s'applique à un PC avec le système d'exploitation Microsoft Windows Vista. La procédure pour les PC avec le système d'exploitation Microsoft Windows XP est analogue à celle décrite ci-dessous.

Étape par étape

1) Cliquez sur **Démarrer** dans Windows Vista et sélectionnez **Se connecter à**. La fenêtre **Se connecter à un réseau** s'affiche.
2) Cliquez sur **Configurer une connexion ou un réseau**.
3) Cliquez sur l'option de connexion **Se connecter à un lieu de travail**, puis sur **Suivant**.
4) Cliquez sur **Composer directement**.
5) Dans le champ **Numéro de téléphone**, entrez le code CO (par exemple, `0`), suivi de l'indicatif local (par exemple, `089`), du numéro PABX (par exemple, `12345678`) et du numéro d'appel (par exemple, `666`).

   La saisie complète pour l'exemple ci-dessus serait donc : `008912345678666`
6) Saisissez une désignation pour cette connexion dans le champ **Nom de la destination**.
7) Activez la case à cocher **Ne pas se connecter maintenant ; il suffit de le configurer pour que je puisse me connecter plus tard**.
8) Cliquez sur **Next** (Suivant).
9) Saisissez le nom d'utilisateur pour accéder au système de communication dans le champ **Nom d'utilisateur**
10) et le mot de passe pour accéder au système de communication dans le champ **Mot de passe**.

Remarque : Le nom d'utilisateur par défaut et le mot de passe par défaut pour l'accès au système via l'outil de service Manager E sont utilisés comme informations d'identification par défaut pour accéder au système de communication.

11) Cliquez sur **Créer**.
12) Cliquez sur **Se connecter maintenant**.

Cela permet un accès à distance au système de communication.

Conseil : Pour désactiver la connexion, cliquez sur **Démarrer** > **Connecter à**. Cliquez sur la désignation de la connexion définie à l'étape 6 (**Nom de la destination**), puis sur **Déconnecter**.

Pour activer la connexion, cliquez sur la désignation définie à l'étape 6 (**Nom de la destination**), puis sur **Connecter**.

24.16.2.3 Comment configurer un PC sous Microsoft Windows 7 pour l'accès à distance via ISDN

Conditions préalables

L'ordinateur est équipé d'une carte RNIS et dispose d'une connexion RNIS.

Il convient d'accéder à un système de communication OpenScape Business X5/X8 avec une connexion point à point. L'indicatif régional et le numéro PABX du système de communication sont connus.

L'accès à distance via ISDN a été activé. Le numéro d'accès à distance au système de communication est disponible.

Le nom d'utilisateur et le mot de passe permettant d'accéder au système de communication sont connus.

Conseil : La description suivante s'applique à un PC équipé du système d'exploitation Microsoft Windows 7.

Étape par étape

1) Cliquez dans le menu **Démarrer** de Windows 7 sur **Panneau de configuration**.
2) Cliquez sur **Réseau et Internet**.
3) Cliquez sur **Centre de réseau et de partage**.
4) Cliquez sur **Configurer une connexion ou un réseau**.
5) Cliquez sur l'option de connexion **Se connecter à un lieu de travail**, puis sur **Suivant**.
6) Cliquez sur **Composer directement**.
7) Dans le champ **Numéro de téléphone**, entrez le code CO (par exemple, `0`), suivi de l'indicatif local (par exemple, `089`), du numéro PABX (par exemple, `12345678`) et du numéro d'appel (par exemple, `666`).

   La saisie complète pour l'exemple ci-dessus serait donc : `008912345678666`
8) Saisissez une désignation pour cette connexion dans le champ **Nom de la destination**.
9) Activez la case à cocher **Ne pas se connecter maintenant ; il suffit de le configurer pour que je puisse me connecter plus tard**.
10) Cliquez sur **Suivant** .
11) Saisissez le nom d'utilisateur pour accéder au système de communication dans le champ **Nom d'utilisateur**
12) et le mot de passe pour accéder au système de communication dans le champ **Mot de passe**.

Remarque : Le nom d'utilisateur et le mot de passe par défaut pour l'accès au système via l'outil de service

Manager E sont utilisés comme identifiants par défaut pour accéder au système de communication.

13) Cliquez sur **Créer** .
14) Cliquez sur **Se connecter maintenant**. Le message `Connexion établie` apparaît alors.
15) Cliquez sur **Fermer** .

Cela permet un accès à distance au système de communication.

Conseil : Pour désactiver la connexion, cliquez sur l'icône **Réseau** dans la barre d'outils. Cliquez sur la désignation de la connexion définie à l'étape 8 (**Nom de la destination**), puis sur **Déconnecter**.

Pour activer la connexion, cliquez sur la désignation définie à l'étape 8 (**Nom de la destination**), puis sur **Connecter**.

24.16.2.4 Comment activer l'accès distant par l'accès Internet avec adresse IP fixe

L'assistant **Accès distant** permet aux techniciens de maintenance autorisés d'accéder au système de communication via une liaison Internet.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Vous disposez d'un numéro de port permettant au technicien de maintenance d'accéder au système de communication en passant par Internet. Ce numéro de port ne doit pas être bloqué par un pare-feu éventuellement en place sur le PC du technicien SAV.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.
3) Cliquez sur **Accès distant**, pour démarrer l'assistant **Accès distant**.
4) Cochez **Accès distant : activé** pour activer l'accès distant.
5) Activez le champ d'option **Accès distant par : Internet** pour activer l'accès distant par Internet.
6) Dans le champ **Numéro de port**, indique le numéro de port via lequel l'accès distant doit avoir lieu.

   Par défaut, le numéro de port 10099 est inscrit.
7) Cliquez sur **OK&Suivant**. Le message `Accès distant activé...` est affiché. Ce message comprend l'URLpermettant d'accéder à distance au système de communication à l'aide du navigateur web.
8) Cliquez sur **Terminer**.

24.16.2.5 Comment activer l'accès distant par l'accès Internet sans adresse IP fixe

L'assistant **Accès distant** permet aux techniciens de maintenance autorisés d'accéder au système de communication via une liaison Internet.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Vous disposez d'un numéro de port permettant au technicien de maintenance d'accéder au système de communication en passant par Internet. Ce numéro de port ne doit pas être bloqué par un pare-feu éventuellement en place sur le PC du technicien SAV.

Il existe un compte DynDNS.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.
3) Cliquez sur **Accès distant**, pour démarrer l'assistant **Accès distant**.
4) Cochez **Accès distant : activé** pour activer l'accès distant.
5) Activez le champ d'option **Accès distant par : Internet** pour activer l'accès distant par Internet.
6) Dans le champ **Numéro de port**, indique le numéro de port via lequel l'accès distant doit avoir lieu.

   Par défaut, le numéro de port 10099 est inscrit.
7) Cliquez sur **OK&Suivant** pour valider les entrées. La fenêtre **Configurer le compte DynDNS** s'affiche.
8) Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur pour votre compte DynDNS chez l'opérateur DynDNS, si celui-ci n'est pas déjà affiché.
9) Dans les champ **Mot de passe** et **Répéter le mot de passe**, entrez le mot de passe de votre compte DynDNS chez le fournisseur DynDNS si celui-ci n'est pas déjà affiché.
10) Dans le champ **Nom d'hôte**, entrez le nom d'hôte attribué par votre fournisseur DynDNS, sans le nom de domaine (par exemple `myhost`), si celui-ci n'est pas déjà affiché.
11) Dans la liste déroulante **Nom de domaine** sélectionnez votre fournisseur DynDNS (par exemple `dyndns.org`), si celui-ci n'est pas déjà affiché. Votre nom de domaine complet est alors par ex. `myhost.dyndns.org`.
12) Cliquez sur **Test connexion**. La fenêtre **Tester l'accès DynDNS** s'affiche.
13) Cliquez sur **OK**. Les données d'accès DynDNS sont transmises au fournisseur. Cela dure environ 10 secondes.
14) Si le test a été passé avec succès, le message `Accès distant activé...` s'affiche. Ce message comprend l'URLpermettant d'accéder à distance au système de communication à l'aide du navigateur web. Cliquez sur **Terminer**.
15) Une fois le test exécuté avec succès, cliquez sur **OK**. Dans la fenêtre **Accès DynDNS** qui s'ouvre ensuite figurent des informations sur les causes possibles des défauts. Cliquez sur **OK**. La fenêtre **Configurer le compte DynDNS** s'affiche. Si nécessaire, vérifiez et corrigez ici les

données d'accès que vous aviez fournies (étapes 8 à 11). Poursuivez comme indiqué à l'étape 12.

24.16.2.6 Comment désactiver l'accès distant

L'assistant **Accès distant** permet de désactiver l'accès distant.

Conditions préalables

Vous êtes connecté à WBM avec le profil **Advanced**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Centre de service**.
2) Dans l'arborescence de navigation, cliquez sur **Accès distant**.
3) Cliquez sur **Accès distant**, pour démarrer l'assistant **Accès distant**. Il est indiqué si l'accès distant est raccordé via Internet ou/et via RNIS.
4) Activez le champ d'option **Accès distant : désactivé** pour désactiver un accès distant.
5) Sélectionnez l'option de l'accès distant que vous souhaitez désactiver :
   - Si vous souhaitez désactiver l'accès distant par Internet, activez le champ d'option **Accès distant par : Internet**.
   - Si vous souhaitez désactiver l'accès distant par le RNIS, activez le champ d'option **Accès distant par : RNIS**.
6) Cliquez sur **OK&Suivant**.
7) Si vous voulez aussi désactiver la seconde option de l'accès distant, cliquez sur **Retour**. Répétez les étapes 4 à 6.
8) Cliquez sur **Terminer**.

24.16.3 Utilisateur en ligne

L'utilisateur en ligne permet la gestion à distance, le contrôle et la surveillance des téléphones OpenStage à partir d'un PC Windows. Le comportement d'un téléphone OpenStage est simulé sur le PC via l'utilisateur en ligne.

Le condition pour communiquer avec un téléphone OpenStage est que le logiciel du téléphone dispose d'une clé dongle.

Pour l'accès à un téléphone OpenStage, il faut effectuer les entrées suivantes via l'utilisateur en ligne :

- Type de téléphone OpenStage
- Adresse IP du téléphone OpenStage
- Mot de passe administrateur du téléphone OpenStage

Des informations sur l'utilisation de l'utilisateur en ligne figurent dans la documentation suivante : *OpenStage HUSIM Phone Tester User Guide*. L'accès est possible via le portail Intranet à la documentation produit technique `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

L'outil de service Manager E offre permet aux abonnés en ligne de télécommander, contrôler et surveiller les téléphones OpenStage.

Remarque : L’adresse IP de la passerelle rapportée par l’utilisateur en ligne est identique à l’adresse IP système. L’adresse IP de la passerelle n’est pas l’adresse IP de la route par défaut.

24.16.3.1 Comment démarrer l'utilisateur en ligne

Conditions préalables

Vous êtes inscrit dans la WBM avec le profil **Expert**.

Étape par étape

1) Cliquez dans la barre de navigation sur **Mode Expert**.
2) Dans l'arborescence de navigation, cliquez sur **Maintenance** > **Utilisateur en ligne**. La fenêtre de connexion de l'utilisateur en ligne s'affiche.
3) Dans la liste déroulante **Modèle** sélectionnez le modèle du téléphone OpenStage souhaité.
4) Dans le champ **Phone IP** entrez l'adresse IP du téléphone OpenStage souhaité.
5) Dans le champ **Mot de passe** entrez le mot de passe administrateur du téléphone OpenStage souhaité. Par défaut, le mot de passe administrateur est `123456`.
6) Dans la liste déroulante **Protocole** sélectionnez le protocole de transport souhaité.
7) Sélectionnez une des possibilités suivantes pour le Internet Protocol Version IPv :
   - Si vous souhaites utiliser Internet Protocol Version 4, activez l'option **IPv4**.
   - Si vous souhaites utiliser Internet Protocol Version 6, activez l'option **IPv6**.
8) Dans la liste déroulante **Number of Key modules** (nombre des périphériques) sélectionnez le nombre des périphériques.
9) Cliquez sur **OK** pour lancer l'accès au téléphone OpenStage souhaité.

Conseil : Vous trouverez des informations sur la commande des utilisateurs en ligne dans *OpenStage HUSIM Phone Tester User Guide* ; ce document est disponible à l'adresse suivante : `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

25 Migration

Les systèmes OpenScape Business V2, V3 et HiPath 3000 peuvent être migrés/mis à niveau vers OpenScape Business V4.

Les scénarios de migration/mise à niveau suivants sont pris en charge par le logiciel OpenScape Business V4.

Remarque : OpenScape Business V4 ne prend pas en charge les systèmes matériels V2 ni le serveur UC Booster (y compris la carte UC Booster). Les systèmes dotés de ce matériel doivent d'abord être migrés vers des systèmes matériels V3.

Remarque : Il est essentiel de supprimer les utilisateurs actifs d'Unify Phone avant, par exemple, les migrations de système, afin d'éviter des divergences critiques entre la base de données OpenScape Business et la base de données cloud. Vous trouverez plus d'informations dans le wiki des experts Unify et dans le livre blanc Unify Phone .

Remarque : Voir aussi Comment retirer ou supprimer des utilisateurs d'Unify Phone à la page 1135.

Système OpenScape Business S

- Mise à niveau du logiciel d'OpenScape Business S V2 vers V4
- Mise à niveau du logiciel d'OpenScape Business S V3 vers V4

Réseau d'entreprises OpenScape

- Migration/mise à niveau d'un réseau OpenScape Business de la version 2 à la version 4
- Migration/mise à niveau d'un réseau OpenScape Business de la version 3 à la version 4

HiPath 3000 incluant OpenScape Office HX

- Migration matérielle HiPath 3000 incluant OpenScape Office HX

Selon le système source, les licences existantes peuvent être transférées intégralement ou partiellement. Il en va de même pour l'utilisation ultérieure des modules périphériques et des terminaux connectés.

La prise en charge logicielle existante pour OpenScape Business Systems restera inchangée après la migration.

Vous pouvez réduire les efforts de migration/mise à niveau pour l'utilisation continue des licences existantes, par rapport à un transfert de licence « hors ligne », en connectant le système OpenScape Business au serveur de licences Unify Central et en utilisant la fonctionnalité **CLS Connect** .

Dans cette section, les termes suivants sont utilisés :

Migration	en cas de modification du matériel et des logiciels

Mise à niveau	en cas de modification purement logicielle
Carte mère V2	Terme utilisé pour désigner la famille de cartes mères introduite avec OpenScape Business.
carte mère V3	Terme utilisé pour désigner la famille de cartes mères introduite avec le logiciel V3.

Remarque : Une condition préalable à toute migration visant à passer d'un système avec carte mère V2 à un système avec carte mère V3 est que l'administrateur télécharge le jeu de sauvegarde via un périphérique HTTPS. Les autres périphériques tels que les disques durs, les serveurs FTP ou les lecteurs réseau ne sont pas pris en charge et entraîneront l'échec du processus de migration.

Remarque : Il existe deux voies de migration valides selon la version logicielle du système OSBiz. Utilisez soit un ensemble de sauvegarde d'un système matériel V2 sur la dernière liaison V2R7, soit la même liaison logicielle V3 sur les systèmes à carte mère V2 et V3 pour garantir la cohérence de la base de données.

Remarque : Si un système OpenScape Office V3 MX/LX doit être remplacé par un système OpenScape Business, ce dernier doit être commandé comme un nouveau système.

25.1 Mise à niveau logicielle pour les systèmes OpenScape Business X

Une mise à niveau logicielle des systèmes OpenScape Business X implique essentiellement le remplacement de certains des composants du logiciel.

Avant de mettre à niveau le logiciel d'un système OpenScape Business X, vous devez déterminer la configuration actuelle du système et les composants matériels/logiciels et de licence à remplacer, le cas échéant.

Tableau 31 : Mise à niveau du logiciel OpenScape Business X - Liste de contrôle du matériel/logiciel

Composantes	Remplacé par
Composants matériels	
Composants logiciels	
Logiciel système V2 sur carte SDHC	Logiciel système V3 (image du serveur de téléchargement de logiciels)

Composantes	Remplacé par
Logiciel système V3 (image du serveur de téléchargement de logiciels)	Logiciel système V3 (image du serveur de téléchargement de logiciels)
Fin du VPN sur le WAN dans le système	Fin du VPN dans le routeur externe
myPortal Smart	myPortal @work
Composant de licence	
Licences dans le fichier de licence	Transfert des licences dans un nouveau fichier de licence

25.1.1 Mise à niveau logicielle d'OpenScape Business X V2 vers OpenScape Business X V3

Lorsque vous mettez à niveau un modèle OpenScape Business X de la version logicielle V2 vers la version V3, seul le logiciel système est remplacé - la carte mère V2 et toute carte UC Booster ou serveur Booster serveur existant sont conservés. Les licences existantes et la configuration du client sont maintenues. L'assistance logicielle existante restera inchangée après la migration.

Avant la mise à niveau du logiciel de la version V2 vers la version V3, si elle n'existe pas encore, vous devez établir un accès permanent au serveur de licence Unify (via Internet) dans le système et activer la fonction **CLS Connect**. Cela simplifie le transfert de licence et raccourcit considérablement la durée de la migration.

Conditions requises

Pour la mise à niveau du logiciel et le transfert de la configuration client existante, le système doit être exploité avec la dernière version du logiciel V2R7 avant la mise à niveau. Si nécessaire, mettez le système à niveau vers la dernière version du logiciel. Pour ce faire, le système doit avoir un statut d'assistance logicielle valide.

Pour la mise à niveau du logiciel système de V2 vers V3, selon que CLS Connect est utilisé ou non, l'élément suivant est nécessaire :

- Licence de mise à niveau du logiciel OpenScape Business V3 (uniquement lorsque **CLS Connect** n'est pas utilisé)

Conditions limites fonctionnelles et restrictions

Vous pouvez transférer complètement les licences existantes de la carte mère V2 vers la carte mère V3 au cours de la migration. Le transfert de licence sans activation de la fonction CLS Connect nécessite la licence "Mise à niveau du logiciel" et une manipulation et un temps de travail beaucoup plus complexes que l'utilisation de la fonction CLS Connect.

La configuration du client et les données du client sont automatiquement transférées de la version V2 vers la version V3 du logiciel pendant le processus de mise à niveau du logiciel.

Les principales étapes techniques de la mise à niveau du logiciel sont décrites dans les chapitres suivants. Afin de conserver les licences existantes, une distinction est faite entre le traitement :

- Mise à niveau du logiciel pour une licence permanente avec et sans CLS Connect
- Mise à niveau du logiciel avec la licence PayGo

25.1.1.1 Mise à niveau des systèmes sous licence permanente avec CLS Connect

Effectuez les étapes de mise à niveau suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business
   a) Mettre à niveau le système existant vers la version logicielle V2R7.
   b) Configurer l'accès au serveur licences central (CLS) de Unify dans le système et tester la connexion.
   c) Activer **CLS Connect** dans le système.

2) Effectuer la mise à niveau du logiciel
   a) Effectuer la mise à niveau du logiciel vers V3 via OpenScape Business Assistant.
   b) La configuration du système est automatiquement transférée à V3.
   c) Les licences existantes sont reprises après V3.

3) Génération automatique du fichier de licence par le serveur de licences central.

   Après le redémarrage du système, le système transfère au CLS l'information selon laquelle les licences existantes sont exploitées avec la version 3 du logiciel.

25.1.1.2 Mise à niveau des systèmes sous licence permanente sans CLS Connect

Effectuez les étapes de mise à niveau suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business.
   a) Mettre à niveau le système existant vers la version logicielle V2R7.

2) Créer un "fichier de licence de mise à niveau" pour le système V2 sur le serveur de licences central (CLS)
   a) Activer la "Licence de mise à niveau du logiciel" pour le système existant.
   b) Générer un nouveau fichier de licence pour l'adresse MAC de la carte mère V2
   c) Télécharger le fichier de licence du CLS

3) Importer et activer le fichier de licence dans le système OpenScape Business V2.

4) Effectuer la mise à niveau du logiciel.
   a) Effectuer la mise à niveau du logiciel vers V3 via OpenScape Business Assistant.
   b) La configuration du système est automatiquement transférée à V3.
   c) Les licences existantes dans le système sont transférées à V3
5) Redémarrez le système après la mise à niveau du logiciel.

25.1.1.3 Mise à niveau des systèmes sous licence PayGo

Effectuez les étapes de mise à niveau suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business
   a) Mettre à niveau le système existant vers la version logicielle V2R7.
2) Régénérer le fichier de licence sur le serveur de licences central (CLS)
   a) Régénérer un nouveau fichier de licence pour l'adresse MAC de la carte mère V2.
   b) Télécharger le fichier de licence du CLS.
3) Importer et activer le nouveau fichier de licence dans le système OpenScape Business V2.
4) Mettre à niveau le logiciel OpenScape Business.
   a) Exécuter la mise à niveau du logiciel vers V3 via OpenScape Business Assistant.
   b) La configuration du système est automatiquement transférée à V3.
   c) Le système est prêt à fonctionner après le redémarrage.

25.1.2 Mise à niveau logicielle d'OpenScape Business X V3 vers OpenScape Business X V4

Lorsque vous mettez à niveau le logiciel d'un modèle OpenScape Business X équipé d'un matériel V3 de la version logicielle V3 vers V4, seul le logiciel système est remplacé. Les licences existantes et la configuration client sont conservées. L'assistance logicielle existante restera inchangée après la mise à niveau.

Effectuez la mise à niveau logicielle vers V4 via OpenScape Business Assistant.

25.2 Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3

La mise à niveau du logiciel de UC Booster Server V2 vers la version V3 peut être effectuée en une seule étape.

La mise à niveau du logiciel de UC Booster Server V1 vers la version V3 doit se faire en deux étapes. Passez d'abord de V1 à V2R7, puis de V2R7 à V3.

25.2.1 Comment mettre à niveau UC Business Booster Server de V2 vers V3

La mise à niveau de UC Booster Server de V2 vers V3 n'est nécessaire que pour les systèmes OpenScape Business X équipés d'une carte mère V2. Les systèmes OpenScape Business X équipés de cartes mères V3 ne nécessitent plus UC Booster Server. Dans ce cas, la version V2.7 du logiciel est nécessaire sur UC Booster Server pour migrer la configuration et les licences des clients vers la carte mère V3.

Conditions préalables

- Le système d'exploitation Linux doit être vérifié et mis à niveau si nécessaire (voir la *Note de mise à jour technique pour le logiciel du système OpenScape Business V3*)
- UC Booster Server fonctionne avec la dernière version logicielle V2R7 avant la mise à niveau. Si nécessaire, mettez le système à niveau vers la dernière version du logiciel.
- Commencer par mettre à jour le système OpenScape Business X auquel UC Booster Server est connecté avec la version V3 du logiciel, avec les licences conformément à la description figurant dans Mise à niveau logicielle d'OpenScape Business X V2 vers OpenScape Business X V3 à la page 1314
- Logiciel UC Booster Server Image V3

Avant de procéder à la mise à niveau du logiciel UC Booster Server, déterminez la configuration actuelle du système et les composants matériels et logiciels et de licence qui doivent éventuellement être remplacés.

Tableau 32 : Migration OpenScape Business S - Liste de contrôle matérielle et logicielle

Composantes	Remplacé par
Composants matériels	
PC serveur	La réutilisation est possible. Les exigences en matière de matériel doivent être vérifiées pour les extensions d'Unify OpenScape Business S.[8]
Composants logiciels	

[8] Le PC serveur existant peut être utilisé lorsque la configuration du système UC Booster Server reste inchangée après la mise à niveau du logiciel. Si des extensions sont prévues après la mise à niveau du logiciel, il peut être nécessaire d'adapter les exigences matérielles conformément aux spécifications du *guide d'installation d'OpenScape Business S, chapitre Conditions préalables*.

Composantes	Remplacé par
Système d'exploitation SLES 12 ou SLES 15	La réutilisation est possible. Une mise à niveau vers le dernier service pack peut être nécessaire. [9]
myPortal Smart	myPortal @work
Composant de licence	
Licences dans le fichier de licence (fait partie du fichier de licence d'OpenScape Business X)	Transfert des licences dans un nouveau fichier de licence
Application CSTA (via carte UC Booster / serveur)	Licence CSTA pour la connexion de solutions externes (non requise pour UC Suite, TAPI 170 et TAPI 120)

Ce qui suit décrit la mise à niveau du logiciel OpenScape Business tout en conservant le système d'exploitation SLES.

Étape par étape

1) Mettez à niveau le système OpenScape Business X vers la version V3.
   Voir Mise à niveau logicielle d'OpenScape Business X V2 vers OpenScape Business X V3 à la page 1314 pour les détails.
2) Mettre à niveau le logiciel UC Booster Server vers la version V3
   Utilisez la fonction de mise à niveau dans OpenScape Business Assistant de UC Booster Server pour mettre à niveau le logiciel V2R7 vers la version V3 (voir Mise à jour du système de communication à la page 1193).
3) Effectuer une sauvegarde des données après la mise à niveau du logiciel
   Sauvegardez vos données V3 (voir Sauvegarde immédiate à la page 1186).

25.3 Migration matérielle et logicielle des systèmes OpenScape Business X vers V3

Lors de la migration des systèmes OpenScape Business X, les composants matériels, logiciels et les licences sont échangés.

Avant de migrer un système Business X, déterminez la configuration actuelle du système et les composants matériels et logiciels ainsi que les licences à remplacer.

[9] Le système d'exploitation SLES installé sur le PC serveur peut être adopté en cas de mise à niveau du logiciel UC Booster Server. Toutefois, il doit être mis à niveau avec le dernier service pack publié avant la mise à niveau du logiciel.

Si Novell a interrompu le support logiciel pour la version SLES utilisée, le client doit en être informé et, si nécessaire, une mise à niveau du SLES doit être commercialisée.

La mise à niveau du SLES peut devoir être effectuée en plusieurs étapes pour reprendre les installations existantes d'OpenScape Business S, y compris la configuration et les données du client. Une clé de mise à jour SLES existante reste valable avec une mise à jour SLES. Toutefois, il se peut qu'il faille le désenregistrer auprès de Novell avant la mise à niveau SLES et le réenregistrer pour le nouveau système.

Remarque : La carte OCCLA avec le système V3 peut aller jusqu'à 60 (+16) canaux MEB. La migration vers la nouvelle carte restaure la configuration existante de la carte OCC. Si vous souhaitez utiliser des canaux MEB supplémentaires, vous devez reconfigurer votre système en utilisant les assistants/ pages WBM appropriés.

Les modules présents dans l'emplacement 10 des systèmes OpenScape Business X5 muraux ne peuvent pas être utilisés avec les cartes mères V3. Ces modules doivent être remplacés par des modules ou solutions de versions ultérieures.

Tableau 33 : Migration OpenScape Business X - Liste de contrôle matériel et logiciel

Composant	Remplacé par
Composants matériels	
"Carte mère V2" existante	Carte mère V3 (de base ou avancée, selon la configuration)
UC Booster Card / Server (avec UC Suite)	Disque SSD M.2 supplémentaire
Module CMA	Module CMAe
Module EXMR pour les dispositifs d'annonce externe	Carte mère V3 (prise d'entrée audio sur le panneau avant)
Interfaces S0 sur la carte mère V2	Terminal S0 de la carte périphérique S0
Téléphones Optipoint 500	Téléphones OpenScape Deskphone CP
Téléphones Optipoint 400	
Composants logiciels	
Logiciel système V2 sur carte SDHC	Logiciel système V3 (Image du serveur de téléchargement de logiciels)
SW système V3	Logiciel système V3 (Image du serveur de téléchargement de logiciels)
Fin du VPN sur le WAN dans le système	Fin du VPN dans le routeur externe
myPortal Smart	myPortal @work
Composant de licence	
Licences dans le fichier de licence	Transfert des licences dans un nouveau fichier de licence
Applications CSTA externes (jusqu'à présent sans licence, car connectées à UC Booster Card/au serveur matériel)	Licence CSTA séparée pour la connexion de solutions externes (non requise pour UC Suite, TAPI 170 et TAPI 120)

25.3.1 Migration d'OpenScape Business X V2 vers OpenScape Business X V3

Lors de la migration d'un modèle OpenScape Business X de la version V2 vers la version V3, la carte mère et le logiciel système sont remplacés. Les licences existantes et la configuration client peuvent être transférées. L'assistance logicielle existante est maintenue sans changement après la migration.

Avant la migration, si ce n'est déjà fait, configurez un accès permanent au serveur de licences Unify (via Internet) dans le système et activez la fonction « CLS Connect ». Cela simplifie le transfert de licence et réduit considérablement la durée de la migration. Le client doit être informé de l'accès requis depuis le système OpenScape Business au CLS.

Conditions requises

Le système fonctionne avec la dernière version logicielle V2R7 publiée avant la mise à niveau. Si nécessaire, mettez à niveau le système vers la dernière version du logiciel. Pour ce faire, le système doit disposer d'un statut de support logiciel valide.

Pour la migration de la version V2 à la version V3, selon que vous utilisez CLS Connect, UC Suite ou des applications CSTA externes, les éléments suivants sont nécessaires :

- Carte mère V3
- Logiciel V3 sur stockage de données SSD M.2 SATA
- SSD M.2, 256 Go de stockage de données de masse (en option avec l’application UC Suite)
- Licence de migration matérielle OpenScape Business V3 (si CLS Connect n'est pas utilisé)
- Licence OpenScape Business CSTA (facultatif)

Conditions limites fonctionnelles et restrictions

Les licences existantes peuvent être entièrement transférées de la carte mère V2 existante vers la carte mère V3 pendant la migration. Le transfert de licence sans activation de la fonction CLS Connect nécessite la licence « HW Migration » et implique une manipulation et un investissement en temps beaucoup plus complexes que l'utilisation de la fonction CLS Connect.

La configuration client et les données client sont migrées de la version V2 à la version V3 du logiciel via un processus de sauvegarde/restauration.

Les principales étapes techniques de la migration sont décrites dans les rubriques suivantes. Afin de conserver les licences existantes, une distinction est faite en termes de traitement entre :

- Mise à niveau logicielle pour les licences permanentes avec et sans CLS Connect
- Mise à niveau logicielle avec licence PayGo

Remarque : Lors de la migration de la carte mère V2 vers la carte mère V3, les ports EVM supplémentaires ne sont pas inclus dans le groupe de recherche SmartVM. Cela nécessite une configuration manuelle, au cours de laquelle la restriction COS doit également être effectuée.

Remarque : Lors d'une migration matérielle d'un matériel V2 configuré avec une adresse IP DSP non par défaut vers un système matériel V3, l'adresse IP DSP sera réinitialisée à sa valeur par défaut. Après la migration, l'administrateur doit reconfigurer manuellement l'adresse IP DSP ainsi que l'adresse IP FPGA en fonction des besoins spécifiques du client.

25.3.1.1 Comment migrer vers des systèmes à licence permanente V3 avec CLS Connect

Effectuez les étapes de la migration suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business
   a) Mettre à niveau le système existant vers la version V2R7 du logiciel
   b) Configurer l'accès au serveur de licences central (CLS) dans le système et tester la connexion
   c) Activer CLS Connect dans le système

2) Générer un fichier de licence sur le serveur de licences central (CLS)
   a) Transférer les licences existantes de l'adresse MAC de la carte mère V2 vers l'adresse MAC de la carte mère V3 en utilisant la fonction **Régénérer**
   b) Générer un nouveau fichier de licence pour l'adresse MAC de la carte mère V3

3) Sauvegarder la configuration du système V2 et les données des clients.

4) Échanger les cartes mères
   a) Fermer le système et couper toutes les tensions d'alimentation
   b) Utiliser le support de données V3 et, si nécessaire, le stockage optionnel de données de masse sur la carte mère V3
   c) Retirer la carte OCCB Voice Channel Booster de la carte mère V2 et la brancher sur la carte mère V3.
   d) Remplacer la carte mère V2 par la carte mère V3 dans le système
   e) Rétablir la tension d'alimentation

      Le système démarre automatiquement.

5) Définir les paramètres de base du système au sein de WBM après le démarrage
   a) Régler la date et l'heure du système
   b) Installer le pack d'application

      UC Smart pour système sans UC ou avec UC Smart

      UC Suite pour systèmes avec UC Suite

6) Restaurer la configuration du système
   a) Restaurer la sauvegarde à l'aide de la fonction de restauration
   b) Importer le fichier de licence nouvellement créé

25.3.1.2 Comment migrer vers des systèmes à licence permanente V3 sans CLS Connect

Effectuez les étapes de la migration suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business
   a) Mettre à niveau le système existant vers la version V2R7 du logiciel

2) Créer un "fichier de licence de migration" pour le système V2 sur le serveur de licences central (CLS)
   a) Activer la "licence de migration matérielle" pour le système existant
   b) Générer un nouveau fichier de licence pour l'adresse MAC de la carte mère V2.

      Pour cela, entrez l'adresse MAC de la carte mère V3.
   c) Télécharger le fichier de licence du CLS

3) Importer le fichier de licence dans le système OpenScape Business V2

4) Noter le **code de confirmation** affiché dans l'OpenScape Business Assistant

5) Générer un nouveau fichier de licence pour la carte mère V3 sur le serveur de licences central (CLS)
   a) Créer un nouveau fichier de licence pour l'adresse MAC de la carte mère V3 au CLS en régénérant l'adresse MAC de la carte mère V2 et le code de confirmation noté précédemment
   b) Rechercher le système OpenScape Business avec l'adresse MAC de la carte mère V3 dans le CLS.
   c) Déverrouiller le système OpenScape Business en saisissant et en activant le code de confirmation
   d) Régénérer le fichier de licence
   e) Télécharger le fichier de licence nouvellement généré à partir du CLS

6) Sauvegarder la configuration du système V2 et les données des clients.

7) Échanger les cartes mères
   a) Fermer le système et couper toutes les tensions d'alimentation
      a) Utiliser le support de données V3 et, si nécessaire, le stockage optionnel de données de masse sur la carte mère V3
      b) Retirer la carte OCCB Voice Channel Booster de la carte mère V2 et la brancher sur la carte mère V3.
      c) Remplacer la carte mère V2 par la carte mère V3 dans le système
   b) Rétablir la tension d'alimentation

      Le système démarre automatiquement.

8) Définir les paramètres de base du système au sein de WBM après le démarrage
   a) Régler la date et l'heure du système
   b) Installer le pack d'application

      UC Smart pour système sans UC ou avec UC Smart

      UC Suite pour systèmes avec UC Suite

9) Restaurer la configuration du système
   a) Restaurer la sauvegarde à l'aide de la fonction de restauration

10) Importer manuellement le nouveau fichier de licence dans le système V3 après le démarrage du système

25.3.1.3 Comment migrer vers les systèmes avec licence V3 PayGo

Effectuez les étapes de la migration suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business
   a) Mettre à niveau le système existant vers la version V2R7 du logiciel
2) Sauvegarder la configuration du système V2 et les données des clients.
3) Régénérer le fichier de licence sur le serveur de licences central (CLS)
   a) Régénérer un nouveau fichier de licence pour l'adresse MAC de la carte mère V3

      Transférer les licences existantes de l'adresse MAC de la carte mère V2 vers l'adresse MAC de la carte mère V3.
   b) Télécharger le nouveau fichier de licence du CLS
4) Échanger les cartes mères
   a) Fermer le système et couper toutes les tensions d'alimentation
   b) Utiliser le support de données V3 et, si nécessaire, le stockage optionnel de données de masse sur la carte mère V3
   c) Retirer la carte OCCB Voice Channel Booster de la carte mère V2 et la brancher sur la carte mère V3.
   d) Remplacer la carte mère V2 par la carte mère V3 dans le système
   e) Rétablir la tension d'alimentation

      Le système démarre automatiquement.
5) Définir les paramètres de base du système au sein de WBM après le démarrage
   a) Régler la date et l'heure du système
   b) Installer le pack d'application

      UC Smart pour système sans UC ou avec UC Smart

      UC Suite pour systèmes avec UC Suite
6) Restaurer la configuration du système
   a) Restaurer la sauvegarde à l'aide de la fonction de restauration
7) Importer manuellement le nouveau fichier de licence dans le système V3 et activer le fichier de licence

25.3.2 Migration d'OpenScape Business X V3 avec carte mère V2 vers OpenScape Business X V4 avec carte mère V3

Lors de la migration d'un modèle OpenScape Business X de V3 avec carte mère V2 vers V4 avec carte mère V3, le logiciel système et la carte mère sont remplacés. Les licences existantes et la configuration du client peuvent être transférées. L'assistance logicielle existante est maintenue sans modification après la migration.

Remarque :

Si le **connecteur CLS** n'est pas actif, une licence OpenScape Business Hardware Migration est requise.

Étape par étape

1) Mettez à niveau le système existant vers la dernière version logicielle V3R4 FR1/FR2
2) Migrez vers la carte mère V3 en suivant la procédure décrite dans Migration d'OpenScape Business X V2 vers OpenScape Business X V3 à la page 1320.
3) Effectuez la mise à jour logicielle vers V4 via OpenScape Business Assistant.

25.3.3 Migration d'OpenScape Business X V2 avec carte mère V2 vers OpenScape Business X V4 avec carte mère V3

Lors de la migration d'un modèle OpenScape Business X de V2 vers V4, la carte mère et le logiciel système sont remplacés. Les licences existantes et la configuration du client peuvent être transférées. L'assistance logicielle existante est maintenue sans modification après la migration.

Remarque :

Si **CLS Connect** n'est pas actif, une licence OpenScape Business Hardware Migration est requise.

Étape par étape

1) Mettre à niveau vers la dernière version logicielle V2R7
2) Suivez la procédure relative à la migration de la carte mère V2 vers la carte mère V3Migration d'OpenScape Business X V2 vers OpenScape Business X V3 à la page 1320.
3) Si myPortal @work est actif, installez la version V3R4 FR1/FR2 avant la mise à niveau vers V4.
4) Effectuez la mise à niveau logicielle vers V4 via OpenScape Business Assistant.

25.4 Migration d’un système OpenScape Business X V3 de la carte mère V2 vers la carte mère V3

Dans ce scénario, la carte mère V2 existante d’OpenScape Business System et tout matériel UC Booster pouvant être présent sont remplacés par une carte mère V3. Le système a déjà été mis à niveau vers la version V3 du logiciel, par exemple, dans le cadre de l’assistance logicielle.

Les licences existantes et la configuration du client peuvent être transférées. Le service d’assistance logicielle existante restera inchangée après la migration.

Une éventuelle carte UC Booster existante ou un serveur UC Booster n'est plus nécessaire en liaison avec la carte mère V3. Un stockage de données de masse supplémentaire est utilisé à cet effet sur la carte mère V3.

Dans Tableau 33 : Migration OpenScape Business X - Liste de contrôle matériel et logiciel à la page 1319 vous trouverez des informations sur les composants qui sont remplacés par la carte mère V3 ou qui sont supprimés sans substitution. Une licence CSTA est nécessaire pour une connexion existante d'applications CSTA externes. Cela ne s'applique pas à la connexion d'OpenScape TAPI 170 ou TAPI 120.

Conditions requises

Le système fonctionne avec la dernière version logicielle V2R7 avant la mise à niveau. Si nécessaire, mettez le système à niveau vers la dernière version du logiciel. Pour ce faire, le système doit avoir un statut d'assistance logicielle valide.

Pour la migration, les éléments suivants sont nécessaires, selon que l'on utilise CLS Connect, UC Suite ou des applications CSTA externes :

- Carte mère V3
- Logiciel V3 sur le stockage de données SSD M.2 SATA
- SSD M2, 256 Go de stockage de données de masse (en option avec l'application UC Suite)
- Licence de migration matériel OpenScape Business V3 (facultatif)
- Licence OpenScape Business CSTA (facultatif)

Conditions limites fonctionnelles et restrictions

Les licences existantes peuvent être entièrement transférées de la carte mère V2 existante vers la carte mère V3 au cours de la migration. Le transfert de licence sans activation de la fonction CLS Connect nécessite la licence "HW Migration" et une manipulation beaucoup plus complexe et longue que l'utilisation de la fonction CLS Connect.

La configuration du client et les données du client sont transférées par un processus de sauvegarde/restauration.

Les principales étapes techniques de la migration sont décrites dans les rubriques suivantes. Afin de conserver les licences existantes, une distinction est faite en ce qui concerne le traitement :

- Mise à niveau du logiciel pour une licence permanente avec et sans CLS Connect
- Mise à niveau du logiciel avec la licence PayGo

Remarque : Lors de la migration de la carte mère V2 vers la carte mère V3, les ports EVM supplémentaires ne sont pas inclus dans le groupe de recherche SmartVM. Cela nécessite une configuration manuelle, au cours de laquelle il convient de restreindre la discrimination.

Manager E ne prend pas en charge la conversion d'un KDS (service de distribution de clés) de la même version logicielle vers un type de système différent. Si vous souhaitez utiliser uniquement les données du KDS, vous pouvez suivre les étapes suivantes :

- Effectuez une migration complète de la carte mère V2 vers la carte mère V3.

- Téléchargez le KDS du système avec carte mère V3 à l'aide de Manager E et stockez-le localement.
- Rechargez le système avec carte mère V3.
- Chargez le KDS du système avec carte mère V3 précédemment stocké dans votre système avec carte mère V3.

Le système avec carte mère V3 utilisera la configuration de la base de données du KDS, et vous pouvez continuer avec la configuration manuelle de l'UC.

Remarque : La migration du KDS du système avec carte mère V2 vers le système avec carte mère V3 n'est pas prise en charge, car la base de données de la carte mère V2 n'est pas compatible avec la base de données de la carte mère V3.

25.4.1 Comment migrer vers des systèmes à licence permanente de carte mère V3 avec CLS Connect

Effectuez les étapes de la migration suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business
   a) Configurer l'accès au serveur de licences central (CLS) dans le système et tester la connexion
   b) Activer CLS Connect dans le système

2) Générer un fichier de licence sur le serveur de licences central (CLS)
   a) Transférer les licences existantes de l'adresse MAC de la carte mère V2 vers l'adresse MAC de la carte mère V3 en utilisant la fonction **Régénérer**
   b) Générer un nouveau fichier de licence pour l'adresse MAC de la carte mère V3

3) Sauvegarder la configuration du système V3 et les données des clients.

4) Créer une sauvegarde de la configuration de Booster Server si nécessaire.

5) Échanger les cartes mères
   a) Fermer le système et couper toutes les tensions d'alimentation
   b) Utiliser le support de données V3 et, si nécessaire, le stockage optionnel de données de masse sur la carte mère V3
   c) Retirer la carte OCCB Voice Channel Booster de la carte mère V2 et la brancher sur la carte mère V3.
   d) Remplacer la carte mère V2 par la carte mère V3 dans le système
   e) Rétablir la tension d'alimentation

      Le système démarre automatiquement.

6) Définir les paramètres de base du système au sein de WBM après le démarrage
   a) Régler la date et l'heure du système
   b) Installer le pack d'application

      UC Smart pour système sans UC ou avec UC Smart

      UC Suite pour systèmes avec UC Suite

7) Restaurer la configuration du système
   a) Importer le fichier de licence nouvellement créé
   b) Restaurer la sauvegarde du système et, le cas échéant, la sauvegarde de Booster Server à l'aide de la fonction de restauration

25.4.2 Comment migrer vers des systèmes à licence permanente de carte mère V3 sans CLS Connect

Effectuez les étapes de la migration suivantes, dans l'ordre indiqué.

Étape par étape

1) Créer un "fichier de licence de migration" pour la carte mère V2 existante sur le serveur de licences central (CLS)
   a) Activer la "licence de migration matérielle" pour le système existant
   b) Générer un nouveau fichier de licence pour l'adresse MAC de la carte mère V2

      Pour cela, l'adresse MAC de la carte mère V3 doit être saisie.
   c) Télécharger le fichier de licence du CLS

2) Importer le fichier de licence dans le système OpenScape Business System avec la carte mère V2.

3) Noter le **code de confirmation** affiché dans l'OpenScape Business Assistant

4) Générer un nouveau fichier de licence pour la carte mère V3 sur le serveur de licences central (CLS)
   a) Créer un nouveau fichier de licence pour l'adresse MAC de la carte mère V3 au CLS en régénérant l'adresse MAC de la carte mère V2 et le code de confirmation précédemment noté.

      a) Rechercher le système OpenScape Business avec l'adresse MAC de la carte mère V3 dans le CLS.
      b) Déverrouiller le système OpenScape Business en saisissant et en activant le code de confirmation
      c) Régénérer le fichier de licence
   b) Télécharger le fichier de licence nouvellement généré à partir de CLS.

5) Sauvegarder la configuration du système et les données des clients.

6) Échanger les cartes mères
   a) Fermer le système et couper toutes les tensions d'alimentation
   b) Utiliser le support de données V3 et, si nécessaire, le stockage optionnel de données de masse sur la carte mère V3
   c) Retirer la carte OCCB Voice Channel Booster de la carte mère V2 et la brancher sur la carte mère V3.
   d) Remplacer la carte mère V2 par la carte mère V3 dans le système
   e) Rétablir la tension d'alimentation

      Le système démarre automatiquement.

7) Définir les paramètres de base du système au sein de WBM après le démarrage
   a) Régler la date et l'heure du système
   b) Installer le pack d'application

      UC Smart pour système sans UC ou avec UC Smart

      UC Suite pour systèmes avec UC Suite
8) Restaurer la configuration du système après le démarrage
   a) Restaurer la sauvegarde à l'aide de la fonction de restauration
9) Importer manuellement le nouveau fichier de licence dans le système V3 après le démarrage du système.

25.4.3 Comment migrer vers des systèmes de licence Carte mère V3 PayGo

Effectuez les étapes de la migration suivantes, dans l'ordre indiqué.

Étape par étape

1) Sauvegarder la configuration du système et les données des clients.
2) Régénérer le fichier de licence sur le serveur de licences central (CLS)
   a) Régénérer un nouveau fichier de licence pour l'adresse MAC de la carte mère V3

      Transférer les licences existantes de l'adresse MAC de la carte mère V2 vers l'adresse MAC de la carte mère V3.
   b) Télécharger le nouveau fichier de licence du CLS
3) Échanger les cartes mères
   a) Fermer le système et couper toutes les tensions d'alimentation
   b) Utiliser le support de données V3 et, si nécessaire, le stockage optionnel de données de masse sur la carte mère V3
   c) Retirer la carte OCCB Voice Channel Booster de la carte mère V2 et la brancher sur la carte mère V3.
   d) Remplacer la carte mère V2 par la carte mère V3 dans le système
   e) Rétablir la tension d'alimentation

      Le système démarre automatiquement.
4) Définir les paramètres de base du système au sein de WBM après le démarrage
   a) Régler la date et l'heure du système
   b) Installer le pack d'application

      UC Smart pour système sans UC ou avec UC Smart

      UC Suite pour systèmes avec UC Suite
5) Restaurer la configuration du système après le démarrage
   a) Restaurer la sauvegarde à l'aide de la fonction de restauration
6) Importer manuellement le nouveau fichier de licence dans le système V3 et activer le fichier de licence

25.5 Mise à niveau logicielle d'OpenScape Business S

Avant de procéder à une mise à niveau du logiciel système d'OpenScape Business S, déterminez la configuration actuelle du système et les composants matériels et logiciels et de licence qui doivent éventuellement être remplacés.

Tableau 34 : Migration OpenScape Business S - Liste de contrôle matérielle et logicielle

Composantes	Remplacé par
Composants matériels	
PC serveur	La réutilisation est possible. Les exigences en matière de matériel doivent être vérifiées pour les extensions d'Unify OpenScape Business S.[10]
Téléphones Optipoint 400	Téléphones OpenScape Deskphone CP
Composants logiciels	
Système d'exploitation SLES12	La réutilisation est possible. Une mise à niveau vers le dernier service pack peut être nécessaire.[11]
Logiciel système V2 sur carte SDHC	Logiciel système V3 (Image du serveur de téléchargement de logiciels)
Logiciel système V3 (Image du serveur de téléchargement de logiciels)	Logiciel système V3 (Image du serveur de téléchargement de logiciels)
myPortal Smart	myPortal @work
Composant de licence	

10 Le PC serveur existant peut être utilisé si la configuration du système UC Booster Server reste inchangée après la mise à niveau du logiciel. Si des extensions sont prévues après la mise à niveau du logiciel, il peut être nécessaire d'adapter les exigences matérielles conformément aux spécifications du *guide d'installation d'OpenScape Business S, chapitre Conditions préalables*.

11 Le système d'exploitation SLES installé sur le PC serveur peut être adopté en cas de mise à niveau du logiciel Unify OpenScape Business S / UC Booster Server. Toutefois, il doit être mis à niveau avec le dernier service pack publié avant la mise à niveau du logiciel.

Si Novell a interrompu le support logiciel pour la version SLES utilisée, le client doit en être informé et, si nécessaire, une mise à niveau du SLES doit être commercialisée.

La mise à niveau du SLES peut devoir être effectuée en plusieurs étapes pour reprendre les installations existantes d'OpenScape Business S, y compris la configuration et les données du client. Une clé de mise à jour SLES existante reste valable avec une mise à jour SLES. Toutefois, il se peut qu'il faille le désenregistrer auprès de Novell avant la mise à niveau SLES et le réenregistrer pour le nouveau système.

Ce qui suit décrit la mise à niveau du logiciel OpenScape Business tout en conservant le système d'exploitation SLES.

Composantes	Remplacé par
Licences dans le fichier de licence	Transfert des licences dans un nouveau fichier de licence
Application CSTA (via carte UC Booster / serveur)	Application CSTA (via carte UC Booster / serveur)

25.5.1 Mise à niveau logicielle d'OpenScape Business S V3 vers OpenScape Business S V4

Lors de la mise à niveau d'un modèle OpenScape Business S de la version logicielle V3 vers V4, seul le logiciel système est remplacé.

Les licences existantes et la configuration client sont conservées. L'assistance logicielle existante restera inchangée après la mise à niveau.

Dans ce cas, aucun poste de commande distinct n'est requis pour la mise à niveau du logiciel système de V3 vers V4.

Remarque : Il est recommandé de procéder d'abord à la mise à niveau vers la dernière version logicielle V3R4 FR3, puis vers V4.

Remarque : Il est recommandé de procéder d'abord à la mise à niveau vers SLES 15 SP7.

Copie d'évaluation de SUSE Linux Enterprise Server | SUSE

La mise à niveau logicielle d'OpenScape Business S V3 vers OpenScape Business S V4 peut être effectuée en exécutant la mise à niveau vers V4 via OpenScape Business Assistant.

25.5.2 Mise à niveau logicielle d'OpenScape Business S V2 vers OpenScape Business S V4

Une mise à niveau logicielle directe d'OpenScape Business S V2 vers OpenScape Business S V4 n'est pas prise en charge. Pour passer de V2 à V4, le système doit d'abord être mis à niveau vers V3.

Lors de la mise à niveau d'un modèle OpenScape Business S de la version logicielle V2 vers V3, seul le logiciel système est remplacé.

Procédure

Passez de V2 à V3 en suivant la procédure décrite dans Mise à niveau logicielle d'OpenScape Business S V2 vers OpenScape Business S V3 à la page 1331.

Après avoir terminé avec succès la mise à niveau vers OpenScape Business S V3, passez de V3 à V4 en suivant la procédure décrite dans Mise à niveau logicielle d'OpenScape Business S V3 vers OpenScape Business S V4 à la page 1330.

25.5.3 Mise à niveau logicielle d'OpenScape Business S V2 vers OpenScape Business S V3

Lors de la mise à niveau d'un modèle OpenScape Business S de la version V2 vers la version V3 du logiciel, seul le logiciel système est échangé.

Les licences existantes et la configuration du client sont reprises. L'assistance logicielle existante restera inchangée après la migration.

Dans ce cas, aucun poste de commande séparé n'est nécessaire pour la mise à niveau du logiciel système de V2 vers V3.

Que la version V3 de du logiciel ne supporte plus certaines fonctions et certains composants matériels. Dans Tableau 34 : Migration OpenScape Business S - Liste de contrôle matérielle et logicielle à la page 1329 vous trouverez des informations sur les composants qui sont substitués dans la version V3 et sur les composants qui sont omis sans substitution. Cela dépend de l'expansion du système du client.

Conditions requises

Le système fonctionne avec la dernière version logicielle V2R7 avant la mise à niveau. Si nécessaire, mettez le système à niveau vers la dernière version du logiciel. Pour ce faire, le système doit avoir un statut d'assistance logicielle valide.

Avant la mise à niveau du logiciel de la version V2 vers la version V3, installez un accès permanent au serveur de licence Unify (via Internet) dans le système et activez la fonction **CLS Connect**.

Conditions limites fonctionnelles et restrictions

Les licences existantes ne peuvent être reprises au cours de la mise à niveau du logiciel que si la fonction CLS Connect est activée.

La configuration du client et les données du client sont automatiquement transférées de la version V2 vers la version V3 du logiciel pendant le processus de mise à niveau du logiciel.

Les principales étapes techniques de la migration sont décrites dans les chapitres suivants. Afin de conserver les licences existantes, une distinction est faite entre le traitement :

- Mise à niveau du logiciel pour une licence permanente avec et sans CLS Connect
- Mise à niveau du logiciel avec la licence PayGo

Gestion technique de la mise à niveau

Les principales étapes techniques de la mise à niveau sont décrites ci-dessous. Une distinction est établie entre

- Mise à niveau pour une licence permanente avec CLS Connect
- Mise à niveau avec la licence PayGo

25.5.3.1 Comment passer à la version V3 des systèmes sous licence permanente avec CLS Connect

Effectuez les étapes de la migration suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business V2
   a) Mettre à niveau le système existant vers la version V2R7 du logiciel
   b) Configurer l'accès au serveur de licences central (CLS) dans le système et tester la connexion
   c) Activer CLS Connect dans le système V2

2) Préparer le système d'exploitation SLES

   Mettre à niveau le système d'exploitation vers le dernier Service Pack de la version SLES utilisée en relation avec OpenScape Business S.

3) Mettre à niveau le logiciel OpenScape Business.
   a) Exécuter la mise à niveau du logiciel vers V3 via OpenScape Business Assistant.
   b) La configuration du système est automatiquement transférée à V3.
   c) Les licences existantes sont transférées à V3.

4) Le fichier de licence est généré automatiquement par le serveur de licences central (CLS)
   a) Après le redémarrage du système, le système transfère l'information selon laquelle les licences existantes sont exploitées avec la version 3 du logiciel.
   b) Le serveur de licences génère automatiquement un nouveau fichier de licence avec les informations de la version V3 et le renvoie au système.

25.5.3.2 Comment passer à des systèmes sous licence V3 PayGo

Effectuez les étapes de la migration suivantes, dans l'ordre indiqué.

Étape par étape

1) Préparer le système OpenScape Business
   a) Mettre à niveau le système existant vers la version V2R7 du logiciel

2) Préparer le système d'exploitation SLES

   Mettre à niveau le système d'exploitation vers le dernier Service Pack de la version SLES utilisée en relation avec OpenScape Business S.

3) Régénérer le fichier de licence sur le serveur de licences central (CLS)
   a) Régénérer un nouveau fichier de licence pour le système V2
   b) Télécharger le nouveau fichier de licence du CLS

4) Importer et activer le nouveau fichier de licence dans le système OpenScape Business V2.

5) Mettre à niveau le logiciel OpenScape Business.
   a) Exécuter la mise à niveau du logiciel vers V3 via OpenScape Business Assistant.
   b) La configuration du système est automatiquement transférée à V3.
   c) Le système est prêt à fonctionner après le redémarrage.

25.5.4 Mise à niveau logicielle d'OpenScape Business S V2 vers OpenScape Business S V3

Pour faire évoluer un système OpenScape Business S V1 vers un système OpenScape Business S V2, il faut effectuer les étapes de la migration décrites ci-après.

Conditions requises

Avant la migration, il faut vérifier si les caractéristiques matérielles et logicielles du serveur Linux sont suffisantes pour OpenScape Business S V2. Il est parfois suffisant de mettre à niveau le serveur Linux (par ex. augmenter la capacité de la mémoire de travail). Le système d'exploitation Linux 64 bits SLES, qui a été publié pour OpenScape Business V2, est une condition préalable. Pour l'étape de mise à niveau vers la version V3 du logiciel OpenScape Business, la version SLES 64 qui a été publiée pour la version V3 est requise.

Si un nouveau serveur Linux est nécessaire, il faut, après l'installation de Linux, installer le logiciel de communication OpenScape Business S. Une sauvegarde des données V1 peut être reprise et vous pouvez ensuite continuer par l'étape 1 de la migration.

Conditions limites fonctionnelles et restrictions

Lorsqu'il est effectué une mise à jour de OpenScape Business V1 vers OpenScape Business V2, aucune activation/désactivation ITSP ne peut être effectuée dans l'assistant de téléphonie Internet tant qu'il n'a pas été effectué de réinitialisation de LCR. Les ITSP déjà configurés dans OpenScape Business V1 continuent à être opérationnels dans OpenScape Business V3 aussi, même sans réinitialisation de LCR. Il est possible de modifier l'ITSP déjà activé, mais pas de le désactiver. Pour pouvoir effectuer une modification d'activation/ désactivation dans l'assistant, il est nécessaire d'effectuer une réinitialisation LCR. Cela permet de réaliser les modifications nécessaires correspondant à l'augmentation du nombre d'ITSP de 4 à 8. Pour réinitialiser LCR, allez à **Mode Expert** > **LCR** > **Flags LCR** et cliquez sur le flag **Réinitialiser les données LCR**.

Procédure de mise à niveau

Effectuez les étapes de mise à niveau suivantes.

1) **Actualiser le logiciel OpenScape Business V1**

   Actualisez à l'aide de la WBM le logiciel OpenScape Business V1 vers la version V1 R3.3 ou ultérieure (voir Mise à jour du système de communication à la page 1193).

2) **Charger le fichier de licence OpenScape Business V2**

   Charger le fichier de licence OpenScape Business V2 dans le système OpenScape Business V1 et activer les licences (voir Activation des licences (Standalone) à la page 263).

   La licence des mises à jour gratuites SLES peut continuer à être utilisée.

3) **Charger le logiciel OS Biz V2 actuel**

   Chargez à l'aide de la WBM le logiciel actuel OpenScape Business V2 dans le système de communication. Les données V1 sont dans ce cadre automatiquement converties en données V3 (voir Mise à jour du système de communication à la page 1193).

4) Réaliser la sauvegarde des données

Sauvegardez vos données V2 (voir Sauvegarde immédiate à la page 1186).

25.6 Migration/mise à niveau du réseau OpenScape Business V2 vers V3

Lors de la migration ou de la mise à niveau d'un réseau OpenScape Business vers la version V3, tous les nœuds du réseau doivent être mis à niveau vers la version V3 du logiciel. Pour les fonctions de mise en réseau, il importe peu que la version V3 du logiciel soit exploitée sur un système OpenScape Business X en réseau avec une carte mère V2 ou V3.

Mettez à niveau chaque nœud OpenScape Business du réseau séparément. Les composants requis pour une mise à niveau doivent être déterminés par nœud en fonction des systèmes individuels, conformément aux descriptions des chapitres Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313, Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316, Migration matérielle et logicielle des systèmes OpenScape Business X vers V3 à la page 1318 ou Migration d'un système OpenScape Business X V3 de la carte mère V2 vers la carte mère V3 à la page 1324.

Les licences pour les nœuds du réseau V2 peuvent être transférées aux systèmes V3 via le serveur de licences central. Il existe différentes procédures pour les systèmes avec ou sans fonction **CLS Connect** . La procédure de licence ""Pay as yo go"" n'est pas prise en charge par le réseau OpenScape Business.

L'effort requis pour le transfert de licences avec **CLS Connect** est nettement moins important dans un réseau que sans la fonction CLS Connect.

Important : Mise à niveau des nœuds d'un réseau dans l'ordre décrit pour chaque scénario. Il est essentiel que tous les nœuds esclaves fonctionnent avec la version logicielle V3 avant que le nœud maître puisse être migré ou mis à niveau vers la version logicielle V3.

Pendant la mise à niveau du réseau, un réseau hétérogène avec les logiciels V2 et V3 sera mis en place pendant une période transitoire. Pendant cette période, la pleine fonctionnalité de la gamme de performances du réseau ne peut être garantie. Dans certains scénarios, les systèmes mis à niveau/migrés fonctionneront en mode d'urgence uniquement jusqu'à ce que le fichier de licence soit mis à jour par le nœud maître.

Les réseaux OpenScape Business peuvent être réalisés selon diverses combinaisons concernant l'utilisation des systèmes OpenScape Business X et S et la concession de licences pour les systèmes du réseau. Les étapes les plus importantes de la migration ou de la mise à niveau d'un réseau OpenScape Business et leur séquence sont illustrées au moyen de combinaisons types.

La description suppose toujours qu'un fichier de licence de réseau existe dans le serveur de licences central pour le réseau, au moyen duquel le nœud maître fournit à tous les nœuds esclaves des informations de licence.

- **Réseau composé uniquement de systèmes OpenScape Business X**
  - Scénario 1 : Migration matérielle uniquement dans le nœud maître, mise à niveau du logiciel dans tous les nœuds esclaves
  - Scénario 2 : Mise à niveau du logiciel de tous les nœuds OpenScape Business X du réseau
- **Réseau composé de systèmes OpenScape Business S et OpenScape Business X**
  - Scénario 3 : OpenScape Business S est un nœud maître et les systèmes OpenScape Business X sont des nœuds esclaves
    - Scénario 3a : Mise à niveau du logiciel de tous les nœuds OpenScape Business du réseau
    - Scénario 3b : Mise à niveau du logiciel dans le nœud maître d'OpenScape Business S, migration des nœuds esclaves

25.6.1 Scénario 1 : Migration matérielle du nœud maître, mise à niveau logicielle des nœuds esclaves

Lors de la migration du réseau, il convient de distinguer la fonction **CLS Connect** de la procédure de transfert de licence.

25.6.1.1 Migration/mise à niveau avec CLS Connect dans le nœud maître

Conditions préalables

- Tous les nœuds du réseau fonctionnent avec la dernière version V2R7.x du logiciel.
- Le serveur de licences central (CLS) contient un fichier de licence de réseau central pour le nœud maître du réseau.
- La fonction **CLS Connect** est activée dans le nœud maître. CLS Connect n'a pas besoin d'être activé dans les nœuds esclaves.

Étape par étape

1) Mettez à niveau tous les nœuds esclaves vers la version V3 du logiciel (pour plus de détails, voir Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313 ou Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316)

a) Importez le logiciel V3 via OpenScape Business Assistant (WBM) et mettez le système à niveau.

b) Les informations relatives à la configuration et aux licences sont conservées.

Le système n'est pas opérationnel après le démarrage, en raison d'un fichier de licence non valide.

2) Générez un nouveau fichier de licence réseau sur le serveur de licences.

a) Régénérez le fichier de licence réseau pour le nœud maître à l'adresse MAC de la carte mère V3

b) Téléchargez le nouveau fichier de licence de réseau à partir du CLS

3) Migrez le nœud maître vers la carte mère V3 (pour plus de détails, voir Migration matérielle et logicielle des systèmes OpenScape Business X vers V3 à la page 1318)
   a) Sauvegardez la configuration du système via WBM
   b) Échangez la carte mère
   c) Réglez la date/heure et le pack d'application via WBM
   d) Importez et activez le nouveau fichier de licence réseau via WBM.
   e) Restaurez la configuration du système via WBM

   Le fichier de licence n'est pas écrasé dans ce cas.
4) Le nœud maître transfère automatiquement les nouvelles informations de licence aux nœuds esclaves.

Remarque : Cette transmission des licences aux nœuds esclaves peut prendre jusqu'à 15 minutes.

25.6.1.2 Migration/mise à niveau sans CLS Connect dans le nœud maître

Conditions préalables

- Tous les nœuds du réseau fonctionnent avec la dernière version V2R7.x du logiciel.
- Le serveur de licences central (CLS) contient un fichier de licence de réseau central pour le nœud maître du réseau.
- La licence de migration de matériel pour le nœud maître est disponible
- Des licences de mise à niveau logicielle sont disponibles pour chaque nœud esclave

Étape par étape

1) Générez un nouveau fichier de licence réseau sur le serveur de licences
   a) Décomposez le fichier de réseau au CLS en fichiers de licence individuels
   b) Générez un fichier de licence pour le nœud maître

      Activez la licence de migration du matériel pour le nœud maître
   c) Générez un fichier de licence pour les nœuds esclaves

      Activez la licence de mise à jour du logiciel pour chaque nœud esclave individuel
   d) Fusionnez les fichiers de licence des nœuds individuels en un nouveau fichier de licence de réseau
   e) Téléchargez le nouveau fichier de licence de réseau à partir du CLS
2) Mettez à niveau les nœuds esclaves vers V3 (pour plus de détails, voir Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313 ou Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316)
   a) Importez le logiciel V3 via OpenScape Business Assistant (WBM) et mettez le système à niveau.
   b) Les informations relatives à la configuration et à la licence sont automatiquement transférées.

   Le système n'est pas opérationnel après le démarrage, en raison d'un fichier de licence non valide.

3) Migrez le nœud maître vers V3 (pour plus de détails, voir Migration matérielle et logicielle des systèmes OpenScape Business X vers V3 à la page 1318)
   a) Sauvegardez la configuration du système via WBM
   b) Échangez la carte mère
   c) Réglez la date/heure et le pack d'application via WBM
   d) Importez et activez le nouveau fichier de licence réseau via WBM.
   e) Restaurez la configuration du système via WBM (le fichier de licence n'est pas écrasé dans ce cas)
4) Le nœud maître transfère automatiquement les nouvelles informations de licence aux nœuds esclaves.

Remarque : Cette transmission des licences aux nœuds esclaves peut prendre jusqu'à 15 minutes.

25.6.2 Scénario 2 : Mise à niveau logicielle de tous les systèmes du réseau vers la version 3

Lors de la mise à jour du logiciel de réseau, l'utilisation de la fonction **CLS Connect** ou non définit la procédure à suivre pour le transfert de la licence.

25.6.2.1 Mise à jour du logiciel avec CLS Connect dans le nœud maître

Conditions préalables

- Tous les nœuds du réseau fonctionnent avec la dernière version V2R7.x du logiciel.
- Le serveur de licences central (CLS) contient un fichier de licence de réseau central pour le nœud maître du réseau.
- La fonction **CLS Connect** est activée dans le nœud maître. CLS Connect n'a pas besoin d'être activé dans les nœuds esclaves.

Étape par étape

1) Migrez tous les nœuds esclaves vers la version V3 du logiciel (pour plus de détails, voir Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313 ou Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316)
   a) Importez le logiciel V3 via OpenScape Business Assistant (WBM) et mettez le système à niveau.
   b) Les informations relatives à la configuration et aux licences sont conservées.

   Le système n'est pas opérationnel après le démarrage, en raison d'un fichier de licence non valide.
2) Mettez à niveau le nœud maître vers V3 (pour plus de détails, voir Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313 ou Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316
   a) Importez le logiciel V3 via OpenScape Business Assistant (WBM) et mettez le système à niveau.

b) Les informations relatives à la configuration et à la licence sont conservées.
c) Redémarrez le système.

3) Les étapes suivantes sont automatiques (aucune intervention manuelle n'est nécessaire)
a) Le nœud maître informe le CLS après le démarrage avec la version 3 du logiciel.
b) Le CLS génère un nouveau fichier de licence réseau.
c) Le CLS transfère le nouveau fichier de licence de réseau au nœud maître.
d) Le nœud maître transmet automatiquement les informations relatives à la nouvelle licence aux nœuds esclaves.

Remarque : Cette transmission des licences aux nœuds esclaves peut prendre jusqu'à 15 minutes.

25.6.2.2 Mise à jour du logiciel sans CLS Connect dans le nœud maître

Conditions préalables

- Tous les nœuds du réseau fonctionnent avec la dernière version V2R7.x du logiciel.
- Le serveur de licences central (CLS) contient un fichier de licence de réseau central pour le nœud maître du réseau.
- Des licences de mise à niveau logicielle sont disponibles pour chaque nœud

Étape par étape

1) Générez de nouveaux fichiers de licence réseau sur le serveur de licences
a) Décomposez le fichier de réseau au CLS en fichiers de licence individuels
b) Générez un fichier de licence pour le nœud maître
Activez la licence de mise à jour du logiciel pour le nœud maître
c) Générez un fichier de licence pour les nœuds esclaves
Activez la licence de mise à jour du logiciel pour chaque nœud esclave individuel
d) Fusionnez les fichiers de licence des nœuds individuels en un nouveau fichier de licence de réseau
e) Téléchargez le nouveau fichier de licence de réseau à partir du CLS

2) Migrez tous les nœuds esclaves vers la V3 (pour plus de détails, voir Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313 ou Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316)
a) Importez le logiciel V3 via OpenScape Business Assistant (WBM) et mettez le système à niveau.
b) Les informations relatives à la configuration et à la licence sont conservées.
c) Le système n'est pas prêt à fonctionner après le démarrage, en raison d'un fichier de licence non valide.

Le système n'est pas opérationnel après le démarrage, en raison d'un fichier de licence non valide.

3) Mettez à niveau le nœud maître vers V3 (pour plus de détails, voir Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313 ou Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316
   a) Importez le logiciel V3 via OpenScape Business Assistant (WBM) et mettez le système à niveau.
   b) Les informations relatives à la configuration et à la licence sont conservées.
   c) Importez le fichier de licence du réseau dans le nœud maître et activer le fichier de licence
4) Le nœud maître transfère automatiquement les nouvelles informations de licence aux nœuds esclaves.

Remarque : Cette transmission des licences aux nœuds esclaves peut prendre jusqu'à 15 minutes.

25.6.3 Scénario 3a : Mise à niveau logicielle de tous les nœuds

Dans ce scénario, le nœud maître est un système OpenScape Business S, et les nœuds esclaves sont des systèmes OpenScape Business X.

Ce scénario est identique à celui de Scénario 2 : Mise à niveau logicielle de tous les systèmes du réseau vers la version 3 à la page 1337

25.6.4 Scénario 3b : Mise à niveau logicielle dans le nœud maître, migration du matériel dans les nœuds esclaves

Dans ce scénario, les nœuds esclaves sont migrés vers la carte mère V3 et la version 3 du logiciel par un échange matériel/logiciel. Dans le système maître OpenScape Business S, le logiciel est mis à niveau de V2 vers V3. Pour la mise à niveau matérielle et logicielle du réseau, l'utilisation de la fonction CLS Connect définit la procédure de transfert de licence.

25.6.4.1 Migration / Mise à niveau avec CLS Connect dans le nœud maître

Conditions préalables

- Tous les nœuds du réseau fonctionnent avec la dernière version V2R7.x du logiciel.
- Le serveur de licences central (CLS) contient un fichier de licence de réseau central pour le nœud maître du réseau.
- La fonction **CLS Connect** est activée dans le nœud maître. CLS Connect n'a pas besoin d'être activé dans les nœuds esclaves.
- Les cartes mères V3, avec le logiciel V3, sont disponibles

Étape par étape

1) Migrez tous les nœuds esclaves vers la carte mère V3 (pour plus de détails, voir Migration matérielle et logicielle des systèmes OpenScape Business X vers V3 à la page 1318)
   a) Sauvegardez la configuration du système via WBM
   b) Remplacez les cartes mères
   c) Réglez la date/heure et le pack d'application via WBM
   d) Restaurez la configuration du système via WBM

   Le système n'est pas opérationnel après le démarrage, en raison d'un fichier de licence non valide.
2) Mettez à niveau le nœud maître vers V3 (pour plus de détails, voir Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313 ou Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316
   a) Importez le logiciel V3 via OpenScape Business Assistant (WBM) et mettez le système à niveau.
   b) Les informations relatives à la configuration et à la licence sont conservées.
   c) Redémarrez le système.
3) Les étapes suivantes sont automatiques (aucune intervention manuelle n'est nécessaire)
   a) Le nœud maître informe le CLS après le démarrage avec la version 3 du logiciel.
   b) Le CLS génère un nouveau fichier de licence réseau.
   c) Le CLS transfère le nouveau fichier de licence de réseau au nœud maître.
   d) Le nœud maître transmet automatiquement les informations relatives à la nouvelle licence aux nœuds esclaves.

Remarque : Cette transmission des licences aux nœuds esclaves peut prendre jusqu'à 15 minutes.

25.6.4.2 Migration / Mise à jour sans CLS Connect dans le nœud maître

Conditions préalables

- Tous les nœuds du réseau fonctionnent avec la dernière version V2R7.x du logiciel.
- Le serveur de licences central (CLS) contient un fichier de licence de réseau central pour le nœud maître du réseau.
- La licence de mise à jour du logiciel pour le nœud maître est disponible
- Des licences de migration matérielle sont disponibles pour chaque nœud esclave
- Les cartes mères V3, avec le logiciel V3, sont disponibles

Étape par étape

1) Générez un nouveau fichier de licence réseau sur le serveur de licence

a) Décomposez le fichier de réseau au CLS en fichiers de licence individuels

b) Générez un fichier de licence pour le nœud maître

Activez la licence de mise à jour du logiciel pour le nœud maître

c) Générez un fichier de licence pour les nœuds esclaves

Activez la licence de migration du matériel pour chaque nœud esclave

d) Fusionnez les fichiers de licence des nœuds individuels en un nouveau fichier de licence de réseau

e) Téléchargez le nouveau fichier de licence de réseau à partir du CLS

2) Migrez tous les nœuds esclaves vers la carte mère V3 (pour plus de détails, voir Migration matérielle et logicielle des systèmes OpenScape Business X vers V3 à la page 1318)

a) Sauvegardez la configuration du système via WBM

b) Remplacez les cartes mères

c) Réglez la date/heure et le pack d'application via WBM

d) Restaurez la configuration du système via WBM

Le système n'est pas opérationnel après le démarrage, en raison d'un fichier de licence non valide.

3) Mettez à niveau le nœud maître vers V3 (pour plus de détails, voir Mise à niveau logicielle pour les systèmes OpenScape Business X à la page 1313 ou Mise à niveau logicielle de UC Booster Server vers OpenScape Business X V3 à la page 1316

a) Importez le logiciel V3 via OpenScape Business Assistant (WBM) et mettez le système à niveau.

b) Les informations relatives à la configuration et à la licence sont conservées.

c) Importez le fichier de licence du réseau dans le nœud maître et activer le fichier de licence

4) Le nœud maître transfère automatiquement les nouvelles informations de licence aux nœuds esclaves.

Remarque : Cette transmission des licences aux nœuds esclaves peut prendre jusqu'à 15 minutes.

25.7 Migration de HiPath 3000 vers OpenScape Business V4

Cette section décrit la migration technique des systèmes autonomes HiPath 3000 / HiPath 500 V9 et des réseaux HiPath 3000 vers OpenScape Business V4 avec cartes mères V3.

Lors de la migration des systèmes HiPath 3000 vers OpenScape Business X V4 avec cartes mères V3, en fonction de la configuration matérielle, une partie des équipements matériels du système et des terminaux/clients connectés peuvent être transférés.

Avant de migrer un HiPath 3000, la configuration système actuelle et les composants matériels/logiciels ainsi que les licences à remplacer, le cas échéant, doivent être déterminés par des vérifications ultérieures.

Contrôles généraux

- **vérification de compatibilité fonctionnelle**

  Veuillez vous renseigner sur les fonctionnalités qui ne sont plus prises en charge ou qui ont changé par rapport à HiPath 3000 V9. Chapitre Fonctionnalités et interfaces modifiées/supprimées du HiPath 3000 à la page 1361 Cette liste répertorie les fonctionnalités HiPath 3000 qui ne sont plus prises en charge dans OpenScape Business ou qui ont été remplacées par des fonctionnalités plus récentes.
- **vérification de la version du logiciel**

  Le système doit fonctionner sous la version logicielle V9 avant la migration. Les systèmes dont la version du logiciel est inférieure à V9 doivent être mis à niveau vers la version V9 et mis en service avant la migration.
- **vérification de la mise à la terre de protection**

  Pour tous les systèmes de communication OpenScape Business X, une mise à la terre de protection via un conducteur de terre supplémentaire est obligatoire !

vérification de compatibilité matérielle

Pour des raisons techniques, certains modules et périphériques ne peuvent pas être utilisés dans les systèmes OpenScape Business X. Lors de la migration de HiPath 3000 V9 vers OpenScape Business V4, ces modules et terminaux doivent être supprimés. Si nécessaire, utilisez plutôt les types successeurs respectifs. La liste des modules qui ne sont plus pris en charge et de leurs successeurs se trouve dans la *documentation de service Unify OpenScape Business X5/X8* dans la zone *Composants HW non pris en charge*.

- **Alimentation**

  OpenScape Business 33xx / 35xx peut être utilisé avec une alimentation UPSC-D / DR ou OCPSM. Toute alimentation restante doit être remplacée par une alimentation OCPSM. Des kits de mise à niveau d'alimentation compatibles sont disponibles.
- **Composants périphériques**

  Veuillez vérifier si le matériel existant peut encore être utilisé. Les modules ou périphériques finaux qui ne sont plus pris en charge doivent être retirés et remplacés, le cas échéant, par leurs successeurs.
- **vérification du fond de panier**

  Dans les systèmes HiPath 3550, l'emplacement 10 du fond de panier n'est plus adressé par la carte mère V3. Les modules périphériques existants qui utilisent cet emplacement ne peuvent pas être utilisés dans OpenScape Business.
- **vérification de l'appareil téléphonique**

  Les systèmes OpenScape Business V4 avec cartes mères V3 prennent en charge les périphériques analogiques, ISDN, SIP et OpenStage ou OpenScape Deskphone IP / CP. Les appareils Optiset E, Optipoint 4xx et Optipoint 5xx existants doivent être remplacés.
- **Vérification du logement**

  Dans les systèmes HiPath 33xx/35xx migrés, les capuchons du boîtier peuvent devoir être remplacés et des unités de ventilation installées si nécessaire.

  Des articles de livraison correspondants sont disponibles.

Autres vérifications

- **Plan de numérotation des appels pour les systèmes en réseau**

  Avec les réseaux vocaux purs, la numérotation ouverte et fermée est possible. Lors de l'utilisation de UC Suite, une numérotation fermée est requise sur le réseau (fonctionnalité UC à l'échelle du réseau).

25.7.1 Migration des systèmes HiPath 33xx, 35xx et 3800 vers OpenScape Business X5/X8 V4

Lors de la migration d'un système HiPath 33xx, 35xx ou 3800 vers OpenScape Business X V4, la carte mère, les groupes de périphériques et les terminaux déterminés ainsi que le logiciel système sont remplacés. Les licences existantes peuvent être migrées grâce à une licence de mise à niveau. La configuration du système peut être transférée. Après la migration, le système OpenScape Business V4 bénéficie d'un support logiciel de 3 ans.

Pour la migration de HiPath 3000 V9 vers OpenScape Business V4, les éléments suivants sont en principe requis :

- Carte mère V3
- Logiciel V4 sur stockage de données SSD
- SSD M2 de 256 Go pour le stockage de données de masse (en option avec l'application UC Suite)
- Mise à niveau d'OpenScape Business HiPath 3000 V9 (migration de licence), ou
- Mise à niveau d'OpenScape Business HiPath 3000 V8 (migration de licence), ou
- Mise à niveau d'OpenScape Business HiPath 3000 V7 (migration de licence)
- Licence OpenScape Business CSTA (facultative)

Si nécessaire, des composants matériels et des licences supplémentaires doivent être commandés en sus. Cela dépend de la configuration du système du client.

Dans la *Documentation de maintenance d'Unify OpenScape Business X5/X8*, zone *Composants matériels non pris en charge*, vous trouverez des informations sur les composants remplacés dans la version V4 ou abandonnés sans remplacement. Veuillez noter qu'une licence CSTA est requise pour une connexion existante à des applications CSTA externes. Ceci ne s'applique pas à la connexion d'OpenScape Business TAPI 170 ou TAPI 120.

Prérequis

Tous les composants matériels et logiciels ont été vérifiés en vue de leur réutilisation.

Tous les nouveaux composants matériels et logiciels sont disponibles.

Une licence de mise à niveau pour passer de HiPath 3000 V7, V8 ou V9 à OpenScape Business V4 a été commandée et le LAC de la licence de mise à niveau est disponible pour récupérer la nouvelle licence auprès du serveur de licences.

Le système a été mis à jour vers la dernière version logicielle V9 pour la migration technique du logiciel et le transfert de la configuration client existante.

La dernière version du logiciel Manager E est utilisée.

Détermination des licences OpenScape Business lors de la migration

Les licences existant dans les systèmes HiPath 3000 peuvent être transférées vers le système Unify OpenScape Business V4 en activant la licence “Unify OpenScape Business Upgrade HiPath 3000 (V7, V8 ou V9)” dans le serveur de licences central. Lors du transfert de licence, un nouveau fichier de licence pour le système OpenScape Business V3 / V4 est créé avec les licences suivantes.

Tableau 35 : Migration de licence HiPath 3000

Licence HP 3000	Licence commerciale OpenScape	Remarques
	Licence de base	Nouvelle formule incluant 3 ans de support logiciel
	Licence de base OpenDirectory	Nouvellement créé
	Licence utilisateur TDM	Nombre calculé à partir de la configuration du système[12]
Abonné IP (ComScendo)	Licence d'utilisateur de propriété intellectuelle	Transfert 1:1 à partir du fichier de licence HP 3000
	Gestionnaire de licences utilisateur TDM	calculé à partir de la configuration du système[12]
Chaînes S2M	Licences de jonction IP/ S2M/TI	Transfert 1:1 à partir du fichier de licence HP 3000
Entrée mobilité	Licences utilisateur pour la mobilité	Transfert 1:1 à partir du fichier de licence HP 3000

Détermination des licences utilisateur TDM dans le fichier de licence

Lors de la conversion technique de la configuration du système HiPath 3000, le nombre d'abonnés TDM actifs est déterminé par l'outil Manager E et enregistré dans un fichier « inventaire (XML) ».

Le nombre de licences utilisateur TDM est déterminé comme suit :

- 1 licence utilisateur TDM par port UP0 actif - téléphone (maître/esclave) prêt, numéro de téléphone disponible
- 1 licence utilisateur TDM par téléphone DECT enregistré - numéro de téléphone disponible
- 1 licence utilisateur TDM par port a/b actif (numéro de téléphone) pour les modules connectés
- 1 licence utilisateur TDM par port S0 actif (numéro de téléphone MSN) pour les modules actifs

12 Déterminé au cours de la description de la conversion technique (voir ci-dessous).

La migration des licences utilisateur TDM elle-même est effectuée hors ligne sur le CLS via le fichier d'inventaire XML.

Le serveur de licences central vérifie si un fichier de licence existe pour l'adresse MAC de la carte mère HiPath 3000.

Si un fichier de licence est disponible, la migration de licence est effectuée sur la base de ce fichier de licence et des informations contenues dans le « fichier d'inventaire ».

Si aucun fichier de licence n'est disponible, la mise à niveau d'OpenScape Business est effectuée sur la base des informations contenues dans le fichier « Inventaire (XML) ».

En fonction de la licence de mise à niveau disponible (V7, V8 ou V9), le pourcentage suivant des utilisateurs TDM déterminés est transféré vers OpenScape Business.

- Mettez à niveau votre version HiPath 3000 V4 ou antérieure vers OpenScape Business V4 :

  Aucun utilisateur TDM n'est pris en compte pour les licences de mise à niveau OpenScape Business à prix réduit ou gratuites.
- Mise à niveau depuis HiPath 3000 V5, V6 ou V7 vers OpenScape Business V4 :

  On estime que 70 % des utilisateurs de TDM bénéficieraient de licences de mise à niveau OpenScape Business moins chères, voire gratuites.
- Mise à niveau de HiPath 3000 V8 vers OpenScape Business V4 :

  On estime que 80 % des utilisateurs de TDM bénéficieraient de licences de mise à niveau OpenScape Business moins chères, voire gratuites.
- Mise à niveau depuis HiPath 3000 V9 OpenScape Business V4 :

  100 % des utilisateurs de TDM sont éligibles à des licences de mise à niveau OpenScape Business moins chères ou gratuites.

Conditions aux limites fonctionnelles et restrictions

- La migration de licence ne peut être effectuée que vers les versions V3 et V4. La migration de licence vers la version 2 n'est pas prise en charge par Manager E.
- La migration de licence d'un système HiPath 3000 (carte mère) ne peut être effectuée qu'une seule fois, et la carte mère est bloquée pour toute action ultérieure au niveau du CLS après la migration.
- Pour migrer les lignes S2M et les abonnés ComScendo, un fichier de licence HiPath 3000 doit être disponible sur le serveur de licences central.
- Les licences utilisateur TDM générées lors de la migration ne peuvent pas être transférées vers d'autres systèmes ou vers un compte CLS.
- Les licences utilisateur et les licences UC orientées utilisateur sont attribuées de manière permanente aux abonnés d'OpenScape Business. Veuillez noter que le nombre de licences disponibles est suffisant pour les utilisateurs de myAgent et de myAttendant. Dans OpenScape Business, les modifications du statut de présence d'autres utilisateurs effectuées par les utilisateurs de myAgent sont liées à la licence myAttendant. Ces articles doivent être commandés séparément.
- La fonctionnalité Deskshare User (mobilité IP) nécessite une licence dans OpenScape Business, contrairement à HiPath 3000. Des licences utilisateur IP supplémentaires doivent être disponibles et attribuées aux « Utilisateurs

Deskshare » dans la boîte de dialogue de licences de l'Assistant d'affaires OpenScape.

- Aucune migration de licence n'est effectuée pour les produits et fonctionnalités suivants :
  - Canaux B du HG1500 : La carte est abandonnée, car la fonctionnalité est intégrée sur la nouvelle carte mère.
  - optiClient Attendant V8 : ne fonctionne pas sur OpenScape Business.

    Produit complémentaire : OpenScape Business Attendant
  - optiClient BLF V1/V2 : ne fonctionne pas sur OpenScape Business.

    Produit complémentaire : OpenScape Business BLF
  - HiPath TAPI 120/170 V2 : ne fonctionne pas sur OpenScape Business.

    Produit complémentaire : OpenScape Business TAPI 120/170
  - Messagerie vocale d'entrée : ce module est supprimé, car il est intégré à la nouvelle carte mère.

    Produit complémentaire : Messagerie vocale intelligente
  - Clients de communication des services Web de myPortal connectés au PC.
  - Stations de base : les licences pour les stations de base ne sont plus requises.
  - Accès aux lignes ITSP : des licences doivent être achetées pour utiliser les canaux ITSP pour la téléphonie sur Internet dans OpenScape Business.
  - Comme par le passé, aucune licence n'est requise pour les liaisons S0, analogiques et CAS.
  - Pour la mise en réseau et la connexion de systèmes externes via des lignes de liaison, une licence réseau par nœud doit être achetée dans OpenScape Business.

manutention technique

Effectuez les étapes de migration suivantes dans l'ordre :

1) **Téléchargez la base de données client (CDB) HiPath 3000 depuis le système.**

   Téléchargez la CDB HiPath 3000 actuelle à partir du système HiPath 3000 en utilisant la dernière version de Manager E.
2) **Enregistrez les paramètres du HG1500 (facultatif)**

   Si une ou plusieurs cartes HG1500 sont branchées, vous devez noter les paramètres HG1500 qui ont été modifiés par rapport aux paramètres par défaut à l'aide du WBM HG1500 :

   - Routage IP
   - Routage PSTN
   - Pare-feu IP
   - Pare-feu MAC
   - Pare-feu applicatif
   - Comptabilité de la propriété intellectuelle
   - Cartographie IP
   - SNMP

3) **Convertir la base de données HiPath 3000**

   Convertissez la base de données HiPath 3000 actuelle en base de données OpenScape Business V4 en utilisant la dernière version de Manager E.

4) **Remplacez le matériel**

   Remplacez l'ancienne carte mère HiPath 3000 par la nouvelle carte mère OpenScape Business V3. Retirez toutes les cartes HG1500 ainsi que toutes les cartes et sous-cartes qui ne sont plus prises en charge. Tous les systèmes de communication OpenScape Business doivent être mis à la terre à l'aide d'un fil de terre supplémentaire.

5) **Effectuez l'installation initiale**

   Configurez le système de communication via le WBM à l'aide de l'assistant **d'installation initiale** . Notez que les paramètres HG1500 que vous avez enregistrés précédemment doivent également être pris en compte ici.

6) **Charger la base de données CDB convertie**

   Chargez le fichier CDB converti dans le système OpenScape Business V2 à l'aide de la dernière version de Manager E. Le système OpenScape Business redémarrera ensuite automatiquement.

7) **Générez un nouveau fichier de licence sur le CLS**

   Générez un nouveau fichier de licence sur le CLS avec le LAC de la licence de mise à niveau, le fichier de configuration (fichier XML) et l'ID de verrouillage d'OpenScape Business.

8) **Activer et attribuer des licences**

   Obtenez une licence pour le système de communication OpenScape Business dans les 30 jours grâce au fichier de licence.

9) **Réinitialiser les entrées LCR**

   Si nécessaire, vous pouvez réinitialiser les entrées LCR configurées dans le système HiPath 3000 (par exemple, les plans de numérotation, les tables de routage, les règles de numérotation) aux entrées par défaut d'OpenScape Business. Ce paramètre se trouve dans le WBM, dans l'assistant **d'installation de base** .

25.7.1.1 Comment charger KDS à partir de HiPath 3000

Conditions préalables

Un système de communication HiPath 3000 (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 ou HiPath 3800) est disponible.

Tous les téléphones sont raccordés et actifs.

Le Manager E le plus récent est installé sur le PC Admin.

Le PC Admin est relié au système de communication HiPath 3000.

Étape par étape

1) Ouvrez une session sur le PC Admin de Manager E.
2) Dans la barre de menu, cliquez sur **Fichier** > **Transférer**.
3) Cliquez sur l'onglet **Communications**.
4) Dans la zone **Accès**, activez l'option correspondante, en fonction du type de connexion du PC Admin au système de communication.
5) Activez le bouton **lecture/écriture KDS** et cliquez sur **Système** > **PC**.

6) Cliquez sur **OK**. Le KDS est transféré de HiPath 3000 vers Manager E.
7) Une fois la transmission effectuée, cliquez sur **OK** puis sur **Fermer**.
8) Dans la barre de menu, cliquez sur **Fichier** > **Sauvegarder KDS**, puis sauvegardez le KDS sur le PC Admin dans un répertoire de votre choix.

Étapes suivantes

Comment lire les paramètres HG1500 à la page 1348

25.7.1.2 Comment lire les paramètres HG1500

Conditions préalables

Un ou plusieurs modules HG1500 sont insérés.

Vous êtes connecté à Manager E.

Étape par étape

1) Dans Manager E, dans la vue de l'installation, cliquez sur l'entrée de HG1500. La WBM de la HG1500 s'ouvre.
2) Notez les paramètres qui ont été modifiés par rapport aux paramètres par défaut. Les paramtères HG1500 ne sont pas repris lors de la conversion du KDS ; ils doivent donc être de nouveau configurés dans la WBM lors de la première mise en service de OpenScape Business.

Étapes suivantes

Comment convertir la KDS HiPath 3000 V9 à la page 1348

25.7.1.3 Comment convertir la KDS HiPath 3000 V9

Conditions préalables

Un système de communication HiPath 3000 (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 ou HiPath 3800) est disponible.

Le PC Admin est relié au système de communication HiPath 3000.

Étape par étape

1) Dans la barre de menu, cliquez sur **Fichier** > **Convertir base de données client**.
2) Sélectionnez le KDS enregistré précédemment sur PC Admin et cliquez sur **OK**.
3) Entrez votre **Nom** et votre **Numéro de contrat** en tant que données client et cliquez sur **Suivant**.
4) Sélectionnez **OpenScape Business V2** comme **Version** et cliquez sur **Suivant**.
5) Confirmez les remarques concernant les modules qui ne sont plus pris en charge en cliquant sur **OK**.
6) Cliquez sur **Oui** pour confirmer la fenêtre qui vous informe du nombre d'utilisateurs TDM pour effectuer la migration et procéder à la migration.

   Le nombre d'utilisateurs TDM qui effectueront la migration est calculé automatiquement

7) Confirmez l'affichage des modules insérés en cliquant sur **Suivant**.
8) Dans la barre de menu, cliquez sur **Fichier** > **Sauvegarder KDS**, puis sauvegardez le KDS sous un autre nom sur le PC Admin dans un répertoire de votre choix.
9) Fermez Manager E.

Étapes suivantes

Comment remplacer le matériel HiPath 3300/3500 à la page 1349 ou

Comment remplacer le matériel dans HiPath 3350/3550 ou

Comment remplacer le matériel du HiPath 3800 à la page 1350

25.7.1.4 Comment remplacer le matériel HiPath 3300/3500

Conditions préalables

Un système de communication HiPath 3000 (HiPath 3300 ou HiPath 3500, montage en rack) est opérationnel.

Carte mère OpenScape Business V3 (OCCMRA ou OCCMRB).

Avertissement :

Risque de choc électrique par contact avec des fils électriques sous tension

Assurez-vous qu'un fil de terre de protection séparé avec la section minimale requise soit disponible pour le système de communication (voir la documentation de service, Installation matérielle).

Étape par étape

1) Éteignez le système HiPath 3000 et débranchez sa prise d'alimentation.
2) Débranchez tous les connecteurs (tels que les stations analogiques, les lignes RNIS, etc.) de la carte mère.
3) Desserrez les deux vis de verrouillage du panneau avant de la carte mère.
4) Détachez la carte mère du fond de panier à l'aide de deux clés à carte (C39165-A7027-C26).
5) En utilisant les deux mains, faites glisser délicatement la carte mère HiPath 3000 horizontalement depuis le support et placez-la sur une surface conductrice plane et mise à la terre.
6) Retirez toutes les cartes HG1500 existantes du boîtier. Les emplacements HG1500 libérés peuvent être utilisés pour des cartes supplémentaires.
7) Si nécessaire, retirez les cartes qui ne sont plus fixées au boîtier. Les emplacements libérés peuvent être utilisés pour des cartes supplémentaires.
8) Retirez toutes les sous-cartes insérées dans la carte mère HiPath 3000 et branchez-les (si elles sont encore nécessaires et prises en charge) dans la carte mère OpenScape Business V3.
9) Branchez le SSD M.2 SATA avec le logiciel système et le SSD M.2 NVMe optionnel sur la carte mère V3.
10) Branchez des modules optionnels tels que OCCBH ou OCCBL

11) En utilisant les deux mains, faites glisser avec précaution la carte mère OCCMRA ou OCCMRB horizontalement dans le même emplacement que celui où se trouvait auparavant la carte mère HiPath 3000.
12) Connectez les modules optionnels tels que STRBR à la carte mère V3.
13) Rebranchez tous les connecteurs sur la carte mère (tels que les stations analogiques, les lignes RNIS, etc.).

Remarque : Si plus de 2 ports analogiques a/b ont été utilisés dans HiPath 3300 ou 3500, 1 ou 2 câbles adaptateurs en Y seront nécessaires dans OpenScape Business. Il est possible de connecter jusqu'à 4 ports a/b via les 2 prises RJ11 physiques. En raison de contraintes d'espace, la nouvelle carte mère ne dispose que de 2 prises RJ11 par lesquelles les 4 stations a/b doivent être connectées.

14) Assurez-vous que votre système de communication est correctement connecté au fil de terre.
15) Rebranchez la prise d'alimentation du système et mettez-le sous tension.

Étapes suivantes

Comment lancer la première installation à la page 1351

25.7.1.5 Comment remplacer le matériel du HiPath 3800

Conditions préalables

Un système de communication HiPath 3800 est opérationnel.

Carte mère OpenScape Business OCCLA.

Avertissement :

Risque de choc électrique par contact avec des fils électriques sous tension

Assurez-vous qu'un fil de terre de protection séparé avec la section minimale requise soit disponible pour le système de communication (voir la documentation de service, Installation matérielle).

Étape par étape

1) Éteignez le système HiPath 3000 et débranchez sa prise d'alimentation.
2) Débranchez tous les connecteurs de la carte mère.
3) En utilisant les deux mains, faites glisser délicatement la carte mère HiPath 3000 de son support et placez-la sur une surface conductrice plane et mise à la terre.
4) Retirez toutes les cartes HG1500 déjà présentes sur l'étagère. Les emplacements HG1500 libérés peuvent être utilisés pour des cartes supplémentaires.
5) Le cas échéant, retirez de l'étagère à cartes toutes les cartes qui ne sont plus supportées. Les emplacements libérés peuvent être utilisés pour des cartes supplémentaires.

6) Retirez toutes les sous-cartes insérées dans la carte mère HiPath 3000 et branchez-les (si elles sont encore nécessaires et prises en charge) dans la carte mère OpenScape Business.
7) Branchez le SSD M.2 SATA avec le logiciel système et le SSD M.2 NVMe optionnel sur la carte mère V3.
8) Branchez les modules optionnels tels que OCCBH ou OCCBL.
9) Insérez soigneusement la carte mère OpenScape Business OCCLA dans le même emplacement que celui où se trouvait précédemment la carte mère HiPath 3000.
10) Rebranchez tous les connecteurs à la carte mère.
11) Assurez-vous que votre système de communication est correctement connecté au fil de terre.
12) Rebranchez la prise d'alimentation du système et mettez-le sous tension.

Étapes suivantes

Comment lancer la première installation à la page 1351

25.7.1.6 Comment lancer la première installation

L'installation initiale du système de communication est décrite dans la section Intégration dans le réseau local du client).

La première installation englobe la configuration de l'adresse IP de système, les paramètres DHCP ainsi que les réglages de pays et de temps.

Si le système HiPath 3000 est équipé en plus du HG 1500, il faut, lors de la première installation utiliser l'adresse IP de HG 1500 comme adresse IP de OpenScape Business.

Après la première installation, le système de communication procède à un redémarrage.

Étapes suivantes

Comment charger le KDS converti dans le nouveau système à la page 1351

25.7.1.7 Comment charger le KDS converti dans le nouveau système

Conditions préalables

Le matériel a été remplacé.

Le PC Admin est connecté au système de communication OpenScape Business (via l'interface LAN).

Le PC Admin est configuré de manière à pouvoir recevoir l'adresse IP et le masque de réseau du serveur DHCP de OpenScape Business.

Étape par étape

1) Ouvrez une session sur le PC Admin de Manager E.
2) Dans la barre de menu, cliquez sur **Fichier** > **Ouvrir KDS**.
3) Allez à l'emplacement d'enregistrement du KDS OpenScape Business converti et cliquez sur **OK**.

4) Confirmez la remarque avec **OK**.
5) Dans la barre de menu, cliquez sur **Fichier** > **Transférer**
6) Cliquez sur l'onglet **Communications**.
7) Dans la zone **Accès**, activez l'option **IP - HiPath** et dans le champ Adresse IP entrez l'adresse IP du système de communication OpenScape Business. Par défaut : `192.168.1.2`.
8) Activez le champ d'option **Sécurité**.
9) Cliquez sur **Modifier le mot de passe**.
10) Entrez l'ancien mot de passe et le nouveau et confirmez avec **OK**.
11) Activez le champ d'option **Lecture/Écriture KDS**.
12) Cochez les cases **Taxes** et **Matériel** et cliquez sur **PC** > **Système**.
13) Cliquez sur **OK**. Le KDS est transmis au système par Manager E.
14) Une fois la transmission de KDS effectuée, cliquez sur **OK** puis sur **Fermer**.
15) Quittez Manager E. Le système effectue automatiquement un redémarrage.

Étapes suivantes

Comment générer un nouveau fichier de licence à la page 1352

25.7.1.8 Comment générer un nouveau fichier de licence

Conditions préalables

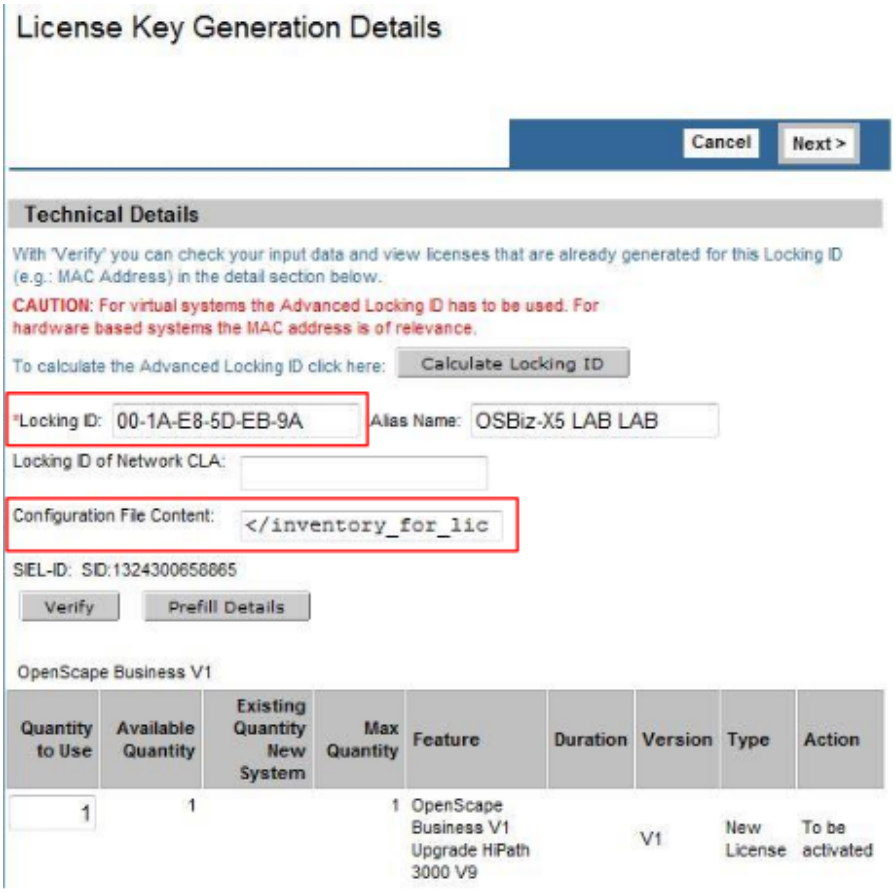
Le code LAC de la licence de mise à niveau est disponible.

Les données d'inscription du clients sont disponibles.

Étape par étape

1) Ouvrez une session sur WBM avec le profil **Advanced**.
2) Cliquez sur **Gestion des licences** dans la barre de navigation.
3) Notez l'ID de verrouillage d'OpenScape Business, indiquée au-dessus du tableau.
4) Dans l'arborescence de navigation, cliquez sur **Enregistrement**.
5) Entrez vos données et cliquez sur **OK & Suivant**.
6) Cliquez sur **Exporter les données**. Il est généré un fichier de configuration (fichier XML) avec les données d'inscription et les informations Inventory, y compris le nombre des abonnés TDM raccordés.
7) Sauvegardez le fichier de configuration dans un répertoire de votre choix.
8) Ouvrez une session sur le serveur CLS avec votre nom d'utilisateur et le mot de passe.
9) Dans l'arborescence du menu, cliquez sur **License** > **Generate License Key**.
10) Dans **LAC**, indiquez le code LAC de la licence de mise à jour et cliquez sur **Generate Key**.

11) Sélectionnez la fonctionnalité **OpenScape Business V2 Update HiPath 3000** et cliquez de nouveau sur **Generate Key**.



12) Dans le champ **Locking ID** (ID de verrouillage), entrez l'ID de verrouillage d'OpenScape Business.

13) Ouvrez le fichier de configuration avec un éditeur de texte (par ex. Notepad) et copiez le contenu complet du fichier de configuration dans le champ **Contenu du fichier de configuration**.

14) Cliquez sur **Next** (suivant) et suivez les instructions relatives à la génération d'un nouveau fichier de licence.

Remarque : La procédure de la migration de licence sur CLS n'est possible qu'une seule fois. Veillez donc à avoir des indications correctes !

---

15) Sauvegardez le nouveau fichier de licence dans un répertoire de votre choix.

Étapes suivantes

Comment activer le fichier de licence hors ligne à la page 1353

25.7.1.9 Comment activer le fichier de licence hors ligne

L'activation de licence hors ligne est décrite dans le chapitre Comment activer les licences hors ligne (autonome).

Étapes suivantes

Comment affecter les licences à la page 1354

25.7.1.10 Comment affecter les licences

L'affectation de licence est décrite dans le document Attribution de licences (autonome) à la page 266.

25.7.1.11 Comment réinitialiser les entrées LCR

L'installation de base du système de communication est décrite dans Configuration de base à la page 126.

L'installation de base comprend la configuration du numéro d'appel du système, des abonnés, ainsi que l'accès à Internet et la téléphonie Internet.

Dans l'assistant **Installation de base**, vous trouvez dans la fenêtre **Fonctions centrales pour les abonnés** un champ d'option supplémentaire **Effacer les données LCR configurées et initialiser avec les données LCR standard**. Ce champ d'option n'apparaît que s'il a été chargé auparavant dans le système un KDS converti. Si ce champ d'option est activé, les entrées LCR configurées dans le système HiPath 3000 sont effacées et remplacées par les entrées standard du système OpenScape Business.

Concepts associés

Données abonnés à la page 130

25.7.2 Migration d'un système HiPath 3000 avec OpenScape Office V3 HX vers OpenScape Business V3 avec carte mère V3

Lors de la migration de systèmes HiPath 3000 avec un OpenScape Office HX Server connecté, le serveur externe n'est pas nécessaire. Sa fonction est reprise par la carte mère V3 correspondante du système OpenScape Business X.

Le système HiPath 3000 est migré comme décrit dans Migration des systèmes HiPath 33xx, 35xx et 3800 vers OpenScape Business X5/X8 V4 à la page 1343.

Les licences OpenScape Office HX font partie du fichier de licence HiPath 3000. Par conséquent, elles sont également transférées vers les licences OpenScape Business au cours de la migration des licences HiPath 3000.

Exigences

Pour migrer des licences OpenScape Business HX, un fichier de licence HiPath 3000 doit être disponible sur le serveur de licences central.

Pour les licences HiPath 3000, la migration des licences s'effectue comme indiqué dans Tableau 35 : Migration de licence HiPath 3000 à la page 1344. Pour les migrations de licence OpenScape Office HX les dispositions suivantes s'appliquent :

Tableau 36 : Migration de la licence OpenScape Office HX

Licence OpenScape Office HX	Licence OpenScape Business	Remarques
Par licence de base	1x licence AutoAttendant	
Par utilisateur d'OpenScape Office Standard :	1x UC User 1x Voicemail User 1x Fax User	S'applique aux licences d'utilisateur standard dans les licences de base HX 5/10 ainsi qu'aux licences d'utilisateur unique
Licence de messagerie vocale OpenScape Office HX	500 x Voicemail User	
myPortal for Outlook	Utilisateur Groupware	Numéro comme dans le fichier de licence
myAttendant	myAttendant	Numéro comme dans le fichier de licence
myAgent	Utilisateur myAgent	Numéro comme dans le fichier de licence
Centre d'appels fax	Utilisateur du centre d'appels fax	Numéro comme dans le fichier de licence
Centre d'appels e-mail	Utilisateur Centre d'appels e-mail	Numéro comme dans le fichier de licence
myReports	myReports	Numéro comme dans le fichier de licence
Application Launcher	Application Launcher	Numéro comme dans le fichier de licence
Connecteur OpenDirectory	Connecteur OpenDirectory	Numéro comme dans le fichier de licence

Conditions limites fonctionnelles et restrictions

La migration des licences ne peut se faire que vers V3. Une migration de licence vers la version V2 n'est pas prise en charge par Manager E.

La migration de licence n'est possible qu'une seule fois.

Les licences utilisateur et les licences orientées utilisateur UC sont attribuées de manière permanente aux utilisateurs dans OpenScape Business. Veuillez noter que pour les utilisateurs de myAgent et myAttendant, le nombre de licences disponibles est suffisant.

Dans OpenScape Business, les modifications des états Présence pour d'autres utilisateurs par un utilisateur myAgent sont liées à la licence myAttendant. Celles-ci doivent être commandées séparément.

Il n'est pas possible de transférer des annonces, des images, des messages vocaux, des fax, des journaux, des données de centre de contact, la configuration des abonnés, des profils, un répertoire externe, des horaires d'OpenScape Office HX vers OpenScape Business V3 avec la carte mère V3.

25.7.3 Migration d’un réseau HiPath 3000 vers un réseau OpenScape Business

Pour faire évoluer un réseau HiPath 3000 vers un réseau OpenScape Business, il faut effectuer les étapes de la migration décrites ci-après.

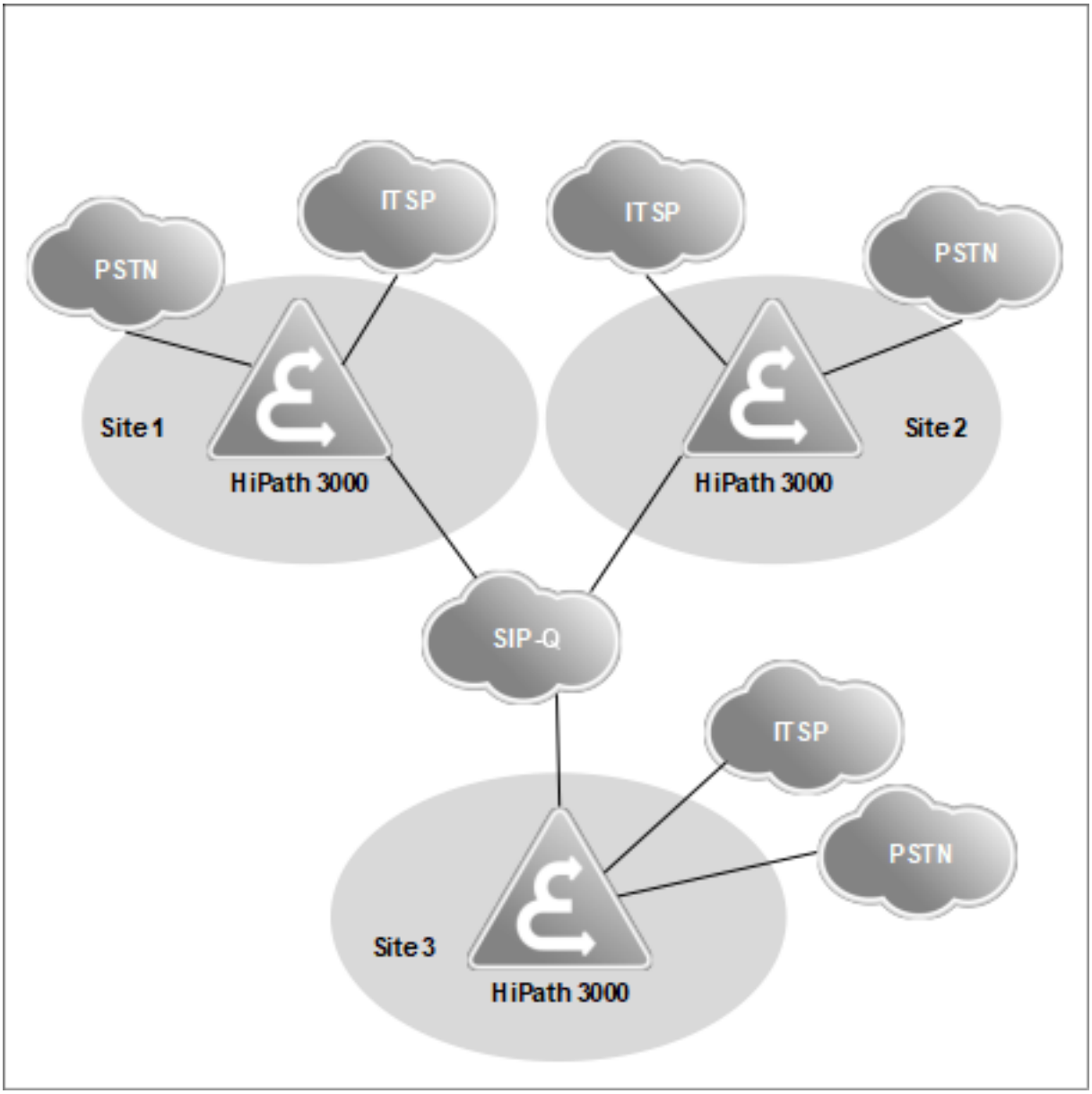


Illustration 17 : Interconnexion de réseaux HiPath 3000 V9

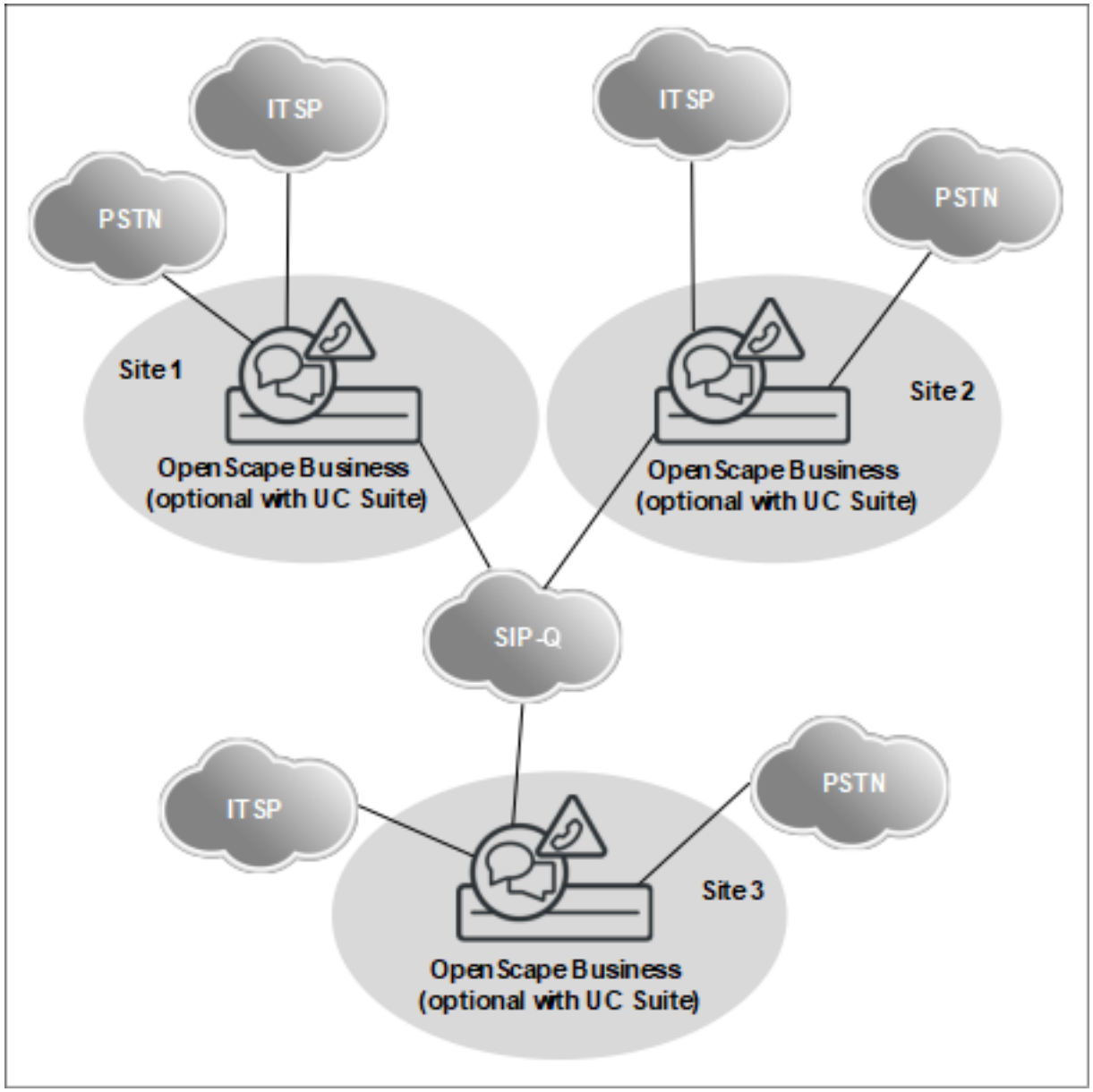


Illustration 18 : Interconnexion de réseaux OpenScape Business

Etapes de la migration

Effectuez les opérations suivantes dans l'ordre :

1) **Mise à niveau de HiPath 3000**

   Tous les systèmes HiPath 3000 de l'interconnexion de réseaux doivent être mis à niveau séparément conformément à la description de la migration d'un système indépendant (voir 1.7.1).

2) **Adapter la configuration**

   Les paramètre de configuration ci-après doivent être adaptés ultérieurement à l'aide de WBM-Mode Expert.

   - Entrées LCR
   - Système de messagerie vocale (groupe de recherche, indicatif pour sélectionner la messagerie vocale)
   - Annonces

3) **Réaliser la procédure de licence**

   Une fois que tous les systèmes ont été mis à niveau, tous les fichiers de licence sont regroupés en une licence pour l'ensemble du réseau dans CLS.

25.7.4 Migration d'une interconnexion de réseaux HiPath 3000 V9 avec HiPath 5000 RSM

Un réseau HiPath 3000/5000 avec fichier de licence réseau commun doit être transformé via le Serveur de licence central (CLS) en systèmes indépendants avec fichiers de licences individuels Chaque système autonome est désormais migré vers OpenScape Business et fait l'objet d'une licence distincte.

Si nécessaire, les systèmes OpenScape Business peuvent de nouveau être regroupés dans une interconnexion de réseaux avec un seul fichier de licence réseau sur le CLS après la migration.

L'étendue des fonctionnalités de HiPath 5000 RSM est intégrée dans OpenScape Business, donc HiPath 5000 RSM n'est plus nécessaire dans l'interconnexion de réseaux OpenScape Business.

Pour la mise en réseau des systèmes OpenScape Business, des licences de mise en réseau OpenScape Business doivent être disponibles en plus par nœud.

Pour la téléphonie par Internet et les lignes T1, des licences supplémentaires sont nécessaires.

Les étapes de migration suivantes doivent être accomplies comme décrit ci-dessous.

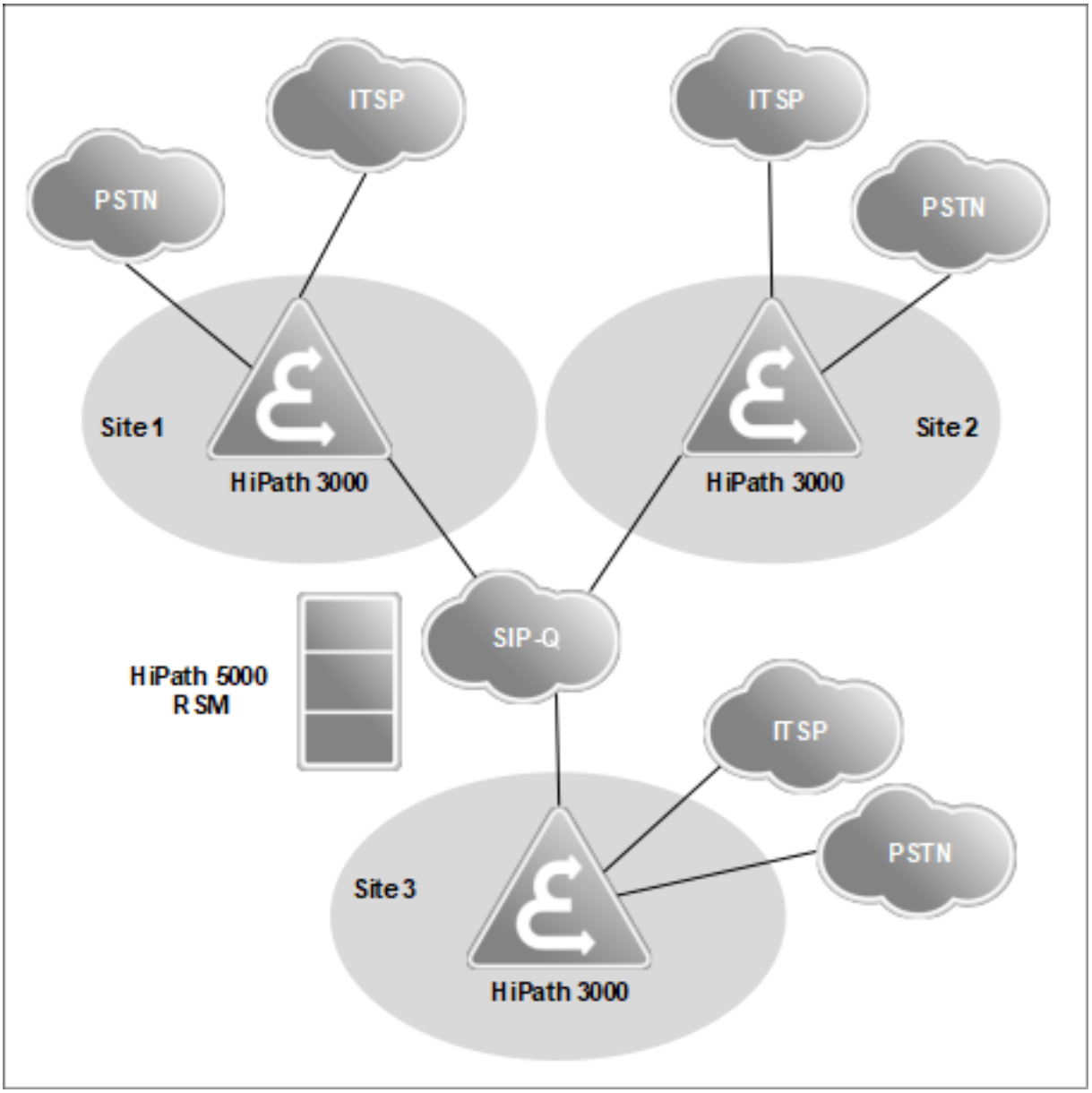


Illustration 19 : Interconnexion de réseaux HiPath 3000 V9

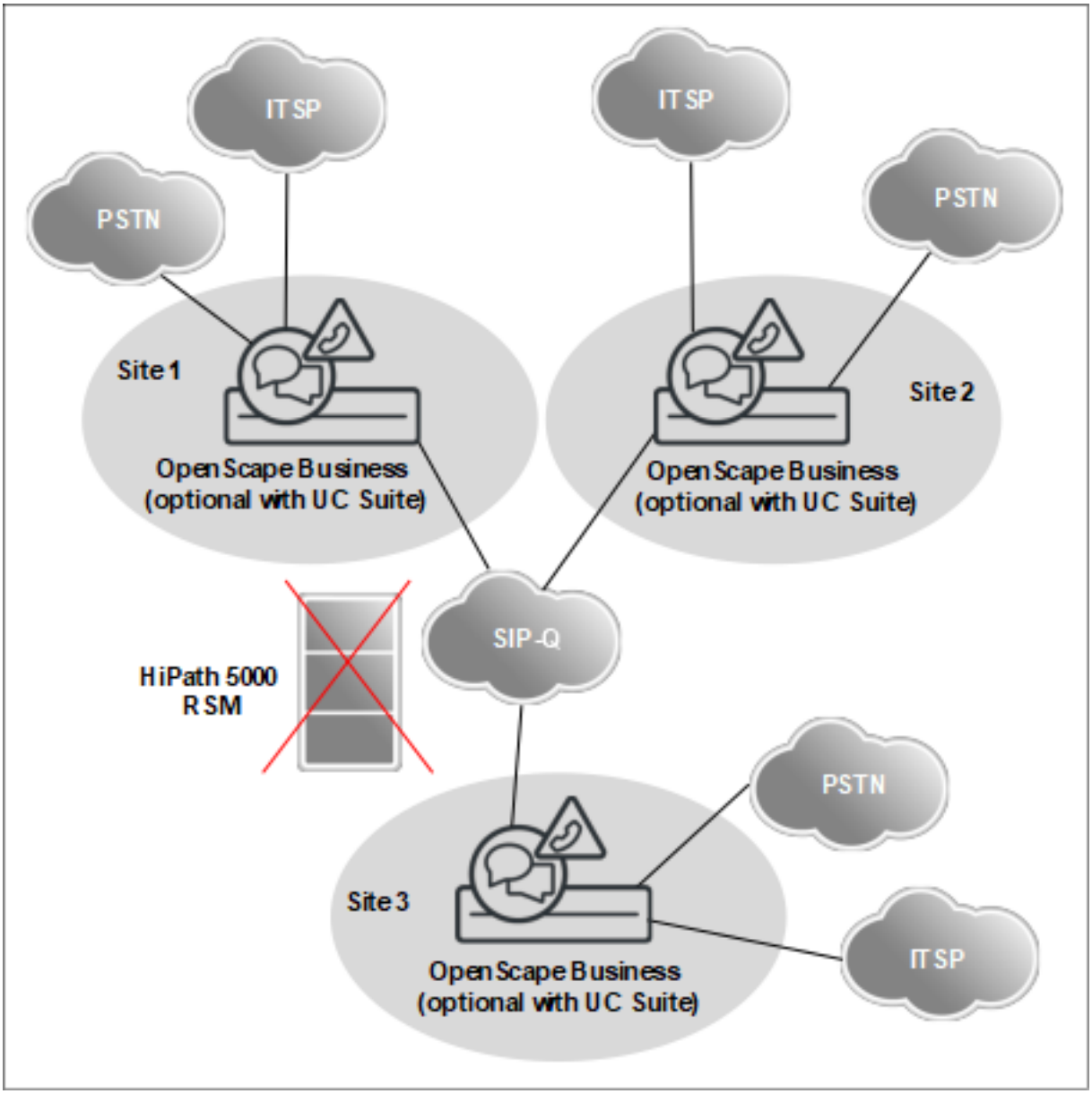


Illustration 20 : Interconnexion de réseaux OpenScape Business

Etapes de la migration

Effectuez les opérations suivantes dans l'ordre :

1) Libérez la procédure de licence sur l'ensemble du réseau

Une interconnexion de réseaux HiPath 3000 avec HiPath 5000 RSM utilise la licence pour l'ensemble du réseau. Le fichier de licence réseau doit, dans un premier temps, être converti en différents fichiers de licence dans CLS, avec affectation des identifiants de verrouillage (adresses MAC) des systèmes HiPath 3000 V9, avant que la migration vers OpenScape Business puisse commencer à proprement parler.

- Tout d'abord, attribuez les licences de l'interconnexion de réseaux HiPath 5000 RSM aux identifiants de verrouillage correspondants des noeuds HiPath 3000. Recommandation : Créez une liste Excel avec l'attribution

correspondante des licences aux ID de verrouillage des systèmes HiPath 3000.
- Contactez la ligne directe des licences pour faire effectuer la distribution des licences suivant liste Excel.
- Chargez les licences individuelle des systèmes HiPath 3000 pour contrôle de CLS. Une activation des licences, c.-à-d. la transmission de licence aux systèmes HiPath 3000 n'est pas nécessaire.

2) **Supprimer HiPath 5000 RSM**

   Avant la mise à niveau des systèmes HiPath 3000, HiPath 5000 RSM est déconnecté.

3) **Mise à niveau de HiPath 3000**

   Tous les systèmes HiPath 3000 de l'interconnexion de réseaux doivent être mis à niveau séparément conformément à la description de la migration d'un système indépendant. Voir 1.7.1

4) **Adapter la configuration**

   Les paramètres de configuration ci-après doivent être adaptés ultérieurement dans les systèmes OpenScape Business à l’aide de WBM-Mode Expert :

   - Entrées LCR
   - Système de messagerie vocale (groupe de recherche, indicatif pour sélectionner la messagerie vocale)
   - Annonces

5) **Réaliser la procédure de licence**

   Une fois que tous les systèmes ont été mis à niveau, tous les fichiers de licence OpenScape Business sont regroupés en une licence pour l’ensemble du réseau sur le CLS.

Remarque : Dans le cas de l'extension d'une fonctionnalité UC sur l'ensemble du réseau, il est nécessaire de passer d'une numérotation ouverte à une numérotation fermée afin d'adapter les numéros internes. Donc, la numérotation ouverte doit être désactivée tandis que le numéro de noeud doit être effacé et ensuite ajouté comme préfixe (par exemple numéro interne étendu 87100 à la place de 100 et 88100 à la place de 100).

Différences :

- La sélection des participants dans leur propre noeud est effectuée avec le numéro interne étendu.

- Le numéro d'appel interne et le numéro SDA peuvent différer si nécessaire, mais les numéros SDA ne doivent pas être modifiés.

25.7.5 Fonctionnalités et interfaces modifiées/supprimées du HiPath 3000

Certaines fonctionnalités et interfaces de HiPath 3000 ont été adaptées à OpenScape Business et améliorées.

Remplacement de la carte MMC

Pour des raisons techniques, la carte SSD SDHC / M.2 SATA ne peut pas être remplacée lorsque le système est allumé (une procédure connue sous le nom de mise à jour de vitesse pour HiPath 3000). De plus, la carte SSD SDHC/ M.2 SATA d'un système A sous licence ne peut pas être utilisée sur un autre système B car la licence est liée à l'identifiant de verrouillage de la carte mère A. Si la carte SSD SDHC/M.2 SATA doit être utilisée sur le système B, elle doit d'abord être initialisée avec un nouveau logiciel à l'aide du Gestionnaire de cartes.

Canaux DSP HG1500 / Canaux B

Le module HG1500 n'est plus nécessaire. La fonctionnalité DSP est intégrée à OpenScape Business sur la carte mère V3 et via des cartes d'amplification de canal vocal optionnelles.

Veuillez déterminer le nombre de canaux DSP requis. Des canaux DSP sont nécessaires pour mettre en œuvre les transitions réseau de la téléphonie TDM à la VoIP. OpenScape Business possède 8 canaux DSP intégrés sur la carte mère V3. Pour étendre les canaux DSP, le module DSP OCCB1/OCCBL (jusqu'à 40 canaux) ou le module DSP OCCB3/OCCBH (jusqu'à 120 canaux) peuvent être utilisés.

Services Web d'accès

Les services Web d'entrée ne sont plus pris en charge. Le successeur de l'entrée myPortal s'appelle myPortal @work et offre des fonctionnalités étendues.

Messagerie vocale d'entrée

Le module de messagerie vocale d'entrée a été supprimé d'OpenScape Business ; la fonction est intégrée sous le nom de messagerie vocale intelligente dans la carte mère d'OpenScape Business. Les utilisateurs de la messagerie vocale intelligente doivent posséder une licence.

Messagerie vocale externe

Si le HiPath 3000 utilise une solution de messagerie vocale externe telle que Xpressions, les dix ports EVM doivent être modifiés de **PhoneMail** à **Standard** dans Manager E après la conversion CDB.

Fonctionnalités SIP améliorées

Les fonctionnalités SIP suivantes ont été implémentées en plus par rapport à HiPath 3000 V9 :

- Appel terminé ailleurs
- Indication de message en attente pour la messagerie vocale
- Présentation du nom d'appel (CNIP)
- Sonnerie distinctive (appels internes/externes)
- Contrôle d'appel par un tiers
- Renvoi d'appel occupé/pas de réponse/inconditionnel (contrôlé par le combiné)

Liaison SIP

Pour connecter des serveurs SIP externes (par exemple, OpenScape Alarm Server, HiPath 4000, OpenScape Voice ou UC Suite), des routes SIP/SIP-

Q natives supplémentaires sont disponibles dans OpenScape Business (contrairement à HiPath 3000 qui ne propose qu'une seule route SIP-Q). Ainsi, en plus des itinéraires classiques pour le CO, le réseau et l'ITSP, des interfaces de jonction SIP/SIP-Q natives indépendantes (appelées interconnexion SIP) sont fournies pour les applications SIP certifiées.

Voir Réseau Unify OpenScape Business

LCR

Les tables de routage 1 à 15 sont destinées aux entrées par défaut ou à la configuration à l'aide d'assistants. Lors d'une migration, les entrées existantes dans le HiPath 3000 ne sont pas transférées vers ces tables de routage. Un post-traitement manuel des tables de routage est donc nécessaire.

Numérotation simplifiée

Soit la fonction « LCR », soit la fonction « Prime Line (numérotation simplifiée) » peut être activée, mais pas les deux en même temps. Pour cette raison, « LCR » est activé automatiquement pendant la migration tandis que « Prime Line (numérotation simplifiée) » est désactivé. Pour désactiver « LCR » et activer « Prime Line (numérotation simplifiée) », l'assistant d'installation de base doit être terminé avant que les indicateurs correspondants puissent être définis dans Manager E (non pour OpenScape Business X1 car il ne permet pas l'administration via Manager E).

Remarque : La numérotation simplifiée n'est pas prise en charge dans les applications CSTA.

VoIP sur PPP via ISDN

Les appels vocaux acheminés sur des lignes à faible bande passante ne sont plus pris en charge.

Support G.723

Les codecs G.723 ne sont plus pris en charge.

Babyphone

La fonction Babyphone (surveillance de la chambre) n'est plus prise en charge. Étant donné que la « surveillance CSTA » est toujours active (un téléphone système peut être surveillé par une application telle que myAgent ou myPortal, par exemple), la « surveillance de salle » ne peut plus être activée pour ce téléphone système. Lors de la conversion CDB avec Manager E, le code d'activation du moniteur de salle est supprimé.

HiPath 3000 BS4

Les licences de station de base ne sont plus requises dans OpenScape Business.

SSDP basé sur le PC Plug

SSDP est intégré à OpenScape Business. Le PC Plug n'est plus nécessaire.

Interface comptable

Les interfaces des données comptables ont changé par rapport à HiPath 3000.

Applications V24

Les applications V24 ne sont plus prises en charge.

Demandes CSTA

Dans OpenScape Business V4, une carte mère V3 est requise pour la connexion des applications CSTA. Dans un réseau, une carte mère V3 ne doit exister que dans le nœud maître. Les applications doivent prendre en charge le protocole CSTAv3. Par rapport à HiPath 3000, des modifications ont été apportées au protocole CSTA. Par conséquent, les applications CSTA sur HiPath 3000 V9 peuvent ne pas fonctionner de manière compatible sur les systèmes OpenScape Business. Le protocole CSTAv2 n'est plus pris en charge.

Dans les versions 3 et 4 du logiciel, une licence CSTA est requise pour l'utilisation de l'interface CSTA, à l'exception des éléments suivants :

- Connexions CSTA OpenScape Business TAPI 120 ou TAPI 170 en général

Par rapport à l'interface CSTA HiPath 3000, l'interface CSTA OpenScape Business a été modifiée comme suit :

- La connexion à l'interface CSTA est identique pour un nœud esclave OpenScape Business autonome et en réseau. CSTA au niveau du nœud maître d'un réseau offre des fonctionnalités améliorées. Cela se produit exclusivement via le réseau local. Les interfaces RS-232 (V.24) et S0 ne sont plus prises en charge.
- OpenScape Business ne nécessite plus de composants matériels et logiciels supplémentaires tels que le fournisseur de services CSTA (CSP), la carte HG 1500 ou le système HiPath 5000 RSM. Il faut en revanche des cartes mères V3.
- L'interface CSTA est soumise à licence, à l'exception des connexions UC Booster Card et TAPI 120/170.
- Un maximum de 4 liaisons CSTA peuvent être utilisées pour la connexion d'applications externes. Dans l'état d'usine par défaut, 3 des 4 interfaces CSTA sont préconfigurées pour l'utilisation des applications internes d'OpenScape Business. Ces interfaces peuvent également être utilisées, en option, pour connecter des applications externes.
- La protection des interfaces CSTA contre les abus a été améliorée. Le mécanisme d'accès a été revu.
- La surveillance MULAP via CSTA n'est possible que si un point de surveillance est défini sur le numéro MULAP. Les membres individuels du MUALP ne peuvent être surveillés. Si une application CSTA souhaite néanmoins surveiller des membres MULAP individuels, aucun événement CSTA ne sera transmis à l'application par OpenScape Business. Cela s'applique également aux membres de MULAP qui font partie d'un groupe de chasse.
- Les fonctions CSTA fournies ont été étendues. Vous trouverez plus de détails dans le manuel d'interface CSTA d'OpenScape Business.
- La version du protocole CSTA Phase II n'est plus prise en charge.
- Les applications CSTA destinées à être utilisées avec OpenScape Business doivent être testées et publiées conjointement avec OpenScape Business.

Applications HiPath TAPI 120/170 V2

Pour HiPath TAPI 120/170 V2, les licences existantes ne peuvent pas être transférées. De nouvelles licences doivent être achetées. HiPath TAPI 120/170

V2 doit être désinstallé et OpenScape Business TAPI 120/170 V1 doit être installé et configuré à la place.

Les licences TAPI peuvent être configurées dans OpenScape Business par utilisateur, éliminant ainsi le besoin de licences TAPI au sein du périphérique TAPI. Une licence est requise dès le premier utilisateur de TAPI (donc même TAPI120 n'est plus gratuit pour les 6 premiers utilisateurs). Le CMD (CSTA Message Dispatcher) est intégré à OpenScape Business. Un serveur Windows distinct pour l'invite de commandes n'est donc plus nécessaire. La connectivité aux applications TAPI externes est possible pour OpenScape Business et OpenScape Business S. OpenScape Business nécessite une carte mère V3. Dans un réseau, soit une carte mère OpenScape Business S doit exister, soit une carte mère V3 doit exister au moins sur le nœud maître.

Par rapport à HiPath TAPI 120/170 V2, OpenScape Business TAPI 120/170 V2 V1 a été modifié comme suit :

- L'accès au système n'est possible que via un réseau local Ethernet. Les interfaces RS-232 et S0 ne sont plus prises en charge.
- Nouvelle licence TAPI partagée sur une base « par utilisateur » pour TAPI 120 TSP et TAPI 170 TSP.
- Les licences sont liées à l'identifiant de verrouillage d'OpenScape Business.
- Les licences utilisateur HiPath TAPI 120 TSP ou HiPath TAPI 170 TSP existantes ne sont pas prises en charge par le nouveau mécanisme de licence.
- Aucune rétrocompatibilité avec HiPath 3000 V8 ou V9
- Les dispositions suivantes s'appliquent au TAPI 170 TSP :
  - Par défaut, l'accès au système se fait via le port 8800.
  - La configuration des identifiants CSTA dans la boîte de dialogue de configuration est obligatoire.
  - Prise en charge multi-nœuds dans le réseau via le CSP du nœud maître central.
- Les dispositions suivantes s'appliquent au TAPI 120 TSP :
  - Par défaut, l'accès au système se fait via le port 8900.
  - Prise en charge d'un seul nœud, même lorsqu'il est connecté au nœud maître d'un réseau.

Autres applications externes

Les applications ultérieures connectées en externe à HiPath 3000 ne peuvent plus être exécutées sur OpenScape Business.

Application HiPath 3000	Application successeur pour OpenScape Business	Remarques
optiClient Attendant	Gestionnaire d'entreprise OpenScape	Nouvelle demande Aucun transfert de licence possible
optiClient BLF V1/V2	Gestionnaire de compte OpenScape Business (OpenScape Business BLF)	Nouvelle demande Aucun transfert de licence possible

Application HiPath 3000	Application successeur pour OpenScape Business	Remarques
HiPath TAPI 120/170	OpenScape Business TAPI 120/170	Nouvelle demande Aucun transfert de licence possible
Clients de communication der Entry WEB Services sur Plug PC	Solution UC intégrée	Nouvelle demande Aucun transfert de licence possible
myPortail pour mobile/ tablette	myPortal à visiter	Nouvelle demande Aucun transfert de licence possible

Fonctionnalités modifiées/supprimées du HiPath 5000 RSM

Le système HiPath 5000 RSM n'est plus pris en charge. Les fonctionnalités de HiPath 5000 RSM ont été intégrées à OpenScape Business. Cela signifie qu'un serveur séparé n'est plus nécessaire.

Tableau 37 : Différences entre HiPath 5000 RSM et OpenScape Business V3

Fonctionnalité	HiPath 5000 RSM	OpenScape Business
Gestion des licences à l'échelle du réseau, attribution de licences aux nœuds individuels	Toutes les licences système du réseau sont regroupées au niveau du CLS en une licence réseau unique.	Toutes les licences système du réseau sont regroupées au niveau du CLS en une licence réseau unique.
Administration à l'échelle du réseau	Serveur de fonctionnalités de base de données : tous les nœuds du réseau sont combinés en une base de données de base de données réseau à l’aide de Manager E. Le schéma de numérotation est synchronisé sur l’ensemble du réseau.	Tous les nœuds du réseau sont enregistrés via OpenScape Business Assistant (WBM) avec un assistant réseau. Le système de numérotation est synchronisé à l'échelle du réseau (numérotation fermée).
Connexion à des nœuds externes ou à des applications externes	Connexion SIP-Q jusqu'à 4 nœuds externes	Jusqu'à 10 routes d'interconnexion SIP avec jusqu'à 2 SIP-Q, ou jusqu'à 10 routes SIP natives, ou jusqu'à 8 routes ITSP.

Fonctionnalité	HiPath 5000 RSM	OpenScape Business
Résilience / Survie	Survie de l'utilisateur pour les téléphones HFA à numérotation fermée	Survie des utilisateurs pour les téléphones HFA avec numérotation fermée (passage d'OpenScape Business S à OpenScape Business X5/X8)
Sauvegarde / Restauration	Netwide	Locale
Fonction d'inventaire	Netwide	Locale
Gestionnaire de présence	Fonctionnement à l'échelle du réseau avec la mise à disposition de 5000 RSM	Fonction à l'échelle du réseau avec la fourniture d'un CSP multi-nœuds basé sur OpenScape Business S. Prérequis : numérotation fermée.
TAPI 170 sur un système autonome	Le TAPI 170 sur un système autonome fonctionne sur un PC Windows avec sa propre licence (fichier de licence séparé pour le TAPI 170).	Le TAPI 170, installé sur un système autonome, fonctionne sur un PC Windows. La demande de licence et la fourniture de la base de données TAPI 170 se font à partir de la base de données SQL d'OpenScape Business. La connexion du TAPI 170 s'effectue via le CSP du système (OpenScape Business S).
TAPI 170 dans un réseau	TAPI 170 fonctionne sur 5000 RSM avec sa propre licence (fichier de licence séparé pour TAPI 170). La base de données TAPI 170 est obtenue à partir du serveur de fonctionnalités de base de données du 5000 RSM.	Comme pour le système autonome, mais la connexion du TAPI 170 se produit au niveau du CSP multinœud d'un nœud maître (c'est-à-dire à l'échelle du réseau). Prérequis : numérotation fermée.

Réseaux mixtes

Les réseaux mixtes composés d'OpenScape Business et d'OpenScape Office ne sont pas pris en charge.

25.8 Migration au sein d'OpenScape V3 Business

Les différentes options de migration au sein des systèmes OpenScape Business X V3 avec cartes mères V2 sont décrites ici.

Remarque : Ces scénarios sont obsolètes (non valides) pour les systèmes OpenScape Business X V3 avec cartes mères V3 !

Augmenter le nombre d'utilisateurs UC Smart

Vous pouvez choisir parmi les options suivantes :

- Migration d'Unify **OpenScape Business X** (UC Smart) vers Unify **OpenScape Business X** avec **UC Booster Server** (UC Smart)

  Utile pour 50 à 500 utilisateurs UC Smart. Toutes les données de configuration et les données utilisateur sont transférées. Aucun transfert de données n'a lieu lors des rétrogradations. Des licences utilisateur UC supplémentaires sont requises pour les nouveaux utilisateurs UC Smart.

Passez de UC Smart à UC Suite

Vous pouvez choisir parmi les options suivantes :

- Migration d'Unify **OpenScape Business X** (UC Smart) vers Unify **OpenScape Business X** avec **UC Booster Server** (UC Suite)

  Les données de configuration et les données utilisateur ne sont pas transférées. Une licence de mise à niveau vers les clients UC Suite est requise pour les clients UC Smart existants. La conversion de la solution UC en UC Suite s'effectue dans le Web based Management (Web admin) avec l'assistant de **Première Installation**.
- Migration d'Unify **OpenScape Business X** avec **UC Booster Card** (UC Smart) vers Unify **OpenScape Business X** avec **UC Booster Server** (UC Suite)

  Les données de configuration et les données utilisateur ne sont pas transférées. Une licence de mise à niveau vers les clients UC Suite est requise pour les clients UC Smart existants. La conversion de la solution UC en UC Suite s'effectue dans le Web based Management (Web admin) avec l'assistant de **Première Installation**.
- Migration au sein d'Unify **OpenScape Business S** de UC Smart vers UC Suite

  Les données de configuration et les données utilisateur ne sont pas transférées. Une licence de mise à niveau vers les clients UC Suite est requise pour les clients UC Smart existants. La conversion de la solution UC en UC Suite s'effectue dans le Web based Management (Web admin) avec l'assistant de **Première Installation**.
- Migration dans Unify **OpenScape Business UC Booster Server** de UC Smart vers UC Suite

  Les données de configuration et les données utilisateur ne sont pas transférées. Une licence de mise à niveau vers les clients UC Suite est requise pour les clients UC Smart existants. La conversion de la solution UC en UC Suite s'effectue dans le Web based Management (Web admin) avec l'assistant de **Première Installation**.

Augmenter le nombre d'utilisateurs de UC Suite

Vous pouvez choisir parmi les options suivantes :

- Migration d'Unify **OpenScape Business X** avec **UC Booster Card** (UC Suite) vers Unify **OpenScape Business X** avec **UC Booster Server** (UC Suite)

  Utile pour 150 à 500 utilisateurs de UC Suite. Toutes les données de configuration et les données utilisateur sont transférées. Aucun transfert de données n'a lieu lors des rétrogradations. Des licences supplémentaires d'utilisateur UC ou d'utilisateur de logiciel de groupe sont requises pour les nouveaux utilisateurs de la suite UC.

25.9 Migration des modules matériels

Les actions de migration matérielle suivantes sont possibles dans le cas d'un système OpenScape Business X8 :

- Remplacements de SLMO24N par SLMU
- Remplacements de SLMO8N par SLMU
- Remplacements de SLCN par SLMUC (SLMU + CMAe)

25.9.1 Remplacement de SLMO24N par SLMU

Un simple échange de cartes est pris en charge. La carte SLMO24N peut être retirée du système et la nouvelle carte SLMU peut être branchée. Tous les ports configurés restent inchangés. Il n'est pas nécessaire d'arrêter le système.

25.9.2 Remplacement de SLM8N par SLMU

Puisque la carte SLMU possède plus de ports que la carte SLMO8, la carte SLMO8 doit être retirée par l'administration. Pour retirer la carte du système, l'Utilisateur en ligne doit être utilisé avec la boîte de dialogue suivante :

`Administration système 29- 4 - 1`

et le type de carte doit être défini sur SLMUC.

Remarque :

Si les utilisateurs sont configurés pour UC Suite, ils sont créés avec les paramètres par défaut. Toutes les données précédentes (par exemple, les paramètres de messagerie vocale, de fax ou d'utilisateur) sont perdues.

Remarque :

Si la carte SLMO8 est remplacée par la carte SLMU mais pas via la procédure décrite, les 16 ports supplémentaires de la carte SLMU peuvent être perdus car ils n'ont pas pu être configurés. Cela se produira si une autre carte utilisant la plage de ces 16 ports est déjà en service. Si le système possède une

unique carte SLMO8 remplacée par une carte SLMU, tous les ports seront disponibles.

25.9.3 Remplacement de SLCN par SLMUC (SLMU + CMAe)

Comme la carte SLMU possède plus de ports que la carte SLCN, cette dernière doit être retirée par l'administration avant que la carte SLMUC ne soit mise en service dans cet emplacement. Le processus de retrait de la carte est le suivant :

1) **Annuler l'enregistrement de tous les combinés CMI de leur station de base**
2) **Retirer la carte du système**
3) **Retirer la carte SLCN via l'Utilisateur en ligne à l'aide de la boîte de dialogue :**

   `Administration système 29- 4 - 1`

   et le type de carte doit être défini sur SLMUC.
4) **Installer la carte SLMUC**
5) **Configurer le combiné utilisé**
6) **Enregistrer les combinés CMI**

   Tous les téléphones DECT concernés (128 au maximum) doivent être connectés pour être réinscrits.

Remarque :

Lorsque vous remplacez une carte SLCN par une carte SLMUC, vous avez également besoin d'un cache borgne pour le SLMUC au lieu du cache en plastique utilisé pour la carte SLCN.

Remarque :

Si les utilisateurs sont configurés pour UC Suite, ils sont créés avec les paramètres par défaut. Toutes les données précédentes (par exemple, les paramètres de messagerie vocale, de fax ou d'utilisateur) sont perdues.

26 Configurations et capacités

Les limites de configuration décrites ici sont des valeurs maximales déterminées par le système pour un seul système. Les valeurs maximales d'un système dans un réseau peuvent être différentes.

26.1 Valeurs maximales pour les stations

- Les données relatives aux systèmes dotés de cartes mères V2 OCC se trouvent dans Tableau 38 : Stations/utilisateurs de niveau d'extension avec cartes mères OCCx à la page 1371
- Les données relatives aux systèmes dotés de cartes mères V3 OCC se trouvent dans Tableau 39 : Stations/utilisateurs de niveau d'extension avec cartes mères OCCSB/R, OCCMA/B ou OCCLA à la page 1372
- Les données relatives aux systèmes OpenScape Business S Server se trouvent dans Tableau 40 : Stations/utilisateurs de niveau d'extension avec OpenScape Business S à la page 1373

Tableau 38 : Stations/utilisateurs de niveau d'extension avec cartes mères OCCx

Gares	X1	X5R	X8
Stations maximum			
Nombre maximal de stations[13]	30	500	500
Stations IP			
Système de stations IP (HFA)	20[14]	500	500
Stations IP (SIP)	20[14]	500	500
Stations TDM			
Nombre maximal de stations TDM[15 19]	30	384	384
Stations analogiques (TDM)	4	68	384
Stations maîtres U $_{P0}$ (TDM)[19]	8	56	384
Stations esclaves U $_{P0}$ (TDM) (incluant les adaptateurs a/b et S0)	8	56	116
Stations ISDN S0 (TDM)	2	52	128
Stations DECT-CMI (TDM)	16	64	250
Utilisateur mobile			
Nombre maximal d'utilisateurs de mobilité[16]	30	150	150
utilisateurs de Mobility Entry	20	150	150
utilisateurs de Skype Entreprise	30	150	150
Autres utilisateurs			

Gares	X1	X5R	X8
utilisateurs RAS	2	500	500
Stations virtuelles librement configurables	30	250	250

Remarque : Pour chaque configuration système, il convient de vérifier si la puissance nominale de l'alimentation native est suffisante ou si une alimentation auxiliaire externe est nécessaire (voir *la documentation OpenScape Business Service - Besoins en alimentation d'un système de communication*).

Tableau 39 : Stations/utilisateurs de niveau d'extension avec cartes mères OCCSB/R, OCCMA/B ou OCCLA

Gares	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Stations maximum						
Nombre maximal de stations[13]	500	500	500	500	500	500
Stations IP						
Système de stations IP (HFA)	500	500	500	500	500	500
Stations IP (SIP)	500	500	500	500	500	500
Stations TDM						
Nombre maximal de stations TDM[15] [19]	30	30	384	384	384	384
Stations analogiques (TDM)	4	4	68	68	384	384
Stations maître/esclave U_{P0} (TDM)[19]	8	8	56	56	384 maître 116 esclaves	384 maître 116 esclaves

13 Somme de : IP (HFA), IP (SIP), Analogique, UP0 Maître/Esclave, DECT (CMI), ISDN S0, abonnés Mobilité et Desk Share

14 Somme des utilisateurs IP et Desk Share (limitation via la configuration)

15 Somme des abonnés : Analogique, UP0, DECT (CMI) et ISDN S0

16 Somme des participants : Mobility Entry, Skype for Business

17 Le nombre de connexions VoIP simultanées de l'abonné dépend de :

1) les canaux DSP disponibles dans le système pour les appels de passerelle (transition IP/TDM).

2) les canaux proxy RTP internes disponibles dans le système pour les appels VoIP via Internet.

18 Le nombre de connexions simultanées dépend des canaux DSP disponibles dans le système pour les appels de passerelle (transition IP/TDM).

19 Selon les types de téléphones et les besoins énergétiques totaux du système de communication

Gares	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Stations ISDN S0 (TDM)	0	0	48	48	128	128
Stations DECT-CMI (TDM)	16	16	64	64	250	250
Utilisateur mobile						
Nombre maximal d'utilisateurs de mobilité[16]	150/ 500[20]	150/ 500[20]	150/ 500 [20]	150/ 500[20]	500	500
utilisateurs de Mobility Entry	150	20	150	150	150	150
utilisateurs de myPortal pour les équipes[17]	150/ 500[20]	30	150/ 500[20]	150/ 500[20]	500	500
utilisateurs de Skype Entreprise	150/ 500[20]	30	150/ 500[20]	150/ 500[20]	500	500

Tableau 40 : Stations/utilisateurs de niveau d'extension avec OpenScape Business S

Gares	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Stations maximum			
Nombre maximal de stations	50	500	1500
Stations IP			
Système de stations IP (HFA)	50	500	1500
Stations IP (SIP)	50	500	500
Utilisateur mobile			
Nombre maximal d'utilisateurs de mobilité	50	250	500
utilisateurs de Mobility Entry	50	150	150
utilisateurs de myPortal pour les équipes	50	250	500
utilisateurs de Skype Entreprise	50	250	500

26.2 Valeurs maximales des lignes

- Des canaux de tous types de lignes (ligne, interautomatique, interconnexion, etc.) dans les cartes mères V2 OCC sont disponibles dans Tableau 41 : Niveau d'extension des canaux de ligne avec cartes mères OCCx à la page 1374.
- Des canaux de tous types de lignes (ligne, interautomatique, interconnexion, etc.) dans les cartes mères V3 OCC sont disponibles dans Tableau 42 : Niveau d'extension des canaux de ligne avec cartes mères OCCSB/R, OCCMA/B ou OCCLA à la page 1374

[20] Les valeurs sont décalées selon la version du plateau : Basique/Avancée

- Des canaux de tous types de lignes (ligne, interautomatique, interconnexion, etc.) dans OpenScape Business S sont disponibles dans Tableau 43 : Niveau de configuration canaux de ligne avec OpenScape Business S à la page 1375

Tableau 41 : Niveau d'extension des canaux de ligne avec cartes mères OCCx

	X1	X5R	X8
Canaux de ligne maximum			
Nombre maxi. de canaux de ligne[21]	250	250	250
Canaux de ligne pour la connexion du fournisseur de services de téléphonie, de la mise en réseau, de l'ordinateur externe			
Canaux de ligne SIP (ITSP)	30	60[22]	60[22]
Canaux SIPQ (Mise en réseau)	100	100	100
Canaux RNIS S_0 (BRI)	4	52	128
Canaux RNIS S_{2M} (PRI)	-	30	79
Canaux RNIS CAS (PRI)	-	30	180
Canaux analogiques (a/b)	-	24	120
Canaux téléphoniques à usage interne			
Canaux du MEB pour les annonces internes[23]	0	16	16
Canaux de ligne MEB Trunk pour UC Suite[24]	0	0	0

Tableau 42 : Niveau d'extension des canaux de ligne avec cartes mères OCCSB/R, OCCMA/B ou OCCLA

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Canaux de ligne maximum						
Nombre maxi. de canaux de ligne[21]	250	250	250	250	250	250
Canaux de ligne pour la connexion du fournisseur de services de téléphonie, de la mise en réseau, de l'ordinateur externe						

21 Somme des canaux Trunk SIP, ITSP, SIPQ, TDM et MEB Trunk sans (canaux d'annonce MEB).

22 En réseau avec OpenScape Business S comme passerelle ITSP, plus de 60 canaux sont également possibles.

23 Les canaux MEB sont attribués dynamiquement par le système pour les annonces internes au système. Ils sont toujours inclus dans le nombre maximum de canaux de ligne.

24 Pour les systèmes avec UC Suite, les canaux Media Extension Bridge (MEB) sont générés dynamiquement pour : la messagerie vocale, AutoAttendant, Fax, les connexions Appelle-moi, les annonces et les conférences téléphoniques. Ils ne comptent que pour le nombre maximum de canaux de ligne dans les systèmes UC Suite.

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Canaux de ligne SIP (ITSP)	60/120[25]	60/120[25]	60/120[25]	60/120[25]	120	120
Canaux SIPQ (Mise en réseau)	100	100	100	100	100	100
Canaux RNIS S_0 (BRI)	-	-	48	48	128	128
Canaux RNIS S_{2M} (PRI)	-	-	30	30	180	120
Canaux RNIS CAS (PRI)	-	-	30	30	180	120
Canaux analogiques (a/b)	-	-	24	X5R : 24	120	120
Canaux téléphoniques à usage interne						
Canaux du MEB pour les annonces internes[23]	16	16	16	16	16	16
Canaux de ligne MEB Trunk pour UC Suite[24]	0	30/60[25]	0	30/60[25]	0	60

Tableau 43 : Niveau de configuration canaux de ligne avec OpenScape Business S

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Canaux de ligne maximum			
Nombre maxi. de canaux de ligne[21]	250	250	250
Canaux de ligne pour la connexion du fournisseur de services de téléphonie, de la mise en réseau, de l'ordinateur externe			
Canaux de ligne SIP	180	180	180
Canaux SIPQ (Mise en réseau)	100	100	100
Canaux téléphoniques à usage interne			
Canaux du MEB pour les annonces internes[23]	16	16	16
Canaux de ligne MEB Trunk pour UC Suite[24]	60	60	60

[25] Les valeurs sont échelonnées en fonction de la version du module :

26.3 Valeurs maximum des ressources

Tableau 44 : Niveau d'expansion autres fonctions / ressources

	X1	X5	X8	Serveur (S)
	Rack	**Rack**	**OCCL/OCCLA**	
Ressources système				
Canaux DSP				
DSP G.711 sans cryptage	8	128/ 48/ 8[30]	128/ 48/ 8[30]	n/a
DSP G.711 + G.729 sans cryptage	8	104/ 40/ 8[30]	104/ 40/ 8[30]	n/a
DSP G.711 avec cryptage	6	102/ 38/ 6[30]	102/ 38/ 6[30]	n/a
DSP G.711 + G.729 avec cryptage	6	81/ 31/ 6[30]	81/ 31/ 6[30]	n/a
DSP Fax T.38 (pour la passerelle RNIS)[28]	3	12/ 6/ 3[30]	12/ 6/ 3[30]	n/a
DSP Fax T.38 (pour UC Suite Fax)[29]	-	8/ 6/ 0[30]	8/ 6/ 0[30]	n/a
Canaux RTP Proxy				
Canaux RTP Proxy	30	60	60	180
Canaux de ligne MEB				
Total des canaux de ligne MEB	**0**	**0**	**0**	**75**
Canaux de ligne MEB pour les annonces	0	0	0	16
Canaux de ligne MEB pour UC Suite	-	0	0	60
Musique d'attente et PPP				
Sources MOH[26] (G.711a, G.711u, G.729ab, G.729a)	4	4	4	32
Canaux PPP	8	8	8	n/a
Annonces				
Nombre de dispositifs d'annonce par système	16	16	16	16
Dispositifs d'annonce via a/b	4	16	16	n/a
Annonces via Smart VM	6	6	6	6

26 16 connexions simultanées maximum par source MOH

	X1	X5	X8	Serveur (S)
	Rack	Rack	OCCL/OCCLA	
Annonce via UC-Suite	16	16	16	16
Annonce avant de répondre (système, pas UC-Suite)				
Nombre d'appelants pour lesquels une annonce peut être diffusée simultanément	24	24	24	24
Destinataires DTMF				
Destinataires DTMF	16	16	16	par communication via ITSP

26.3.1 Détails sur l’utilisation des canaux DSP

Dans OpenScape Business, les "canaux DSP" sont utilisés pour la conversion (transcodage) des flux de données. En principe, cela est nécessaire s’il y a une transition d’IP à TDM ou de TDM à IP pour les données vocales ou si un cryptage des données vocales est nécessaire. En détail :

- Connexion vocale entre le téléphone IP et le RNIS ou une ligne analogique (interurbaine).
- Connexion vocale via une ligne IP SIP/ITSP et des téléphones internes UP0/E, a/b ou RNIS.
- Connexion vocale à partir d’une ligne IP ou d’un abonné IP à une conférence interne. Ici, un canal de passerelle est nécessaire pour chaque client de ligne/IP participant à une conférence.
- Connexions à partir de téléphones UP0/E, a/b ou RNIS ou de lignes RNIS/analogiques vers les annonces, la messagerie vocale, le fax ou les conférences de UC Suite.
- Connexions vocales cryptées entre terminaux et connexions vocales cryptées sur les lignes ITSP. Ce n'est pas le cas pour la famille de cartes mères V3, à partir d'OpenScape Business V3R4.
- Les connexions à Music on Hold interne nécessitent un canal DSP par codec MoH configuré.

Pour les connexions suivantes, aucun canal DSP n'est nécessaire :

- Connexion entre utilisateurs IP internes sans cryptage (charges utiles directes).
- Connexion entre l’ITSP et l’abonné IP sans cryptage.

[27] La valeur dépend de UC Suite : Système avec UC Suite / Système sans UC Suite

[28] Les valeurs s'appliquent à OpenScape Business en tant que passerelle RNIS. G.711 à T38 ou vice versa sans UC Suite Fax

[29] UC Suite peut généralement gérer jusqu'à 8 connexions de fax simultanées. OpenScape Business X3/X5/X8 en tant que passerelle RNIS peut traiter 3 à 12 fax simultanés, en fonction du module DSP. La combinaison de ces deux paramètres détermine le nombre de connexions de fax T.38 ou G.711 simultanées.

[30] Les valeurs sont échelonnées en fonction de la configuration du Voice Channel Booster : avec OCCBH ou OCCB3 / avec OCCBL ou OCCB1 / carte mère uniquement

Les canaux DSP sont réalisés par un processeur de signal, qui est intégré sur la carte mère OCCL ou OCCLA respective dans les modèles X1, X3, X5 et X8.

Selon le type de transcodage, un processeur de signal peut traiter plus ou moins de canaux DSP simultanément. Les codecs audio suivants sont supportés :

- **Pour les connexions vocales**
  - Conversion IP (G.711) vers TDM avec G.711 ou vice versa.
  - Conversion IP (G.711) vers TDM avec G.711 ou vice versa avec le cryptage (SPE).
  - Conversion IP (G.729) vers TDM avec G.711 ou vice versa.
  - Conversion IP (G.729) vers TDM avec G.711 ou vice versa avec le cryptage (SPE).
- **Pour les connexion fax**
  - Conversion T.38 vers G.711 lors de l'utilisation d'OpenScape Business comme passerelle RNIS.
  - Conversion de la télécopie G.711 en télécopie T.38 ou vice versa en utilisant la fonction UC-Suite Fax.

Si la capacité du processeur de signal intégré à la carte mère n'est pas suffisante pour réaliser le nombre requis de canaux DSP, ceux-ci peuvent être étendus en utilisant les cartes "Voice Channel Booster" OCCBL ou OCCBH disponibles en option.

Le nombre maximum de canaux DSP disponibles en fonction du codage est indiqué dans le tableau 11. Veuillez noter que chaque ligne représente le nombre maximum de canaux DSP similaires, mais ceux-ci sont alloués dynamiquement par le système pendant le fonctionnement. Le nombre de canaux DSP actuellement occupés pendant le fonctionnement peut être déterminé via OpenScape Business Assistant (WBM). Vous trouverez d'autres notes sur la détermination du nombre de canaux DSP requis dans le manuel d'administration.

26.3.2 Détails sur l'utilisation des canaux proxy RTP

OpenScape Business utilise un "proxy RTP" interne pour toutes les connexions VoIP via l'Internet. Le proxy offre un ensemble de canaux RTP qui sont affectés aux connexions VoIP via Internet comme suit.

- 1 canal proxy RTP par appel ITSP
- 1 canal proxy RTP par appel Unify Phone
- 1 canal proxy RTP par système Device @Home en un seul appel
- 1 canal proxy RTP par SIP Device @Home en un seul appel
- 1 canal proxy RTP par myPortal @work VoIP @Home en un seul appel

Dans les différents modèles OpenScape Business, un nombre différent de canaux proxy RTP est disponible. Voir Tableau 44 : Niveau d'expansion autres fonctions / ressources à la page 1376.

Exemples

- Un appel vocal externe sortant d'un abonné au système IP interne via une ligne ITSP nécessite un canal proxy RTP.
- Un appel vocal externe arrivant via ITSP à un client VoIP myPortal @work au bureau à domicile nécessite deux canaux proxy RTP. Un canal proxy

RTP est nécessaire pour la connexion de l'ITSP au système OpenScape Business et un autre pour la connexion d'OpenScape Business via Internet au client VoIP de myPortal @work au bureau à domicile.

26.4 Valeurs maximales des ressources

Les valeurs maximales indiquées ici sont les capacités logicielles d'OpenScape Business.

26.4.1 Connexion au fournisseur de services

	X1R		X5R		X8W/R		Serveur (S)
	V2	V3	V2	V3	V2	V3	
Connexion à un fournisseur de services de téléphonie sur Internet (ITSP)							
canaux de jonction SIP	30	120	60	120	60	120	180
ITSP activé simultanément	8	8	8	8	8	8	8
Itinéraires							
Itinéraires	16	16	16	16	16	16	16
itinéraires de débordement par itinéraire	1	1	1	1	1	1	1

26.4.2 Abonnés

	X1R	X5R	X8	Serveur (S)
Numéro de téléphone d'abonné/Numéro SDA :				
Chiffres par numéro d'abonné/ numéro SDA	16 (par défaut = 3)	16 (par défaut = 3)	16 (par défaut = 3)	16 (par défaut = 3)

26.4.3 Niveaux d'extension UC Smart

- Les niveaux d'extension avec cartes mères V2 OCC peuvent être trouvés dans Tableau 45 : Niveau d'extension UC Smart avec cartes mères OCCx à la page 1380
- Les niveaux d'extension avec cartes mères V3 OCC peuvent être trouvés dans Tableau 46 : Niveau d'extension UC Smart avec cartes mères OCCSB/R, OCCMA/B ou OCCLA à la page 1381
- Les niveaux d'extension avec systèmes de serveurs OpenScape Business S peuvent être trouvés dans Tableau 47 : Niveau de configuration UC Smart avec OpenScape Business S à la page 1382

Tableau 45 : Niveau d'extension UC Smart avec cartes mères OCCx

	X1	X5R	X8
Utilisateurs UC Smart maxi.			
Nombre maximum d'utilisateurs de UC Smart (comptes)	30	50	50
UC Smart Clients			
Nombre de clients UC actifs simultanés.[31]	30	150	150
myPortal @work	30	50	50
myPortal @work Appels parallèles de la VoIP vers d'autres parties appelées[32]	20	30	30
Téléphone de bureau CP 400/600/600E/ 700/700X/710 (mode UC)	30	50	50
État de présence			
Statut par utilisateur	9	9	9
Annonces de messagerie vocale par état de présence	1	1	1
Favoris			
Favoris par utilisateur	100	100	100
Groupes favoris par utilisateur	10	10	10
Journal des appels			
Entrées du journal des appels par utilisateur	100	100	100
UC Smart Managed Conference (via UC Client)			
Nombre de conférences gérées	5	5	5
Nombre d'utilisateurs par conférence gérée	16	16	16
Canaux pour les conférences gérées	30	30	30

31 Somme de : myPortal @work, CP 400/600/600E/700/700X/710 Mode UC, Lanceur d'applications, TAPI 120 (WSI), clients WSI tiers (Contexte : plusieurs clients avec le même compte UC Smart peuvent se connecter au système)

32 Le nombre de connexions VoIP simultanées de l'abonné dépend de :

1) les canaux DSP disponibles dans le système pour les appels de passerelle (transition IP/TDM).

2) les canaux proxy RTP internes disponibles dans le système pour les appels VoIP via Internet.

33 le nombre de connexions simultanées en fonction des canaux DSP disponibles dans le système pour les appels de passerelle (transition IP/TDM).

Tableau 46 : Niveau d'extension UC Smart avec cartes mères OCCSB/R, OCCMA/B ou OCCLA

	X1R		X5		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Utilisateurs UC Smart maxi.						
Nombre maximum d'utilisateurs de UC Smart (comptes)	150	150	150/ 500[34]	150/ 500[34]	500	500
UC Smart Clients						
Nombre de clients UC actifs simultanés.[31]	150	150	150/ 500[34]	300/1 000[34]	1000	1000
myPortal @work	150	150	150/250[34]	150/250[34]	250	250
myPortal @work Appels parallèles de la VoIP vers d'autres parties appelées[32]	150	150	30/70[34]	30/70[34]	69	69
myPortal for Teams	150	150	150/ 500[34]	150/ 500[34]	500	500
Téléphone de bureau CP 400/600/600E/ 700/700X/710 (mode UC)	150	150	150/ 500[34]	150/ 500[34]	500	500
État de présence						
Statut par utilisateur	9	9	9	9	9	9
Annonces de messagerie vocale par état de présence	1	1	1	1	1	1
Favoris						
Favoris par utilisateur	100	100	100	100	100	100
Groupes favoris par utilisateur	10	10	10	10	10	10
Journal des appels						
Entrées du journal des appels par utilisateur	100	100	100	100	100	100
UC Smart Managed Conference (via UC Client)						
Nombre de conférences gérées	5	5	5	5	5	5
Nombre d'utilisateurs par conférence gérée	16	16	16	16	16	16
Canaux pour les conférences gérées	30	30	30	30	30	30

Tableau 47 : Niveau de configuration UC Smart avec OpenScape Business S

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Utilisateurs UC Smart maxi.			
Nombre maximum d'utilisateurs de UC Smart (comptes)	50	500	1500
UC Smart Clients			
Nombre de clients UC actifs simultanés.[31]	50	500	1500
myPortal @work	50	250	500
myPortal for Teams	50	250	500
Téléphone de bureau CP 400/600/600E/ 700/700X/710 (mode UC)	50	250	500
État de présence			
Statut par utilisateur	9	9	9
Annonces de messagerie vocale par état de présence	1	1	1
Favoris			
Favoris par utilisateur	100	100	100
Groupes favoris par utilisateur	10	10	10
Journal des appels			
Entrées du journal des appels par utilisateur	100	100	100
UC Smart Managed Conference (via UC Client)			
Nombre de conférences gérées	10	10	10
Nombre d'utilisateurs par conférence gérée	16	16	16
Canaux pour les conférences gérées	30	30	30

26.4.4 Niveaux d'extension de Smart Voicemail

- Les niveaux d'extension avec cartes mères V2 OCC peuvent être trouvés dans Tableau 48 : Niveau d'extension Smart Voicemail avec cartes mères OCCx à la page 1383
- Les niveaux d'extension avec cartes mères V3 OCC peuvent être trouvés dans Tableau 49 : Niveau d'extension Smart Voicemail avec cartes mères OCCSB/R, OCCMA/B ou OCCLA à la page 1383

[34] Les valeurs sont échelonnées en fonction de la version du module :

- Les niveaux d'extension avec systèmes de serveurs OpenScape Business S peuvent être trouvés dans Tableau 50 : Niveau d'extension Smart Voicemail avec OpenScape Business S à la page 1384

Tableau 48 : Niveau d'extension Smart Voicemail avec cartes mères OCCx

	X1R	X5R	X8	Serveur (S)
Smart Voicemail				
Boîtes Smart Voicemail	30	320	320	1500
Messages par boîte Voicemail	100	100	100	100
Durée d'enregistrement par appel (minutes)	2	2	2	2
Capacité d'enregistrement totale en heures	32	32	32	32
Connexions Voicemail simultanées (canaux)	10	10	10	60
Annonces	16	16	16	16
Standards automatiques/ d'entreprise	100	100	100	100
Standards automatiques/ d'entreprise (actifs simultanément)	6	6	6	6

Tableau 49 : Niveau d'extension Smart Voicemail avec cartes mères OCCSB/R, OCCMA/B ou OCCLA

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Smart Voicemail						
Boîtes Smart Voicemail	320	320	320/500[35]	320/500[35]	500	500
Messages par boîte Voicemail	100	100	100	100	100	100
Durée d'enregistrement par appel (minutes)	2	4	4	4	4	4
Capacité d'enregistrement totale en heures	32	64	32	64	32	64
Connexions Voicemail simultanées (canaux)	30	30	30	30	30	30
Annonces	16	16	16	16	16	16
Standards automatiques/ d'entreprise	100	100	100	100	100	100

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Standards automatiques/ d'entreprise (actifs simultanément)	6	6	6	6	6	6

Tableau 50 : Niveau d'extension Smart Voicemail avec OpenScape Business S

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Smart Voicemail			
Boîtes Smart Voicemail	1500	1500	1500
Messages par boîte Voicemail	100	100	100
Durée d'enregistrement par appel (minutes)	4	4	4
Capacité d'enregistrement totale en heures	64	64	64
Connexions Voicemail simultanées (canaux)	60	60	60
Annonces	16	16	16
Standards automatiques/d'entreprise	100	100	100
Standards automatiques/d'entreprise (actifs simultanément)	6	6	6

26.4.5 Niveaux d'extension UC Suite

- Les niveaux d'extension avec cartes mères V2 OCC peuvent être trouvés dans Tableau 51 : Niveau d'extension UC Suite avec cartes mères V2 à la page 1384
- Les niveaux d'extension avec cartes mères V3 OCC peuvent être trouvés dans Tableau 52 : Niveau d'extension UC Suite avec cartes mères OCCSB, OCCMA/B ou OCCLA à la page 1387
- Les niveaux d'extension avec systèmes de serveurs OpenScape Business S peuvent être trouvés dans Tableau 53 : Niveau de configuration UC Suite avec OpenScape Business S à la page 1390

Tableau 51 : Niveau d'extension UC Suite avec cartes mères V2

	X1	X5R	X8	Serveur (S)
Utilisateurs UC Suite maxi.				
Nombre maximum d'utilisateurs de UC Suite (Comptes)	-	0	0	1500

[35] Les valeurs sont échelonnées en fonction de la version du module :

	X1	X5R	X8	Serveur (S)
UC Suite Clients				
Nombre de clients UC actifs simultanés.[36]	-	0	0	1500
myPortal for Desktop	-	0	0	1500
myPortal for Outlook	-	0	0	1500
myAgent (actifs simultanés)	-	64	64	64
myAgent (configurable)	-	192	192	192
myReports	-	1	1	1
myAttendant	-	20	20	20
myPortal @work	-	0	0	250
myPortal @work Appels parallèles de la VoIP vers d'autres parties appelées[38]	-	30	30	60
Téléphone de bureau 400/600/600E/700/700X/710	-	0	0	250
État de présence				
État par abonné UC Suite	-	9	9	9
Annonces de messagerie vocale par état de présence	-	1	1	1
Journaux des appels (myPortal for Desktop et myPortal for Outlook) :				
Durée d'archivage dans les clients UC (jours)	-	30 par défaut = 30	30 par défaut = 30	30 par défaut = 30
Durée d'archivage dans le système de communication	-	365 par défaut = 30	365 par défaut = 30	365 par défaut = 30
Entrées du journal des appels[39]	-	Aucune limitation[39]	Aucune limitation[39]	Aucune limitation[39]
Entrées du journal des appels Interface graphique moderne de myPortal for Desktop	-	100 après le démarrage >100 pendant l'utilisation	100 après le démarrage >100 pendant l'utilisation	100 après le démarrage >100 pendant l'utilisation
UC Suite VoiceMail				
Boîtes VM	-	500/ 500/ 0	500/ 500/ 0	1500
Groupes VM	-	20/ 20/ 0	20/ 20/ 0	20
Messages par boîte vocale[39]	-	n/a	n/a	n/a
Durée d'enregistrement par appel (minutes)	-	15	15	15

	X1	X5R	X8	Serveur (S)
Durée d'enregistrement pouvant être transmise par courrier électronique (minutes)[40]	-	~10	~10	~10
Capacité d'enregistrement totale (heures)[39]	-	n/a	n/a	n/a
Connexions simultanées à la messagerie vocale (canaux MEB)	-	30	30	60
Standard automatique UC Suite				
Standard automatique personnel	-	0	0	20
Standard automatique de l'entreprise	-	0	0	1
Chat multi-utilisateurs (messagerie instantanée)				
Partenaires de communication internes	-	sans restriction	sans restriction	sans restriction
Annonces par utilisateur UC Suite				
Messages d'accueil	-	0	0	1
Annonces liées à l'état de présence	-	0	0	1
Annonce du standard automatique personnel	-	0	0	1
Enregistrement des appels UC Suite				
Durée d'enregistrement par appel/ conférence	-	Limité par la durée de l'appel	Limité par la durée de l'appel	Limité par la durée de l'appel
UC Suite Fax				
Boîtes Fax	-	0	0	1500
Groupes boîtes Fax	-	0	0	60
Abonnés par groupe boîtes Fax	-	0	0	10
Longueur de fax en pages	-	0	0	500
Fax T.38 simultanés	-	0	0	8
Destinataires de fax fusionnés	-	aucune limitation	aucune limitation	aucune limitation
Conférences UC Suite				
Conférences simultanées UC Suite	-	0	0	10
Participants par conférence UC Suite	-	0	0	16
Participants externes par conférence UC Suite	-	0	0	15

	X1	X5R	X8	Serveur (S)
Nombre maximum de Nombre maxi. de canaux pour les conférences UC Suite	-	0	0	60
Nombre de canaux réservés aux conférences ad hoc et Meet Me de UC Suite	-	0	0	60
Connexion à la base de données externe (LDAP)				
Connexions externes à la base de données UC Server	-	0	0	10

Tableau 52 : Niveau d'extension UC Suite avec cartes mères OCCSB, OCCMA/B ou OCCLA

	X5R		X8	
		+ SSD NVMe		+ SSD NVMe
Utilisateurs UC Suite maxi.				
Nombre maximum d'utilisateurs de UC Suite (Comptes)	-	50/500[41]	-	500 300 en cas de centre d'appels
UC Suite Clients				
Nombre de clients UC actifs simultanés.[36]	-	100/1 000[41] 600 en cas de centre d'appels	-	1000 600 en cas de centre d'appels
myPortal for Desktop	-	50/500[41] 300 en cas de centre d'appels	-	500 300 en cas de centre d'appels

36 Somme de : myPortal Desktop, myPortal for Outlook, myAttendant, myAgent, myReports, myPortal @work, myPortal for Teams, mode UC CP 400/600/600E/700/700X/710 (Arrière-plan : plusieurs clients avec le même compte UC Suite peuvent se connecter au système)

37 La valeur inférieure s'applique aux systèmes avec UC Suite Contact Center

38 Le nombre de connexions VoIP simultanées de l'abonné dépend de

1) les canaux DSP disponibles dans le système pour les appels de passerelle (transition IP/TDM).

2) les canaux proxy RTP internes disponibles dans le système pour les appels VoIP via Internet.

39 La valeur dépend de la capacité de stockage HD / SSD du disque dur disponible. Aucune limitation liée à l'abonné n'est implémentée.

1) Une durée d'enregistrement d'une minute utilise environ 1 Mo d'espace de stockage

2) Un fax normalisé (2 pages DIN A4) correspond à env. 48 Ko d'espace de stockage)

Exemple : Pour un disque dur de 160 Go, la capacité mémoire de la partition servant à enregistrer les annonces vocales, les messages vocaux, les appels vocaux et les fax représente 20 Go. Cela correspond à une durée d'enregistrement totale d'environ 20 000 minutes.

40 En cas d'enregistrements plus longs, l'enregistrement est fractionné et envoyé dans plusieurs fichiers.

	X5R		X8	
		+ SSD NVMe		+ SSD NVMe
myPortal for Outlook	-	50/500[41] 300 en cas de centre d'appels	-	500 300 en cas de centre d'appels
myAgent (actifs simultanés)	-	0/64[41]	-	64
myAgent (configurable)	-	0/192[41]	-	192
myReports	-	0/1[41]	-	1
myAttendant	-	4/20[41]	-	20
myPortal @work	-	50/250[41] 300 en cas de centre d'appels	-	250 300 en cas de centre d'appels
myPortal @work Appels parallèles de la VoIP vers d'autres parties appelées[38]	-	30/70[41]	-	69
myPortal for Teams	-	50/500[41] 300 en cas de centre d'appels	-	500 300 en cas de centre d'appels
Téléphone de bureau CP 400/600/600E/ 700/700X/710	-	50/500[41] 300 en cas de centre d'appels	-	500 300 en cas de centre d'appels
État de présence				
État par abonné UC Suite	-	9	-	9
Annonces de messagerie vocale par état de présence	-	1	-	1
Journaux des appels (myPortal for Desktop et myPortal for Outlook) :				
Durée d'archivage dans les clients UC (jours)	-	30 par défaut = 30	-	30 par défaut = 30
Durée d'archivage dans le système de communication	-	365 par défaut = 30	-	365 par défaut = 30
Entrées du journal des appels[39]	-	Aucune limitation[39]	-	Aucune limitation[39]
Entrées du journal des appels Interface graphique moderne de myPortal for Desktop	-	100 après le démarrage >100 pendant l'utilisation	-	100 après le démarrage >100 pendant l'utilisation
UC Suite VoiceMail				

	X5R		X8	
		+ SSD NVMe		+ SSD NVMe
Boîtes VM	-	50/500[41]	-	500
Groupes VM	-	32	-	32
Messages par boîte vocale[39]	-	n/a	-	n/a
Durée d'enregistrement par appel (minutes)	-	15	-	15
Durée d'enregistrement pouvant être transmise par courrier électronique (minutes)[40]	-	~10	-	~10
Capacité d'enregistrement totale (heures)[39]	-	n/a	-	n/a
Connexions simultanées à la messagerie vocale (canaux MEB)	-	30/60[41]	-	60
Standard automatique UC Suite				
Standard automatique personnel	-	20	-	20
Standard automatique de l'entreprise	-	1	-	1
Chat multi-utilisateurs (messagerie instantanée)				
Partenaires de communication internes	-	sans restriction	-	sans restriction
Annonces par utilisateur UC Suite				
Messages d'accueil	-	1	-	1
Annonces liées à l'état de présence	-	1	-	1
Annonce du standard automatique personnel	-	1	-	1
Enregistrement des appels UC Suite				
Durée d'enregistrement par appel/conférence	-	Limité par la durée de l'appel	-	Limité par la durée de l'appel
UC Suite Fax				
Boîtes Fax	-	50/500[41]	-	500
Groupes boîtes Fax	-	60	-	60
Abonnés par groupe boîtes Fax	-	10	-	10
Longueur de fax en pages	-	500	-	500
Fax T.38 simultanés	-	3/8[41]	-	8
Destinataires de fax fusionnés	-	aucune limitation	-	aucune limitation
Conférences UC Suite				

	X5R		X8	
		+ SSD NVMe		+ SSD NVMe
Conférences simultanées UC Suite	-	5	-	5
Participants par conférence UC Suite	-	16	-	16
Participants externes par conférence UC Suite	-	15	-	15
Nombre maximum de Nombre maxi. de canaux pour les conférences UC Suite	-	30	-	30
Nombre de canaux réservés aux conférences ad hoc et Meet Me de UC Suite	-	20	-	20
Connexion à la base de données externe (LDAP)				
Connexions externes à la base de données UC Server	-	10	-	10

Tableau 53 : Niveau de configuration UC Suite avec OpenScape Business S

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Utilisateurs UC Suite maxi.			
Nombre maximum d'utilisateurs de UC Suite (Comptes)	150	500	1500
UC Suite Clients			
Nombre de clients UC actifs simultanés.[36]	150	500	1500
myPortal for Desktop	50	500	1500
myPortal for Outlook	50	500	1500
myAgent (actifs simultanés)	0	64	64
myAgent (configurable)	0	192	192
myReports	1	1	1
myAttendant	20	20	20
myPortal @work	50	250	500
myPortal @work Appels parallèles de la VoIP vers d'autres parties appelées[38]	30	60	60

41 Les valeurs sont échelonnées en fonction de la version du module :

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
myPortal for Teams	50	250	500
Téléphone de bureau CP 400/600/600E/ 700/700X/710	50	250	500
État de présence			
État par abonné UC Suite	9	9	9
Annonces de messagerie vocale par état de présence	1	1	1
Journaux des appels (myPortal for Desktop et myPortal for Outlook) :			
Durée d'archivage dans les clients UC (jours)	30 par défaut = 30	30 par défaut = 30	30 par défaut = 30
Durée d'archivage dans le système de communication	365 par défaut = 30	365 par défaut = 30	365 par défaut = 30
Entrées du journal des appels[39]	Aucune limitation[39]	Aucune limitation[39]	Aucune limitation[39]
Entrées du journal des appels Interface graphique moderne de myPortal for Desktop	100 après le démarrage >100 pendant l'utilisation	100 après le démarrage >100 pendant l'utilisation	100 après le démarrage >100 pendant l'utilisation
UC Suite VoiceMail			
Boîtes VM	150	500	1500
Groupes VM	32	32	32
Messages par boîte vocale[39]	n/a	n/a	n/a
Durée d'enregistrement par appel (minutes)	15	15	15
Durée d'enregistrement pouvant être transmise par courrier électronique (minutes)[40]	~10	~10	~10
Capacité d'enregistrement totale (heures)[39]	n/a	n/a	n/a
Connexions simultanées à la messagerie vocale (canaux MEB)	60	60	60
Standard automatique UC Suite			
Standard automatique personnel	20	20	20
Standard automatique de l'entreprise	1	1	1
Chat multi-utilisateurs (messagerie instantanée)			
Partenaires de communication internes	sans restriction	sans restriction	sans restriction
Annonces par utilisateur UC Suite			

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Messages d'accueil	1	1	1
Annonces liées à l'état de présence	1	1	1
Annonce du standard automatique personnel	1	1	1
Enregistrement des appels UC Suite			
Durée d'enregistrement par appel/ conférence	Limité par la durée de l'appel	Limité par la durée de l'appel	Limité par la durée de l'appel
UC Suite Fax			
Boîtes Fax	1500	1500	1500
Groupes boîtes Fax	60	60	60
Abonnés par groupe boîtes Fax	10	10	10
Longueur de fax en pages	500	500	500
Fax T.38 simultanés	8	8	8
Destinataires de fax fusionnés	aucune limitation	aucune limitation	aucune limitation
Conférences UC Suite			
Conférences simultanées UC Suite	10	10	10
Participants par conférence UC Suite	16	16	16
Participants externes par conférence UC Suite	15	15	15
Nombre maximum de Nombre maxi. de canaux pour les conférences UC Suite	60	60	60
Nombre de canaux réservés aux conférences ad hoc et Meet Me de UC Suite	60	60	60
Connexion à la base de données externe (LDAP)			
Connexions externes à la base de données UC Server	10	10	10

26.4.6 Fonctions sur le téléphone

	X1R	X5R	X8	Serveur (S)
Liste des appelants pour les téléphones du système (HFA)				
Listes des appelants par système	650	650	650	1300
Listes des appelants par station dans le système	1	1	1	1
Entrées par liste des appelants	10	10	10	10
Chiffres enregistrés par entrée plus indicatif de prise de ligne	25 + (6)	25 + (6)	25 + (6)	25 + (6)

	X1R	X5R	X8	Serveur (S)
Touches d'appel direct (touches DSS) :				
Satellites par système de communication	250	250	250	250
Satellites par téléphone	2	2	2	2
Touches par module OpenStage Key	12	12	12	12
Touches par module OpenStage Key 15	18	18	18	18
Satellites de supervision (BLF) par système de communication	12	25	25	25
Touches par satellite de supervision	90	90	90	90
Numéro abrégé individuel (KWI)				
Entrées dans la base KWI par système de communication	2000	2000	2000	2000
Entrées par abonné	10	10	10	10
Chiffres par entrée	25	25	25	25
(plus indicatif de prise de ligne)	(+ 6)	(+ 6)	(+ 6)	(+ 6)
Numérotation abrégée centralisée (KWZ)				
Entrées dans la base KWI par système de communication	8000	8000	8000	8000
Nombre de caractères du nom	16	16	16	16
Chiffres par entrée	25	25	25	25
(plus indicatif de prise de ligne)	(+ 6)	(+ 6)	(+ 6)	(+ 6)
Répétition de la numérotation				
Entrées par OpenStage 20/ 20E/ 20G/ 40/ 40G	3	3	3	3
Entrées par OpenStage 15	10	10	10	10
Entrées par OpenStage 60/ 60G/ 80/ 80G	30	30	30	30
Entrées par téléphone sans écran	1	1	1	1
Chiffres enregistrés par entrée	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Avertissement/indication d'appel				
Appelants en attente par téléphone	16			
Parcage				
Positions de parcage par système	10			
Rappels				
Demandes de rappel par téléphone	5			

	X1R	X5R	X8	Serveur (S)
Textes d'absence/textes de message				
Textes d'absence par système	250	250	250	250
Textes de message par système	150	150	150	150
Textes d'absence configurables + textes de message par système	10 + 10	10 + 10	10 + 10	10 + 10
Nombre de caractères d'un texte d'absence configurable/d'un texte de message	24	24	24	24
Textes d'absence reçus/textes de message par téléphone avec écran	5	5	5	5
Textes d'absence reçus/textes de message par téléphone sans écran	1	1	1	1
Pilotage activé				
Abonnés inclus	5			
Renvoi d'appel				
Destinations de renvoi par téléphone	4	4	4	4
Chiffres par destination externe CFW (plus code de prise de ligne)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Séquence de destinations de renvoi				5
Conférences gérées par le système				
Conférences système simultanées par système	10	10	10	8
Abonnés par conférence	8	8	8	8
Abonnés externes par conférence	7	7	7	7
Canaux de conférence	32	32	32	20
Poste de portier/ouverture de la porte				
Connexions via interfaces a/b par système	4	4	4	-
Chiffres par entrée de code	5	5	5	-
Réservation de ligne				
Entrées simultanées par système	32	32	32	-

Remarque : Pour tous les scénarios de renvoi d'appel ci-dessus, les utilisateurs ne peuvent saisir qu'une seule destination de renvoi par MSN. Le nombre de MSN pouvant être renvoyés est limité à 10.

En cas de ITSP ou RNIS configuré avec un SDA, le nombre est 249.

26.4.7 Travailler en équipe (groupes)

- Des informations sur les cartes mères V2 OCC sont disponibles dans Tableau 54 : Données pour cartes mères V2 à la page 1395
- Des informations sur les cartes mères V3 OCC sont disponibles dans Tableau 55 : Données pour cartes mères V3 à la page 1396
- Des informations sur les systèmes de serveurs OpenScape Business S sont disponibles dans Tableau 56 : Données de OpenScape Business S à la page 1398

Tableau 54 : Données pour cartes mères V2

	X1	X5R	X8
Groupes d'interception			
Groupes d'interception d'appel par système	32	32	32
Abonnés par groupe d’interception	32	32	32
Sonnerie d'appel (groupe configurable par l'utilisateur)			
Nombre de postes dans le groupe de sonnerie d'appel	5	5	5
Appels de groupe, groupes de recherche, MULAP de base			
Total des appels collectifs, groupes de recherche, MULAP de base, MULAP chef et groupes de messagerie vocale par système de communication	800	800	800
Longueur du nom du groupe	16	16	16
Nombre de groupes auxquels un utilisateur peut être affecté	32	32	32
Abonnés par Appel de groupe, groupe de recherche, MULAP de base	20	20	20
MULAP Chefs, groupes Team, groupes Top et groupes Messagerie vocale :			
Nombre total de groupes MULAP Chefs, Team et Top par	500	500	500
Abonnés par MULAP chef, Groupe Team, Groupe Top	10	10	10
Touches MULAP par téléphone	10	10	10
Groupes de messagerie vocale			
Nombre de groupes de messagerie vocale	20	20	20
Abonnés par groupe de messagerie vocale	20	20	20
Diffusion interne (Voice Paging)			
Diffusions simultanées par système de communication	1	1	1
Destinataires de la diffusion	20	20	20
Groupes UCD			
Groupes UCD par système	60	60	60

	X1	X5R	X8
Annonces par groupe UCD	7	7	7
Niveaux de priorité par groupe UCD	10	10	10
Appels en attente par groupe UCD (dernier groupe max 72)	30	30	30
Agents UCD			
ID agents UCD par système de communication	330	330	330
Agents UCD actifs simultanément par système de communication	64	64	64
Annonces de l'UCD			
Nombre d'appelants par système de communication pouvant écouter simultanément une annonce.	8	8	8

Tableau 55 : Données pour cartes mères V3

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Groupes d'interception						
Groupes d'interception d'appel par système	64	64	64/128[42]	64/128[42]	128	128
Abonnés par groupe d'interception	32	32	32	32	32	32
Sonnerie d'appel (groupe configurable par l'utilisateur)						
Nombre de postes dans le groupe de sonnerie d'appel	5	5	5	5	5	5
Appels de groupe, groupes de recherche, MULAP de base						
Total des appels collectifs, groupes de recherche, MULAP de base, MULAP chef et groupes de messagerie vocale par système de communication	800	800	800	800	800	800
Longueur du nom du groupe	16	16	16	16	16	16
Nombre de groupes auxquels un utilisateur peut être affecté	32	32	32	32	32	32

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Abonnés par Appel de groupe, groupe de recherche, MULAP de base	20	20	20/32[42]	20/32[42]	32	32
MULAP Chefs, groupes Team, groupes Top et groupes Messagerie vocale :						
Nombre total de groupes MULAP Chefs, Team et Top par	500	500	500	500	500	500
Abonnés par MULAP chef, Groupe Team, Groupe Top	10	10	10	10	10	10
Touches MULAP par téléphone	10	10	10	10	10	10
Groupes de messagerie vocale						
Nombre de groupes de messagerie vocale	20	20	20	20	20	20
Abonnés par groupe de messagerie vocale	20	20	20	20	20	20
Diffusion interne (Voice Paging)						
Diffusions simultanées par système de communication	1	1	1	1	1	1
Destinataires de la diffusion	20	20	20/32[42]	20/32[42]	32	32
Groupes UCD						
Groupes UCD par système	60	60	60	60	60	60
Annonces par groupe UCD	7	7	7	7	7	7
Niveaux de priorité par groupe UCD	10	10	10	10	10	10
Appels en attente par groupe UCD (dernier groupe max 72)	30	30	30	30	30	30
Agents UCD						
ID agents UCD par système de communication	330	330	330	330	330	330
Agents UCD actifs simultanément par système de communication	64	64	64	64	64	64

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Annonces de l'UCD						
Nombre d'appelants par système de communication pouvant écouter simultanément une annonce.	8	8	8	8	8	8

Tableau 56 : Données de OpenScape Business S

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Groupes d'interception			
Groupes d'interception d'appel par système	32	64	128
Abonnés par groupe d'interception	32	32	32
Sonnerie d'appel (groupe configurable par l'utilisateur)			
Nombre de postes dans le groupe de sonnerie d'appel	5	5	5
Appels de groupe, groupes de recherche, MULAP de base			
Total des appels collectifs, groupes de recherche, MULAP de base, MULAP chef et groupes de messagerie vocale par système de communication	800	800	800
Longueur du nom du groupe	16	16	16
Nombre de groupes auxquels un utilisateur peut être affecté	32	32	32
Abonnés par Appel de groupe, groupe de recherche, MULAP de base	32	32	32
MULAP Chefs, groupes Team, groupes Top et groupes Messagerie vocale :			
Nombre total de groupes MULAP Chefs, Team et Top par	500	500	500
Abonnés par MULAP chef, Groupe Team, Groupe Top	10	10	10
Touches MULAP par téléphone	10	10	10
Groupes de messagerie vocale			
Nombre de groupes de messagerie vocale	20	20	20
Abonnés par groupe de messagerie vocale	20	20	20
Diffusion interne (Voice Paging)			

[42] Les valeurs sont échelonnées en fonction de la version du module :

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Diffusions simultanées par système de communication	1	1	1
Destinataires de la diffusion	20	20	20
Groupes UCD			
Groupes UCD par système	60	60	60
Annonces par groupe UCD	7	7	7
Niveaux de priorité par groupe UCD	10	10	10
Appels en attente par groupe UCD (dernier groupe max 72)	30	30	30
Agents UCD			
ID agents UCD par système de communication	330	330	330
Agents UCD actifs simultanément par système de communication	64	64	64
Annonces de l'UCD			
Nombre d'appelants par système de communication pouvant écouter simultanément une annonce.	8	8	8

26.4.8 Routage des appels

	X1R	X5R	X8	Serveur (S)
Routage au moindre coût (LCR)				
chiffres composés	24	24	24	24
chiffres vérifiés	24	24	24	24
Plans de numérotation (10 champs maximum par plan)	1000	1000	1000	1000
Tables de routage	254	254	254	254
Routes par table de routage	16	16	16	16
Règles de numérotation par itinéraire	254	254	254	254
Nombre de fuseaux horaires par jour/semaine	8	8	8	8
Règle du nombre de chiffres par numérotation	40	40	40	40
Service de nuit				
Stations autorisées par système	5	5	5	5
Service d'appel d'urgence E911 (États-Unis uniquement)				

	X1R	X5R	X8	Serveur (S)
Chiffres par LIN (Numéro d'identification de l'emplacement)	16	16	16	16
Ligne d'assistance après expiration du délai/Ligne d'assistance				
Destinations des lignes d'assistance téléphonique par système de communication	6	6	6	6
Groupes CON				
Groupes CON par système	64	64	64	64

Assistants pour cartes mères V2

	X1R	X5R	X8	Serveur (S)
mon assistant				
mon assistant (suite UC) par système	-	20	20	20
Répondeur automatique (UC Smart)				
Répondeur automatique de l'entreprise	100	100	100	100
Répondeur automatique (UC Suite)				
Répondant automatique	-	0	0	20

Assistants pour cartes mères V3

	X1R	X5R	X8	Serveur (S)
mon assistant				
mon assistant (suite UC) par système	4	4/20[43]	20	20
Répondeur automatique (UC Smart)				
Répondeur automatique de l'entreprise	100	100	100	100
Répondeur automatique (UC Suite)				
Répondant automatique	20	20/ 20[43]	20/ 20[43]	20

26.4.9 Centre de contacts multimédia

	X1R	X5R	X8	Serveur (S)
Files d'attente du centre de contacts				
Files d'attente par système de communication	-	50	50	50

[43] Les valeurs sont décalées selon la version du plateau : Basique/Avancée

	X1R	X5R	X8	Serveur (S)
Terminer				
Codes de post-traitement	-	aucune limitation	aucune limitation	aucune limitation
Agents				
Agents actifs simultanés)	-	64	64	64
Agents (configurables)	-	192	192	192
Rapports historiques				
Clients myReports simultanément actifs par système	-	1	1	1

26.4.10 Limites d'extension Mobility

Tableau 57 : Données pour cartes mères V2 OCC

	X1	X5R	X8
Postes de travail de télétravailleurs			
Postes de télétravailleurs via VPN par système de communication	10	10	10
Abonnés Mobility			
Abonnés Mobility Entry par système	30	150	150

Tableau 58 : Données pour cartes mères V3 OCC

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Postes de travail de télétravailleurs						
Postes de télétravailleurs via VPN par système de communication	10	10	10	10	10	10
Abonnés Mobility						
Abonnés Mobility Entry par système	150/ 500[45]	150/ 500[45]	150/ 500[45]	150/ 500[45]	500	500
myPortal for Teams (UC Smart) : abonnés par système	150	150	150/ 500[45]	150/ 500[45]	500	500
myPortal for Teams (UC Suite) : abonnés par système	-	50	-	50/500 300 en cas de centre d’appels	-	500 300 en cas de centre d’appels

[44] Les valeurs sont échelonnées en fonction de la configuration de l'UC Booster : Serveur Booster/Carte Booster/ sans UC Booster

Tableau 59 : Données de OpenScape Business S

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Abonnés Mobility			
Abonnés Mobility Entry par système	50	150	150
myPortal for Teams (UC Smart) : abonnés par système	50	250	500
myPortal for Teams (UC Suite) : abonnés par système	50	250	500

26.4.11 Sécurité

	X1R	X5R	X8	Serveur (S)
Code de verrouillage individuel				
Chiffres par code de verrouillage du téléphone	5	5	5	5
Caractères autorisés	0 - 9	0 – 9	0 – 9	0 – 9
Discrimination réseau				
Nombre de listes autorisées	6	6	6	6
Nombre de listes refusées	6	6	6	6
Numéros autorisés liste courte (10 entrées de 32 chiffres chacune)	5	5	5	5
Numéros autorisés liste longue (100 entrées avec 32 chiffres chacune)	1	1	1	1
Numéros interdits liste courte (10 entrées de 32 chiffres chacune)	5	5	5	5
Numéros interdits liste longue (50 entrées avec 32 chiffres chacune)	1	1	1	1
Classes de service				
Classes de service par système	15	15	15	15
Taille de la matrice - jour et nuit - nombre de lignes	30	30	30	30
Listes des numéros autorisés et des numéros interdits	15	15	15	15
Groupes utilisés fermés (groupes ITR - VBZ Gruppen)				

[45] Les valeurs sont échelonnées en fonction de la version du module :

	X1R	X5R	X8	Serveur (S)
Groupes de RTI par système	16	64	64	64
Taille de la matrice - jour et nuit - nombre de lignes	30	30	30	30
Listes des numéros autorisés et des numéros interdits	15	15	15	15

26.4.12 Mise en réseau de OpenScape Business

Mise en réseau OpenScape Business X1R, OpenScape Business X5R, OpenScape Business X8, OpenScape Business S : des versions spécifiques au projet peuvent être demandées pour les exigences de mise en réseau au-delà des limites de configuration énumérées ici. Veuillez tenir compte de la validation de distribution actuelle.

	X1R	X5R	X8	Serveur (S)
Mise en réseau de OpenScape Business				
Systèmes de communication en réseau (nœuds)	8/ 32[46]	8/ 32[46]	8/ 32[46]	8/ 32[46]
Abonnés dans le réseau	1000	1000	1000	1000

26.4.13 Connectivité des applications

Tableau 60 : Données pour les cartes mères V2 OCC

	X1R	X5R	X8
Interface CSTA			
Liens CSTA via CSP par système	-	4/ 4/ 0[47]	4/ 4/ 0[47]
Points de surveillance pour les lignes ou les stations	-	1500	1500
Serveur intermédiaire TAPI 170	-	4	4
Clients TAPI 120 (CSTA)	-	150/ 150/ 0[47]	150/ 150/ 0[47]
Interface de services Web (WSI)			
WSI - nombre total de clients actifs simultanés	30	500/ 300/ 150[47]	500/ 300/ 150[47]
myPortal au travail	30	250/ 150/ 50[47]	250/ 150/ 50[47]
Téléphone de bureau CP 400/600/600E/ 700/700X/710 avec WSI	30	150/ 150/ 50[47]	150/ 150/ 50[47]

[46] Les valeurs sont échelonnées selon : Réseau avec UC Suite / Réseau sans UC Suite

	X1R	X5R	X8
Lanceur d'applications	30	250/ 150/ 50[47]	250/ 150/ 50[47]
TAPI 120 (mode WSI)	30	0/ 0/ 30[47]	0/ 0/ 30[47]
application tierce	repos	repos	repos

Tableau 61 : Données pour les cartes mères V3 OCC

	X1R		X5R		X8	
		+ SSD NVMe		+ SSD NVMe		+ SSD NVMe
Interface CSTA						
Liens CSTA via CSP par système	-	-	4	4	4	4
Points de surveillance pour les lignes ou les stations	1650	1650	1650/ 3750[48]	1650/ 3750[48]	3750	3750
Serveur intermédiaire TAPI 170	4	4	4	4	4	4
Clients TAPI 120 (CSTA)	150	150	150/ 500[48]	150/ 500[48]	500	500
Interface de services Web (WSI)						
WSI - nombre total de clients actifs simultanés	150	300	150/ 500[48]	300/ 1000[48]	1000	1000
myPortal au travail	150	150	150/ 250[48]	150/ 250[48]	250	250
myPortail pour les équipes	150	150	150/ 500[48]	150/ 500[48]	500	500
Téléphone de bureau CP 400/600/600E/ 700/700X/710 avec WSI	150	150	150/ 500[48]	150/ 500[48]	500	500
Lanceur d'applications	150	150	150/ 500[48]	150/ 500[48]	500	500
TAPI 120 (mode WSI)	**Remarque :** Suppression progressive sur les cartes mères V3 OCC. Prise en charge en V3 uniquement pour les cartes mères V2.					
application tierce	repos	repos	repos	repos	repos	repos

47 Les valeurs sont échelonnées selon la configuration du UC Booster : Serveur Booster / Carte Booster / sans UC Booster

48 Les valeurs sont décalées selon la version du plateau : Basique/Avancée

Tableau 62 : Données pour OpenScape Business S

	Serveur de base (S)	Serveur standard (S)	Serveur avancé (S)
Interface CSTA			
Liens CSTA via CSP par système	4	4	4
Points de surveillance pour les lignes ou les stations	3750	3750	3750
Serveur intermédiaire TAPI 170	4	4	4
Clients TAPI 120 (CSTA)	50	500	1500
Interface de services Web (WSI)			
WSI - nombre total de clients actifs simultanés	150	500	1500
myPortal au travail	50	250	500
myPortail pour les équipes	50	250	500
400/600/600E/ 700/700X/710 avec WSI	50	250	500
Lanceur d'applications	50	250	500
TAPI 120 (mode WSI)	0	0	0
application tierce	repos	repos	repos

26.4.14 Comptabilité

	X1R	X5R	X8	Serveur (S)
Centre d'enregistrement des détails d'appel				
Nombre d'entrées dans la mémoire tampon de données d'appel par système	20000	20000	20000	20000
Code de compte (ACCT) :				
Saisie des codes de compte par système de communication	1000	1000	1000	1000
Chiffres vérifiables par code de compte	11	11	11	11
Caractères autorisés	0-9	0-9	0-9	0-9

27 Mode Expert

Le Mode Expert fournit des menus avec des fonctions pour la configuration et la maintenance du système de communication.

27.1 Conventions de présentation des discriptions de paramètres

Les descriptions de paramètres sont effectuées selon la structure du mode Expert dans WBM.

Entrée menu	A chaque entrée de menu du mode Expert correspond une rubrique d'Aide que vous pouvez appeler directement (de manière contextuelle) à partir de la WBM. Le titre de la rubrique Aide indique le chemin de la fenêtre WBM. Exemple : **Configuration de base** > **Système** > **Flags système**
Onglet	Dans la rubrique Aide, il est affecté à chaque onglet un tableau de paramètres propre. Les mêmes paramètres de différents onglets sont décrits dans le même tableau de paramètres. Au dessus de chaque table de paramètres figure une liste des onglets auxquels correspondent les paramètres. Exemple : • **Ajouter une adresse IP statique** • **Modifier l'adresse IP statique** • **Effacer l'adresse IP statique**
Zone	Si les fenêtres WBM sont structurées en zones, vous retrouvez cette structure dans le tableau des paramètres. Le tableau des paramètres comprend, pour chaque zone, un titre intermédiaire, suivi des paramètres de cette zone.

Paramètres	Les paramètres sont décrits dans un tableau des paramètres à deux colonnes. La colonne de gauche correspond aux paramètres. La colonne de droite correspond à la description des paramètres. Les paramètres qui s'expliquent tous seuls sont cités, mais ne sont pas décrits. A la fin de la description, figurent la plage de valeurs et la valeur par défaut, s'il y en a.
Paramètres (option)	Paramètres qui ne doivent pas nécessairement être définis sont identifiés par le terme Option.
Entrée de la liste déroulante	Les paramètres qui ne s'expliquent tous seuls et figurent dans une liste déroulante sont aussi cités dans la colonne de gauche du tableau des paramètres. L'entrée est séparée par deux points du nom de la liste déroulante. Exemple : **Algorithmes de chiffrement : AES**
Case à cocher/champ d'option/flag	La description de la case à cocher / du champ d'option / du flag correspond toujours à l'état activé.

27.2 Maintenance

Les fonctions de maintenance du système de communication, par exemple pour le téléchargement de la musique d'attente ou la mise à jour des images logicielles, sont regroupées sous la rubrique **Maintenance**.

27.2.1 Configuration

Dans **Configuration** figurent des fonctions permettant par ex. de charger une Musique d'attente (MOH) ou d'afficher la configuration matérielle.

27.2.1.1 Configuration > Musique d'attente (MoH) > Charger sur la passerelle

Description des paramètres des onglets :

- **Charger les fichiers de musique d'attente (MoH) via HTTP**

Paramètres	Description
Charger les fichiers de musique d'attente (MoH) via HTTP	

Paramètres	Description
Fichier MoH journés	Sélection du fichier MoH Jour à partir du système de fichier local. Format du fichier : voir indications dans WBM.
Fichier MoH nuit	Sélection du fichier MoH Nuit à partir du système de fichier local. Format du fichier : voir indications dans WBM.
Charger	Chargement du fichier MoH sélectionné dans le système (nécessite un redémarrage). Activation dans Configuration, Téléphonie centrale > Musique d'attente/ Annonces.

Description des paramètres des onglets :

- **Charger les fichiers audio via HTTP**

Paramètres	Description
Charger les fichiers audio via HTTP	
Fichier d'annonce	Sélection du fichier WAV avec annonce à partir du système de fichier local. Format du fichier : voir indications dans WBM.
Fichiers audio déjà chargés	
Fichier son	Affichage des fichiers d'anonce chargé dans le système de communication
Effacer	Effacement du fichier d'annonce
Charger	Chargement du fichier d'annonce sélectionné dans le système. Activation dans Configuration, Téléphonie centrale > Musique d'attente/ Annonces.

27.2.1.2 Configuration > Annonces > Charger vers la passerelle

Description des paramètres des onglets :

- **Charger des fichiers audio via HTTP**

Paramètres	Description
Charger des fichiers audio via HTTP	
Fichier d'annonce	Sélectionnez le fichier WAV contenant l'annonce dans le système de fichiers local. Format de fichier : voir la remarque dans WBM.
Fichiers audio déjà téléchargés	
Fichier Wave	Affiche les fichiers d'annonce chargés dans le système de communication
Supprimer	Supprime le fichier d'annonce

Paramètres	Description
Charger	Charge le fichier d'annonce sélectionné dans le système. Activation sous Configuration, Téléphonie centrale> Musique d'attente/ Annonces.

27.2.1.3 Configuration > Configuration de port

Description des paramètres de l'onglet :

- **Exporter la configuration**

Paramètres	Description
Exporter la configuration	
Nom de fichier	Nom du fichier exporté.
Action	Exportation d'un fichier XML zippé (par ex. pour traitement dans Excel) avec les données suivantes : Nom, Numéro de l'abonné, Numéro SDA, Type de poste, Licences, Groupes/Groupement (pas Team/Top), Abonnés virtuels, Lignes, Groupes de lignes, Messagerie vocale, etc.

27.2.1.4 Configuration > SmartVM

Description des paramètres des onglets :

- **Vue d'ensemble**

Paramètres	Description
Langues Affichage de toutes les langues dans lesquelles le guide utilisateur est disponible. La convention d'appellation suivante est appliquée : aabb aa = code langue de deux caractères bb = code pays de deux caractères Le code pays (bb) est en règle générale identique au code langue (aa).	
Informations sur la boîte de messagerie	
Numéro d'appel	Affichage du numéro de téléphone de la boîte de messagerie
Nom	Affichage du nom de la boîte de messagerie
Messages	Affichage du nombre des nouveaux messages / nombre de tous les messages.
Utilisation totale de la boîte de messagerie	Affichage du taux d'occupation de l'emplacement de mémoire en pourcentage.

27.2.1.5 Configuration > SmartVM > Opérations boîte de messagerie

Description des paramètres des onglets :

- **Effectuer opérations boîte de messagerie**

Paramètres	Description
Réinitialiser toute la configuration de boîte de messagerie (effacer tous les messages et annonces)	Si ce flag est activé, tous les messages d'accueil et tous les messages de toutes les boîtes vocale sur SmartVM sont effacés. Par défaut : Désactivé.
L'index	Affichage de l'index de la boîte vocale.
Numéro	Affichage du numéro de téléphone de la boîte de messagerie
Nom	Affichage du nom de la boîte de messagerie
Réinitialiser les mots de passe	Si ce flag est activé, le mot de passe de la boîte vocale est replacé sur le mot de passe par défaut `123456`. L'utilisateur doit modifier le mot de passe lors de l'utilisation suivante de la boîte vocale. Par défaut : Désactivé.
Initialiser les boîtes de messagerie	Si ce flag est activé, les actions indiquées ci-après sont réalisées pour la boîte vocale sélectionnée. Boîtes vocales par défaut : – Le mot de passe est réinitialisé – Le flag **Enregistrement** est activé – Suppression des messages – Les messages d'accueil sont effacés – Le contrôle de message d'accueil est défini sur manuel – Message d'accueil actif : Message d'accueil 1 Boîtes vocales Standard automatique : – Le mot de passe est réinitialisé – Le flag **Renvoi après annonce** est désactivé – Les numéros abrégés sont effacés – Les messages d'accueil sont effacés – Le contrôle de message d'accueil est défini sur manuel – Message d'accueil actif : Message d'accueil 1 Par défaut : Désactivé.

27.2.1.6 Configuration > SmartVM > Opérations sur les fichiers

Description des paramètres des onglets :

- **Sauvegarde**

Paramètres	Description
Sauvegarde	
Messages	Si ce flag est activé, en plus des messages d'accueil, les messages des boîtes vocales sélectionnées sont sauvegardés. Par défaut : Désactivé.
Boîtes de messagerie disponibles	Liste de toutes les boîtes vocales disponibles. Il est possible d'intégrer certaines boîtes vocales ou toutes dans la listes des boîtes vocales à sauvegarder.
Boîtes de messagerie pour sauvegarde	Liste des boîtes vocales à sauvegarder.
Boutons	
Appliquer	Les messages d'accueil (et les messages si le flag **Messages** a été activé) des boîtes vocales à sauvegarder sont enregistrés dans un fichier de sauvegarde (`*.tar`).

Description des paramètres des onglets :

- **Données d'annonce**

Paramètres	Description
Données d'annonce	
Sélection de la boîte de messagerie	Sélection de la boîte vocale.
Message d'accueil 1 (jour)	Affichage du message d'accueil actuellement utilisé. **Standard** signifie qu'il n'existe pas de message d'accueil individuel pour l'abonné.
Message d'accueil 2 (nuit)	Affichage du message d'accueil actuellement utilisé. **Standard** signifie qu'il n'existe pas de message d'accueil individuel pour l'abonné.
Message d’accueil 3	Affichage du message d'accueil actuellement utilisé. **Standard** signifie qu'il n'existe pas de message d'accueil individuel pour l'abonné.
Message d’accueil 4	Affichage du message d'accueil actuellement utilisé. **Standard** signifie qu'il n'existe pas de message d'accueil individuel pour l'abonné.
Boutons	
Parcourir	Navigation vers chemin d'archivage du fichier d'accueil.
Charger	Un message d'accueil sauvegardé précédemment ou un fichier Wave est chargé dans SmartVM. Le fichier Wave à charger doit avoir le format suivant : PCM, 16 bits, 8kHz, mono Le fichier Wave sélectionné est converti lors du chargement. Cela peut prendre plusieurs minutes suivant la taille du fichier Wave.

Paramètres	Description
Sauvegarder	Le message d'accueil utilisé momentanément est enregistré sur le PC. Le message d'accueil est enregistré en format binaire sur le PC (fichier vma) et ne peut donc pas être écouté ou modifié.
Effacer	Le message d'accueil utilisé momentanément est effacé dans SmartVM.

Description des paramètres des onglets :

- **Rétablir**

Paramètres	Description
Rétablir	
Messages	Ecrase non seulement les messages d'accueil des boîtes vocales sélectionnées, mais aussi les messages. Par défaut : Désactivé.
Entrée en tiers	Si ce flag est désactivé, seuls sont remplacés les messages d'accueil des boîtes vocales qui figurent dans les données de sauvegarde. Si, en plus, le flag **Messages** est activé, il est également ajouté les messages contenus dans les données de sauvegarde. Les messages déjà existants sont conservés. Si ce flag est activé, avant le rétablissement tous les messages d'accueil et tous les messages des boîtes vocale sont effacées dans SmartVM. Si des boîtes vocales qui ne figurent pas dans les données de sauvegarde sont sélectionnées, elle sont également effacées. Les messages d'accueil figurant dans les données de sécurité sont transférés. Si en plus le flag **Messages** est activée, les messages contenus dans les données de restauration sont également transférés. Par défaut : Désactivé.
Boîtes de messagerie disponibles	Liste de toutes les boîtes vocales figurant dans le fichier de sauvegarde. Il est possible d'intégrer certaines boîtes vocales ou toutes dans la listes des boîtes vocales à rétablir.
Boîtes de messagerie pour sauvegarde	Liste des boîtes vocales à rétablir.
Boutons	
Parcourir	Navigation vers chemin d'archivage du fichier de sauvegarde.
Charger	Les boîtes vocales comprises dans le fichier de sauvegarde sont indiquées. Un nouveau clic sur le bouton rétablit les messages d'accueil et messages des boîtes vocales sélectionnées.

27.2.1.7 Configuration > Branding

Description des paramètres de l'onglet :

- **Branding**

Paramètres	Description
Branding	Sélection de la désignation du produit.

27.2.1.8 Configuration > Adresse passerelle IP

Description des paramètres de l'onglet :

- **Modifier l'adresse de la passerelle IP**

Paramètres	Description
Modifier l'adresse de la passerelle IP	
Adresse IP de la passerelle	Entrée de l'adresse IP du système de communication, par ex. : 192.168.1.2

27.2.2 Image logicielle

Les fonctions pour la mise à jour du logiciel de passerelle et des images de téléphones sont réunies sous **Image logicielle**.

27.2.2.1 Image logicielle > Logiciel système > Mise à jour via Internet

Description des paramètres des onglets :

- **Charger les images logicielles à partir d'un serveur Web**

Paramètres	Description
Paramètres du serveur Web	
Image logicielle URL	Affichage et modifications du lien en direction du serveur logiciel y compris chemin vers le fichier Image.
Nom utilisateur	Nom utilisateur pour la connexion sur le serveur logiciel.
Mot de passe	Mot de passe pour la connexion sur le serveur logiciel.
Informations sur la mise à jour logicielle	Activation de l'interrogation pour savoir si une nouvelle version est disponible sur le serveur de logiciels.
Heure de début	Moment de l'interrogation. Plage de valeurs : 00.00 à 24.00, valeur par défaut : 02,00
Utiliser le proxy	Activation du proxy si un proxy est utilisé.
Proxy HTTP	
Proxy HTTP	Entrée du lien avec le serveur Proxy.
Port proxy HTTP	Entrée du port du serveur proxy. Valeur par défaut : 80
Nom utilisateur	Nom utilisateur pour la connexion au serveur proxy.

Paramètres	Description
Mot de passe	Mot de passe pour la connexion au serveur proxy.
Utiliser une route statique dédiée	Les clients disposant d'une connexion WAN pour les jonctions SIP sans volume de données Internet peuvent utiliser la fonctionnalité **Utiliser une route statique dédiée** pour effectuer une mise à jour du logiciel OSBiz via une interface LAN alternative. L'adresse IP dynamique du serveur de mise à jour est déterminée automatiquement et est alors disponible en tant qu'entrée de routage pour ce processus. Pour utiliser cette option : • Activer l'indicateur **Utiliser une route statique dédiée**
Route statique dédiée pour la mise à jour du logiciel via l'interface LAN	
Adresse IP de la passerelle pour la route	Configurez l'adresse IP de la passerelle par défaut de l'interface LAN - par laquelle une connexion à Internet est possible - comme adresse IP de la passerelle pour la route.
Dernière mise à jour logicielle	Indication de la date à laquelle la dernière mise à jour logicielle a été effectuée.
Boutons	
Par défaut	Rétablit les valeurs par défaut pour les valeurs modifiées.

27.2.2.2 Image logicielle > Logiciel système > Mise à jour via chargement de fichier

Description des paramètres des onglets :

- **Charger images logiciel via chargement du fichier**

Paramètres	Description
Nom de fichier distant (système de fichiers PC)	Navigation vers l'emplacement de stockage du fichier Image.
Nettoyer l'espace de stockage avant le transfert	Lorsque la mise à jour est exécutée avec cet indicateur activé, les journaux, les traces, les images logicielles du téléphone et les vidages TCP sont supprimés pour libérer de la mémoire.
Activation du logiciel	
Démarrage de l'action immédiatement après la transmission	Le logiciel est immédiatement transmis au système de communication, en arrière-plan. Après deux redémarrages, le logiciel est actualisé.
Démarrage de l'action dans	Le logiciel est immédiatement transmis au système de communication, en arrière-plan. Une fois écoulé l'intervalle de temps indiqué, le logiciel est activé. Entrée de la période en jours, heures et minutes.
Démarrage de l'action le	Le logiciel est immédiatement transmis au système de communication, en arrière-plan. Le logiciel est activé au moment défini. Entrée du moment sous forme de date et d'heure.
Heure du système local	Affichage de la date et l'heure du système.

Paramètres	Description
Version logicielle des images du logiciel actuellement utilisé	Affichage de la version logicielle du fichier Image actuel.

27.2.2.3 Image logicielle > Logiciel système > Mise à jour via chargement de fichier

Description des paramètres des onglets :

- **Charger images logiciel depuis clé &USB**

Paramètres	Description
Liste de tous les fichiers Image compatibles qui sont disponibles	
Version	Affichage du numéro de version des fichiers Image trouvés sur le support USB.
Charger	Sélection du fichier Image trouvé sur le support USB qui servira pour l'actualisation logicielle.
Nom de fichier	Affichage des noms de fichier des fichiers Image trouvés sur le support USB.
Taille du fichier (Mo)	Affichage de la taille des Image trouvés sur le support USB.
Activation du logiciel	
Démarrage de l'action immédiatement après la transmission	Le logiciel est immédiatement transmis en arrière-plan dans le système de communication et activé. Pour l'activation, il est réalisé une interruption momentanée de l'exploitation du système.
Démarrage de l'action dans	Le logiciel est immédiatement transmis au système de communication, en arrière-plan. Une fois écoulé l'intervalle de temps indiqué, le logiciel est activé. Entrée de la période en jours, heures et minutes.
Démarrage de l'action le	Le logiciel est immédiatement transmis au système de communication, en arrière-plan. Le logiciel est activé au moment défini. Entrée du moment avec date et heure.
Heure du système local	Affichage de la date et l'heure du système.
Version logicielle des images du logiciel actuellement utilisé	Affichage de la version logicielle activée.

27.2.2.4 Image logicielle > Images du téléphone > Charger

Description des paramètres des onglets :

- **Charger le logiciel téléphonique**

Paramètres	Description
Nom de fichier distant (système de fichiers PC)	Sélection du logiciel téléphonique (fichier Image)

Paramètres	Description
Images actuellement installées	
Effacer	Les images téléphone sont sélectionnées en vue de l'effacement.
Nom de fichier	Affichage du nom du fichier Image.
Type d'équipement	Affichage du type de téléphone système correspondant au fichier Image.
Version	Affichage de la version du fichier Image.
Boutons	
Charger	L'image téléphone indiquée est chargée dans le système de communication.
Effacer	Les fichiers image téléphone sélectionnés sont effacés du système de communication.

27.2.2.5 Image logicielle > Images du téléphone > Distribuer

Description des paramètres des onglets :

- **Distribution du logiciel du téléphone**

Paramètres	Description
Images actuellement installées	
Distribuer	Si la case est cochée, le logiciel de téléphonie est transmis à tous les téléphones système raccordés du type de téléphone.
Nom de fichier	Affichage du nom du fichier Image.
Type d'équipement	Affichage du type de téléphone système correspondant au fichier Image.
Version	Affichage de la version du fichier Image.
Type	Type de téléphone système.
Standard	Le logiciel de téléphonie sélectionné par défaut est automatiquement transmis au téléphone système correspondant à ce type lors de la première connexion sur le système.

27.2.2.6 Image logiciel > Images téléphone > Déploiement vers le terminal

Description des paramètres des onglets :

- **Diffusion du logiciel du téléphone par terminal**

  Si l'utilisateur est un Utilisateur Deskshare, la case à cocher est grisée. Vous ne pouvez donc pas déployer de périphérique sur cet utilisateur.

Paramètres	Description
Images actuellement installées	
Numéro	Numéro d'appel du téléphone système

Paramètres	Description
Type d'équipement	Type de téléphone système.
Adresse IP	Adresse IP du téléphone système ; lien direct avec WBM du téléphone IP.
Adresse MAC	Adresse MAC du téléphone système.
Version actuelle du logiciel	Version logicielle actuelle du téléphone système.
Logiciel distribuable	Sélection de l'images du téléphone qui doit être transmise au téléphone système.

27.2.2.7 Image logicielle > Images du téléphone > Charger

Une image (par ex. logo de l'entreprise) peut être chargée sur l'écran des téléphones système (OpenStage 40/60/80 ou variantes Telekom), affichage à l'état de repos (on-hook). Spécifications du fichier Logo, voir Logos Téléphone.

Description des paramètres des onglets :

- **Charger les logos téléphone**

Paramètres	Description
Nom de fichier distant (système de fichiers PC)	Sélection du fichier avec le logo Téléphone.
Images logo actuellement installées	
Effacer	Les fichiers de logo téléphone sont sélectionnés en vue de l'effacement.
Nom de fichier	Affichage du nom du fichier Logo téléphone.
Boutons	
Charger	Le fichier de logo téléphone indiqué est chargé dans le système de communication.
Effacer	Les fichiers de logo téléphone sélectionnés sont effacés du système de communication.

27.2.2.8 Image logicielle > Images du téléphone > Distribuer

Une image (par ex. logo de l'entreprise) peut être chargée sur l'écran des téléphones système (OpenStage 40/60/80 ou variantes Telekom), affichage à l'état de repos (on-hook). Spécifications du fichier Logo, voir Logos Téléphone.

Description des paramètres des onglets :

- **Diffusion du logo téléphone**

Paramètres	Description
Images logo actuellement installées	
Distribuer	Si la case est cochée, ce fichier de logo téléphone est transmis aux téléphones système sélectionnés.

Paramètres	Description
Nom de fichier	Affichage du nom du fichier Logo téléphone.
Étendre aux postes avec le type d'équipement sélectionné	Sélection pour définir si le logo Téléphone sera transmis à tous les téléphones système ou uniquement à un certain type de téléphone système.

27.2.3 Cordless

Dans **Cordless**, les fonctions de toutes les stations de base configurées sont regroupées.

27.2.3.1 Cordless > Stations de base

Description des paramètres des onglets :

- **État de la station de base**

Paramètres	Description
Données de station de base	
Fréquence de la SB	Indique les fréquences de la station de base sélectionnée. Il est possible de sélectionner simultanément jusqu'à 10 canaux de fréquences différents (voir tableau ci-après).
Station de base	Numéro de la station de base.
Version logicielle	Version logicielle de la station de base.
Version matérielle	Version matérielle de la station de base.
État	État du port correspondant : port actif Port non verrouillé Port verrouillé Port raccordé, non actif Port raccordé, non actif 1er port supplémentaire pour... (n° du port principal) 2er port supplémentaire pour... (n° du port principal)
Surcharge	Nombre de situations de surcharge au niveau de l'interface UP0/E.
Redémarrage	Nombre des redémarrages de la station de base.
Erreur L1/L2	Nombre d'erreurs L1/L2 survenues au niveau de la station de base.
Libération anormale	Nombre des communications coupées de la station de base.
Appels par BS	Nombre des communications passant par la station de base (entrantes et sortantes)

Paramètres	Description
Mode de saut	Les systèmes Cordless Version 2 fonctionnent toujours en "mode Fast Hopping" (saut rapide). En d'autres termes, il est possible d'utiliser toutes les paires d'intervalles de temps de fréquence. 120 canaux duplex sont donc disponibles. Lorsque l'on a une station de base à saut lent, on ne peut utiliser qu'une paire d'intervalles de temps de fréquence sur deux. 60 canaux duplex sont donc disponibles. Tous les systèmes Cordless Version 1 fonctionnent en ”mode saut lent”.
Compt. BHO OK	Nombre de transferts intracellulaires réussis (Bearer Handovers BHO), en d'autres termes, les changements de la fréquence du support et/ou de l'intervalle de temps à l'intérieur d'une cellule radio. Non pris en charge par Hicom cordless EM V2.1 et V2.2. Le compteur n'est certes pas pris en charge, mais la fonctionnalité du transfert de support (Bearer Handover) est disponible.
Compt. BHO pas OK	Nombre de transferts intracellulaires (Bearer Handovers BHO) ayant échoué. Non pris en charge par Hicom cordless EM V2.1 et V2.2. Le compteur n'est certes pas pris en charge, mais la fonctionnalité du transfert de support (Bearer Handover) est disponible.
Transfert Intra SLC	Nombre de procédures de transfert au sein de la carte SLC. Le décompte est effectué au niveau de la nouvelle station de base.
Transfert Inter SLC	Nombre des procédures de transfert effectuées entre des cartes SLC. Le décompte est effectué au niveau de la nouvelle station de base.
Dans SLC	
Appels perdus	Nombre des communications n'ayant, pour des raisons de ressources, pas pu avoir lieu.
Surcharge SLMUC	Nombre des situations de surcharge sur le module SLC. Le nombre des éléments pool libres sur la carte SLC est inférieur à une valeur minimum. Toutes les prises de ligne entrantes seront rejetées par l'IWU de la SLC, cela jusqu'à ce que la situation de surcharge ait pris fin.
Roam LR	Roam LR comptabilise chaque prise de ligne d'un téléphone sans fil avec un PMID par défaut et une SLC de localisation modifiée. Il s'agit du nombre des messages de demande de position (Locate Request) faisant part d'un roaming (en d'autres termes, la position du téléphone sans fil a changé). Le téléphone mobile exécute une demande de position (Locate Request) à chaque activation. Si le téléphone mobile est éteint puis rallumé au sein d'une autre cellule radio, ce compteur n'effectue pas de comptabilisation.
LR async	LR async comptabilise chaque prise de ligne d'un téléphone sans fil avec un PMID par défaut dans le cas d'une SLC de localisation restant inchangée. Il s'agit ici du nombre des messages de demande de position donnant des informations sur les couches asynchrones (en d'autres termes, la position du téléphone sans fil est inchangée). La comptabilisation n'est cependant pas effectuée au niveau de la SLC d'attache, et c'est la raison pour laquelle elle est seulement prise en compte si la connexion radio aboutit ou si elle soutient le CHO avec PMID par défaut. De plus, pour les prises de ligne, les conditions requises pour une actualisation du lieu de séjour doivent obligatoirement être remplies. Cela signifie qu'une demande de position doit avoir été reçue ou que les mesures de sécurité, l'authentification (et cryptage) doivent avoir été exécutés pour le lien.
Erreur HDLC	Nombre des messages d'erreur HDLC non critiques n'ayant pas été signalés au système (débordement, pénurie, erreur CRC).

Paramètres	Description
Version CMI	La version Cordless actuelle est affichée ici.

Fréquence (canal)	DECT	Europe 1880 – 1900 MHz	Amérique latine 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

27.2.4 Etat des ports/modules

L'état de tous les modules peut être affiché. De plus, les modules et leurs ports peuvent être validés et verrouillés.

27.2.4.1 Etat des ports/modules > Etat des modules

Description des paramètres des onglets :

- **Etat des modules**

Paramètres	Description
Emplacement	Numéro physique de l’emplacement.
Module	Dénomination de la carte.
Non connecté(e)	Une croix apparaît dans cette colonne lorsque la carte n’est pas insérée.
Incorrect(e)	Une croix apparaît dans cette colonne lorsque la carte est défectueuse (non chargée). Il est également possible qu'un module défectueux ou non configuré ne soit pas affiché.
Bloqué	Une croix apparaît dans cette colonne lorsque au moins un port de cette carte est verrouillé.
Libre	Une croix apparaît dans cette colonne lorsque tous les ports de cette carte sont libres.
Occupé	Coché si au moins un abonné ou une ligne de ce module a décroché, est appelé ou est en conversation.

Paramètres	Description
Référence temporelle	Une croix apparaît dans cette colonne lorsque la carte fournit l'horloge source.
Boutons	
Démarrage	Démarrage de l'actualisation de l'affichage. L'état est actualisé toutes les 3 secondes.
Arrêter	Arrêt de l'actualisation de l'affichage.

27.2.4.2 Etat port/modules > Out of Service (hors service)

Description des paramètres des onglets :

- **Port hors service**
- **Carte hors service**

Paramètres	Description
Accès	Emplacement et port auxquels l'abonné ou la ligne sont raccordés.
N° d'appel	Numéro de téléphone attribué au port.
Nom	Il s'agit du nom associé à l'abonné ou à la ligne.
État	Les ports peuvent être soit **actifs** soit **inactifs**, selon qu'un terminal valide ou une ligne valide sont connectés au port ou non. Les ports peuvent également être mis **en service** (par défaut) ou **hors service par l'outil**, ce qui signifie qu'ils ont été bloqués sous **Verrouiller carte**. L'état **En service** n'est pas identique à **Activé**. Par exemple, un port peut être à l'état **actif**, **en service** mais également à l'état **Inactif**, **en service**.
Boutons	
Mise hors service	Les ports marqués sont verrouillés. Lorsque les ports $U_{P0/E}$ sont verrouillés, le port physique correspondant est automatiquement mis hors service. Par conséquent, si un port maître est sélectionné, le port esclave correspondant est également mis hors service.
Mise en service	Les ports marqués sont validés.
Verrouiller carte	Les modules marqués et leurs ports sont verrouillés. Lorsque certains téléphones mobiles d'un module Cordless sont verrouillés, le module entier est toujours verrouillé et donc tous les téléphones mobiles. Le verrouillage des téléphones mobiles individuels est réalisé en modifiant le PIN des téléphones mobiles.
Libérer carte	Les modules marqués et leurs ports sont validés.

27.2.5 Traces

Les fonctions de trace sont regroupées sous **Traces**. L'administrateur peut démarrer et arrêter des traces, ainsi que modifier les paramètres de trace.

27.2.5.1 Traces > Configuration du format Trace

La Configuration du format Trace permet de définir quelles données d'en-tête doivent figurer dans l'édition Trace et quel doit être le formatage des données Trace.

Description des paramètres des onglets :

- **Modifier la configuration des traces**

Paramètres	Description
Données d'en-tête contenues dans l'édition Trace	
Paramètres de format d'en-tête de trace généraux	Lorsque le flag est activé, il est possible d'activer ou de désactiver les options pour les données d'en-tête ci-après. Valeur par défaut : Activé
ID de sous-système	Lorsque le flag est activé, l'ID de sous-système figure dans l'édition Trace. Valeur par défaut : Activé
Nom de tâche	Lorsque le flag est activé, le nom de la tâche figure dans l'édition Trace. Valeur par défaut : Activé
ID de tâche	Lorsque le flag est activé, l'ID de tâche figure dans l'édition Trace. Valeur par défaut : Activé
Heure	Lorsque le flag est activé, l'indication de temps figure dans l'édition Trace. Valeur par défaut : Activé
Nom du module	Lorsque le flag est activé, le nom de module figure dans l'édition Trace. Valeur par défaut : Activé
Numéro de ligne	Lorsque le flag est activé, le numéro de ligne figure dans l'édition Trace. Valeur par défaut : Activé
Préparation des données Trace	
Formatage complet avec extension de paramètres (par défaut)	Mode d'édition par défaut : tous les types de données sont représentés de manière complète. Edition Trace : normale (convient à l'exploitation normale) Valeur par défaut : Activé
Limité (types de messages binaires, spécialement pour X-Tracer)	Dans ce mode d'édition restreint, les types de données sont représentés au format binaire, c.-à-d. de la manière dont ils sont disponibles au moment de la Trace. Le format binaire est destiné à l'analyse avec le X-Tracer-Tool. Edition Trace : rapide (convient pour une charge moyenne à élevée) Valeur par défaut : Désactivé
Limité (uniquement extension de types de données élémentaires)	Dans ce mode d'édition, seuls les types de données élémentaires (par exemple integer, short, long, string) sont représentés de manière complète. Edition Trace : très rapide (convient à une charge élevée) Valeur par défaut : Désactivé

Paramètres	Description
Trace avec optimisation de performances sans extension de paramètre	Dans ce mode d'édition, aucun type de données n'est représenté de manière complète. Le formatage Trace n'est donc pas une tâche lourde. Edition Trace : extrêmement rapide (convient à une charge très élevée) Valeur par défaut : Désactivé

27.2.5.2 Traces > Interfaces d'édition Trace

Description des paramètres des onglets :

- **Modifier les interfaces d'édition Trace**

Paramètres	Description
Trace de fichier	
Activer la trace de fichier	Lorsque le flag est activé, les messages de trace sont inscrites dans un fichier journal dans le système de communication. Valeur par défaut : Activé
Quota de trace maximum (koctets)	Affichage de la taille maximale de la mémoire de trace en Ko.
Police pour gérer l'atteinte du quota maximum	Sélection de ce qui peut passer une fois atteint le quota de trace maxi.
Police pour gérer l'atteinte du quota maximum : Wrap Around (supprimer le fichier Trace le plus ancien)	Lorsque le quota de trace maximum est atteint, le fichier journal de trace le plus ancien est écrasé. Valeur par défaut : Activé
Police pour gérer l'atteinte du quota maximum : Arrêter temporairement le fichier Trace	Lorsque le quota de trace maximum est atteint, l'édition de la trace fichier est arrêtée. Valeur par défaut : Désactivé
Délai entre la création de nouveaux fichiers Trace (s)	Affichage du temps en secondes à l'issue duquel un nouveau fichier journal de trace est créé.
Plage de temps pendant laquelle les fichiers trace sont disponibles	Affichage de la plage de temps pour laquelle des fichiers journal de trace sont disponibles.
Trace par LAN	
Activer la trace par LAN	Les messages Trace sont transmis via l'interface LAN. Valeur par défaut : Désactivé
Valeur de temporisation (s)	Affichage du temps en seconde à l'issue duquel les données de trace sont transmises.

27.2.5.3 Traces > Journal de trace

Description des paramètres des onglets :

- **Charger par HTTP**
- **Effacer le fichier-journal de trace**

Conseil : L'effacement des données journal de trace ne peut pas être annulé.

Paramètres	Description
Fichier-journal de trace	
Protocole global	Tous les fichiers journal de Suivi sont téléchargés.
Protocole d'aujourd'hui	Les fichiers journal de trace de la journée d'aujourd'hui (à partir de 00h00) sont téléchargés.
Propre sélection	Les fichiers journal de trace de la période sélectionnée sont téléchargés.

27.2.5.4 Traces > Bouclage numérique

La configuration de boucles de contrôle numériques est exclusivement possible avec Manager E.

Le bouclage numérique est utilisé pour contrôler la ligne des canaux B des interfaces S_0, S_{2M} et T1 d'éventuels modules disponibles. L'activation des boucles numériques de contrôle ne doit être effectuée qu'à la demande du fournisseur de services.

Description des paramètres des onglets :

- **Modifier le bouclage numérique**

27.2.5.5 Traces > Journal Trace client

Cette fonction permet de démarrer l'affichage des événements (Trace client). Les types de messages sont entre autres les suivants : système, SIP, STUN et LDAP.

Description des paramètres des onglets :

- **Afficher**
- **Charger par HTTP**
- **Effacer le fichier-journal de trace**

Paramètres	Description
Actualisation automatique	Lorsque le flag est activé, il se produit une actualisation automatique de l'affichage du journal de trace client. Valeur par défaut : Activé

Paramètres	Description
Secondes jusqu'à la prochaine actualisation	Durée en secondes à l'issue de laquelle a lieu une actualisation du protocole Trace client.

27.2.5.6 Traces > Composante de trace M5T

Cette fonction sert à la surveillance de la pile SIP.

Les paramètres ne doivent être modifiés que sur instruction du support SAV compétent.

Description des paramètres des onglets :

- **Modifier toutes les composants Trace M5T**
- **Démarrer/Arrêter la composante de trace**

Paramètres	Description
Nom du pack	Nom de la composante de trace M5T
Niveau Trace	Niveau de détail de l'enregistrement de la composante Trace M5T (niveau de trace 0 = plus bas niveau de détail à niveau de trace 9 = plus haut niveau de détail) Valeur par défaut : 0
Trace activée	Lorsque le flag est activé, il est effectué un enregistrement des données de la composante de trace M5T. Valeur par défaut : Désactivé
Fourche	Etapes de l'activation

27.2.5.7 Traces > Secure Trace

Cette fonction sert à enregistrer les flux de données de signalisation et de données de charge utile VoIP chiffrées.

L'enregistrement des données de connexion chiffrées nécessite impérativement l'autorisation du client et il ne doit être effectué qu'avec l'accord du support SAV compétent. Informations sur la procédure, voir Traces (Secure Trace)

Remarque : L'enregistrement des communications et des données de connexion constitue un délit si les abonnés concernés n'ont pas été informés.

Description des paramètres des onglets :

- **Modifier le mot de passe SecureTrace**
- **Importer le fichier X.509 pour Secure Trace**

Paramètres	Description
Modifier la phrase de passe servant à activer Secure Trace	

Paramètres	Description
Phrase de passe actuelle	Mot de passe actuel (phrase) pour démarrer ou arrêter le chiffrement de la trace
Nouvelle phrase de passe	Nouveau mot de passe (passphrase) pour démarrer et arrêter Secure Trace Plage de valeurs : 5 à 12 caractères
Confirmer nouveau mot de passe	Nouveau mot de passe (passphrase) pour démarrer et arrêter Secure Trace Plage de valeurs : 5 à 12 caractères
Fichier de certificat (PEM ou binaire)	Sélection du fichier X.509 qui contient le certificat à importer dans le système de communication. Après sélection du fichier W.509, l'empreinte digitale du certificat à importer est affiché, puis le certificat est importé dans le système de communication. ***INFO :*** l'importation du certificat doit se faire après le contrôle de l'empreinte digitale.

27.2.5.8 Traces > Secure Trace (chiffrement de la trace) > Certificat SecureTrace

Cette fonction sert à afficher le certificat Secure Trace importé.

Description des paramètres des onglets :

- **Afficher le certificat SecureTrace**

27.2.5.9 Traces > Secure Trace (chiffrement de la trace) > Paramètres SecureTrace

Cette fonction sert à interroger l'état et à démarrer/arrêter Secure Trace (chiffrement de la trace).

Description des paramètres des onglets :

- **Etat SecureTrace**
- **Comment démarrer/arrêter Secure Trace**

Paramètres	Description
Etat SecureTrace actuel	
SecureTrace est actif	Etat du chiffrement de la trace (Secure Trace)
Heure de désactivation automatique	Heure à laquelle Secure Trace est automatiquement désactivé.
SecureTrace pour ces protocoles	Affichage de la journalisation créée pour Secure Trace.
Paramètres de démarrage	
Phrase de passe pour l'activation de SecureTrace	Mot de passe (phrase de passe)pour le démarrage et l'arrêt du chiffrement de la trace

Paramètres	Description
Durée de SecureTrace (min.)	Période en minutes durant laquelle Secure Trace doit être activé. ***INFO :*** il est absolument nécessaire d'entrer une valeur.
SecureTrace pour ces protocoles	
TC (TLS)	Lorsque le flag est activé, Secure Trace se conforme au protocole TC (TLS). Valeur par défaut : Désactivé
H.323 Core/HSA (TLS)	Lorsque le flag est activé, Secure Trace se conforme au protocole H.323 Core / HSA (TLS). Valeur par défaut : Désactivé
MMX (PEP)	Lorsque le flag est activé, Secure Trace se conforme au MMX (PEP). Valeur par défaut : Désactivé
SIP Core/SSA (TLS)	Lorsque le flag est activé, Secure Trace se conforme au protocole SIP Core/ SSA (TLS). Valeur par défaut : Désactivé
MSC (SRTP)	Lorsque le flag est activé, Secure Trace se conforme au MSC (SRTP). Valeur par défaut : Désactivé

27.2.5.10 Traces > Trace de pile H.323

Cette fonction sert à suivre les problèmes relatifs aux composantes qui utilisent le protocole H.323.

Les paramètres ne doivent être modifiés que sur instruction du support SAV compétent.

Description des paramètres des onglets :

- **Modifier la configuration de la trace de pile H.323**
- **Modifier tous les modules H.323**
- **Charger le fichier-journal de trace de la pile H.323**
- **Effacer le fichier-journal de trace de la pile H.323**

Paramètres	Description
Général	
Niveau Trace	Niveau de détail du suivi (Niveau de suivi 0 = niveau de détail minimum jusqu'au niveau de suivi 4 = niveau de détail maximum) Valeur par défaut : 2
Trace de console	
Activer la trace de console	Lorsque le flag est activé, les message de trace de la pile H.323 dont déposés sur le satellite. Valeur par défaut : Désactivé
Trace de fichier	

Paramètres	Description
Activer la trace de fichier	Lorsque le flag est activé, les messages de trace de la pile H.323 sont inscrits dans un fichier journal. Valeur par défaut : Désactivé
Taille maxi. du tampon de trace (octets)	Taille maxi. du tampon de trace en octets (quantité de données conservées en mémoire tampon.)
Taille maxi. du fichier de trace (octets)	Taille maxi du fichier journal de trace en octets
Temporisation de trace (s)	Durée en secondes à l'issue de laquelle les données de trace sont inscrites dans le fichier journal.
Nom du module	Nom du module de trace de pile H.323
Trace activée	Lorsque le flag est activé, le module de trace de pile H.323 est activé.

27.2.5.11 Traces > Surveillance d’appel

Cette fonction permet de mettre en marche et d'arrêter la surveillance des interfaces de ligne et d'abonné.

Description des paramètres des onglets :

- **Démarrer/Arrêter le protocole**
- **Afficher**
- **Charger par HTTP**

Paramètres	Description
Port sélectionné	Interface de ligne ou d’abonné pour laquelle la surveillance d’appel doit être démarrée ou arrêtée.
N°	Numéro séquentiel.
Heure	Heure de l'événement (event).
Callnumber/Access	Numéro de téléphone et interface physique.

Paramètres	Description
État	Etat de l'interface. Les états d'interface suivants sont possibles : • Dispo. (l'interface est à l'état dispo.) • Call Initiated (appel initialisé) (interface prête.) • Overlap Sending (envoi avec chevauchement) (émission de chiffres externe) • Outgoing Call Proc (procédure d'appel externe) (fin de la numérotation) • Call Request (demande d'appel) (en attente de Alert) • Call Present (appel reçu) (appel de l'interface.) • Active (interface est à l'état communication.) • Hold (interface est à l'état en garde) • Disconnect Indication (demande de déconnexion d'une communication en cours) • Direct (interface est en mode appel interphone.) • Intrusion (entrée en tiers est activée.) • Call Back A (rappel abonné A) • Call Back B (rappel abonné B) • Busy (interface est occupée.) • Error (Erreur) • Disconnect PI (déconnexion PI) (en attente de la déconnexion de PI (Progress Indicator)) • Capteur (Un signal a été envoyé par le capteur.) • Conference Master (Maître de la conférence) • Paging (recherche de personne) • Help Dial (aide numérotation) (utilisation de la numérotation associée.) • Remote (interface occupée par Remote Service ou DISA.) • ACD (distribution d'appels) • Unknown State (état inconnu)

Paramètres	Description
Evénement	Evénement Les événements suivants sont possibles : • Setup (prise) (interface de ligne : prise entrante ou sortante) • Setup Ackn (acquittement de la prise de ligne) (interface de ligne : acquittement de la prise de ligne) • Info (interface de ligne: Info (chiffres du numéro d'appel)) • Callme Proxy (interface de ligne: fin de numérotation non évaluée) • Progress (interface de ligne : information supplémentaire pour établissement de la liaison) • Alerte (interface de ligne : fin de la numérotation évaluée) • Connect (connexion) (interface de ligne : connexion canal B) • Connect Ackn (accusé de réception de connexion) (interface de ligne : accusé de réception de la connexion canal B) • Disconnect (déconnexion) (interface de ligne : demande de déconnexion) • Release (libération) (interface de ligne : accusé de réception de la déconnexion) • Release Compl (libération effectuée) (interface de ligne : connexion libérée) • Monitor On (surveillance activée) (interface de ligne / d'abonné : surveillance d'appel démarrée) • Monitor Off (surveillance désactivée) (interface de ligne / d'abonné : surveillance d'appel arrêtée) • Off Hook (décrocher) (interface d'abonné : combiné décroché) • On Hook (raccrocher) (interface d'abonné : combiné accroché) • Digit (chiffre) (interface d'abonné : composition des chiffres)
Actualisation automatique	Lorsque le flag est activé, il se produit une actualisation automatique de l'affichage de la surveillance d'appel. Valeur par défaut : Activé
Secondes jusqu'à la prochaine actualisation	Durée, en secondes, à l'issue de laquelle l'actualisation de la surveillance d'appel se produit.

27.2.5.12 Traces > Composante de licence

Cette fonction sert serveiller l'agent de licence CLA (Customer License Agent) interne au système.

Les paramètres ne doivent être modifiés que sur instruction du support SAV compétent.

Description des paramètres des onglets :

- **Modification de la composante Trace CLA**

Paramètres	Description
Nom du pack	Nom de la composante de licence Trace.

Paramètres	Description
Niveau Trace	Définition du niveau de détails de l'enregistrement de la composante de licence Trace. Valeur par défaut : Standard
Niveau Trace : bas	Bas niveau de détails pour l'enregistrement Trace.
Niveau Trace : Standard	Niveau de détails moyen pour l'enregistrement Trace.
Niveau Trace : Tout	Niveau de détails élevé pour l'enregistrement Trace.
Niveau Trace : Désactivé	Composante de licence Trace arrêtée.

27.2.5.13 Traces > Profils de trace

Les profils de trace comprennent des composantes de trace prédéfinies servant à surveille des unités fonctionnelles complètes du système de communication.

Description des paramètres des onglets :

- **Afficher tous les profils de trace**
- **Ajouter un profil de trace (profil vide)**
- **Ajouter un profil de trace (avec les paramètres de trace actuels)**
- **Arrêter tous les profils de trace**
- **Démarrer/Arrêter le profil de trace**

Paramètres	Description
Nom du profil	Nom du profil de trace
Profil démarré	Affichage, pour indiquer si le profil de trace a été ou non démarré.
Profil protégé en écriture	Affichage, pour indiquer si le profil de trace est protégé ou non en écriture (tous les profils de trace disponibles par défaut sont protégés en écriture).
Composante de trace	Nom du composant Trace
Inclus	Lorsque le flag est activé, la composante de trace est reprise dans le nouveau profil de trace à ajouter. Valeur par défaut : Activé
Niveau	Niveau de détail de l'enregistrement de la composante Trace (niveau de trace 0 = plus bas niveau de détail à niveau de trace 9 = plus haut niveau de détail)

27.2.5.14 Traces > Composants Trace

Les composants Trace peuvent être utilisés pour enregistrer les informations de processus et d'état des différents composants du système de communication.

Description des paramètres des onglets :

- **Afficher toutes les composantes de trace**
- **Afficher les composantes de trace démarrées**
- **Afficher les composantes de trace arrêtées**

- **Modifier la composante de trace**
- **Arrêter toutes les composantes de trace**
- **Démarrer/Arrêter la composante de trace**
- **Paramètres de trace par défaut**

Paramètres	Description
Nom du sous-système	Nom du composant Trace
Index de composante Trace	Numéro séquentiel
Niveau Trace	Niveau de détail du suivi (Niveau de suivi 0 = niveau de détail minimum jusqu'au niveau de suivi 9 = niveau de détail maximum)
Trace activée	Lorsque cet indicateur est activé, les données du composant Trace sont enregistrées.

27.2.5.15 Traces > TCP- Dump

Un TCP-Dump sert à surveiller et analyser le trafic de données dans un réseau IP. Pour le diagnostic des fichiers TCP-Dump, une application correspondante est nécessaire.

Description des paramètres des onglets :

- **Etat TCP-Dump**

Paramètres	Description
Lancer TCP-Dump	Démarrer le TCP-Dump
Paramètres de démarrage	
Nom d'interface	Interface, pour laquelle il y a évaluation du trafic de données. Les interfaces disponibles sont affichées dans **Détails de l'interface**. L'entrée **any** lance une évaluation du trafic de données sur toutes les interfaces disponibles. Valeur par défaut : any
Taille de paquet	Taille en octets des paquets de données à enregistrer. L'entrée **0** indique que chaque paquet est entièrement enregistré. Plage de valeurs : 0 à 2000000000, valeur par défaut : 0
Critères de fin	
Nombre de paquets	Nombre de paquets de données qui active l'arrêt de TCP-Dump.
Délai jusqu'à la fin (s)	Durée en secondes à l'issue de laquelle le déroulement du TCP-Dump est arrêté.
Terminer TCP-Dump	Arrêter TCP-Dump
Préparer TCP-Dump	Effacer dans le système de communication les données TCP-Dump enregistrées

Paramètres	Description
Actualisation automatique	Lorsque le flag est activé, il se produit une actualisation automatique de l'affichage d'état. Valeur par défaut : Activé

27.2.5.16 Traces > rpcap Daemon

Un Démon RPCAP (Remote Packet Capture) sert à surveiller et analyser le trafic de données dans un réseau IP. Via le démon RPCAP, il est possible que des applications externes accèdent aux paquets TCP/IP des interfaces LAN du système de communication. Un Démon RPCAP est souvent utilisé pour les suivis de longue durée parce que les fichiers trace sont enregistrés sur PC et non pas dans le système de communication.

Remarque : Les consignes de sécurité figurant dans l'onglet doivent être respectées.

Description des paramètres des onglets :

- **rpcap**

Paramètres	Description
Adresse à lier à	
Adresse IP (numérique ou littérale)	Adresse IP de l'hôte où sont faits les enregistrements. Valeur par défaut : 0.0.0.0
Port (choisir un port libre)	Port de l'hôte où sont faits les enregistrements.
Trace LAN interne	Lorsque le flag est activé, le trafic des données entre deux modules est enregistré via l'interface eth9. Valeur par défaut : Désactivé
Identification client pour autorisation d'accès	
Adresse IP (numérique ou littérale)	Adresse IP du client distant à laquelle Trace est fournie. Valeur par défaut : 0.0.0.0

27.2.5.17 Traces > Données de crash du noyau

Le service de données de crash du noyau permet de collecter automatiquement les données de crash du noyau. Il est uniquement disponible sur les systèmes OSBiz X avec cartes mères V3 : OCCLA, OCCMA(R), OCCMB(R).

Le service nécessite 200 Mo d'espace de stockage. Les disques affectés sont les suivants :

- SSS SATA 16 Go (si pas de SSD NVMe)
- SSD NVMe

Si vous souhaitez libérer de l'espace de stockage, il est recommandé de supprimer les traces avant de démarrer le service. S'il n'y a pas d'espace suffisant, le service ne collecte pas les données.

Description des paramètres des onglets :

- **Données de crash du noyau**

Paramètres	Description
Service des données de crash du noyau	État du service : Vert : Le service est activé. Gris : Le service est désactivé.
Démarrer	Démarre le service de données de crash du noyau.
Arrêter	Arrête le service de données de crash du noyau.

Au démarrage ou à l'arrêt du service de données de crash du noyau, un redémarrage du système est automatiquement lancé. Le service conserve l'état après redémarrage du système.

Si le service est activé, après un redémarrage du système avec le motif WATCHDOG ou KERNEL_OOPS, les données de crash du noyau sont disponibles dans l'espace de stockage de diagnostic oso. Pour collecter les données de crash du noyau, vous devez cocher la case **Protocole CoreLog** dans **Centre de service** > **Diagnostics** > **Trace** > **Journaux de diagnostic**.

Après la collecte des données de crash du noyau, le service doit être désactivé manuellement.

27.2.5.18 Traces > Trace du serveur média

Les traces du serveur média peuvent être utilisées pour enregistrer les informations de processus et d'état des différents composants du serveur média du système de communication.

Description des paramètres des onglets :

- **Modifier la composante Trace du serveur média**

Paramètres	Description
Nom du pack	Nom du composant Trace Valeur par défaut : Serveur média
Niveau de trace	Niveau de détail de la trace (Aucun, Non spécifié, Par défaut, Fatal, Erreur, Avertissement, Info, Inattendu, Débogage, Fin, Plus fin)
État de la trace	État de la trace : Vert : La trace est activée. Gris : La trace est désactivée.
Démarrage	Lance la trace du serveur média.
Arrêt	Arrête la trace du serveur média.

27.2.6 Evénements (events)

Le menu **Evénements** regroupe les fonctions d'affichage et de commande des événements (Events). Ces fonctions comprennent notamment la configuration des événements et les paramètres de messagerie électronique.

27.2.6.1 Evénements > Configuration des événements

Description des paramètres des onglets :

- **Modifier la configuration des événements**

Paramètres	Description
Paramètres du fichier d'événements	
Taille maxi. du tampon d'événements (octets)	Affichage de la taille maximale du tampon d'événements en octets
Taille maxi. du fichier d'événements (octets)	Affichage de la taille maximale du fichier de journal d'événements en octets
Temporisation d'événements (s)	Affichage du temps en seconde à l'issue duquel un nouveau fichier de journal d'événements est créé.
Evénement par LAN	
Activer la consignation des événements par LAN	Lorsque le flag est activé, les message d'événements sont transmis via l'interface LAN. Valeur par défaut : Désactivé
Valeur de temporisation (s)	Affichage du temps en secondes à l'issue duquel un les données de protocole Event sont transmises à l'interface LAN.

27.2.6.2 Evénements > Fichier-journal d'événements

Cette fonction permet de télécharger ou d'effacer le fichier-journal d'événements.

Description des paramètres des onglets :

- **Charger par HTTP**
- **Effacer le fichier-journal d'événements**

27.2.6.3 Evénements > E-mail

Description des paramètres des onglets :

- **Modifier les paramètres e-mail**

Paramètres	Description
Paramètres e-mail	

Paramètres	Description
Objet	Texte indiqué dans le champ Objet de l'e-mail.
Adresses e-mail du destinataire	
Destinataire 1	Adresse e-mail à laquelle l'e-mail est envoyé en cas de survenance d'un événement.
Destinataire 2	Adresse e-mail à laquelle l'e-mail est envoyé en cas de survenance d'un événement.
Destinataire 3	Adresse e-mail à laquelle l'e-mail est envoyé en cas de survenance d'un événement.
Destinataire 4	Adresse e-mail à laquelle l'e-mail est envoyé en cas de survenance d'un événement.
Destinataire 5	Adresse e-mail à laquelle l'e-mail est envoyé en cas de survenance d'un événement.
Destinataire des notifications d'urgence	
Destinataire d'urgence	Adresse e-mail d'un agent de sécurité sur site à laquelle un e-mail est envoyé lorsqu'un numéro d'urgence est composé.

27.2.6.4 Evénements > Tableau de réactions

A l'aide du tableau de réactions, il est possible de définir individuellement pour chaque événement comment réagir lorsque cet événement survient.

Description des paramètres des onglets :

- **Modifier tous les évènements**
- **Rétablir les paramètres par défaut pour Tous les évènements**
- **Modifier l'évènement**
- **Démarrer/Arrêter le profil de trace affecté;**

Paramètres	Description
Nom de l'événement	Nom de l'événement
Envoyer un Trap SNMP	Lorsque le flag est activé, un trap SNMP est envoyé lorsque survient un événement.
Envoyer par e-mail	Lorsque le flag est activé, lorsqu'il se produit un événement, il est envoyé un e-mail au destinataire inscrit dans **Modifier les Paramètres e-mail**.
Profil de trace affecté	Profil de trace qui est démarré ou arrêté lorsque survient l'événement.
Démarrer le profil de trace	Lorsque le flag est activé, le profil de trace sélectionné est démarré lorsque l'événement survient.
Arrêter le profil de trace	Lorsque le flag est activé, le profil de trace sélectionné est arrêté lorsque l'événement survient.
Redémarrer la passerelle	Indique si, lorsque l'événement survient, le système de communication est de nouveau démarré.

Paramètres	Description
Redémarrer la passerelle : Oui	Lorsque l'événement survient, un redémarrage du système de communication est effectué.
Redémarrer la passerelle : Non	Lorsque l'événement survient, aucun redémarrage du système de communication n'est effectué.
Av. OpenScape	Indique si, lorsque l'événement survient, il est envoyés un message au système de communication.
Av. OpenScape: Oui	Lorsque l'événement survient, un message est envoyé au système de communication.
Av. OpenScape : Non	Lorsque l'événement survient, aucun message n'est envoyé au système de communication.

27.2.6.5 Evénements > Journaux de diagnostic

Sont affichés ici les journaux de diagnostic ((Fichiers journal)) qui sont automatiquement générés lors des états critiques du système.

Description des paramètres des onglets :

- **Récupérer les journaux de diagnostic**
- **Effacer les journaux de diagnostic**

Paramètres	Description
Nom de fichier	Nom des Journaux de diagnostic ((fichier journal) enregistrés dans le système de communication.
Taille (en octets)	Taille des journaux de diagnostic en octets
Modifié	Date de modification du journal de diagnostic
Autorisations	Attributs du journal de diagnostic : • r = Lecture (Read) • w = Ecriture (Write)

27.2.6.6 Evénements > Signalisation d'alarme

Les terminaux (téléphones du système avec affichage, UP0 et HFA) doivent être notifiés lorsque la température du système dépasse 55 degrés Celsius. Si la température dépasse 60 degrés Celsius, les cartes responsables de la surchauffe (par exemple, SLAD60/16) sont arrêtées de manière contrôlée ou éteintes.

Description des paramètres des onglets :

- **Modifier l'alarme**

Paramètres	Description
Port de signalisation d'alarme de température	

Paramètres	Description
Abonné 1	Destination 1 (abonnés avec téléphone système).
Abonné 2	Destination 2 (abonnés avec téléphone système).
Abonné 3	Destination 3 (abonnés avec téléphone système).

27.2.7 Redémarrer / Recharger

Peut être utilisé pour lancer un redémarrage ou un rechargement d'OpenScape Business et pour un arrêt contrôlé d'OpenScape Business X. De plus, un redémarrage de l'application UC (UC Smart ou UC Suite) est déclenché. Pour permettre l'arrêt contrôlé d'OpenScape Business X via un téléphone système, un code PIN peut être défini. Dans le cas d'un réseau, les systèmes de communication en réseau peuvent être synchronisés.

27.2.7.1 Redémarrer / Recharger > Redémarrer / Recharger

Paramètres	Description
Système	
Maintenance du serveur	Redémarrage contrôlé d'OpenScape Business : • OpenScape Business S et OpenScape Business X : un redémarrage contrôlé du système de communication a lieu.
Système de rechargement	Recharger OpenScape Business : • OpenScape Business S et OpenScape Business X : le système de communication a été mis à jour. Après le redémarrage suivant, le système de communication sera dans son état par défaut. Tous les paramètres spécifiques au pays et au client ont été supprimés (code pays du système = Allemagne). Le système de communication a l'adresse IP par défaut 192.168.1.2 et la plage d'adresses IP internes 192.168.3.xxx. La licence est conservée.
Système d'arrêt	Arrêt contrôlé d'OpenScape Business X : • OpenScape Business X3/X5 : Le redémarrage ultérieur du système de communication n’est possible qu’en débranchant puis en rebranchant la prise d’alimentation. • OpenScape Business X8 : le redémarrage ultérieur du système de communication n’est possible qu’en coupant l’alimentation de tous les blocs d’alimentation LUNA2, puis en les remettant en marche.
Activer/désactiver l'arrêt	Définissez un code PIN pour activer l'arrêt (l'arrêt contrôlé du système de communication) sur un téléphone système.
Applications	

Paramètres	Description
Réseau de synchronisation	Synchronisation des systèmes de communication en réseau : Après toute modification de numéros de téléphone, de numéros DID ou de noms, les données de tous les systèmes de communication en réseau sont mises à jour par synchronisation.
Redémarrer l'application UC	Redémarrage contrôlé de l'application UC (UC Smart ou UC Suite) : Lors d'un redémarrage de l'application UC, toutes les applications actives telles que myPortal pour ordinateur et my Attendant, par exemple, sont déconnectées. Après le redémarrage, toutes les connexions sont automatiquement rétablies.

27.2.8 SNMP

Le menu **SNMP** regroupe les fonctions pour la configuration de communautés et de traps. Les droits d'accès aux données SNMP sont définis via les communautés. Les traps sont générés en cas de problèmes dans le système pour informer l'administrateur des erreurs et des pannes.

27.2.8.1 SNMP > Communautés

Description des paramètres des onglets :

- **Afficher les communautés**

Paramètres	Description
Adresse IP	Adresse IP du partenaire de communication SNMP. Dans l'adresse 127.0.0.1, la communication avec les adresses IP externes est verrouillée.
Communauté	Mot de passe d'identification/d'accès qui est utilisé pour l'utilisateur SNMP. ***INFO :*** Pour améliorer la sécurité, il est conseillé de ne pas utiliser la valeur standard **public**.
Type	Sélection du type.
Type : Communauté de lecture	Partenaire de communication avec accès lecture SNMP.
Type : Communauté de lecture	Partenaire de communication avec accès lecture et écriture SNMP.
Type : Communauté Trap	Partenaire de communication auquel ont été envoyés les messages d'erreur (traps)

27.2.8.2 SNMP > Communautés > Communautés de lecture

Description des paramètres des onglets :

- **Afficher les communautés de lecture**

- **Ajouter une communauté de lecture**

Paramètres	Description
Adresse IP	Adresse IP du partenaire de communication SNMP. Dans l'adresse 127.0.0.1, la communication avec les adresses IP externes est verrouillée.
Communauté	Mot de passe d'identification/d'accès qui est utilisé pour l'utilisateur SNMP. ***INFO :*** Pour améliorer la sécurité, il est conseillé de ne pas utiliser la valeur standard **public**.

27.2.8.3 SNMP > Communautés > Communautés d'écriture

Description des paramètres des onglets :

- **Afficher les communautés d'écriture**
- **Ajouter une communauté d'écriture**

Paramètres	Description
Adresse IP	Adresse IP du partenaire de communication SNMP. Dans l'adresse 127.0.0.1, la communication avec les adresses IP externes est verrouillée.
Communauté	Mot de passe d'identification/d'accès qui est utilisé pour l'utilisateur SNMP. ***INFO :*** Pour améliorer la sécurité, il est conseillé de ne pas utiliser la valeur standard **public**.

27.2.8.4 SNMP > Communautés > Trap Communautés

Description des paramètres des onglets :

- **Afficher les communautés Trap**
- **Ajouter une communauté Trap**

Paramètres	Description
Adresse IP	Adresse IP du partenaire de communication SNMP. Dans l'adresse 127.0.0.1, la communication avec les adresses IP externes est verrouillée.
Communauté	Mot de passe d'identification/d'accès qui est utilisé pour l'utilisateur SNMP. ***INFO :*** Pour améliorer la sécurité, il est conseillé de ne pas utiliser la valeur standard **public**.

27.2.8.5 SNMP > Traps

Description des paramètres des onglets :

- **Afficher tous les Traps**

- **Afficher tous les Traps critiques**

Paramètres	Description
VarBind1 (gravité)	Classification des traps : • Critique : message d'erreur. L'erreur a des conséquences problématiques. • Majeur : message d'erreur. L'erreur peut avoir des conséquences problématiques. • Mineur : message d'erreur. L'erreur n'a pas de conséquences problématiques. • Avertissement : message concernant un processus ou un état pouvant être problématique. • Cleared : le message d'erreur a été supprimé (par ex. le port est de nouveau en service) • Information : pur message d'état, n'est pas un message d'erreur
VarBind2 (Nom)	Nom du trap
Nom générique	Désignation générale comme Entreprise Specific
Nom spécifique	Type de Traps : • 1 = Logiciel • 2 = Matériel
Entreprise	(non utilisé)
Heure	Heure de survenance de l'erreur
L'index	Numéro séquentiel

27.2.9 Protocole Admin

Le menu **Protocole Admin** permet à l'administrateur de modifier la configuration (par ex. la langue) du protocole d'administration.

27.2.9.1 Protocole Admin > Configuration

Description des paramètres de l'onglet :

- **Modifier la configuration**

Paramètres	Description
Langue du protocole d'admin.	Réglage de la langue souhaitée pour le protocole d'admin. Le protocole Admin fournit une présentation des modifications opérées sur le système de communication. Langues disponibles : Allemand, Anglais, Français, Espagnol, Italien, Portugais, Néerlandais

27.2.9.2 Protocole d'admin > Données du protocole d'admin

Description des paramètres de l'onglet :

- **Charger par HTTP**

Paramètres	Description
Charger par HTTP	Enregistre le protocole d'administration du système de communication. Le protocole d'administration vous donne la possibilité quand des modifications ont été apportées au système de communication et qui en est l'auteur. Les connexions au système de communication sont consignées.

27.2.10 Actions

Les fonctions qui permettent à l'administrateur d'exécuter des tâches d'administration récurrentes, telles que la suppression de données de protocoles, sont regroupées sous **Actions**.

27.2.10.1 Actions > Actions manuelles > Journaux de diagnostic

Description des paramètres des onglets :

- **Charger les données par HTTP**

Paramètres	Description
Fichier-journal de trace	Lorsque le flag est activé, les fichiers journal de trace système sont téléchargés. Les possibilités suivantes existent : • Journal complet : la totalité des fichiers journal Trace sont téléchargés. • Protocole d'aujourd'hui : Les fichiers journal de trace système du jour (à partir de 00h00) sont téléchargés. • Propre sélection : De : XXX À : YYY : Les fichiers journal de trace système de la période sélectionnée sont téléchargés. Valeur par défaut : activée, Journal complet
Journal des événements	Lorsque le flag est activé, les fichiers journal avec indication sur les actions/ événements du système de communication (réinitialiser, activer/désactiver, etc.) sont téléchargés. Valeur par défaut : Activé
Protocole d'admin.	Lorsque le flag est activé, les fichiers journal avec indications sur les procédures administratives (tentatives de connexion, etc.) sont téléchargés. Valeur par défaut : Activé
Protocoles de licences	Lorsque le flag est activé, les fichiers journal avec messages sur les ccomposantes du système de communication qui nécessitent une licence sont téléchargés. Valeur par défaut : Activé
Trace client	Lorsque le flag est activé, les fichiers journal avec messages sur la Trace client (connexion distante, connexion ITSP, etc.) sont téléchargés. Les messages pour la Trace client sont représentés sous une forme complète, par exemple dans le fichier-journal de trace. Valeur par défaut : Activé

Paramètres	Description
Protocole Framework	Lorsque le flag est activé, les fichiers journal avec messages du WBM sont téléchargés. Valeur par défaut : Activé
Protocole de diagnostic	Lorsque le flag est activé, les journaux de diagnostic du système de communication sont téléchargés. Valeur par défaut : Activé
Comptes rendus Suite UC	Lorsque le flag est activé, les fichiers journal avec messages de UC Suite (journaux UC Suite, CSP et MEB) sont téléchargés. Les possibilités suivantes existent : • Journal complet : Tous les fichiers-journaux Suite UC, CSP et MEB sont téléchargés. • Protocole d'aujourd'hui : les fichiers journal suite UC, CSP et MEB du jour (à partir de 00h00) sont téléchargés. • Propre sélection : De : XXX À : YYY : les fichiers journal suite UC, CSP et MEB de la période sélectionnée sont téléchargés. Tous les fichiers journaux sont regroupés dans un fichier comprimé. Pour les protocoles OpenScape Business on utilise les désignations de fichiers ci-après. Fichiers-journaux Suite UC = vs_jjjj_mm_tt.log, fichiers-journaux CSP = csptrace_jjjj_mm_tt.log, fichiers-journaux MEB = mebtrace_jjjj_mm_tt.log Valeur par défaut : Désactivé
Protocoles d'application	Lorsque le flag est activé, les fichiers journal avec messages de la partie Application du système de communication (par exemple journaux CSP) sont téléchargés. • Journal complet : Tous les fichiers journal existants sont téléchargés. • Protocole d'aujourd'hui : Les fichiers journal de la journée d'aujourd'hui (à partir de 00h00) sont téléchargés. • Propre sélection : De : XXX À : YYY : Les fichiers journal de la période sélectionnée sont téléchargés. Tous les fichiers journaux sont regroupés dans un fichier comprimé. Valeur par défaut : Désactivé
Protocoles Diagnostics système	Lorsque le flag est activé, les journaux de diagnostic du système de communication sont téléchargés. Valeur par défaut : Activé
Protocole PPP	Lorsque le flag est activé, les fichiers journal avec messages concernant le protocole point-à-point sont téléchargés. Valeur par défaut : Activé
Protocole CoreLog	Lorsque le flag est activé, les fichiers journal avec des information sur l'état le plus récent du système d'exploitation sont téléchargés. Les CoreLogs sont par exemple créé lors des restarts. Valeur par défaut : Désactivé

27.2.10.2 Actions > Actions manuelles > Maintenance DLI

Description des paramètres des onglets :

- **Maintenance des équipements DLI**

Paramètres	Description
Supprimer l'équipement	Sélectionnez le téléphone système à supprimer. Avec cette action, le téléphone système est supprimé de la base de données DLI. **Remarque :** Avant toute action de maintenance DLI (suppression), vous devez d'abord vous assurer que l'appareil n'est plus utilisé.
Numéro	Numéro d'appel du téléphone système
Type d'équipement	Type de téléphone système.
Adresse IP	Adresse IP du téléphone système ; lien direct avec WBM du téléphone IP.
Adresse MAC	Adresse MAC du téléphone système.
Version actuelle du logiciel	Version logicielle actuelle du téléphone système.

27.2.10.3 Actions > Actions automatiques > Regroupement des positions non utilisées

Description des paramètres des onglets :

- **Modifier l'action**
- **Démarrer/Arrêter l'action**

Paramètres	Description
Action activée	Lorsque le flag est activé, il est effectué régulièrement un nettoyage automatique des mémoires d'enregistrement sur le système de communication. Une fois terminé le nettoyage automatique de la mémoire, le système de communication effectue un redémarrage (Restart). Valeur par défaut : Désactivé
Heure de début après minuit	Heure après minuit où l'action Regroupement des positions non utilisées est effectuée. Exemple: Dans le champ **h**. il a été inscrit 3 et dans le champ **min**. 30. Cela signifie que l'action Regroupement des positions non utilisées sera lancée le matin, à 3h30. Valeur par défaut : 3 heures, 00 min.
Exécuter l'action les jours de semaine suivants	L'action de regroupement des positions non utilisées est effectuée les jours de la semaine sélectionnés. Valeur par défaut : Activé

27.2.10.4 Actions > Actions automatiques > Notification DLS

Description des paramètres des onglets :

- **Modifier l'action**
- **Démarrer/Arrêter l'action**

Paramètres	Description
Action activée	Lorsque le flag est activé, lors de la mise en route du système de communication, la connexion automatique à un serveur DLS externe est lancée. Valeur par défaut : Désactivé
Adresse IP	Adresse IP du serveur DLS externe Valeur par défaut : 0.0.0.0
Port	Port du serveur DLS Valeur par défaut : 10444
Nom utilisateur	Nom utilisateur pour la connexion au serveur DLS externe
Mot de passe	Mot de passe pour la connexion au serveur DLS externe

27.2.10.5 Actions > Actions automatiques > Contrôle d'intégrité SDHC

Description des paramètres des onglets

- Contrôle d'intégrité SDHC

Paramètres	Description
Contrôle d'intégrité SDHC	
Contrôle d'intégrité SDHC	Active immédiatement le contrôle d'intégrité de la carte
Démarrer le contrôle d'intégrité	Active un jour, un mois, une année et une heure programmés pour le contrôle d'intégrité de la carte.
Fichier journal Le résultat des derniers contrôles de fichier s'affiche.	
Etat/action recommandé(e) Actions recommandées pour chaque état d'intégrité de la carte.	

27.2.11 Diagnostic de la plate-forme

Possibilité de diagnostic des plateformes (seulement pour le développement).

27.2.12 Diagnostics des applications

Possibilité de diagnostic des applications (seulement pour le développement).

27.2.12.1 Diagnostics des applications > Paramètres développeur > Sortie console de trace

Possibilité de diagnostic des applications (seulement pour le développement).

27.2.12.2 Diagnostics des applications > Paramètres développeur > Reprendre le jeton écriture

Possibilité de diagnostic des applications (seulement pour le développement).

27.2.12.3 Diagnostics des applications > Carte mère

Les paramètres ne doivent être modifiés que sur instruction du support SAV compétent.

27.2.12.4 Diagnostics des applications > Paramètres développeur > Profils de fournisseur SIP

Description des paramètres des tags :

- Ajouter des profils de fournisseur SIP
- Modifier les profils de fournisseur SIP

Cette page est destinée à être utilisée par des techniciens formés lors de la certification d'un nouvel ITSP. Veuillez consulter les documents disponibles sur le wiki Unify : http://wiki.unify.com/index.php/ Collaboration_with_VoIP_Providers # How_to_get_a_new_VoIP_provider_released pour plus d'informations.

27.2.13 Diagnostic IP

Possibilité de diagnostic IP (seulement pour le développement).

27.2.13.1 Diagnostic IP > Carte mère > Protocole ARP

Cette fonction sert à afficher les données du protocole ARP (Address Resolution Protocol). La table Mapping indique l'affectation des adresses réseau aux adresses MAC.

Description des paramètres des onglets :

- **Afficher le protocole ARP**

Paramètres	Description
Adresse IP	Indique les adresses réseau qui sont actuellement raccordés à la carte mère du système de communication.
Adresse MAC	Indique l'adresse physique correspondante des adresses réseau raccordées
Type	Indique l'affectation des adresses. Est possible une affectation fixe (statique) ou une affectation dynamique.
Interface	Désignation interne des interfaces LAN existantes (par exemple eth0, eth1, eth2, eth3)

27.2.13.2 Diagnostic IP > Carte mère > Demande ICMP > Ping

A l'aide de cette fonction, il est possible de contrôler la connexion réseau entre le système de communication et une adresse de destination librement sélectionnable, à l'aide d'une commande Ping (demande d'écho).

Description des paramètres des onglets :

- **Exécuter Ping**

Paramètres	Description
Paramètres ICMP	
Adresse de destination	la destination dont la connexion réseau avec le système de communication est contrôlée à l'aide des paquets de demande d'écho. Valeur par défaut : 127.0.0.1
Nombre de demandes d'écho à envoyer	Nombre des paquets de demande d'écho à envoyer pour le contrôle de la connexion réseau Valeur par défaut : 3

27.2.13.3 Diagnostic IP > Carte mère > Demande ICMP > Itinéraire de trace

A l'aide de cette fonction il est déterminé avec la demande d'écho ICMP les routeurs qui serviront à transmettre les paquets de données jusqu'à l'adresse de destination interrogée.

Description des paramètres des onglets :

- **Itinéraire de trace**

Paramètres	Description
Paramètres ICMP	
Adresse de destination	Adresse IP de la destination dont la route de trace, en direction du système de communication est contrôlée à l'aide des paquets de demande d'écho ICMP. Valeur par défaut : 127.0.0.1

Paramètres	Description
Octet TOS	Indication précisant si des octets TOS (Type of Service) ont été envoyés. Les octets TOS donnent une idée sur la qualité d'un service. Plage de valeurs : 0 à 255, valeur par défaut : 0

27.2.14 Utilisateur en ligne

Web-Tool pour télécommande des téléphones OpenStage.

27.2.14.1 Abonné en ligne

Avec l'abonné en ligne s'ouvre Java Husim Phone Tester (jHPT). Il s'agit d'un outil Web pour la télécommande des téléphones OpenStage via Internet.
A partir de l'interface Web, le téléphone système disponible est contrôlé de sorte que les appuis réels sur les boutons et les affichages du système de communication sont transmis. Il existe sur jHPT une documentation séparée qui peut être téléchargée au moyen de la fonction Aide de l'outil (il n'est pas donné ici de description des pages jHPT).

27.3 Téléphonie

Dans **Téléphonie** sont regroupées les fonctions servant à la configuration de la téléphonie, par ex. pour paramétrer les abonnés ou la gestion des appels (CM).

27.3.1 Configuration de base

Configuration de base regroupe des fonctions telles que Flags système, Paramètres pour les répertoires téléphoniques et Numéros abrégés, DynDNS, QoS (qualité de service), Date et heure ainsi que la taxation.

27.3.1.1 Configuration de base > Système > Indicateurs système

Description des paramètres des onglets :

- **Modifier les indicateurs système**

Paramètres	Description
Connexion traversante pour FWD externe sur	Lorsque cette option est activée, les appels transférés vers une destination externe sont acheminés immédiatement. Le transfert s'effectue indépendamment du fait qu'il s'agisse d'un appel interne ou externe (MSI/ ISDN). Si le transfert d'appel s'effectue via une ligne ISDN et que la destination de transfert externe se trouve sur un autre réseau (par exemple, un réseau GSM), l'établissement de l'appel depuis le central ISDN est signalé par l'indicateur de progression « Quitter ISDN ». À compter de ce moment, l'appelant encourt des frais de connexion. Valeur par défaut : Désactivé

Paramètres	Description
Le renvoi d'appel vers l'interface de la station principale est autorisé.	Lorsque ce drapeau est activé, les appels via les lignes analogiques (MSI) suivent le renvoi d'appel externe. Valeur par défaut : Activé
Recherche vers une destination de transfert d'appel externe	Lorsque cette option est activée, les règles suivantes s'appliquent : si la destination de renvoi d'appel externe est injoignable, l'appel est renvoyé vers la prochaine destination saisie dans la liste des destinations d'appel. Valeur par défaut : Désactivé
Ton de conférence	Lorsque ce signal est activé, un signal sonore spécial, émis à intervalles de 20 secondes, rappelle aux participants d'une conférence qu'ils sont actuellement en conférence téléphonique. Valeur par défaut : Désactivé
Signal d'avertissement pour les groupes de prise d'appel	Lorsque ce drapeau est activé, un appel destiné à un membre d'un groupe de prise d'appel est signalé aux autres membres du groupe par un signal optique (via l'écran). Si l'appel n'est pas pris dans les quatre cycles d'appel (4 x 5 secondes), les autres membres du groupe reçoivent également une tonalité d'avertissement. Valeur par défaut : Activé
Augmenter le volume pour les terminaux optiPoint/ OpenStage	Lorsque ce paramètre est activé, les téléphones optiPoint et OpenStage passent à un mode d'atténuation alternatif, ce qui augmente le volume. Valeur par défaut : Désactivé
Déménagement autorisé	Lorsque cette option est activée, les téléphones du système peuvent être déplacés physiquement sans modifier la configuration logique (numéro d'appel, nom, programmation des touches, etc.). Valeur par défaut : Désactivé
Plus d'un membre externe à la conférence	Lorsque cette option est activée, plusieurs abonnés externes peuvent participer à une conférence. Valeur par défaut : Activé
Réservation de coffre automatique	Lorsque cette option est activée, un abonné peut réserver une ligne à l'avance s'il n'y a pas de lignes libres disponibles (signal d'occupation). L'abonné reçoit une notification dès que cette ligne est libre et peut alors établir la connexion externe. Valeur par défaut : Désactivé
Non, recomposer avec le code du compte	Lorsque cette option est activée, lors de la recomposition du numéro, tout code de compte saisi est également répété en plus du numéro de poste. Valeur par défaut : Désactivé

Paramètres	Description
Numérotation simplifiée	Lorsque ce paramètre est activé, la composition d'un seul chiffre sur un téléphone du système déclenche immédiatement la prise de ligne et le numéro d'appel requis est composé. Il n'est pas nécessaire de composer le code d'accès. Pour composer un numéro de poste interne, l'une des procédures suivantes doit être utilisée : • Appuyez sur la touche Interne (la touche Muet se transformera en Interne si la numérotation simplifiée est activée) et composez le numéro de poste • ou appuyez sur la touche DSS correspondante. Cette fonction n'est disponible que si une seule route (voir Routes) a été configurée. Si des téléphones Entry, ISDN ou a/b sont encore connectés au système de communication, la numérotation automatique LCR n'est pas possible.
Utilisez uniquement le numéro par défaut pour MSN	Lorsque ce drapeau est activé, sur un bus S0, les MSN (Multiple Subscriber Numbers) ne peuvent être créés que pour les numéros de station internes déjà existants (afin d'empêcher toute fraude éventuelle au péage). Valeur par défaut : Désactivé
Optimisation de trajectoire	Lorsque ce paramètre est activé, une optimisation du chemin est effectuée dans les systèmes de communication en réseau. Cette option doit être activée pour tous les systèmes de communication appartenant au réseau. Exemple pour deux systèmes en réseau (système 1 et système 2) : Pour un appel de l'abonné A (système 1) à l'abonné B (système 2) et un transfert d'appel ultérieur vers l'abonné C (système 1), deux lignes sont réservées. Grâce à l'optimisation du chemin, la connexion de A à C bascule automatiquement sur un seul tronc. Valeur par défaut : Activé
DTMF automatique	Lorsque ce paramètre est activé, le mode DTMF est activé à chaque fois qu'un appel sortant est établi. Cela permet par exemple de consulter à distance les répondeurs automatiques. Valeur par défaut : Activé
Diffusion avec connexion	Lorsque cette option est activée, la fonction d'appel du haut-parleur (messagerie vocale) vous permet d'établir une connexion interne sans que l'abonné appelé ait à décrocher le combiné. En décrochant le combiné, l'appel devient un appel normal à deux interlocuteurs. Valeur par défaut : Activé
Tonalité du CO	Lorsque ce drapeau est activé, une connexion est établie avec le bureau central ou avec un système de communication en réseau, même si aucune tonalité n'est envoyée par le pair. Valeur par défaut : Désactivé
Protection contre les retours d'appel	Lorsque cette option est activée, les appels en PCV sont automatiquement libérés. Valeur par défaut : Désactivé

Paramètres	Description
Euro-impédance	Lorsque ce drapeau est activé, les valeurs d'impédance suivantes s'appliquent en Europe : Interfaces a/b pour la connexion de la station analogique : Impédance d'entrée = 270 Ω + 750 Ω || 150 nF, Impédance de la deuxième sonnerie = 270 Ω + 750 Ω || 150 nF, Niveau relatif A/D = 0 dBr, Niveau relatif N/A = –7 à 7 dBr Interfaces a/b pour la connexion analogique principale : Impédance d'entrée = 270 Ω + 750 Ω || 150 nF, Impédance de la deuxième sonnerie = 270 Ω + 750 Ω || 150 nF, Niveau relatif A/D = –6 à 6 dBr, Niveau relatif N/A = –1 à 1 dBr Valeur par défaut : Désactivé
Messages téléphoniques différents Jour/Nuit	Lorsque ce drapeau est activé (dans un système de communication avec messagerie vocale), différentes annonces de messagerie vocale peuvent être activées pour une station en transmettant différents numéros de station pour cette station à la messagerie vocale. Il est indispensable, au préalable, de configurer des destinations de renvoi d'appel différentes pour les modes jour et nuit sur ce poste. Valeur par défaut : Désactivé
Afficher le code international/national	Lorsque cette option est activée, vous pouvez définir le format d'affichage des numéros de numérotation abrégée système (SSD) pour les appels entrants pour lesquels aucun nom n'est stocké dans la mémoire SSD. Le numéro de téléphone complet (numéro PABX + numéro d'appel direct à l'arrivée (DID), y compris l'indicatif régional et l'indicatif du pays, le cas échéant) s'affiche sur l'écran du téléphone. Exemple : Le SSD numéro 06671234 a été configuré sans nom. Indicatif régional = 02302, numéro PABX = 667, numéro DID = 1234. En cas d'appel entrant provenant du 6671234, le numéro 023026671234 apparaît sur l'écran. Valeur par défaut : Désactivé
Changement de ligne pour appel direct	Cet indicateur est utilisé pour définir le comportement d'une touche de sélection directe de station (DSS) pendant un appel actif sur une ligne MULAP. Pertinent pour la configuration d'équipe / groupe d'équipe, direction / secrétaire / groupe supérieur, MULAP de base, MULAP exécutif. En appuyant sur une touche de sélection directe de station (DSS), un changement de ligne est effectué. L'appel est mis en attente et ne peut être repris qu'à partir de ce téléphone. Valeur par défaut : Désactivé (sauf pour les États-Unis et le Canada), Activé (uniquement pour les États-Unis et le Canada)
Recomposition automatique	La recomposition automatique est effectuée lorsqu'un abonné appelé est occupé. Le paramètre temporel « Minuteur pour la recomposition automatique » définit le délai après lequel la recomposition est activée. Valeur par défaut : Désactivé
Numéro d'appel du nœud de messagerie vocale	Lorsque cet indicateur est activé pour les systèmes de communication en réseau, il définit si le numéro de nœud doit être fourni pour l'identification d'un serveur de messagerie vocale central ou de plusieurs serveurs décentralisés. Le numéro de nœud doit être fourni pour l'identification du ou des serveurs de messagerie vocale. Valeur par défaut : Désactivé

Paramètres	Description
Prise d'appel après rappel automatique	Lorsque ce drapeau est activé, les rappels et les rappels sont également signalés aux autres membres d'un groupe de prise d'appel et peuvent être acceptés par eux. Valeur par défaut : Désactivé
CLIP configurable	Lorsque cette option est activée, au lieu du numéro de station réel, c'est le numéro saisi sous Clip/Lin qui est transmis à la connexion externe appelée et affiché sur l'écran. Si le champ Clip/Lin est vide, le numéro de station est transmis. Valeur par défaut : Activé
Liste des appelants à destination en cas de transfert de ligne	Lorsque ce drapeau est activé, en cas de touche de transfert de ligne (MULAP), les appels entrants sont enregistrés dans la liste des appelants du poste de destination. Valeur par défaut : Désactivé
Renvoi d'appel après déviation d'appel / transfert en une seule étape	Lorsque ce paramètre est activé, les règles suivantes s'appliquent : si un abonné a activé le renvoi d'appel vers une destination interne (déviation d'appel), l'appel est signalé à cette destination. Une fois le délai de renvoi d'appel expiré, l'appel est signalé à la première destination enregistrée dans la liste des destinations d'appel, puis à la deuxième destination, le cas échéant, et ainsi de suite. Exemple : Pour la station A, un appel de déviation vers la station B a été exécuté. La première destination enregistrée dans la liste des destinations d'appel du poste B est le poste C, et la seconde est le poste D. Dans ce cas, l'appel sera d'abord signalé au poste C, puis au poste D, une fois le délai de transfert d'appel expiré. L'activation de cet indicateur n'a de sens que si l'indicateur « Suivre la gestion des appels en cas de renvoi d'appel / transfert en une seule étape » est également activé. Pour que cet indicateur ait un quelconque effet, les fonctions de redirection auront lieu lors des appels, des dérivations et des transferts d'appels en une seule étape, et s'appliquent principalement aux appels gérés via UC (groupes de standard automatique/UCD) où ces fonctions de redirection sont applicables. Valeur par défaut : Activé
Suivez la procédure de gestion des appels en cas de renvoi d'appel / transfert en une seule étape	Lorsque ce paramètre est activé, les règles suivantes s'appliquent : si un abonné a activé le renvoi d'appel vers une destination interne (déviation d'appel), l'appel est d'abord signalé à cette destination, puis à toute autre destination saisie dans la liste des destinations d'appel (après expiration du délai de renvoi d'appel). Exemple : Pour la station A, un appel de déviation vers la station B a été exécuté. La première destination enregistrée dans la liste des destinations d'appel du poste B est le poste C. Une fois le délai de renvoi d'appel expiré, l'appel est signalé au poste C. Pour que cet indicateur ait un quelconque effet, les fonctions de redirection auront lieu lors des appels, des dérivations et des transferts d'appels en une seule étape, et s'appliquent principalement aux appels gérés via UC (groupes de standard automatique/UCD) où ces fonctions de redirection sont applicables. Valeur par défaut : Activé

Paramètres	Description
Signal d'avertissement pendant l'enregistrement vocal	Si l'indicateur est activé, les dispositions suivantes s'appliquent à OpenScape Business X : si l'enregistrement vocal (enregistrement des appels en direct) est activé pendant un appel, une tonalité d'avertissement correspondante est émise si l'indicateur est défini. Valeur par défaut : Activé
Schéma de numérotation E.164	Ce paramètre permet d'activer ou de désactiver la mise en réseau CDB des systèmes clients répartis sur plusieurs sites ou à l'échelle mondiale. Les stations peuvent être jointes via un numéro public (le numéro d'appel E.164) au format national ou international (par exemple, le numéro de l'appelant interne au format ISDN), sans composer au préalable un numéro de nœud. Chaque station est représentée par son numéro d'appel E.164, qui peut être affiché dans un format optimisé. Si l'option est activée, la numéro d'appel interne est transférée au format E.164. Si cet indicateur est activé, les stations SIP sont enregistrées avec la version longue du numéro d'appel E.164 (numéro de localisation + numéro d'appel interne, par exemple 4923026673665). Valeur par défaut : Désactivé
Fonctionnalités étendues des touches	Si l'option est activée, une fois qu'une touche est définie comme la « touche Maj », seuls les numéros de téléphone sans prise en charge LED peuvent être enregistrés au deuxième niveau de touche désormais disponible. Toutes les fonctions clés du premier niveau de touches peuvent être programmées. La signalisation par LED est associée uniquement au premier niveau de touche. Valeur par défaut : Désactivé
Numéro d'appel dans les groupes de prise en charge / groupes de sonnerie / CFN / RNA	Lorsque ce drapeau est activé, le numéro de poste et le nom de l'appelant sont affichés à tous les membres d'un groupe de prise d'appel, à tous les membres inclus dans un groupe de sonnerie et aux destinations CFN (renvoi d'appel) et CFNA (renvoi d'appel en cas de non-réponse). Le numéro et le nom de la station sont affichés. Valeur par défaut : Activé
Support SPE	Lorsque ce drapeau est activé, la fonction de chiffrement de la signalisation et de la charge utile (SPE) est prise en charge. Les flux de données utiles et de signalisation VoIP vers et depuis le système de communication et entre les téléphones du système OpenStage sont cryptés. Valeur par défaut : Désactivé **Remarque :** Si vous souhaitez utiliser le service Cloud, Unify Video, le **support SPE** doit être désactivé pour enregistrer la jonction, sauf si un certificat SPE est importé dans le système.

Paramètres	Description
Ton consultatif de SPE	Lorsque ce drapeau est activé, ce qui suit s'applique : lorsque le drapeau système SPE Support est activé et qu'un téléphone OpenStage 15, 20, 20 E ou 20 G est utilisé, les abonnés sont avertis d'une connexion non cryptée par un bip sonore en plus de l'affichage. L'activation du paramètre de station « Sécurité de la charge utile » est une condition préalable à l'utilisation du SPE par un abonné. Aucun bip sonore n'est émis lors de l'utilisation d'un téléphone OpenStage 40, 40 G, 60, 60 G, 80 ou 80 G. L'état de la connexion (chiffrée/ non chiffrée) est affiché en permanence. Valeur par défaut : Désactivé **Remarque :** Si vous souhaitez utiliser le service Cloud, Unify Video, la **tonalité consultative SPE** doit être désactivée pour enregistrer le trunk, à moins qu'un certificat SPE ne soit importé dans le système.
Transit de fournisseur SIP à fournisseur SIP	Lorsque ce paramètre est activé, les connexions aux lignes de transit sont autorisées pour les connexions ITSP. Une connexion est une connexion de transit lorsqu'un seul appel occupe deux lignes dans le même système de communication. Exemple : Un flux externe est acheminé vers une station interne via un fournisseur de services de messagerie (ITSP). La station interne transfère ensuite l'appel vers une destination externe via un fournisseur de services de télécommunications (ITSP). Cela crée une connexion de ligne de transit au sein du système de communication. Deux lignes sont occupées pendant toute la durée de l'appel. Les correspondances de lignes de transport en commun qui en résultent sont autorisées. Valeur par défaut : Désactivé
Numérotation transparente des touches * et # sur les interfaces de jonction	Lorsque ce paramètre est activé, les fonctionnalités Centrex peuvent être activées ou désactivées via des liaisons IP (ITSP) et des liaisons ISDN. Plusieurs fournisseurs proposent des fonctionnalités Centrex (Central Office Exchange) qui peuvent être activées ou désactivées à l'aide de codes. La saisie du code doit avoir lieu en mode numérotation (par exemple, après avoir saisi le code du réseau). La saisie commence toujours par * (astérisque) ou # (dièse). Ceci doit être suivi du code proprement dit (chiffres de 0 à 9) et se terminer par # (dièse). Il n'est pas possible d'activer ou de désactiver les fonctionnalités de Centrex en mode conversation. Les fonctionnalités de Centrex peuvent être activées ou désactivées via des liaisons IP (ITSP) et des liaisons RNIS. Valeur par défaut : Désactivé

Paramètres	Description
Ajouter le code de saisie pour MEX	S'applique uniquement aux appels externes initiés via la fonction « Extension mobile (MEX) » du fournisseur de services de téléphonie sur IP. Si l'option est activée, le système ajoute automatiquement l'indicatif CO au numéro de téléphone pour les appels sortants externes si ce numéro comporte plus de 7 chiffres, car le système l'interprète alors comme un numéro de téléphone externe. Si le numéro de téléphone comporte moins de 7 chiffres, l'indicatif CO n'est pas ajouté, car le système interprète le numéro comme un numéro d'appel interne. Si l'indicateur est désactivé, le fournisseur de services doit ajouter le code CO au numéro de téléphone pour tous les appels sortants externes. Valeur par défaut : Désactivé
Sonnerie CMI MWI	Si cette option est activée, le bip d'indication de message en attente (MWI) est activé pour les téléphones DECT (CMI : intégration multicellulaire sans fil). Autrement dit, lorsqu'un nouveau message est reçu dans la boîte vocale, une tonalité d'alerte est émise. Valeur par défaut : Désactivé
Mise à jour automatique du logiciel des téléphones Openstage TDM	Si cette option est activée, lorsque la version logicielle d'un téléphone TDM est antérieure à celle du système, le logiciel du téléphone est automatiquement mis à jour. Valeur par défaut : Activé
Limiter les connexions indirectes des groupes de troncs conformément à la matrice CON	Si une entreprise possède des succursales dans plusieurs villes, chaque succursale peut être reliée au fournisseur national de télécommunications. Ces branches peuvent également être reliées entre elles par des canalisations de liaison privées. Pour des raisons de réglementation nationale (par exemple, en Inde), il peut être illégal d'effectuer la connexion suivante : une station utilise une liaison privée entre son système de communication et un système de communication privé situé dans une autre ville, puis une liaison d'un opérateur de télécommunications national pour atteindre une destination externe locale. Il faudrait plutôt utiliser directement une ligne interurbaine d'un opérateur de télécommunications national pour les appels entre villes. Cette exigence est mise en œuvre comme suit : • Les connexions entre les liaisons privées peuvent être restreintes en configurant la matrice CON. • Pour les liaisons privées incluant les fonctions de renvoi d'appel, de transfert et de conférence, l'indicateur « Restreindre les connexions indirectes aux groupes de liaisons selon la matrice CON » a été introduit. L'activation/désactivation de cette option a les effets suivants : – Activé : Les appels entre villes utilisant des liaisons privées sont restreints. – Désactivé : Les appels entre villes utilisant des liaisons interurbaines privées sont autorisés. Valeur par défaut : Désactivé
Numérotation ouverte	

Paramètres	Description
actif	Lorsque la numérotation ouverte est utilisée, une station est identifiée par le numéro de nœud, suivi du numéro d'appel ou du numéro DID. Cela permet d'attribuer le même numéro d'appel à des stations situées dans différents nœuds. Dans un système en réseau, cet indicateur est toujours défini de manière identique pour tous les systèmes. Valeur par défaut : Désactivé
Numéro d'appel du nœud	Si la numérotation ouverte est activée, le numéro d'appel du nœud doit être saisi ici. Une station ne peut être jointe depuis d'autres nœuds qu'en composant le numéro d'appel de ce nœud, suivi du numéro de la station. Si le nombre total de chiffres du numéro d'appel du nœud et du numéro de station dépasse 7, un avertissement correspondant est émis. Valeur par défaut : Désactivé
autorisation de transit	
Transports en commun	Lorsque ce paramètre est activé, les connexions de transit associées à des fonctionnalités spécifiques telles que le renvoi d'appel externe, les transferts d'appel et les applications DISA, par exemple, sont autorisées. Ceci s'applique que ce soit par liaison directe ou par connexion entre deux câbles. Valeur par défaut : Activé
Trafic de transit	Lorsque ce drapeau est activé, les connexions de transit en numérotation directe entrante pour les connexions de jonction (systèmes de communication en réseau) sont autorisées. Valeur par défaut : Activé
transit du trafic extérieur	Lorsque ce drapeau est activé, les connexions de transit en numérotation directe entrante pour les connexions inter-réseaux sont autorisées. Valeur par défaut : Désactivé
Interrupteur spécial	
CALL PROC n'envoie pas	Cette option doit être activée si le fournisseur de services ne doit recevoir aucun message de procédure d'appel (message RNIS) du système de communication. Valeur par défaut : Désactivé
Saisie automatique et cyclique de la ligne	Si cette option est activée, les appels sortants s'empareront cycliquement de nouvelles liaisons ISDN lorsque l'établissement de la connexion échoue (par exemple, en l'absence d'accusé de réception ACK). Les numéros de ligne ou d'itinéraire sont incrémentés. Valeur par défaut : Activé
Restriction des appels UC	
Restriction des appels UC	Lorsque ce paramètre est activé, pour tous les appels UC initiés par le système (par exemple, via le service Call-Me), une vérification est effectuée avant la numérotation afin de déterminer si l'utilisateur UC demandeur dispose de la classe de service requise pour cet appel. Si l'utilisateur UC ne dispose pas de la classe de service requise, l'appel n'est pas exécuté. Valeur par défaut : Désactivé

27.3.1.2 Configuration de base > Système > Temporisations

Le tableau contient la liste de toutes les temporisations configurables (colonne **Description**). Les colonnes **Base** et **Facteur** permettent de régler les valeurs de compteur pour les temporisations correspondantes. Elles se calculent ainsi : Temps = Base x Facteur. Si la valeur 255 est entrée dans la colonne **Facteur**, cette temporisation est sans effet.

Description des paramètres des onglets :

- **Modifier les temporisations**

Paramètres	Description
Libération du récepteur de code après prise sans numérotation	Définit la durée de connexion du récepteur de code sur les terminaux MF et par conséquent la durée pendant laquelle une numérotation est possible. Après écoulement du délai spécifié, le récepteur de code est libéré. Plage de valeurs : 5 - 15 s
Temps pour activer une faculté en cours de communication	Est activé si la touche de signal est pressée sur un terminal. La touche de signal aide à faire la distinction entre le fait qu'un abonné veuille reprendre un double appel et le fait qu'il veuille activer une fonctionnalité comme conférence, par exemple. Plage de valeurs : 2 - 4 s
Temps de reprise d'une ligne après libération	Démarré sur les jeux de lignes, empêche une prise de ligne sortante immédiate après libération pendant ce délai. Plage de valeurs : 0 - 5 s
Temps avant activation du rappel automatique	Démarré si un terminal passe en repos. Une fois l'intervalle de temps écoulé, il est déterminé, si un rappel automatique doit être exécuté. Ceci permet à l'abonné d'exécuter d'autres communications sortantes. Plage de valeurs : 0 - 60 s
Durée du rappel automatique	Dans le cas d'un rappel automatique, si le rappel n'est pas desservi au bout de ce délai, l'appel est terminé et le rappel automatique est reporté. Plage de valeurs : 15 - 60 s
Durée avant renvoi PO pour retour d'appel	Si un retour d'appel n'est pas desservi dans un certain délai, la communication est transférée au poste opérateur si ce critère de retour à été sélectionné. Plage de valeurs : 20 - 600 s
Durée de la sonnerie pour transfert avant réponse	Si une communication transférée (pour abonné occupé) n'est pas desservie au bout d'un certain délai, un renvoi s'opère sur le poste qui a initialisé le transfert. Plage de valeurs : 30 - 600 s
Fin de numérotation pour SDA analogique (Autriche)	Compteur de supervision pour SDA. Si aucune sélection n'est effectuée pendant cette durée, la numérotation SDA est reconnue comme étant incomplète ou inexistante. (Valable uniquement en Autriche) Plage de valeurs : 10 - 30 s

Paramètres	Description
Temps de fin de numérotation(pas de num.)	Si la numérotation n'a pas commencé au bout d'un certain délai, une fin de numérotation automatique est générée. Plage de valeurs : 5 - 15 s
Temps entre 1re et 2e annonce pour option Fax/ SDA	Fax/SDA, SDA analogique, Délai après message vocal. Valeur par défaut : 15 s
Temps pour parcage / mise en garde/mise garde commune	La réactivation de la communication parquée doit se faire dans un certain délai. Si la communication parquée n'est pas reprise dans un certain délai, il y a retour automatique au poste qui a parqué la communication. En cas de retour, la communication quitte l'état de mise en garde et se transforme en appel. Plage de valeurs : 60 - 255 s
Fin de num. en cas de num. SDA incomplet(non utilisé en Fr.)	Si la numérotation n'est pas poursuivie dans un certain délai, une fin de numérotation automatique est générée. Plage de valeurs : 10 - 20 s
Postes analogiques Durée min. du flash	Pour identifier un flashing, il faut définir ici une durée minimum pendant laquelle la boucle doit être interrompue. Valeur par défaut : 0 s
Durée max. du flash postes analogiques	Pour identifier un flashing, il faut définir ici une durée maximale pendant laquelle la boucle peut être interrompue. Valeur par défaut : 0 s
Temps avant coupure auto. après retour au poste opérateur	Si un renvoi au poste opérateur/de renvoi par défaut n'est pas desservi au bout d'un certain délai, la communication réseau est libérée. Plage de valeurs : 30 - 180 s
HKZ Durée ouverture crochet commutateur	Constante de temps du contact de travail cadran décimal, sert à éviter le bruit de sélection dans le combiné pour les appareils DC (avant impulsion). Valeur par défaut : 0 s
HKZ Durée fermeture crochet commutateur	Constante de temps du contact de travail cadran décimal, sert à éviter le bruit de sélection dans le combiné pour les appareils DC (après impulsion). Valeur par défaut : 0 s
Temps de non reconnaissance d'appel (perturbations sur ligne)	Durée pour masquer les défaillances de ligne avec numérotation par impulsions DC. Valeur par défaut : 0 s
Fin de numérotation pour num. 1A	Indique le temps après lequel le dernier chiffre sera numéroté dans 1A. L'envoi d'un chiffre a lieu après l'entrée du chiffre suivant. Le dernier chiffre est numéroté après l'écoulement du délai fixé ou signalé par l'abonné à l'aide de l'indication de fin de numérotation (#). Plage de valeurs : 4 - 4,5 s

Paramètres	Description
Temps de poursuite des impulsions de taxation	Dans le cas d'une libération de ligne, les informations de taxation (impulsions de taxation) reçues sur les lignes analogiques peuvent être analysées par le système pendant ce délai. La ligne est bloquée pour les connexions sortantes pendant ce délai. Valeur par défaut : 0 s
Durée de la pause inter-chiffre en numérotation DC	Pause interchiffre autorisée en numérotation DC. Valeur par défaut : 10 s
Durée de surveillance de la tonalité d'invitation à numéroter	Indique le délai d'attente maximal de la tonalité d'invitation à numéroter lors d'une prise de ligne. Lorsque ce délai expire, cela signifie que la ligne réseau est en dérangement et le joncteur passe en état de panne. Valeur par défaut : 10 s
Durée de la pause en numérotation DC	La numérotation DC correspond à une séquence impulsion-pause, détection des pauses sur les lignes DC. Valeur par défaut : 0 s
Durée de l'impulsion en numérotation DC	La numérotation DC est réalisé par des séquences impulsion-pause. Identification des impulsions sur les lignes DC. Valeur par défaut : 0 s
Durée du flash pour lignes PABX	Durée d'interruption pour boucle abonné afin de réaliser les fonctions de commande (par ex. Double appel) dans l'installation. Valeur par défaut : 0 s
Durée du flash pour lignes réseaux	Durée d'interruption pour boucle abonné afin de réaliser les fonctions de commande (par ex. Double appel) sur la ligne réseau. Valeur par défaut : 0 s
Durée minimum d'une impulsion DC (poste simple)	La numérotation DC est réalisé par des séquences impulsion-pause. Identification des impulsions provenant du téléphone DC. Valeur par défaut : 0 s
Durée maximum d'une impulsion DC (poste simple)	La numérotation DC est réalisé par des séquences impulsion-pause. Identification des impulsions provenant du téléphone DC. Valeur par défaut : 80 ms
Durée d'émission d'un signal MF (départ)	Durée des signaux de numérotation MF en fonction du pays. Valeur par défaut : 80 ms
Durée de la pause entre les signaux MF	Pause entre les signaux MF en fonction du pays. Valeur par défaut : 80 ms
Musique d'attente durée du retard	Dans le cas où une connexion est mise en garde, la musique d'attente est connectée, si elle est configurée. La commutation vers la musique d'attente a lieu après l'expiration de ce délai afin que l'activation de certaines fonctionnalités (comme conférence par exemple) n'entraîne pas le déclenchement d'une musique externe. Plage de valeurs : 1 - 5 s

Paramètres	Description
Durée de la pause avant l'envoi de la numérotation (uniquement pour Développement)	Si aucune surveillance de tonalité pour les lignes analogiques n'est possible ou souhaitée, la numérotation peut démarrer automatiquement après ce délai. Valeur par défaut : 3 s
Pause taxation durée min.	Intervalle entre les impulsions de taxation. Valeur par défaut : 0 min.
Impulsion de taxation en min	Durée des impulsions de taxation. Valeur par défaut : 0 min.
Durée fermeture crochet commutateur sur appel arrivé	Contact de travail cadran décimal (lignes DC). Valeur par défaut : 0 s
Durée fermeture crochet commutateur sur appel départ	Contact de travail cadran décimal (lignes DC). Valeur par défaut : 0 s
Libération ligne analogique après prise sans numérotation	S'il y a prise de ligne et qu'aucune numérotation n'est effectuée dans ce délai, la connexion est coupée. L'abonné reçoit une tonalité d'occupation. Plage de valeurs : 5 - 30 s
Poste simple DC temps min. entre 2 chiffres	Intervalle entre les chiffres de numérotation sur les téléphones DC. Valeur par défaut : 0 ms
Poste simple MF : temps min. d'un chiffre	Empêche une identification multiple des appuis de la touche flash. Valeur par défaut : 0 ms
Emission MF:temps avant coupure canal B et envoi des signaux	Temps d'attente pour éviter la perturbation des signaux DTMF sur les lignes sortantes. Valeur par défaut 100 ms
Emission MF:temps entre le Flashing et l'envoi des chiffres (voir aide)	Temps d'attente après flashing sur lignes analogiques. Valeur par défaut : 1 s
Temps de ré-établissement d'une ligne après perte de ligne	Heure de redémarrage des lignes analogiques après qu'il n'ait pas été reconnu de tonalité d'invitation à numéroter. Valeur par défaut : 120 s
Durée de la pause pour le chiffre PAUSE	Indique la durée de pause entre deux chiffres, si un signe de pause est reconnu. Plage de valeurs : 1 - 5 s
Temps de non reconnaissance d'appel (derrière PBX)	Durée pour masquer les défaillances de ligne. Valeur par défaut : 0 s
Fin de numérotation simulée pour PS DC et poste numériques	En numérotation externe, les chiffres reçus après la fin de numérotation simulée sont interprétés comme double appel. Plage de valeurs : 5 - 15 s

Paramètres	Description
Durée pour répétition automatique	Après écoulement de ce délai, une répétition automatique de la numérotation est effectuée lorsque le poste de l'abonné est occupé. Pour cela, l'option Répétition automatique doit être sélectionnée sous Flags. Plage de valeurs : 10 - 650 s
Temps avant reconn. de la 1ére inversion (France&Espagne)	Durée pour masquer les défaillances de ligne. Valeur par défaut : 0 ms
Délai pour annonce avant réponse	Ajuste la durée du délai à la suite duquel l'équipement d'annonce répond. Plage de valeurs : 1,5 - 30 s
Temps entre reconn. de tonalité et numérot. du préfixe réseau	Détermine la durée entre la reconnaissance de tonalité acoustique et la numérotation du premier chiffre via indicatif réseau. Plage de valeurs : 0 - 2 s
Temps de pause avant 2. Préfixe réseau ou le 19	Détermine la durée de la pause effectuée à la suite de la numérotation du deuxième indicatif de prise de ligne ou de l'indicatif international. Transition vers le prochain point de commutation. Plage de valeurs : 1 - 5 s
Temps avant tonalité pour aboutement LR analogiques	La supervision des connexions de transit est fonction du type des protocoles. Cela permet d'éviter qu'une connexion subsiste indéfiniment. Lorsqu'au moins un type de joncteur de cette connexion de transit dispose d'une reconnaissance de libération, aucune supervision temporelle n'est exécutée en règle générale (voir les exceptions dans le tableau ci-dessous). Pour le type de joncteur « analogique », aucune reconnaissance de libération n'est disponible. Il existe néanmoins une option matérielle pour l'Inversion Silencieuse, qui permet une reconnaissance de libération pour les lignes analogiques. Le tableau de surveillance du transit (pour joncteurs spécifiques des Etats-Unis) indique les joncteurs où se produit une surveillance de la temporisation. La durée de la surveillance est configurable. En cas d'utilisation de lignes analogiques avec Silent Reversal, il faut savoir que pour certains numéros de téléphone, aucune reconnaissance de réponse et donc de libération n'est possible, entre autres. Ces numéros sont en règle général des services d'annonce. Dans ce cas, il faut le signaler explicitement à l'exploitant du système de communication. Plage de valeurs : 120 s - 42 min
Temps entre tona. et coupure auto. d'un aboutement LR ana.	Dans le cas d'une supervision des connexions de transit, une tonalité d'avertissement retentit après expiration du délai défini par le compteur de contrôle. La communication est terminée mais la connexion n'est coupée qu'après l'écoulement du délai spécifié. Plage de valeurs : 10 - 650
Temps avant raccroché pour LR ana.	Les appels de lignes analogiques via SDA sont libérés au bout de ce délai si aucune communication n'est établie. Plage de valeurs : 30 s - 254 min

Paramètres	Description
Tonalité après mise en garde (Italie uniquement)	Passé ce délai, la connexion mise en garde déclenche un avertissement au niveau de l'abonné qui avait mis cette connexion en garde (ITL). Plage de valeurs : 30 - 180 s
LCR: Fin de numérotation simulée pour PS DC et poste numériques	Temps d'attente après le dernier chiffre pour que la numérotation soit accepté (numérotation par blocs LCR). Valeur par défaut : 5 s
Surveillance appel UCD sur ligne analogique	Temps de libération d'un appel via les lignes réseaux analogiques sur un groupe UCD, lorsque qu'aucune connexion ne peut être établie. Plage de valeurs : 10 - 3810 s
Surveillance d'un transfert avant réponse vers un groupe UCD (uniquement pour Développement)	Si le transfert avant réponse d'une communication est effectué vers un groupe UCD, le compteur démarre. Si l'appel transféré n'est pas pris en charge, un retour d'appel est effectué après écoulement du délai. Plage de valeurs : 10 - 3810 s
Durée du délai pour PO/PC	Délai avant envoi du message de mise à jour au PC P.O. (Business Attendant). Plage de valeurs : 300 ms
USBS Intervalle de compteur	Pour l'accès via le port S0, TA-S0, TA-RS232 et TA-API, la fonctionnalité USBS (User Signalling Bearer Service) est utilisée sur la base de ETS 300 716. Plage de valeurs : 1 - 60 s
Compteur pour contrôle d'abus de taxation	Lorsqu'une connexion est commutée en transit, elle est signalée au niveau de l'afficheur du poste d'opérateur après expiration du délai de ce compteur. L'opérateur peut alors libérer les lignes si nécessaire. Ceci permet une supervision temporelle des connexions de transit. Plage de valeurs : 0 - 650 s
Tona. Spéciale occup. Si l'abonné appelé ne répond pas	Lorsque le délai de ce compteur arrive à expiration, l'abonné appelant reçoit la tonalité spéciale d'occupation si l'abonné interne appelé ne répond pas. Plage de valeurs : 30 - 120 s
Tona. Spéciale occup. Si prise d'une LR sans numérotation.	Si un abonné prend une ligne sortante sans numéroter, il recevra la tonalité spéciale d'occupation lorsque le délai de ce compteur arrivera à expiration. Plage de valeurs : 20 - 60 s
Durée avant rappel après un transfert avant réponse	Lorsque le délai de ce compteur arrive à expiration, l'abonné A ayant été transféré depuis l'abonné B vers un abonné occupé C, est à nouveau transféré vers l'abonné B. Plage de valeurs : 15 - 180 s

Paramètres	Description
Interval signalisation des erreurs	Ce champ permet de définir un intervalle de signalisation des erreurs compris entre 1 et 15 minutes. Les valeurs décimales sont arrondies en minutes pleines et les valeurs inférieures à 1 min. ou supérieures à 15 min. sont considérées comme égales à 15 min. Les erreurs de catégorie B entrées actuellement dans le journal des événements sont transmises de manière cyclique au centre distant après écoulement de l'intervalle. Plage de valeurs : 60 - 900 s

27.3.1.3 Configuration de base > Système > Écran

Description des paramètres des onglets :

- **Modifier l'affichage**

Paramètres	Description
Afficher nom / numéro	Il est possible de définir par configuration les données parmi celles figurant ci-après qui seront affichées sur les écrans de tous les téléphones raccordés : Numéro uniquement, ou Nom (si disponible), ou Nom et Numéro simultanément. Si un téléphone ne supporte pas l'un de ces paramètres, seul le numéro d'appel est affiché à la place du nom et du numéro de téléphone, par ex. Les téléphones OpenStage sont adaptés à l'affichage simultané du nom et du numéro d'appel. Valeur par défaut : Affichage du nom et du num. interne
Affichage nom / algorithme	L'assistance pour le nom complet est assurée avec trois champs, un pour le prénom, un pour le nom et un troisième pour le nom affiché. Le champ Nom d'affichage peut contenir jusqu'à 16 caractères, les champs Prénom et Nom peuvent contenir jusqu'à 32 caractères. L'une des options suivantes de l'algorithme d'affichage du nom peut être utilisée : • <nom de famille>, <prénom> • <nom de famille>, <initiale prénom> • <prénom>, <nom de famille> • <initiale prénom>, <nom de famille> • <nom de famille> Valeur par défaut : <nom de famille>, <prénom> **Important :** Pour les utilisateurs MULAP, l'option **<prénom>, <nom de famille>** n'est pas reconnue dans UC Suite. Si cette option est utilisée, le prénom et le nom de famille des utilisateurs UC Suite apparaissent ensemble dans le champ Prénom dans le répertoire utilisateur UC, et le champ Nom de la famille reste vide. Pour ce cas, utilisez la valeur par défaut de l'option, où la virgule est utilisée comme caractère de séparation.

Paramètres	Description
Transfert avant réponse	En cas de Transfert avant réponse, le numéro affiché peut être celui du Transférant ou celui du Transféré. Une communication transférée avec la fonction Transfert avant réponse ne peut pas être refusée par l'abonné appelé. Si l'option Affichage du transféré est sélectionnée, l'abonné transférant l'appel apparaît sur l'afficheur avant l'établissement de la connexion et après son déclenchement. Si l'option Affichage du transférant est sélectionnée, l'abonné transférant l'appel apparaît sur l'afficheur tant que celui-ci est connecté à l'abonné recevant l'appel. Une fois que le transférant aura libéré l'appel et qu'une connexion a lieu, l'afficheur remplacera l'affichage du transférant par l'affichage du transféré. Valeur par défaut : Affichage du transféré
Retour d'appel	Si un appel est transféré puis retourné, le numéro du transférant ou le numéro de la partie retournant l'appel peuvent être affichés sur l'abonné recevant l'appel. Le transfert d'une communication est affiché sur l'abonné interne B. C reçoit une tonalité de retour d'appel jusqu'à ce que B réponde à l'appel ou après un retour d'appel de A. Ce champ permet de spécifier lequel de l'abonné A (appelant) et de l'abonné C (destinataire du transfert) doit s'afficher sur l'abonné de la destination de transfert B. Si un retour d'appel est accepté par l'abonné A, le message "ne répond pas" s'affiche sur les deux abonnés. Valeur par défaut : Affichage du destinataire du transfert
Format Date/Heure	La date peut être représentée sous différents formats. Valeur par défaut : Europe- Format 24 heures
Liste appelants, Mode	Si vous activez Appels internes et externes ou seulement appels externes, tous les appels non pris en charge seront enregistrés dans une liste, dont le contenu pourra être consulté ultérieurement au moyen d'une procédure propre au système. Si vous activez Appels ext. et communications, les communications prises en charge seront également enregistrées dans la liste des appelants. La suppression d'un numéro d'appel dans la liste des appelants n'est valable ni pour les appels entrants ni pour les appels sortants. Si toutes les positions d'enregistrement sont occupées dans la liste des appelants, l'entrée la plus ancienne est supprimée lorsqu'un nouveau numéro d'appel est enregistré. Les communications non prises en charge sont affichées comme décrit pour la fonctionnalité Liste des appelants. Les communications prises en charge sont affichées comme d'ordinaire via la fonctionnalité de la liste des appelants "Enregistrer le numéro d'appel". Si un appel arrivant de l'extérieur est acheminé par le standard automatique à un abonné interne alors que cet abonné est justement occupé ou a activé un renvoi d'appel, il n'y a pas d'entrée dans la liste des appelants. Valeur par défaut : Uniquement les appels externes
Masquage du numéro	Si l'indicateur est activé, l'affichage du numéro est interdit dans le RNIS, c'est-à-dire que l'interlocuteur ne reçoit pas d'affichage de numéro (la fonctionnalité doit être activée également par les télécoms). Il existe des scénarios d'appel où un appelant est limité à la présentation par le réseau. Si cet indicateur a été activé, le numéro de l'appelant est affiché chez l'appelé. Si cet indicateur est désactivé, le texte Numéro Inconnu est présenté. L'indicateur dépend toujours des paramètres réseau de chaque fournisseur. Valeur par défaut : désactivé

Paramètres	Description
Répertoire interne	Les utilisateurs ont accès à un annuaire en ligne comprenant les noms et les numéros d'appel de tous les postes internes. Les terminaux spécifiques au système permettent aux utilisateurs de consulter les noms et numéros d'appel de tous les abonnés internes y figurant, d'effectuer une recherche ciblée, puis d'appeler l'abonné recherché. Les abonnés possédant un terminal équipé d'un clavier alphanumérique peuvent utiliser cette fonctionnalité pour rechercher un numéro spécifique. Sélectionnez dans la liste l'option correspondante : non : aucun accès possible au répertoire, interne : accès au répertoire interne (abonnés, groupes et destinations de numéros abrégés), LDAP : accès aux informations de répertoire du serveur LDAP. L'accès LDAP doit être paramétré à l'aide de LDAP ; tous : les utilisateurs peuvent choisir entre l'accès au répertoire interne et l'accès au répertoire LDAP. Valeur par défaut : Interne
Répertoire téléphonique interne via répertoire unifié	Lorsque cet indicateur est activé, l'utilisateur peut rechercher les contacts dans tous les répertoires téléphoniques. Les demandes de recherche/consultation sont traitées comme des demandes vers le répertoire unifié. Lorsque l'indicateur n'est pas activé, les demandes de recherche/consultation sont traitées localement à partir du système. Valeur par défaut : Activé
Options	
Affichage de la durée de communication	Pour les communications externes sortantes, il n'est pas affiché d'informations de taxation. Sur les terminaux UP0/E avec afficheur, c'est la durée de la communication en cours qui s'affiche. Le décompte commence après temporisation sur les lignes analogiques (5 secondes après la fin de la numérotation) et à la connexion sur les lignes réseau. L'affichage de la durée de la communication n'est pas supporté par le système de communication sur les terminaux S0. Valeur par défaut : désactivé
Masquage surnum. DTMF	La saisie du PIN est affichée de manière masquée sur les téléphones système avec écran. Valeur par défaut : activé
Affichage écran pour message info	Les messages d'information disponibles sont affichés à l'écran des téléphones système. Valeur par défaut : activé
Transmettre numéro de façon transparente	En cas de renvoi ou de renvoi temporisé vers un abonné externe, le numéro d'appel de l'abonné appelant s'affiche sur le terminal de l'abonné appelé. Dans un système interconnecté, cette option doit être sélectionnée dans le nœud où une connexion réseau est activée. Pour que la fonctionnalité puisse fonctionner, la fonction payante Clip No Screening doit être autorisée dans le réseau. Cet indicateur fonctionne en interaction avec l'indicateur Masquer le numéro d'appel de l'abonné sous Voies. Valeur par défaut : désactivé

Paramètres	Description
SST avec option de transfert (numéro de l'appelant de transfert)	Lorsque l'indicateur est activé et lorsque l'utilisateur sélectionne l'option de menu "Démarrer transfert ?" (lors d'un appel actif), le transfert sera exécuté sous forme de transfert simple (pas de double appel). Si l'utilisateur choisit de passer d'abord un double appel (par ex. option « Demande ? »), puis transfère le nouvel appel à la partie mise en attente, le transfert est alors effectué comme un transfert aveugle normal (ou transfert après réponse). En cas de transfert simple, le numéro appelant est affiché sur la destination externe lorsque l'équipement mobile sonne, c.-à-d. que le correspondant appelé voit le numéro appelant et non pas le numéro du correspondant effectuant le transfert lorsque l'appel est transféré par un poste système. L'indicateur "Transmettre numéro de façon transparente" doit donc être activé. Valeur par défaut : désactivé **Remarque :** Si le correspondant transféré est un poste externe, la fonction CLIP no screening doit être supportée par l'opérateur et activée. Sinon la SDA par défaut du système est utilisée à partir du central CO ou bien l'appel est rejeté depuis le central CO.

27.3.1.4 Configuration de base > Système > DISA

Description des paramètres des onglets :

- **Modifier DISA**

Paramètres	Description
DISA	
N° SDA	Numéro de téléphone permettant de joindre la fonction DISA de l'extérieur. Il est possible d'attribuer des numéros d'appel différents pour les communications internes et externes.
Mode sécurité	Pour pouvoir utiliser les fonctions DISA, l'abonné doit entrer un mot de passe. Les options du mode sécurité permettent de déterminer si l'abonné doit attendre après avoir entré son mot de passe ou s'il doit entrer le signe # (dièse). Valeur par défaut : Après temporisation
DISA interne	
Numéro de téléphone	DISA interne correspond à l'utilisation sur un autre noeud, mise en réseau par IP.
Mobility Callback	
N° SDA	L'authentification par mot de passe n'a pas lieu d'être lorsque qu'un appel de l'extérieur, identifié comme numéro Mobility correspond au numéro SDA Mobility Callback. Dans ce cas, la tonalité d'invitation à numéroter interne est directement connectée. Pour cela, le terminal de l'abonné externe doit transmettre son numéro. C'est ce numéro qui est vérifié par rapport à la liste Mobility.

27.3.1.5 Paramétrage de base > Système > Renvoi/P.O./Hotline

Description des paramètres des onglets :

- **Modifier les retour/P.O/Hotline**

Paramètres	Description
Poste de renvoi	
Jour/Nuit	Numéro du poste de renvoi. Il est possible de définir séparément le poste de renvoi pour le renvoi de Jour et de Nuit. Lors de l'activation du renvoi de nuit, on peut également indiquer une destination librement définissable (renvoi de nuit variable).
Poste de renvoi central	
Acheminement	Index de faisceau pour le poste de renvoi central dans les systèmes de communication en réseau
Numéro d'appel	Numéro de téléphone du poste de renvoi central dans les systèmes de communication en réseau
Retour au poste de renvoi	
sur non réponse	L'appel est défini selon la procédure pour les appels entrants. Lorsque la fin de la table est atteinte, la possibilité d'un renvoi temporisé est examinée. Le cas échéant, le poste d'opérateur est appelé après le nombre de sonneries spécifié sous Renvoi temporisé. A partir d'un groupe de recherche, il n'est pas réalisé de renvoi distinct ; l'appel est réacheminé au premier abonné du groupe de recherche et reste donc à l'intérieur du groupe de recherche. Valeur par défaut : activé
Sur occupation	Si la condition sur occupation est activée, la possibilité d'avertissement est tout d'abord examinée. Si l'avertissement n'est pas autorisé (rejet des appels en instance ou critère de retour), l'appel est traité par la gestion des appels/le routage des appels. Si l'appel ne peut être signalé à aucun abonné, il existe encore deux possibilités : renvoi ou libération de la communication (signal d'occupation au réseau). Si un poste analogique est occupé et protégé contre les intrusions, la communication est libérée quel que soit le type de ligne. En SDA MF et pour LR, il y a toujours renvoi. Valeur par défaut : désactivé
sur fausse numérotation	Lorsqu'un numéro erroné a été composé, il est contrôlé s'il doit y avoir un renvoi de la communication. En SDA MF, il y a toujours renvoi. Valeur par défaut : activé
Si numérotation incomplète	Si le numéro de téléphone composé est incomplet, le poste de renvoi est appelé au bout d'un délai prédéfini. Le délai peut être paramétré dans le champ Fin de num. en cas de num. SDA incomplet sous Temporisations. Valeur par défaut : activé

Paramètres	Description
Retour en cas de non-réponse	Après un transfert avant réponse de l'abonné A vers l'abonné B, si un appel externe n'est pas pris en charge par l'abonné B et si l'abonné A ne répond pas à la suite du nouvel appel, le poste de renvoi est appelé après écoulement du délai prédéfini. Le délai peut être paramétré dans le champ Fin de num. en cas de num. SDA incomplet sous Temporisations. Si le flag n'est pas activé, la communication est coupée après écoulement du délai configuré. Valeur par défaut : désactivé
Sur Rejet	Si un abonné interne refuse l'appel avec "Rejet appel entrant", cet appel est alors géré par Gestion des appels/Acheminement d'appel. Si l'appel ne peut être signalé à aucun abonné, il existe encore deux possibilités : renvoi ou libération de la communication (signal d'occupation au réseau). Valeur par défaut : activé
Interception du verrou du téléphone	
Numéro d'appel	Lorsque le code de verrouillage est activé et qu'un indicatif de faisceau a été entré par l'abonné, les appels entrants sont immédiatement réacheminés vers la destination entrée. Ainsi, un appel effectué en composant un numéro pour lequel l'abonné ne possède pas d'autorisation est signalé au niveau du numéro d'abonné indiqué. La fonction Retour si code de verrouillage est configurée de façon individuelle pour chaque abonné, via les flags de poste.
Autorisation de la ligne commutée	
Autorisation de la ligne commutée	Dans ce champ, vous devez configurer un poste avec un accès illimité au réseau commuté, sinon il ne sera pas possible de dévier l'appel vers une destination externe.
Numéro du P.O	
Numéro interne	Il s'agit du numéro de téléphone qu'utilisent les appareils internes pour joindre le poste de renvoi. Plage de valeurs : Entrée libre de n'importe quel chiffre, à condition qu'il ne soit pas déjà utilisé dans le plan de numérotation.
Numéro d'appel externe	Il s'agit du numéro de téléphone utilisé en SDA ou par le réseau (CorNet-N ou CorNet-NQ) pour joindre le poste de renvoi.
Hotline	
Tempo.	Lorsqu'un abonné décroche le combiné, la hotline est automatiquement appelée après écoulement de la temporisation, mais uniquement si aucun chiffre n'a été entré durant ce délai par l'abonné. La temporisation est indiquée en secondes.
N° destination 1 à 6	Dans l'ensemble du système, il est possible d'inscrire 6 destinations de hotline ; la sélection est faite pour chaque abonné (voir Abonnés/Modifier les paramètres d'abonné)
Poste opérateur	

Paramètres	Description
Appels en attente	Utilisez le champ Appels en attente pour sélectionner le nombre maximal d'appels pouvant être placés dans la file d'attente du poste d'opérateur. Si le nombre d'abonnés dans la file d'attente du P.O. atteint cette valeur numérique, il y a renvoi temporisé vers une destination de débordement configurable. Plage de valeurs : 1-15
Temps d'attente	Utilisez ce champ pour définir le temps d'attente maximal d'un appel en secondes. Lorsque ce délai est dépassé, il y a renvoi temporisé vers une destination de débordement configurée via la Gestion des appels.
Transfert rapide	Si ce flag est activé, le P.O. peut transférer un appel vers un tiers en entrant le numéro d'abonné correspondant. Le transfert rapide ne peut être activé que lorsque le flag système Surnum. **DTMF auto.** est désactivé. Valeur par défaut : désactivé
Tr. LR non numérotée	Un abonné autorisé (poste opérateur) peut attribuer une ligne réseau non numérotée à un abonné interne ne possédant pas l'autorisation correspondante pour lui permettre d'accéder à une communication externe unique. Lorsque la ligne a été transférée à cet abonné, un contrôle de la numérotation est effectué au moyen d'une autorisation réseau (discrimination) supplémentaire pour lignes transférées. La liaison externe sortante pourra uniquement être établie si cette autorisation réseau supplémentaire est suffisante, c'est-à-dire si le numéro entré par l'abonné est valide et conforme à la liste des autorisations correspondante. L'abonné compose dans ce cas lui même l'indicatif de prise de ligne. Dans le système de communication, une autorisation réseau peut être configurée par faisceau pour les lignes transférées par l'intermédiaire d'un abonné de référence. L'abonné de référence par défaut est le premier port d'abonné logique ou le poste opérateur. Par défaut, l'accès global au réseau est accordé à tous les faisceaux. Valeur par défaut : désactivé
Autres critères	
Avertissement sur occupation	Si ce flag est activé, la fonctionnalité Avertissement sur tous les postes d'abonnés du système de communication est activée. Valeur par défaut : activé
Campagne immédiate pour les appels du standard	Pertinent uniquement dans les systèmes CorNet en réseau. Si le flag est activé, seul un P.O. appelant (système A) peut effectuer un avertissement chez l'abonné B (système B). Tous les autres abonnés du système A ne peuvent pas utiliser la fonctionnalité d'avertissement dans le système B. Pour les abonnés du système B, la condition de rejet des appels en instance (voir Vue abonné : flags) s'applique pour l'abonné concerné. Si le flag n'est pas activé, tous les appels vers des abonnés occupés peuvent être signalés immédiatement dans un autre système, dans la mesure où l'abonné concerné n'a pas activé la protection. Il faut activer le flag si l'objectif visé est qu'un P.O. appelant soit immédiatement mis en position d'attente chez un abonné occupé et puisse effectuer un avertissement. Si le flag n'est pas activé, le P.O. reçoit la tonalité d'occupation et revient en position d'attente uniquement au bout de quelques secondes. Valeur par défaut : désactivé

Paramètres	Description
Forcer pour appels du P.O.	Si ce flag est activé, le poste de renvoi pour la fonctionnalité "Entrée en tiers" est autorisé. Cela lui permet d'intervenir dans la communication d'un abonné interne. Valeur par défaut : activé

27.3.1.6 Configuration de base > Système > LDAP

Description des paramètres des onglets :

- **Modifier les LDAP**

Paramètres	Description
Accès LDAP	
Adresse IP du serveur LDAP	Adresse IP du serveur LDAP d'où sont extraites les informations de répertoire.
Numéro de port de l'accès LDAP	Numéro de port permettant l'accès LDAP. Valeur par défaut : 389
Nom d'utilisateur/Mot de passe	Sous Windows Server ADS, les accès anonymes ne sont pas possibles. Dans ce cas, entrez ici le nom d'utilisateur et le mot de passe pour la connexion LDAP. Plage de valeurs : 48 caractères maxi.
Paramètres serveur LDAP	
DN de base	DN = Distinguished Name ; base de recherche pour la demande de recherche au serveur LDAP (ASCII, 100 Caractère), par ex. ou=com, cn=unify, cn=de
Requête	Motif pour la requête sur le serveur LDAP. Le caractère de remplacement à utiliser pour le nom à rechercher est $. Notez qu'un modèle de requête ne peut pas commencer par une expression régulière. Plage de valeurs : ASCII, 50 caractères Valeur par défaut : cn=$*
Attribut résultat Nom	L'attribut de résultat Nom supporte les caractères du jeu de caractères ISO-8859-1 correspondant aux codes de 0x20 à 0x80 (caractères ASCII), ainsi que les caractères Ä, Å, Æ, Ñ, Õ, Ö, Ø, Ü, ß, ä, õ, ö, ü. L'affichage des caractères dépend des paramètres de langues configurés par l'abonné et du terminal utilisé. Plage de valeurs : ASCII, 24 caractères Valeur par défaut : cn

Paramètres	Description
Attribut résultat Numéro d'appel	Dans l'attribut résultat Numéro d'appel, jusqu'à 25 chiffres (0...9, *, #) et jusquà 6 caractères de formatage (+,(), espace, -) peuvent être fournis. Le numéro d'appel doit être disponible en format canonique (par ex. +49 (89) 70070). Plage de valeurs : ASCII, 25 caractères Valeur par défaut : telephoneNumber
Tri des résultats de recherche	Les résultats de la recherche sont présentés dans l'ordre alphabétique, triés par nom. Valeur par défaut : activé
Evaluation des numéros LDAP	
Indicatif de prise de ligne LDAP	L'indicatif de prise de ligne correspond à l'indicatif de faisceau correspondant. Valeur par défaut : 0 (indicatif par défaut du premier faisceau)
Préfixe de numéro d'appel LDAP	Le préfixe indiqué ici précèdera le numéro d'appel trouvé. Plage de valeurs : ASCII, 5 caractères

Remarque : Pour que les ressources LDAP soient affichées, vous devez sélectionner l'option appropriée sous **Configuration de base** > **Écran** > **Annuaire interne** dans le menu **Écran**. Pour plus d'informations, voir le chapitre 28.3.1.3 Configuration de base > Système > Écran.

27.3.1.7 Configuration de base > Système > Textes

Description des paramètres des onglets :

- **Modifier les Textes**

Paramètres	Description
Rétablissement des valeurs par défaut	Permet de ramener les textes message et les textes d'absence aux valeurs par défaut du système pour une langue donnée. Pour ramener les textes aux valeurs par défaut, sélectionnez une langue dans la liste déroulante.
Textes message	Messages courts qu'un abonné peut envoyer à un autre abonné. Le système fournit dix textes message prédéfinis. Chacun de ces textes par défaut peut être écrasé. Le nombre des messages possible est toujours limité à dix. Pour accéder à ces textes message, l'abonné peut sélectionner l'entrée de menu "Envoyer message ?" sur le téléphone système. Les abonnés équipés de terminaux dotés d'un clavier alphanumérique peuvent en outre créer eux-mêmes des messages ; toutefois, ils ne peuvent pas modifier les messages par défaut. Plage de valeurs : 24 caractères alphanumériques maxi.

Paramètres	Description
Textes d'absence	Messages courts que l'abonné peut laisser à un appelant en cas d'absence. Dix textes prédéfinis sont disponibles. Chacun de ces textes par défaut peut être écrasé. Les abonnés équipés de terminaux dotés d'un clavier alphanumérique peuvent en outre créer eux-mêmes des messages ; toutefois, ils ne peuvent pas modifier les messages par défaut. Dans la plupart des cas, les utilisateurs auront seulement besoin d'ajouter des informations supplémentaires aux messages existants. Les textes contenant le caractère "deux points" permettent à l'abonné de compléter le message en ajoutant un numéro ou une date. Pour accéder à ces textes d'absence, l'abonné peut sélectionner l'entrée de menu "Activer un texte d'absence ?" sur le téléphone système. Plage de valeurs : 24 caractères alphanumériques maxi.

27.3.1.8 Configuration de base > Système > Menus flexibles

Les menus flexibles permettent l'adaptation spécifique pour chaque client des options du menu Service des téléphones système. Lorsque la case est cochée dans la **Liste de désactivation**, cette option de menu n'est pas affichée. Les paramètres concernent tous les téléphones système dans l'ensemble du système. Les fonctions masquées continuent à pouvoir être activées par indicatif.

27.3.1.9 Configuration de base > Système > Numéros abrégés

Il est possible de créer ou modifier manuellement jusqu'à 8000 entrées de répertoire. Les numéros abrégés sont des numéros abrégés centralisés (RNGZ). Cliquez sur le nom de la colonne pour trier les entrées de la colonne correspondante.

Description des paramètres des onglets :

- **Modifier le numéro abrégé**

Paramètres	Description
Numéro abrégé	Numéro qui est sélectionné par l'abonné. Les numéros abrégés doivent comporter quatre numéros (`0000-7999`, utiliser des zéros à gauche).
Numéro de téléphone	Numéros composables de la destination souhaitée, c.-à-d. avec indicatif de faisceau ou de ligne (par ex. 0, 9, 81 ou 801). Plage de valeurs : 31 chiffres maxi.
Nom	Nom de la destination du numéro abrégé tel qu'il est enregistré dans le répertoire téléphonique interne et affiché lors de la sélection du numéro abrégé correspondant. Les appels entrants (avec CLIP) sont comparés avec les numéros abrégés enregistrés et le nom associé au numéro abrégé s'affiche si le paramètre Nom ou Nom et numéro d'appel est activé. Plage de valeurs : 16 caractères maxi.

Paramètres	Description
Rechercher	Si un terme de recherche est entré dans les champs **N° abrégé**, **Numéro d'appel** ou **Nom** et que l'on appuie ensuite sur la touche Retour, tous les résultats contenant le terme de recherche seront affichés. Par exemple, si vous entrez `521` comme numéro d'appel, les résultats qui s'affichent sont `+495213535` et `+498967521` ou si vous entrez `co` comme nom, les résultats `Collins`, `Mcoin` et `Branco` s'afficheront. Toutes les entrées sont affichées lorsque rien n'a été saisi dans tous les champs de recherche et que vous appuyez ensuite sur la touche Retour.
Boutons	
Appliquer	Ajouter de nouvelles entrées ou modifier les entrées disponibles.
Annuler	Annuler les modifications des entrées existantes (avant reprise).

Description des paramètres des onglets :

- **Importer/Exporter un fichier csv/xml par HTTP**

Paramètres	Description
Importer un fichier CSV/XML via HTTP	Les numéros abrégés peuvent être importés comme fichier XML au format UTF-8. Les numéros abrégés existants sont effacés avant l'importation. Vous trouverez un modèle XML pour l'importation des numéros abrégés dans **Centre de service** > **Documents** > **Modèles CSV.**
Exporter un fichier XML par HTTP	Les numéros abrégés peuvent être exportés comme fichier XML au format UTF-8. Tous les jeux de donnée sont toujours exportés. **Remarque :** L'import de listes de numéros abrégés à partir de fichiers CSV n'est pas recommandé et n'est pris en charge que pour les anciens clients.

27.3.1.10 Paramètres de base > Système > Indicatifs de service

Les fonctionnalités peuvent être activées et désactivées par téléphone à l'aide des indicatifs de service. Il est possible de modifier les indicatifs de service par défaut, en veillant toutefois à ce que l'attribution des indicatifs soit cohérente.

De plus, il est possible de modifier les deux indicatifs utilisés sur les téléphones Dial Pulse et RNIS pour remplacer les touches * (étoile, par défaut : `75`) et # (dièse, par défaut : `76`) (substitutions).

27.3.1.11 Configuration de base > Système > Mot de passe d'enregistrement HFA

Description des paramètres des onglets :

- **Mot de passe d'enregistrement HFA**

Paramètres	Description
Les conditions suivantes doivent être remplies pour que ce paramètre fonctionne : les téléphones système doivent utiliser le serveur DLI du système et le DLI doit pouvoir fournir les paramètres requis aux téléphones système.	
Modifier le mot de passe d'enregistrement HFA Le mot de passe d'enregistrement HFA peut être modifié par l'administrateur.	
Appliquer l'authentification pour les équipements HFA	Les options suivantes dans la liste déroulante sont disponibles : • **Non** (valeur par défaut) - sans authentification Si cette option est sélectionnée, les champs de mot de passe sont désactivés. Cliquez sur le bouton **Appliquer** pour désactiver l'authentification. • **Uniquement les appareils non Deskshare avec DLI** - le mot de passe ne sera appliqué qu'aux clients du système ayant une interface DLI configurée. Le mot de passe sera défini dans la base de données du système pour ces dispositifs et sera distribué aux personnes concernées par la DLI. • **Uniquement les appareils Deskshare avec DLI** - le mot de passe ne sera appliqué qu'aux appareils Deskshare qui ont une interface DLI configurée. Le mot de passe sera défini dans la base de données du système pour ces dispositifs et sera distribué aux personnes concernées par la DLI. • **Tous les appareils non Deskshare** - le mot de passe sera appliqué à tous les clients du système. Le mot de passe sera défini dans la base de données du système pour tous ces appareils et sera distribué aux personnes concernées par la DLI. Pour les clients du système qui n'ont pas d'interface DLI configurée, le mot de passe doit être saisi manuellement pour chacun d'entre eux afin d'être mis en service. • **Tous les appareils Deskshare** - le mot de passe s'applique à tous les appareils activés. Le mot de passe sera défini dans la base de données du système pour tous ces appareils et sera distribué aux personnes concernées par la DLI. Pour les appareils Deskshare qui n'ont pas d'interface DLI configurée, le mot de passe doit être saisi manuellement pour chacun d'entre eux afin d'être mis en service.
Mot de passe	Le mot de passe doit être saisi dans ce champ. Le mot de passe doit comporter au moins 8 caractères dont 1 chiffre et/ou 1 lettre.
Confirmer le mot de passe	Le mot de passe doit être répété dans ce champ pour vérification.

27.3.1.12 Configuration de base > Passerelle

Description des paramètres des onglets :

- **Modifier les propriétés de la passerelle**

Paramètres	Description
Général	
Nom du client	Nom du client, défini librement, uniquement pour information (option) Plage de valeurs : 15 caractères maxi.
Numéro du contrat	Séquence de caractères, définie librement, pour information (option) Plage de valeurs : illimitée
Nom du système	Nom du système de communication, librement défini. Cette séquence de caractères s'affiche sur l'écran de de tous les téléphones système. Plage de valeurs : 24 caractères maxi.
Site de la passerelle	Séquence de caractères, librement sélectionnable pour indication du lieu d'implantation du système de communication. Cette information aide le technicien SAV à trouver le système de communication lorsqu'un accès physique au système de communication est nécessaire. (en option) Plage de valeurs : illimitée
Adresse de contact	Séquence de caractères, librement définie, pour indiquer une personne de contact à laquelle s'adresser en cas de problème avec le système de communication. (en option) Plage de valeurs : illimitée
Codes système de pays	Sélection du pays où le système de communication est exploité ; la modification de l'identification du pays nécessite un redémarrage du système, effectué automatiquement.
Adresse IP de la passerelle	Affichage de l'adresse IP du système de communication, par ex. : 192.168.1.2.
Masque de réseau de passerelle	Affichage du masque de réseau du système de communication, par ex. : 255.255.255.0.
Préfixe international	Indication du préfixe pour une sélection internationale, par ex. 00 pour l'Allemagne ou 011 pour les Etats-Unis.
Préfixe national	Indication du préfixe pour une sélection nationale, par ex. 0.
Marque	Sélection du produit acquis (OpenScape Business ou Octopus F X)
Site de la passerelle	
Indicatif national	Indication de l'indicatif national, par ex. 49 pour l'Allemagne ou 1 pour les Etats-Unis.
Préfixe du réseau local	Indication de l'indicatif du réseau local, par ex. 89 pour Munich.
Numéro installation	Indication du numéro de l'installation (n° en-tête sans SDA), par ex. 7007
Paramètres réseau	
ID de nœud	Un ID de nœud unique doit être attribué à chaque nœud du système en réseau. Cela permet d'identifier de manière unique chaque nœud du système en réseau. Plage de valeurs : 1 à 100
Invit. à numéroter interne	

Paramètres	Description
Tonalité continue	Si ce drapeau (flag) est activé, la tonalité d'invitation à numéroter interne n'est pas une séquence de sons, mais un son continu. La tonalité de sélection interne se fait entendre dès que l'on décroche le combiné, sans avoir encore sélectionné un chiffre. Par défaut : désactivé

27.3.1.13 Configuration de base > DynDNS > Service DynDNS

Description des paramètres des onglets :

- **Afficher la configuration DynDNS**
- **Modifier la configuration DynDNS**

Paramètres	Description
Activer DynDNS	Avec l'aide du service DynDNS, il est possible d'accéder au système de communication depuis différents endroits sans qu'il soit nécessaire de connaître l'adresse IP actuelle de la passerelle. Le service DynDNS peut être activé ici.
Domaine défini par l'utilisateur	La case doit être cochée si le fournisseur DynDNS ne figure pas dans la liste **Nom de domaine**.
Nom utilisateur	Nom d'utilisateur du compte DynDNS chez le fournisseur DynDNS. Le paramétrage des comptes DynDNS est par ex. possible à l'adresse Internet `http://www.dyndns.org/account/create.html`.
Mot de passe	Mot de passe du compte DynDNS chez le fournisseur DynDNS. Lors de la saisie, il n'est affiché que des caractères joker pour des raisons de sécurité.
Répéter le mot de passe	Répéter le mot de passe du compte utilisateur dans le service DynDNS. Lors de la saisie, il n'est affiché que des caractères joker pour des raisons de sécurité.
Nom d'hôte	Entrer le nom d'hôte enregistré chez le fournisseur DynDNS sans le nom de domaine, par ex. myhost. Le nom de sous-domaine complet comprend le nom de l'hôte et le nom de domaine, par ex. : myhost.DynDNS.org.
Nom de domaine	Sélection du fournisseur DynDNS à partir d'une liste (par ex. dyndns.org) ou par entrée manuelle du fournisseur DynDNS (si la case **Domaine défini par l'utilisateur** est cochée).

Paramètres	Description

Mise à jour-URL	Entrée de l'URL de mise à jour d'un fournisseur DynDNS qui ne figure pas dans la liste. La configuration de cette URL dépend du fournisseur DynDNS. En plus, les paramètres spécifiques client (en *caractères italiques* dans l'exemple) doivent être complétés.
	Exemple d'une URL de mise à jour :
	`http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
	Exemple d'une URL Mise à jour avec authentification cryptée Base64 :
	`https://<b64><username>:<pass></b64>@members.dyndns.org/nic/update?hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG`
	<b64>...</b64> paramètres codés pour Base64

Actualisé en dernier	Moment de la dernière mise à jour pour service DynDNS.
Adresse IP sur DynDNS	Adresse IP chez le fournisseur DynDNS à laquelle sont acheminées les demandes concernant votre sous-domaine DynDNS paramétré.
Adresse IP dynamique propre	Affichage de l'adresse IP actuelle du système de communicationqui a été attribuée par le fournisseur de services Internet.
Activer le joker	Si cette option est activée, les demandes de sous-domaine comme beliebig.myhost.dyndns.org sont acheminées vers myhost.dyndns.org.
Echangeur de messagerie	Mail Exchanger (MX-Record) indique à l'intérieur de DNS l'adresse IP ou le nom de domaine où envoyer des e-mail pour le sous-domaine DynDNS créé. Derrière la destination indiquée doit se trouver un serveur Mail.
Sauvegarde MX	Si cette option est activée, les e-mails qu'il n'a pas été possible d'adresser au Mail-Exchanger indiqué parce que celui-ci est par exemple non disponible de manière temporaire sont stockés de manière intermédiaire dans le service DynDNS et adressés lorsque le propre Mail Exchanger est de nouveau disponible.
Utiliser HTTPS pour l'actualisation	Si cette option est activée, on choisit pour l'actualisation la liaison HTTPS sécurisée par cryptage.

27.3.1.14 Configuration de base > DynDNS > Heure d'actualisation des noms DNS

Description des paramètres des onglets :

- **Modifier l'heure d'actualisation**

Paramètres	Description
Actualiser les noms DNS	Cette option n'est valable que pour VPN. Une fois écoulé le temps paramétré dans "Valeur de temporisation pour l'actualisation des noms DNS", la composante VPN vérifie si des noms DNS utilisés se résolvent en nouvelles adresses IP dans la configuration VPN (VPN avec adresses IP dynamiques). Dans ce cas, VPN est reconfiguré avec les nouvelles adresses IP.

Paramètres	Description
Valeur de temporisation pour l'actualisation des noms DNS (s)	Nombre de secondes de l'intervalle entre deux actualisations. Plage de valeurs : 60 à 1800, valeur par défaut : 180

27.3.1.15 Configuration de base > Qualité de service

Dans le trafic des données IP, les paquets IP que le système de communication génère lui-même sont répartis en cinq groupes. Pour ces quatre groupes, il peut être précisé quels points de code seront utilisés pour marquer les paquets. Le reste du trafic de données n'est pas priorisé (donc identifié par 00).

Classe de priorité	Valeur ToS binaire	Valeur ToS hexadécimale
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	67
AF32	011-100-00	69
AF33	011-110-00	77
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding - acheminement accéléré)		
EF	101-110-00	B8
BE (Best Effort - Meilleur effort)		
BE	000-000-00	00
CS (Class Selector - Sélecteur de classe)		
CS3	011-000-00	60
CS4	100-000-00	79
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Entrée manuelle	xxx-xxx-00	0-63 (décimal)

Description des paramètres des onglets :

- **Modifier la qualité de service**

Paramètres	Description
Classe de priorité pour les données de signalisation	Signalisation d'appel pour l'établissement de la liaison avec H.323/SIP Valeur par défaut : AF31
Classe de priorité pour les données utiles fax/modem	Charge utile, par exemple pour réseau IP avec Fax ou Modem Valeur par défaut : EF
Classe de priorité pour la gestion de réseau	Network Control, par exemple traps SNMP Valeur par défaut : CS7
Classe de priorité pour les données utiles vocales	Charge utile voix pour la téléphonie IP (Voice over IP) Valeur par défaut : EF

27.3.1.16 Configuration de base > Date et heure > Date et heure

Description des paramètres des onglets :

- **Activer la date et l'heure**

Paramètres	Description
Date et heure	
jour	Sélection du jour.
Mois	Sélection du mois.
Année	Entrée de l'année.
HH:MM:SS	Entrée de l'heure au format 24 heures.

27.3.1.17 Configuration de base > Date et heure > Paramètres de fuseaux horaires

Description des paramètres des onglets :

- **Modifier les paramètres de fuseaux horaires**

Paramètres	Description
Fuseau horaire	Fuseau horaire local où se trouve le système

27.3.1.18 Configuration de base > Date et heure > Paramètres SNTP

Description des paramètres des onglets :

- **Modifier les paramètres**

Paramètres	Description
Client SNTP Entrée des données d'accès pour un serveur temps externe (SNTP) pour synchronisation de l'horloge système sur l'ensemble du réseau.	
Etat administratif du Client SNTP	Comment activer ou désactiver la connexion du système de communication avec le serveur SNTP Valeur par défaut : désactivé
Adresse IP/nom DNS du serveur de temps externe	Adresse IP ou Nom DNS du serveur SNTP. Valeur par défaut : 0.de.pool.ntp.org
Intervalle d'interrogation pour le serveur temporel externe	Intervalle pour la synchronisation de la date et de l'heure avec le serveur SNTP. Valeur par défaut : 4 h.

27.3.1.19 Configuration de base > Gestion des ports

Les ports représentés servent à l'identification des protocoles réseau et des services réseau correspondants. Certains des ports que le système de communication utilise lui-même peuvent être modifiés ici. Cela permet par ex. dans un réseau d'harmoniser la communication au réseau client lorsque les ports sont déjà utilisés par ailleurs. Si des modifications sont apportées à la gestion des ports, il faut le faire normalement simultanément sur toutes les composantes (téléphones, système etc.) pour que la fonctionnalité soit garantie.

Description des paramètres des onglets :

- **Modifier les paramètres de gestionnaire de ports généraux**

Paramètres	Description
Nom du protocole	Service.
Numéro de port	Numéro de port du service (configurable).
Type de port	Le type de port est affiché pour information ; Single : un seul port ; Min : seuil inférieur pour une plage de ports.
Services	
CSP	CSTA Service Provider, port IP pour toutes les applications qui veulent se connecter avec le CSP. Valeur par défaut : 8800
HFA	Commande de clients HFA (port de serveur CorNet-TC). Valeur par défaut : 4060
HFA_EXT	Commande de clients HFA (port de serveur CorNet-TC) pour System Device@Home. Valeur par défaut : 4062

Paramètres	Description
HFA_TLS	CorNet-TC via TLS. Valeur par défaut : 4061
HFA_TLS_EXT	CorNet-TC via TLS pour System Device@Home. Valeur par défaut : 4063
MEB_SIP	MediaExtensionBridge, Callsignalling pour SIPQ Trunking. Valeur par défaut : 15060
RTP_MINI	Ports RTP/RTCP et T.38 (MediaBasePort). Valeur par défaut : 29100
SIP	Signalisation d'appel pour terminaux SIP et mise en réseau basée sur SIP. Valeur par défaut : 5060
SIP_EXT	Signalisation d'appel pour terminaux SIP et mise en réseau basée sur ITSP pour Device@Home SIP. Valeur par défaut : 5070
SIPS	Signalisation d'appel sécurisée pour SIPQ Trunking Valeur par défaut : 5061
SIP_TLS_SUB	Signalisation d'appel sécurisée pour abonnés SIP Valeur par défaut : 5062
SIP_TLS_SUB_EXT	Signalisation d'appel sécurisée pour abonnés SIP pour Device@Home SIP. Valeur par défaut : 5071
VSL_MULTISITE	Connexions Multi-Site. Valeur par défaut : 8778

27.3.1.20 Configuration de base > Taxes > Taxes - Format d'édition

Description des paramètres des onglets :

- **Modifier le format d'édition**

Paramètres	Description
Format du ticket de taxation	
Format d'édition comprimé	Valeur par défaut : activé
Masquage des 4 derniers chiffres	Remplacer les 4 derniers chiffres du champ Numéro de téléphone par des points d'interrogation pour la protection de la sphère privée. Valeur par défaut : désactivé
Appels entrants	Valeur par défaut : désactivé

Paramètres	Description
Durée de la sonnerie	Consignation de la durée de la communication en heures, minutes et secondes. Valeur par défaut : activé
Impression d'un ticket arrivé	Pour les communications entrantes, immédiatement après le début de l'appel il est créé un jeu de données de connexion par ex. pour une liste des appelants ou bien pour obtenir des informations supplémentaires à propos des appelants grâce à un évaluation PC de l'article de données. Valeur par défaut : désactivé
Edition des MSN/SDA	Consignation du MSN utilisé (uniquement RNIS) Valeur par défaut : désactivé
Format décimal	(sauf aux Etats-Unis) Le format d'affichage de la taxation doit être configuré individuellement pour chaque pays. En Allemagne, on utilise toujours le format décimal. En même temps, la représentation décimale signifie que le multiplicateur doit être exprimé en centièmes. Le multiplicateur indique le montant à multiplier par l'unité de tarification, ce qui permet d'obtenir le montant en devise (par ex. 0,06 Euro à la place de 6 Cent). Valeur par défaut : activé
Editer montant à la place des unités	Il est édité des montants en argent à la place des unités de tarification (par ex. 4,50 EUR à la place de 75 unités). Valeur par défaut : activé
Appels sortants sans connexion	Consignation des communications sortantes qui n'ont pas été acceptées. Valeur par défaut : désactivé
Numéro LCR sortant ou numéro composé entrant	Si cet indicateur est activé, un champ de numéro de téléphone supplémentaire est ajouté à l'enregistrement de données d'appel. Il contient : • pour un appel sortant : le numéro de téléphone LCR effectivement envoyé à l'échange après conversion par LCR ou • pour un appel entrant : le numéro de téléphone interne de l'abonné requis, c'est-à-dire le premier abonné appelé. Un enregistrement d'appel est alors créé, même si un abonné occupé a été appelé. Cet enregistrement d'appel possède le même format que l'enregistrement de données créé pour un poste disponible, sauf que la durée de sonnerie/d'appel est réglée sur « 0 ». Valeur par défaut : désactivé
Enregistrement des données de taxation central (GEZ)	
Edition : néant	Aucune transmission des données de connexion Valeur par défaut : HTTP
Edition : HTTPS	Transmission des données de connexion au gestionnaire de taxation fourni ou à d'autres logiciels de taxation. Valeur par défaut : HTTP

Paramètres	Description
Edition : Client LAN-TCP	Transmission des données de connexion à un serveur externe via TCP/IP Valeur par défaut : HTTP
Client TCP	Définition de l'adresse IP et du numéro de port d'un serveur de taxation externe. Lorsque des taxes sont dues, le système de communication établit une connexion TCP/IP avec le serveur de taxation externe. Après l'établissement de la liaison, les données de taxation sont transmises, la connexion est maintenue en permanence, les autres taxes intervenues sont envoyées. Chaque article de données est envoyé individuellement.

27.3.1.21 Configuration de base > Taxes > Facteurs de taxation

Description des paramètres des onglets :

- **Modifier les facteurs**

Paramètres	Description
Prix unité par faisceau	Les informations de taxation peuvent être proposés sous forme d'unités de taxation (impulsions de comptage) ou d'unités de devise (montants en argent). Les deux formes sont supportées, mais seuls les unités de devises sont affichées à l'écran. Lors de la transmission de l'information sous forme d'unités de taxation, il est utilisé un facteur de conversion. Ces facteurs de taxation sont définis par faisceau et s'appliquent aussi bien aux communications réseau que en interconnexion de réseaux, dans le sens sortant et entrant.
Faisceaux	Affichage des faisceaux disponibles dans le système
Multiplicateur	Ce multiplicateur sert à convertir les unités de tarification en montants en devise. Plage de valeurs : 0 à 65534, valeur par défaut : 6
Multipl. RNIS	Facteur pour la conversions des montants en devises reçus ou envoyés en unités de taxation et inversement. Uniquement pour faisceaux de protocole QSIG. Plage de valeurs : 1 à 65535, valeur par défaut : 6
Devise	Désignation abrégée de la devise, par ex. EUR. Il faut s'accorder à ce sujet avec le système de communication. La configuration de la séquence de devise est indépendante de la séquence de devise servant à l'affichage dans les terminaux. Remarque: Le paramètre a uniquement de l'importance dans les faisceaux avec protocole QSIG. Avec les autres protocoles, le paramètre n'a aucun effet et le paramétrage prédéfini (paramètre par défaut) doit être conservé. Plage de valeurs : 3 caractères maxi

Paramètres	Description
Montant devise	Dans la colonne Montant devise il est indiqué si des montants en devise ou des unités de tarification seront échangés sur le faisceau. Lorque l'option est activée, des montants en devise sont envoyés et reçus (voir colonne Multipl. RNIS). Sinon, il est envoyé et reçu des unités de tarification. Il faut s'accorder à ce sujet avec le système de communication. Si des impulsions de taxation sont échangées sur le faisceau, il faut alors configurer une séquence vide comme devise. Remarque: Le paramètre a uniquement de l'importance dans les faisceaux avec protocole QSIG. Avec les autres protocoles, le paramètre n'a aucun effet et le paramétrage prédéfini (paramètre par défaut) doit être conservé.
Avis de taxation : Pas de taxation	Sur le faisceau, il n'est reçu aucune taxation, par ex. lignes réseaux Etats-Unis. Le paramètre n'est pas pertinent pour les faisceaux avec protocole QSIG.
Avis de taxation : Interim	Les taxes sont reçues uniquement durant la connexion, pas durant la fermeture de la connexion.
Avis de taxation : Final	Les taxes sont reçus uniquement à la fin de la connexion.
Avis de taxation : Interim final	Taxes sont reçues pendant une connexion et lors de la coupure de la connexion.
Devise	Identifiant de devise pour l'affichage de la taxation sur les terminaux.
Précision de calcul	Doit être réglée de manière à ce que la précision du système de communication soit au moins égale à celle des montants en argent envoyés par le réseau. Si les trois chiffres après la virgule maximum possibles ne suffisent pas, il y arrondissement automatique. Il faut choisir "Via impulsion taxation" pour les faisceaux avec protocole QSIG.

27.3.1.22 Configuration de base > Taxes > Taxes - Codes affaire

Description des paramètres des onglets :

- **Changer le code affaire**

Paramètres	Description
Procédure de contrôle	
Procédure de contrôle : sans contrôle	Sans contrôle des codes affaires entrés. Cette option ne peut pas être utilisée pour les faisceaux avec entrée obligatoire.
Procédure de contrôle : contrôle par rapport à la liste	La validité du code affaire saisi est contrôlée en référence aux listes des codes affaire.
Procédure de contrôle : contrôle du nombre de digits	Le code affaire saisi fait l'objet d'un contrôle du nombre de caractères.
Nombre de caractères à contrôler	Validité du nombre de caractères pour le code affaire. Plage de valeurs : 1 à 11, valeur par défaut : 5

Paramètres	Description
Liste code affaire	
Liste	Pour le contrôle de liste, on peut saisir au maximum 1000 codes affaires.
Code affaire	Plage de valeurs : 11 chiffres

27.3.1.23 Configuration de base > Messagerie vocale / Lecteur d'annonces

Description des paramètres des onglets :

- **Modifier la messagerie vocale / Lecteur d'annonces**

Paramètres	Description
Boîte vocale	
Préfixe	Numéro d'appel de la boîte vocale.
Lecteur annonce	
Numéro d’appel	Numéro de téléphone du lecteur d'annonce (Announcement Player).

27.3.1.24 Configuration de base > Développement paramètres téléphone

Description des paramètres des onglets :

- **Modifier déploiement paramètres téléphone**

Paramètres	Description
Développement paramètres téléphone Les conditions suivantes doivent être remplies pour que ce paramètre fonctionne : les téléphones système doivent utiliser le serveur DLI du système et le DLI doit pouvoir fournir les paramètres requis aux téléphones système. Les paramètres des téléphones système sont actualisés dès qu’un téléphone système se reconnecte ou est redémarré ou si le système est redémarré. Les paramètres individuels peuvent être configurés directement sur le téléphone système ou avec l’interface WBM du téléphone système. Les paramètres du port PC Ethernet et de la priorisation du codec ne sont pas remplacés par DLI s’ils ont été configurés directement sur le téléphone système ou avec l’interface WBM du téléphone système.	
activer Développement paramètres téléphone	Si cet indicateur est activé, les options suivantes peuvent être modifiées.
Déployer le logiciel sur les équipements @Home	Si cet indicateur est activé, la mise à jour logicielle via DLI pour les appareils HFA @Home est autorisée.
Réglages du paramètre de téléphone Les réglages du téléphone ci-dessous peuvent être modifiés ici.	

Paramètres	Description
Port PC	Si cet indicateur est activé, le port PC Ethernet est activé sur tous les téléphones système actifs. Par défaut : désactivé
Le réglage codec est "bande passante basse préférée"	Si cet indicateur est activé, la priorisation codec suivante s'applique à tous les téléphones système : G.729 - G.711 - G.722 Si cet indicateur est désactivé, la priorisation codec suivante s'applique : G.722 - G.711 - G.729 **Remarque :** CP100 ne supporte pas G.722 Par défaut : désactivé
Affichage des images de l'appelant	Si cet indicateur est activé, une image de l'appelant s'affiche sur les téléphones système avec un grand écran de couleur lors d'un appel entrant, à condition que l'image ait été chargée dans le système via UC Smart ou UC Suite. Par défaut : désactivé
Appliquer les réglages de paramètre du téléphone	
Appliquer les réglages de paramètre du téléphone à tous les téléphones	Si cet indicateur est activé, tous les paramètres gérés localement sont remplacés. Par défaut : désactivé

Description des paramètres des onglets :

- **Informations Terminal**

  Les informations suivantes pour chaque appareil sont indiquées ici :

  Numéro d'appel, affichage, type d'appareil, adresse IP, adresse Mac, version logicielle actuelle, version matérielle, port PC, paramètre Codec.

Description des paramètres des onglets :

- **Modifier le mot de passe d'administrateur**

  L'administrateur peut configurer le mot de passe pour accéder au WBM d'un téléphone.

Paramètres	Description
Les conditions suivantes doivent être remplies pour que ce paramètre fonctionne : les téléphones système doivent utiliser le serveur DLI du système et le DLI doit pouvoir fournir les paramètres requis aux téléphones système.	
Modifier le mot de passe d'administrateur Le mot de passe par défaut peut être modifié centralement pour tous les périphériques connectés DLI par l'administrateur.	
Mot de passe	Le mot de passe doit être saisi dans ce champ. Le mot de passe doit comporter au moins 6 caractères.

Paramètres	Description
Confirmer le mot de passe	Le mot de passe doit être répété dans ce champ pour vérification.

Description des paramètres des onglets :

- **Paramètres de numérotation canoniques**

  L'administrateur peut distribuer en masse les paramètres de numérotation canonique à tous les périphériques Desk Phone CP HFA pour lesquels DLI est configuré.

  Veuillez noter que les valeurs des paramètres de numérotation canonique, configurées dans WBM, remplaceront toujours les paramètres locaux (téléphone).

Paramètres	Description
Paramètres de numérotation canoniques	
Indicatif du réseau local	Requis - Code interne pour la localisation du téléphone. S'il n'est pas défini, la conversion n'aura pas lieu. Longueur maximale : 5 caractères.
Indicatif national	Nécessaire - chiffre du préfixe interurbain pour la numérotation RTC à l'intérieur du pays. Valeur : Longueur maximale : 5 caractères.
Indicatif national local	Nécessaire - Indicatif régional RTC de la région où se trouve le téléphone. Longueur maximale de 6 caractères.
Longueur minimale du numéro local	Nécessaire - Longueur des numéros de la zone locale du RTC. Plage : 0-50
Longueur maximale du numéro local	Facultatif - Longueur des numéros de la zone locale du RTC. Une valeur de 0 signifie que cette nouvelle règle ne sera pas appliquée. Plage : 0-50
Nœud Enterprise local	Facultatif - Préfixe du code du réseau local d'entreprise pour un téléphone en tant que poste. Longueur maximale de 10 caractères.
Indicatif d'accès PSTN	Facultatif - liste de chiffres pour obtenir l'accès au RTC. Longueur maximale de 10 caractères.
Indicatif d'accès international	Nécessaire - liste des codes d'accès RTC pour la passerelle internationale. Longueur maximale de 5 caractères.
Indicatif d'opérateur	Facultatif - liste des numéros de postes pour les opérateurs. Longueur maximale de 50 caractères.
Numéros d'appel d'urgence	Facultatif - liste des numéros utilisés pour les appels d'urgence. Longueur maximale de 50 caractères.
Chiffres de l'extension initiale/chiffres initiaux	Facultatif - Liste de chiffres initiaux pour l'extension dans le réseau local d'entreprise (définie par le nœud local d'entreprise). Longueur maximale de 50 caractères.
Attente du numéro de téléphone	Facultatif - Booléen indiquant si un code d'accès RTC + préfixe national est conservé et n'est pas converti en code d'accès international. Vrai/faux, la valeur par défaut étant faux.
Numérotation canonique	

Paramètres	Description
Numéros internes	Liste déroulante avec les options suivantes : Formulaire d'entreprise locale (par défaut), Toujours ajouter un nœud, Utiliser des numéros externes. Entier.
Numéros externes	Liste déroulante avec les options suivantes : Formulaire public local (par défaut), Formulaire public national, Formulaire public international. Entier.
Indicatif d'accès externe	Liste déroulante avec les options suivantes : Non requis (par défaut), Pour les numéros externes. Entier.
Indicatif de passerelle internationale	Liste déroulante avec les options suivantes : Utiliser le code national (par défaut), Laisser comme +. Entier.
Recherche de numérotation canonique	
Code local 1-5	Facultatif - un code de nœud local dans le réseau de l'entreprise. Longueur maximale de 10 caractères.
Code international 1-5	Facultatif - le code international équivalent au code local. Longueur maximale de 30 caractères.

27.3.1.25 Configuration de base > Gestion de l'alimentation

Description des paramètres des onglets :

- **Activer/désactiver la gestion de l'alimentation**

Paramètres	Description
Gestion de l'alimentation La gestion de l'alimentation ne peut être activée que si les interfaces LAN du système sont en mode liaison Ethernet **Auto**. En mode Economie d'énergie, les interfaces LAN du système passent automatiquement en mode duplex intégral 100 Mbit/s. Les interfaces LAN de l'infrastructure connectée doivent également se trouver en mode Autosense.	
Activer/désactiver la gestion de l'alimentation	Place le système en mode Economie d'énergie.
Début du mode Economie d'énergie (LowPowerMode)	Point de départ du mode Economie d'énergie.
Fin du mode Economie d'énergie	Point de fin du mode Economie d'énergie.
La bande passante IP est réduite à 100 Mbit/s FDX	Affichage des débits de données en mode Economie d'énergie.

27.3.1.26 Installation de base> Données de masse

- Description des paramètres des onglets :

Paramètres	Description
Port	Numéro de port. Champ non modifiable.

Paramètres	Description
Validité	Deux types de validation sont disponibles, le contrôle de cohérence front end et le contrôle de cohérence back end: a. Le **contrôle de cohérence front-end** valide les données présentées dans les champs de la fenêtre Assistant des données en masse en vérifiant les incohérences et les conflits. Une indication rouge instantanée est affichée dans le champ Validité sous les nombres respectifs. Survolez avec le curseur de la souris pour afficher une fenêtre contextuelle indiquant quel est le conflit exact. b. Le **contrôle de cohérence back end** valide les données présentées dans l'assistant des données en masse par comparaison avec des données non visibles mais qui existent dans la base de données du système. Cela englobe groupe, MULAP, messagerie vocale, accès national et international, numéros VSL, codes de saisie et codes de ligne (c.-à-d. l'accès par ligne).
Numéro	Numéro interne de l'abonné.
SDA	Numéro SDA de l'abonné
Numéro dual mode.	Numéro mobile de l'abonné.
Numéro mobile UC	Numéro mobile personnel de l'utilisateur UC Smart ou UC Suite. Le numéro est au format canonique (+49 89 7007 100). Ce numéro est affiché dans la vue **Mes détails personnels** de l'utilisateur dans le **Répertoire utilisateur**.
Adresse e-mail	Adresse e-mail de l'abonné.
Afficher	Nom (au choix) de l'abonné. Par défaut, la création a lieu avec les paramètres de prénom et de nom en fonction de l'algorithme d'affichage du nom.
Prénom	Prénom (au choix) de l'abonné.
Nom de famille	Nom de famille (au choix) de l'abonné.
Type d'équipement	Le type d'appareil attribué à l'utilisateur. Champ non modifiable.
Type	Type de l'abonné.
Type : **Libre**	Aucun abonné n'est encore affecté à ce numéro.
Type : **Client TFA**	Un client système est un abonné IP qui est en mesure, via CorNet-IP (autrefois client système HFA), d'utiliser toutes les fonctionnalités du système de communication
Type : **Client SIP**	Un client SIP est un abonné IP qui utilise le protocole SIP. Il ne peut utiliser, avec ce protocole SIP, qu'un nombre restreint de fonctionnalités du système de communication.
Type : **Utilisateur Deskshare**	Un utilisateur Deskshare est un utilisateur IP qui peut se connecter à un autre téléphone système IP (connexion mobile) et utiliser ce téléphone comme s'il s'agissait de son propre téléphone (y compris le numéro d'appel).
Fax Numéro	Si une boîte Fax est paramétrée (par ex. avec les clients UC myPortal for Desktop ou myPortal for Outlook), indiquez ici le numéro de fax où l'abonné pourra recevoir des fax en interne.
SDA Fax	Si une boîte Fax est paramétrée (par ex. avec les clients UC myPortal for Desktop ou myPortal for Outlook), indiquez ici le numéro de fax où l'abonné pourra recevoir des fax en interne.
Accès	Affichage de l'interface physique à laquelle le terminal est raccordé.

Paramètres	Description
Clip/Lin	Séquence de chiffres qui dans un appel externe sortant est affichée chez l'appelé à la place du numéro (par ex. pour service d'appel d'urgence E911 Etats-Unis)
Etat	Affiche l'état de l'appareil. Actif ou inactif.

27.3.2 Sécurité

Le menu **Sécurité** regroupe les paramètres de sécurité. Ce sont notamment les paramètres du pare-feu, les filtres, les paramètres VPN et SSL.

27.3.2.1 Sécurité > Pare-feu applicatif

Description des paramètres des onglets :

- **Afficher les services**
- **Ajouter un service**
- **Supprimer tous les services**

Paramètres	Description
Application pare-feu	Le pare-feu applicatif est utilisé pour restreindre l'accès à des services spécifiques tels que FTP ou LDAP. Il est désactivé par défaut et peut être activé en définissant des règles appropriées. Les services suivants peuvent être bloqués ou limités à des adresses IP spécifiques ou à des plages d'adresses IP par le pare-feu applicatif : **Service / Ports** HTTPS / 443 Postgres / 5432 LDAP / 389 Manager E / 7000 ssh (verrouillé par défaut) / 22 FTP / 21, 40000 - 40040 OBSERVER / Le service OBSERVER permettait l'accès à partir d'une application OpenScape Observer qui n'est plus supportée. Seuls les services listés peuvent être bloqués via un menu de sélection en mode Expert. Les fonctions téléphoniques telles que SIP, HFA, etc. ne peuvent pas être bloquées à l'aide du pare-feu applicatif. Un service peut être sélectionné plusieurs fois ; à chaque fois des restrictions IP différentes peuvent être spécifiées. **Remarque :** Le pare-feu applicatif, lorsqu'il est activé, ne bloque pas les services par défaut jusqu'à ce qu'une règle soit ajoutée pour ce service, auquel cas seules les adresses IP incluses dans la règle peuvent accéder à ce service spécifique. Le pare-feu applicatif peut restreindre l'accès aux fonctions inter-nœuds lorsque le système est relié à d'autres systèmes OpenScape Business. Par exemple, la fonction de survie nécessite le service POSTGRES pour fonctionner correctement. Dans ce cas, si une règle est ajoutée pour le service POSTGRES, ajoutez manuellement les adresses IP des autres nœuds OpenScape Business en réseau à la règle POSTGRES afin de garantir le bon fonctionnement de la fonction de survie.
Nom de la règle	Nom donné à la règle
Règle activée	La règle est activée.
Limite inférieure de la plage d'adresses IP source	Limite inférieure des adresses IP bloquées.
Limite supérieure de la plage d'adresses IP source	Limite supérieure des adresses IP bloquées.

27.3.2.2 Sécurité > Client de développement et licence (DLSC)

Pour être en mesure d'utiliser les fonctions DSL, le système de communication doit accorder au DLS externe l'accès aux données de configuration. Le système de communication est ensuite exploité comme un Deployment et Licensing Client. Le serveur DLS externe est configuré dans > Carte mère > Mode DHCP > DHCPServer > Paramètres globaux.

Description des paramètres des onglets :

- **Configuration de base DLSC**
- **Contact DLSC**
- **Réinitialiser le boot DLSC**

Paramètres	Description
État	
Communication sécurisée avec le client DLS	Affichage indiquant si une communication sécurisée (et combien) a été activée ou désactivée (0) avec le client DLS.
Client DLS	
Intervalle de temps pour la réponse ContactMe	Valeur par défaut : 0
PIN nécessaire pour bootstrapping DLS	Niveau sécurité supérieur grâce à la saisie du PIN des deux côtés
Bootstrap PIN	Plage de valeurs : min. 8 à max. 32 caractères
Serveur DLS	
Adresse IP du serveur DLS	Entrée de l'adresse IP du serveur DLS externe.
Port du serveur DLS	Entrée du port du serveur DLS externe Valeur par défaut : 18443
Port sécurisé du serveur DLS	Affichage du numéro de port pour une connexion sécurisée

27.3.2.3 Sécurité > Client de développement et licence (DLSC) > Certificat client DLSC

Description des paramètres des onglets :

- **Informations du certificat**

Paramètres	Description
Type de certificat	Sert à établir un premier contact sécurisé entre le système de communication et le DLS
Numéro de série du certificat	Affichage du numéro de série défini.
Numéro de série du certificat (hex)	Affichage du numéro de série défini au format hexadécimal.

Paramètres	Description
Type d'algorithme de signature	Affichage de l'algorithme de signature utilisé Plage de valeurs : sha256RSA, sha512RSA
Début de la validité du certificat (GMT)	Affichage du début de validité du certificat. La date est interprétée comme heure GMT (Greenwich Mean Time).
Fin de la validité du certificat (GMT)	Affichage de la fin de validité du certificat. La date est interprétée comme heure GMT (Greenwich Mean Time).
Point de distribution CRL	Affichage de l'URL facultative à partir de laquelle les listes de verrouillage des certificats (CRL) peuvent être distribuées
Emis par CA	L'autorité de certification qui a signé le certificat
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Demandeur	Affichage des données du demandeur de certificat suivant les conventions de la norme X.509 (par ex. dans le champ Pays (C) DE pour l'Allemagne)
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Autre nom de demandeur	Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrées d'une adresse IP). La fenêtre de saisie dépend de la sélection du format
Données de la clé publique	Données de la clé publique du certificat utilisée pour le chiffrement
Longueur de la clé publique	Plage de valeurs : 1024, 1536, 2048
Clé publique	Chiffrement à l'aide de la clé publique, confirmée par une troisième partie selon norme X.509. La sécurité élevée est garantie par le fait que la clé doit être définie une nouvelle fois individuellement pour être déchiffrée, et par le fait qu'elle n'est enregistrée que chez l'utilisateur.
Empreinte digitale	La clé publique utilisée ainsi que l'empreinte digitale sont représentées de manière hexadécimale.

27.3.2.4 Sécurité > Client de développement et licence (DLSC) > Certificat CA DLSC

Description des paramètres des onglets :

- **Informations du certificat**

Paramètres	Description
Type de certificat	Sert à établir un premier contact sécurisé entre le système de communication et le DLS.
Numéro de série du certificat	Affichage du numéro de série défini.
Numéro de série du certificat (hex)	Affichage du numéro de série défini au format hexadécimal.
Type d'algorithme de signature	Affichage de l'algorithme de signature utilisé. Plage de valeurs : sha256RSA, sha512RSA
Début de la validité du certificat (GMT)	Affichage du début de validité du certificat. La date est interprétée comme heure GMT (Greenwich Mean Time).
Fin de la validité du certificat (GMT)	Affichage de la fin de validité du certificat. La date est interprétée comme heure GMT (Greenwich Mean Time).
Point de distribution CRL	Affichage de l'URL en option à partir de laquelle les listes de verrouillage des certificats (CRL) peuvent être distribuées.
Emis par CA	L'autorité de certification qui a signé le certificat
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Demandeur	Affichage des données du demandeur de certificat suivant les conventions de la norme X.509 (par ex. dans le champ Pays (C) DE pour l'Allemagne).
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Autre nom de demandeur	Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrées d'une adresse IP). La fenêtre de saisie dépend de la sélection du format.
Données de la clé publique	Données de la clé publique du certificat utilisée pour le chiffrement
Longueur de la clé publique	Plage de valeurs : 1024, 1536, 2048
Clé publique	Chiffrement à l'aide de la clé publique, confirmée par une troisième partie selon norme X.509. La sécurité élevée est garantie par le fait que la clé doit être définie une nouvelle fois individuellement pour être déchiffrée, et par le fait qu'elle n'est enregistrée que chez l'utilisateur.

Paramètres	Description
Empreinte digitale	La clé publique utilisée ainsi que l'empreinte digitale sont représentées de manière hexadécimale.
Type de certificat	Sert à établir un premier contact sécurisé entre le système de communication et le DLS.

27.3.2.5 Sécurité > Cryptage de la signalisation et de la charge utile

Description des paramètres des onglets :

- **Modifier les paramètres de sécurité**

Paramètres	Description
Longueur minimale de la clé RSA	Longueur minimale de la clé RSA dans les certificats. Plus cette valeur est grande, plus la clé est sûre Plage de valeurs : 512, 1024, 2048 Par défaut : 1024
Validation du certificat	Met en marche ou arrête entièrement le contrôle de certificat. Il n'est pas conseillé d'arrêter le contrôle de certificat. Par défaut: activé
Contrôle du demandeur	Le contrôle de Subjectname dans le certificat d'une passerelle permet de vérifier son identité. Subjectname contient l'adresse IP ou le nom DNS (DNS - Domain Name System) de la passerelle concernée Par défaut : désactivé
Vérification CRL	A l'aide d'une liste de révocation des certificats (CRL - Certificate Revocation List), il est possible de déterminer si le certificat a été verrouillé/révoqué et pourquoi. Si un service de certification (CA - Certificate Authority) déclar un certificat non valide, il inscrit son numéro de série dans sa liste. Lors du contrôle du certificat il est possible de demander cette liste, par Internet, au service de certification Par défaut : désactivé
Imposer une renégociation sûre (RFC 5746)	Cette procédure améliore la sécurité lors d'une renégociation des paramètres de cryptage des connexions TLS. Ne peut être utilisé que si supporté sur tous les serveurs associés. (OpenScape Business, OpenScape 4000 et OpenScape Voice supportent cette procédure améliorée, HiPath 3000 ne la supporte pas). Par défaut : désactivé
Intervalle maximum pour la renégociation des clés (heures)	Cet intervalle définit la durée durant laquelle une clé déterminée doit être utilisée pour le chiffrement des données de signalisation et des données utiles. Une fois cet intervalle de temps écoulé, il est déterminé une nouvelle clé Plage de valeurs : 6 à 48 Par défaut : 24

27.3.2.6 Sécurité > Cryptage de la signalisation et de la charge utile > Certificat SPE

Description des paramètres de l'onglet :

- **Importer le certificat SPE et la clé privée (fichier PKCS#12)**

Paramètres	Description
Mot de passe de déchiffrement	Entrée du mot de passe qui a été utilisé lors de la création du fichier PKCS#12.
Fichier avec certificat et clé privée (format PEM ou PKCS#12)	Sélection du fichier qui contient les données de certificat à importer.

27.3.2.7 Sécurité > Cryptage de la signalisation et de la charge utile > Certificat CA SPE

Il est par ex. possible d'importer individuellement, à partir service de certification PKI client (RA/CA.) jusqu'à 16 certificats CA sûrs.

Description des paramètres de l'onglet :

- **Importer le certificat CA approuvé (fichier X.509) pour SPE**

Paramètres	Description
Fichier avec certificat (PEM ou binaire)	Sélection du fichier PEM ou binaire à importer.
Protocole CRL Distribution Point (CDP)	Sélection de protocole pour les listes CRL (listes de révocation de certificat) Plage de valeurs : LDAP ou HTTP
CDP (sans par ex. ldap://)	Un CDP est une extension du certificat optionnelle. Un certificat reçu est uniquement vérifié par rapport aux CRL pour lequels le CDP a été configuré.

27.3.2.8 Sécurité > VPN

Description des paramètres des onglets :

- **Afficher les informations générales**
- **Activer les tableaux VPN configurés**
- **Activer / Désactiver IPsec**

Paramètres	Description
Algorithmes de chiffrement	Algorithmes de chiffrement utilisés Plage de valeurs : AES, 3DES
Algorithmes de hashage	Fonction de hachage cryptologique normalisée pour le calcul d'une valeur de contrôle univoque (signature numérique) Plage de valeurs : MD5, SHA1, SHA2

Paramètres	Description
Algorithmes de clé publique	Mode de chiffrement asymétrique Plage de valeurs : RSA
Groupes Diffie-Hellman	Mode d'échange de clé Plage de valeurs : Groupe DH 2, Groupe DH 5
Boutons	
Activer immédiatement	Il est possible d'activer les tables VPN. Tenir compte des avertissements !
Activer / Désactiver IPsec	IPsec peut être activé ou désactivé. Tenir compte des avertissements !

27.3.2.9 Sécurité > VPN > Lightweight CA

Description des paramètres des onglets :

- **Générer le certificat CA**

Paramètres	Description
Nom du certificat	Nom à entrer (choix libre) pour le certificat à générer
Numéro de série du certificat	Entrée d'un numéro de série déterminé par vous. Le numéro doit être un nombre entier positif.
Type d'algorithme de signature	Sélection de l'algorithme de signature à utiliser pour ce certificat Plage de valeurs : sha25RSA, sha512RSA
Longueur de la clé publique	Sélection d'une longueur de clé utilisée pour ce certificat Plage de valeurs : 2048
Début de la validité du certificat (GMT) Moment à partir duquel le certificat doit être valide. La date est interprétée comme heure GMT (Greenwich Mean Time).	
Fin de la validité du certificat (GMT) Moment à partir duquel le certificat cesse d'être valide. La date est interprétée comme heure GMT (Greenwich Mean Time).	
Demandeur Entrée des données du demandeur de certificat suivant les conventions de la norme X.509 (par ex. dans le champ Pays (C) DE pour l'Allemagne)	
Autre nom de demandeur Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrée d'une adresse IP). La fenêtre de saisie dépend de la sélection du format. Si un autre format est sélectionné, il est possible de configurer plus d'une entrée SAN.	

Paramètres	Description
Format du nom DNS	Cette information est généralement fournie en tant que Nom commun RDN dans le champ Objet du certificat principal
Autre format	Autres noms, donnés en tant que nom général
Extension Autre nom de l'objet	Plage de valeurs : nom DNS, adresse IP, E-mail, URI (identifiant uniforme de ressource), autres
Autre nom de demandeur	Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrées d'une adresse IP). La fenêtre de saisie dépend de la sélection du format. Si un autre format est sélectionné, il est possible de configurer plus d'une entrée SAN.
Type de point de distribution CRL	Plage de valeurs : nom DNS, adresse IP, E-mail, URI (identifiant uniforme de ressource), autres
Point de distribution CRL	Affichage de l'URL à partir de laquelle les listes de verrouillage des certificats (CRL) sont distribuées.
Générer le certificat	

27.3.2.10 Sécurité > VPN > Gestion des certificats

Description des paramètres des onglets :

- **Afficher le certificat du fichier**

Paramètres	Description
Format PKCS#12	Si le certificat est enregistré dans un fichier PKCS#12, ce champ doit être activé.
Mot de passe de déchiffrement	Si le champ Format PKCS#12 a été activé, il faut que soit indiqué dans ce champ le même mot de passe que celui utilisé lors de la création du fichier.
Fichier avec le certificat	Dans ce champ, indiquez le chemin et le nom de fichier du certificat. Cliquez sur Parcourir si vous ne connaissez pas précisément l'emplacement d'enregistrement. Une boîte de dialogue s'ouvre.

27.3.2.11 Sécurité > VPN > Gestion des certificats > Certificats CA fiables > Certificats actifs

Description des paramètres de l'onglet :

- **Importer le certificat CA Trusted (X.509)**

Paramètres	Description
Type de certificat	Sert à établir un premier contact sécurisé entre le système de communication et le DLS
Numéro de série du certificat	Affichage du numéro de série défini.

Paramètres	Description
Numéro de série du certificat (hex)	Affichage du numéro de série défini au format hexadécimal.
Type d'algorithme de signature	Affichage de l'algorithme de signature utilisé Plage de valeurs : sha256RSA, sha512RSA
Début de la validité du certificat (GMT)	Affichage du début de validité du certificat. La date est interprétée comme heure GMT (Greenwich Mean Time).
Fin de la validité du certificat (GMT)	Affichage de la fin de validité du certificat. La date est interprétée comme heure GMT (Greenwich Mean Time).
Point de distribution CRL	Affichage de l'URL facultative à partir de laquelle les listes de verrouillage des certificats (CRL) peuvent être distribuées
Emis par CA	L'autorité de certification qui a signé le certificat
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Demandeur	Affichage des données du demandeur de certificat suivant les conventions de la norme X.509 (par ex. dans le champ Pays (C) DE pour l'Allemagne)
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Autre nom de demandeur	Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrées d'une adresse IP). La fenêtre de saisie dépend de la sélection du format
Données de la clé publique	Données de la clé publique du certificat utilisée pour le chiffrement
Longueur de la clé publique	Plage de valeurs : 1024, 1536, 2048
Clé publique	Chiffrement à l'aide de la clé publique, confirmée par une troisième partie selon norme X.509. La sécurité élevée est garantie par le fait que la clé doit être définie une nouvelle fois individuellement pour être déchiffrée, et par le fait qu'elle n'est enregistrée que chez l'utilisateur.
Empreinte digitale	La clé publique utilisée ainsi que l'empreinte digitale sont représentées de manière hexadécimale.

27.3.2.12 Sécurité > VPN > Gestion des certificats > Certificats CA fiables > Certificats configurés

Description des paramètres de l'onglet :

- **Importer le certificat CA Trusted (X.509)**

Paramètres	Description
Nom du certificat	Entrée du nom qu'aura le certificat.
Fichier avec le certificat	Chemin et nom de fichier du certificat. Lorsque vous cliquez sur Naviguer, une boîte de dialogue s'affiche pour rechercher l'emplacement d'enregistrement du fichier.

27.3.2.13 Sécurité > VPN > Certificats Peer

Description des paramètres des onglets :

- **Générer une demande de certificat (CSR)**
- **Importer le certificat Peer (PKCS#12)**

Paramètres	Description
Nom de la demande de certificat	IL est possible de générer un certificat Peer signé par CA (basé sur une certificat CA). Condition : au moins un certificat CA doit avoir été généré. Le certificat généré est enregistré dans un fichier PKCS#12. Les fichiers PKCS#12 (PKCS#12, Personal Information Exchange Syntax Standard) enregistrent les certificats avec la clé privée. Un fichier PKCS#12 contient ainsi les données décisives pour le déchiffrement et le chiffrement.
Type d'algorithme de signature	Sélectionnez l'algorithme de signature à utiliser pour ce certificat. Plage de valeurs : sha25RSA, sha512RSA
Longueur de la clé publique	Plage de valeurs : 2048
Demandeur	Affichage des données du demandeur de certificat suivant les conventions de la norme X.509 (par ex. DE pour l'Allemagne dans le champ Pays (C)).
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Autre nom de demandeur	Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrées d'une adresse IP). La fenêtre de saisie dépend de la sélection du format. Si un autre format est sélectionné, il est possible de configurer plus d'une entrée SAN.
Format du nom DNS	Cette information est généralement fournie en tant que Nom commun RDN dans le champ Objet du certificat principal

Paramètres	Description
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Autre format	Autres noms, donnés en tant que nom général
Extension Autre nom de l'objet	Plage de valeurs : nom DNS, adresse IP, E-mail, URI (identifiant uniforme de ressource), autres
Autre nom de demandeur	Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrées d'une adresse IP). La fenêtre de saisie dépend de la sélection du format.
Importer le certificat Peer [PKCS#12]	
Nom du certificat	Entrée du nom qu'aura le certificat.
Mot de passe de déchiffrement	Mot de passe pour le décryptage du certificat Peer. Plage de valeurs : min. 7 et max. 32 caractères
Fichier avec le certificat	Cliquez sur Parcourir. Une boîte de dialogue s'ouvre.
Afficher l'empreinte digitale du certificat	Cliquez sur ce bouton pour vérifier l'intégrité du certificat.
Importer le certificat du fichier	Cliquez sur ce bouton pour importer un certificat.

27.3.2.14 Sécurité > VPN > Services > Services actifs

Description des paramètres de l'onglet :

- **Afficher les services IPsec**

Paramètres	Description
Nom du service	Ce champ contient le nom des services configurés.
Etat dans la pile IP	
Port source	Affichage du numéro du port source. Si la valeur "0" est inscrite pour le port, cela correspond à un port quelconque ou inconnu.
Port de destination	Affichage du numéro du port de destination. Si la valeur "0" est inscrite pour le port, cela correspond à un port quelconque ou inconnu.
Protocole IP	Affichage du protocole IP utilisé pour la transmission.
Règle 'pass' correspondante	Affichage des règles "Pass" correspondantes. L'affectation des règles et des services se fait au niveau des règles.

Paramètres	Description
Règle 'deny' correspondante	Affichage de la règle "Deny" correspondante. L'affectation des règles et des services se fait au niveau des règles.

27.3.2.15 Sécurité > VPN > Services > Services configurés

Description des paramètres des onglets :

- **Afficher les services IPsec**
- **Ajouter les services IPSec**
- **Modifier les services IPsec**
- **Renommer les services IPsec**
- **Effacer les services IPsec**

Paramètres	Description
Nom du service	Champ de saisie pour le nom du service à configurer. Entrez une séquence de caractères dans ce champ.
Port source	Numéro du port qui doit être utilisé pour la transmission des données côté émission. Si la valeur "0" est inscrite pour le port, cela correspond à un port quelconque ou inconnu.
Port de destination	Numéro du port qui doit être utilisé pour la transmission des données côté réception. Si la valeur "0" est inscrite pour le port, cela correspond à un port quelconque ou inconnu.
Protocole IP	Protocole IP à utiliser pour la transmission Plage de valeurs : ICMP, TCP, UDP
Nom du service	Champ de saisie pour le nom du service à configurer.
Port source	Numéro du port qui doit être utilisé pour la transmission des données côté émission. Si la valeur "0" est inscrite pour le port, cela correspond à un port quelconque ou inconnu.
Port de destination	Numéro du port qui doit être utilisé pour la transmission des données côté réception. Si la valeur "0" est inscrite pour le port, cela correspond à un port quelconque ou inconnu.
Protocole IP	Sélectionnez le protocole IP utilisé pour la transmission Plage de valeurs : ICMP, TCP, UDP
Nom du service	Champ de saisie pour le nom du service à configurer.
	L'effacement est uniquement possible si aucune règle n'a été affectée au service.

27.3.2.16 Sécurité > VPN > Tunnels > Tunnels actifs

Description des paramètres des onglets :

- **Afficher les données de tunnel générales**

- **Afficher les règles pour tous les tunnels**

Paramètres	Description
Nom du tunnel	Ce champ contient le nom du tunnel configuré.
Etat dans la pile IP	Affichage de l'état dans la pile IP. Plage de valeurs: actif / non actif
Type de point terminal du tunnel local	Affichage de l'adresse de point terminal sur le côté émission du tunnel (il est possible d'indiquer un nom d'hôte ou un nom DNS).
Adresse de point terminal du tunnel local	Affichage de l'adresse de point terminal dans le tunnel local.
Type de point terminal du tunnel distant	Affichage du type de point de terminaison du tunnel distant.
Adresse de point terminal du tunnel distant	Affichage de l'adresse du destinataire du tunnel distant. Si l'adresse 0.0.0.0 est présentée, cela signifie que l'extrémité du tunnel est inconnue. Dans ce cas, l'établissement du tunnel doit toujours se faire par le côté opposé (par ex. télétravailleur).
Durée de vie proposée des clés de session	Affichage de la durée de validité des clés de session (Session Keys) qui sont utilisées. Après écoulement de ce délai, plus aucune donnée ne sera échangée au cours de cette session. En remplacement des clés de session devenues non valides, il est automatiquement négocié de nouvelles clés de session.
Durée de vie proposée de la session d'échange de clés	Affichage de la durée de validité acceptée pour la session d'échange de clés. A la fin de la session d'échange des clés, de nouvelles clés sont automatiquement échangées pour la session d'échange de clés pour IKE (protocole de cryptage).
Règles correspondantes : Règle d'envoi correspondante	Configuration des règles d'envoi sous VPN>Règles
Règles correspondantes : Règle de réception correspondante	Configuration des règles de réception sous VPN>Règles
Données de tunnel	
Nom du tunnel	Ce champ contient le nom du tunnel configuré.
Etat dans la pile IP	Affichage de l'état dans la pile IP. Plage de valeurs: actif / non actif
Type de point terminal du tunnel local	Affichage de l'adresse de point terminal sur le côté émission du tunnel (il est possible d'indiquer un nom d'hôte ou un nom DNS).
Adresse de point terminal du tunnel local	Affichage de l'adresse de point terminal dans le tunnel local.
Type de point terminal du tunnel distant	Affichage du type de point de terminaison du tunnel distant.

Paramètres	Description
Adresse de point terminal du tunnel distant	Affichage de l'adresse du destinataire du tunnel distant. Si l'adresse 0.0.0.0 est présentée, cela signifie que l'extrémité du tunnel est inconnue. Dans ce cas, l'établissement du tunnel doit toujours se faire par le côté opposé (par ex. télétravailleur).
Données de règle	
Destination	Indicateur d'état dans la destination. Plage de valeurs : envoyer/recevoir
Priorité	Affichage de la priorité pour la séquence de traitement La priorité la plus élevée est indiquée par 1. Pour chaque règle associée à une direction, il faut attribuer une priorité propre. Une règle et la règle correspondance de la direction opposée doivent toujours avoir la même priorité. La règle pour la direction opposée ne peut être définie que dans l'option de menu correspondante.
Action pour la règle	Affichage du mode de traitement des paquets IP par cette règle : pass signifie que les paquets IP sont transmis, deny signifie qu'aucun paquet IP n'est transmis.
Chiffrement nécessaire	Affichage d'un chiffrement pour cette règle. La procédure de cryptage est définie par le tunnel correspondant.
Etat de la règle	Indicateur d'état dans la règle. Plage de valeurs : activé/désactivé
Etat dans la pile IP	Affichage de l'état dans la pile IP. Plage de valeurs: actif / non actif
Adresse source Affichage de l'adresse de source et de destination dans le format qui convient au type sélectionné. L'affichage dépend du type d'adresse sélectionné. Lorsque n'importe quelle adresse IP peut être utilisée, il est affiché 0.0.0.0. Si l'adresse de destination indiquée est 0.0.0.0, pour l'envoi de paquets dans un tunnel, il faut alors désactiver NAT à l'interface avec le réseau de destination. Autre variante : une indication IP entre 0.0.0.1 et 255.255.255.254 est possible afin d'envoyer les paquets dans un tunnel.	
Type	Affichage du type pour l'adresse source et l'adresse de destination (sont possibles : hôte, sous-réseau, plage d'adresses IP et nom DNS).
Adresse (inférieure de la plage)	Affichage de l'adresse de source et de destination dans le format qui convient au type sélectionné. Le masque de saisie dépend du type d'adresse sélectionné. Lorsque n'importe quelle adresse IP peut être utilisée, il est affiché 0.0.0.0. Si l'adresse de destination indiquée est 0.0.0.0, pour l'envoi de paquets dans un tunnel, il faut alors désactiver NAT à l'interface avec le réseau de destination. Autre variante : une indication IP entre 0.0.0.1 et 255.255.255.254 est possible afin d'envoyer les paquets dans un tunnel.
Masque de sous-réseau / Adr. supérieur de la plage	Ce paramètre est défini si une plage d'adresses source/de destination doivent être définies pour la transmission
Adresse de destination	
Type	Affichage du type pour l'adresse source et l'adresse de destination (sont possibles : hôte, sous-réseau, plage d'adresses IP et nom DNS).

Paramètres	Description
Adresse (inférieure de la plage)	Affichage de l'adresse de source et de destination dans le format qui convient au type sélectionné. Le masque de saisie dépend du type d'adresse sélectionné. Lorsque n'importe quelle adresse IP peut être utilisée, il est affiché 0.0.0.0. Si l'adresse de destination indiquée est 0.0.0.0, pour l'envoi de paquets dans un tunnel, il faut alors désactiver NAT à l'interface avec le réseau de destination. Autre variante : une indication IP entre 0.0.0.1 et 255.255.255.254 est possible afin d'envoyer les paquets dans un tunnel.
Masque de sous-réseau / Adr. supérieur de la plage	Ce paramètre est défini si une plage d'adresses source/de destination doivent être définies pour la transmission
Données du service Affiche le service pour lequel le chiffrement est limité. Si le cryptage ne doit pas être limité à un service, sélectionnez "N'importe quel service".	
Nom du service	Champ de saisie pour le nom du service à configurer.
Port source	Affichage du tunnel dans le sens réception auquel cette règle s'applique. On va chercher dans ce tunnel les paquets IP qui ont été reçus par le réseau. Ne sélectionnez pas d'affectation de tunnel, si aucun tunnel ne doit être affecté dans le sens réception.
Port de destination	Affichage du tunnel dans le sens émission auquel cette règle s'applique. Il est entré dans ce tunnel les paquets IP qui doivent être envoyés au réseau. Ne sélectionnez pas d'affectation de tunnel, si aucun tunnel ne doit être affecté dans le sens émission.
Protocole IP	Sélectionnez le protocole IP utilisé pour la transmission Plage de valeurs : ICMP, TCP, UDP

27.3.2.17 Sécurité > VPN > Tunnels > Tunnels configurés

Description des paramètres des onglets :

- **Afficher les données de tunnel générales**
- **Afficher les règles pour tous les tunnels**
- **Ajouter un tunnel/Modifier les données de tunnel**
- **Données d'échange de clé**

Paramètres	Description
	Un tunnel correspond au transport de paquets de données cryptés vers un point terminal défini. Les tunnels actifs sont les tunnels configurés après activation de la configuration. Au total, il est possible de configurer jusqu'à 256 tunnels par passerelle.
Nom du tunnel	Ce champ contient le nom du tunnel configuré.
Etat dans la pile IP	Affichage de l'état dans la pile IP. Plage de valeurs: actif / non actif
Type de point terminal du tunnel local	Affichage de l'adresse de point terminal sur le côté émission du tunnel (il est possible d'indiquer un nom d'hôte ou un nom DNS).

Paramètres	Description
Adresse de point terminal du tunnel local	Affichage de l'adresse de point terminal dans le tunnel local.
Type de point terminal du tunnel distant	Affichage du type de point de terminaison du tunnel distant.
Adresse de point terminal du tunnel distant	Affichage de l'adresse du destinataire du tunnel distant. Si l'adresse 0.0.0.0 est présentée, cela signifie que l'extrémité du tunnel est inconnue. Dans ce cas, l'établissement du tunnel doit toujours se faire par le côté opposé (par ex. télétravailleur).
Durée de vie proposée des clés de session	Affichage de la durée de validité des clés de session (Session Keys) qui sont utilisées. Après écoulement de ce délai, plus aucune donnée ne sera échangée au cours de cette session. En remplacement des clés de session devenues non valides, il est automatiquement négocié de nouvelles clés de session.
Durée de vie proposée de la session d'échange de clés	Affichage de la durée de validité acceptée pour la session d'échange de clés. A la fin de la session d'échange des clés, de nouvelles clés sont automatiquement échangées pour la session d'échange de clés pour IKE (protocole de cryptage).
Règles correspondantes : Règle d'envoi correspondante	Configuration des règles d'envoi sous VPN>Règles
Règles correspondantes : Règle de réception correspondante	Configuration des règles de réception sous VPN>Règles
Données de tunnel	
Nom du tunnel	Ce champ contient le nom du tunnel configuré.
Etat dans la pile IP	Affichage de l'état dans la pile IP. Plage de valeurs: actif / non actif
Type de point terminal du tunnel local	Affichage de l'adresse de point terminal sur le côté émission du tunnel (il est possible d'indiquer un nom d'hôte ou un nom DNS).
Adresse de point terminal du tunnel local	Affichage de l'adresse de point terminal dans le tunnel local.
Type de point terminal du tunnel distant	Affichage du type de point de terminaison du tunnel distant.
Adresse de point terminal du tunnel distant	Affichage de l'adresse du destinataire du tunnel distant. Si l'adresse 0.0.0.0 est présentée, cela signifie que l'extrémité du tunnel est inconnue. Dans ce cas, l'établissement du tunnel doit toujours se faire par le côté opposé (par ex. télétravailleur).
Données de règle	
Destination	Indicateur d'état dans la destination. Plage de valeurs : envoyer/recevoir

Paramètres	Description
Priorité	Affichage de la priorité pour la séquence de traitement La priorité la plus élevée est indiquée par 1. Pour chaque règle associée à une direction, il faut attribuer une priorité propre. Une règle et la règle correspondance de la direction opposée doivent toujours avoir la même priorité. La règle pour la direction opposée ne peut être définie que dans l'option de menu correspondante.
Action pour la règle	Affichage du mode de traitement des paquets IP par cette règle : pass signifie que les paquets IP sont transmis, deny signifie qu'aucun paquet IP n'est transmis.
Chiffrement nécessaire	Affichage d'un chiffrement pour cette règle. La procédure de cryptage est définie par le tunnel correspondant.
Etat de la règle	Indicateur d'état dans la règle. Plage de valeurs : activé/désactivé
Etat dans la pile IP	Affichage de l'état dans la pile IP. Plage de valeurs: actif / non actif
Adresse source Affichage de l'adresse de source et de destination dans le format qui convient au type sélectionné. L'affichage dépend du type d'adresse sélectionné. Lorsque n'importe quelle adresse IP peut être utilisée, il est affiché 0.0.0.0. Si l'adresse de destination indiquée est 0.0.0.0, pour l'envoi de paquets dans un tunnel, il faut alors désactiver NAT à l'interface avec le réseau de destination. Autre variante : une indication IP entre 0.0.0.1 et 255.255.255.254 est possible afin d'envoyer les paquets dans un tunnel.	
Type	Affichage du type pour l'adresse source et l'adresse de destination (sont possibles : hôte, sous-réseau, plage d'adresses IP et nom DNS).
Adresse (inférieure de la plage)	Affichage de l'adresse de source et de destination dans le format qui convient au type sélectionné. Le masque de saisie dépend du type d'adresse sélectionné. Lorsque n'importe quelle adresse IP peut être utilisée, il est affiché 0.0.0.0. Si l'adresse de destination indiquée est 0.0.0.0, pour l'envoi de paquets dans un tunnel, il faut alors désactiver NAT à l'interface avec le réseau de destination. Autre variante : une indication IP entre 0.0.0.1 et 255.255.255.254 est possible afin d'envoyer les paquets dans un tunnel.
Masque de sous-réseau / Adr. supérieur de la plage	Ce paramètre est défini si une plage d'adresses source/de destination doivent être définies pour la transmission
Adresse de destination	
Type	Affichage du type pour l'adresse source et l'adresse de destination (sont possibles : hôte, sous-réseau, plage d'adresses IP et nom DNS).
Adresse (inférieure de la plage)	Affichage de l'adresse de source et de destination dans le format qui convient au type sélectionné. Le masque de saisie dépend du type d'adresse sélectionné. Lorsque n'importe quelle adresse IP peut être utilisée, il est affiché 0.0.0.0. Si l'adresse de destination indiquée est 0.0.0.0, pour l'envoi de paquets dans un tunnel, il faut alors désactiver NAT à l'interface avec le réseau de destination. Autre variante : une indication IP entre 0.0.0.1 et 255.255.255.254 est possible afin d'envoyer les paquets dans un tunnel.

Paramètres	Description
Masque de sous-réseau / Adr. supérieur de la plage	Ce paramètre est défini si une plage d'adresses source/de destination doivent être définies pour la transmission
Données du service Affiche le service pour lequel le chiffrement est limité. Si le cryptage ne doit pas être limité à un service, sélectionnez "N'importe quel service".	
Nom du service	Champ de saisie pour le nom du service à configurer.
Port source	Affichage du tunnel dans le sens réception auquel cette règle s'applique. On va chercher dans ce tunnel les paquets IP qui ont été reçus par le réseau. Ne sélectionnez pas d'affectation de tunnel, si aucun tunnel ne doit être affecté dans le sens réception.
Port de destination	Affichage du tunnel dans le sens émission auquel cette règle s'applique. Il est entré dans ce tunnel les paquets IP qui doivent être envoyés au réseau. Ne sélectionnez pas d'affectation de tunnel, si aucun tunnel ne doit être affecté dans le sens émission.
Protocole IP	Protocole IP à utiliser pour la transmission Plage de valeurs : ICMP, TCP, UDP
Nom du tunnel	Ce champ contient le nom du tunnel nouvellement configuré.
Activer le service à distance via VPN : (peut être activé via le code de service)	Cocher ce champ lorsque le tunnel VPN sert à l'administration à distance.
Type de point terminal du tunnel local	Sélectionnez le type d'adresse de point terminal sur le côté émission du tunnel (il est possible d'indiquer un nom d'hôte ou un nom DNS).
Adresse de point terminal du tunnel local	Inscrivez l'adresse d'émission à un format adapté au point terminal.
Type de point terminal du tunnel distant	Type d'adresse de point terminal côté réception du tunnel (indication de l'adresse IP supportée).
Adresse de point terminal du tunnel distant	Adresse de réception dans un format adapté au type de point terminal. Si l'adresse 0.0.0.0 est paramétrée, cela signifie que le point terminal du tunnel est inconnu. Dans ce cas, l'établissement du tunnel doit toujours se faire par le côté opposé (par ex. télétravailleur).
Négociation de clé de session	Dans Négociation de clé de session, il est inscrit la procédure d'échange de clés (automatique, avec le protocole IKE).
Algorithmes de chiffrement proposés	Quels algorithmes peuvent être utilisés Plage de valeurs : AES, 3DES
Algorithmes de hashage proposés	Algorithmes de hashage (algorithmes de contrôle) pouvant être utilisés. Les algorithmes sélectionnés sont proposés par l'initiateur de la négociation IKE. Plage de valeurs : MD5, SHA1, SHA2

Paramètres	Description
Durée de vie proposée des clés de session	Durée de validité des clés de session (Session Keys) qui sont utilisées. Après écoulement de ce délai, plus aucune donnée ne sera échangée au cours de cette session. En remplacement des clés de session devenues non valides, il est automatiquement négocié de nouvelles clés de session.
Durée de vie proposée de la session d'échange de clés	Durée de validité de la session d'échange de clés. A la fin de la session d'échange des clés, de nouvelles clés sont automatiquement échangées pour la session d'échange de clés pour IKE
Volume de données proposé des clés de session	Volume de données maximum pour les clés de session (Session Keys). Lorsque le volume de données est dépassé, une nouvelle clé de session est automatiquement négociée avec IKE. Si vous sélectionnez "illimité", la quantité de données n'est pas limitée.
Activer 'Perfect Forward Secrecy'	Il est recommandé de toujours cocher cette option car l'on active ainsi un mécanisme de sécurité amélioré pour le transfert de données via le tunnel
Méthode d'authentification pour les paires VPN	Méthode d'authentification pour les abonnés VPN. Possibilités : signatures numériques (authentification par certificats) et clés pré-partagées (authentification par clé manuelle autodéfinie)
Clé pré-partagée	Ce champ n'est disponible que si la procédure d'authentification a lieu avec clés pré-partagées. Il faut inscrire ici le mot de passe dont se servent les abonnés VPN aux deux extrémités du tunnel. Il faut utiliser au moins 12 caractères.
Répétition de la clé pré-partagée	Ce champ n'est disponible que si la procédure d'authentification a lieu avec clés pré-partagées.
Liste des certificats CA	Ces options ne sont présentes que si la procédure d'authentification est basée sur des signatures numériques. Les abonnés VPN peuvent utiliser pour l'authentification tous les certificats qui ont été établis (signés) dans le cadre des certificats CA cochés.
Groupes Diffie-Hellman proposés	Les abonnés peuvent utiliser toutes les procédures d'échange de clés qui sont cochées

Remarque : L'ajout/la suppression d'un tunnel VPN doit être activé de manière définitive dans "VPN > Activer les tableaux VPN configurés".

27.3.2.18 Sécurité > VPN > Règles > Règles actives

Description des paramètres de l'onglet :

- **Afficher les règles**

Paramètres	Description
Priorité	Affichage de la priorité pour la séquence de traitement (chiffre) La priorité la plus élevée est indiquée par 1. Pour chaque règle associée à une direction, il faut attribuer une priorité propre. Une règle et la règle correspondance de la direction opposée doivent toujours avoir la même priorité.

Paramètres	Description
Service	Affiche le service pour lequel le chiffrement est limité. Si le chiffrement n'est pas limité à un service, il est affiché "N'importe quel service".
Action pour la règle	Affichage du mode de traitement des paquets IP par cette règle : pass signifie que les paquets IP sont transmis, deny signifie qu'aucun paquet IP n'est transmis.
Chiffrement nécessaire	Affichage du chiffrement. La procédure de cryptage est définie par le tunnel correspondant.
Etat de la règle	Indicateur d'état dans la règle. Plage de valeurs : Activer / Désactiver
Etat dans la pile IP	Affichage de l'état dans la pile IP. Plage de valeurs : Activer / Désactiver
Adresse source	
Type	Affichage du type pour l'adresse source. Plage de valeurs : Hôte, sous-réseau, plage d'adresses IP, nom DNS
Adresse (inférieure de la plage)	Affichage de l'adresse de source et de destination dans le format qui convient au type sélectionné. Le masque de saisie dépend du type d'adresse sélectionné. Lorsque n'importe quelle adresse IP peut être utilisée, il est affiché 0.0.0.0. Si l'adresse de destination indiquée est 0.0.0.0, pour l'envoi de paquets dans un tunnel, il faut alors désactiver NAT à l'interface avec le réseau de destination. Autre variante : une indication IP entre 0.0.0.1 et 255.255.255.254 est possible afin d'envoyer les paquets dans un tunnel.
Masque de sous-réseau / Adr. supérieur de la plage	Ce paramètre est défini si une plage d'adresses source/de destination doivent être définies pour la transmission
Adresse de destination	
Type	Affichage du type pour l'adresse de destination. Plage de valeurs : Hôte, sous-réseau, plage d'adresses IP, nom DNS
Adresse (supérieure de la plage)	
Masque de sous-réseau / Adr. supérieur de la plage	Ce paramètre est défini si une plage d'adresses source/de destination doivent être définies pour la transmission
Tunnel pour le chiffrement	
Tunnel côté réception	Affichage du tunnel dans le sens réception auquel cette règle s'applique. On va chercher dans ce tunnel les paquets IP qui ont été reçus par le réseau. Affichage : pas d'affectation de tunnel (dans le cas où aucun tunnel n'a été affecté dans le sens réception).
Tunnel côté émission	Affichage du tunnel dans le sens émission auquel cette règle s'applique. On va chercher dans ce tunnel les paquets IP qui ont été reçus par le réseau. Affichage : pas d'affectation de tunnel (dans le cas où aucun tunnel n'a été affecté dans le sens émission).

27.3.2.19 Sécurité > VPN > Règles > Règles configurées

Les règles définissent ce qui doit se passer avec un paquet IP. L'action de règle Pass signifie que le paquet IP doit continué à être transporté. L'action de règle Deny signifie que le paquet IP ne doit pas continuer à être transporté. Il est possible de sélectionner si le paquet IP utilise ou pas un tunnel VPN (chiffré). Le système de communication est en mesure de gérer 640 règles dont 6 sont prédéfinies (règles par défaut) et 634 sont libres d'attribution.

Description des paramètres des onglets :

- **Afficher les règles**
- **Ajouter une règle**
- **Modifier la règle**
- **Ajouter une règle pour le sens opposé**
- **Effacer la règle**

Paramètres	Description
Priorité	Affichage de la priorité pour la séquence de traitement (chiffre) La priorité la plus élevée est indiquée par 1. Pour chaque règle associée à une direction, il faut attribuer une priorité propre. Une règle et la règle correspondance de la direction opposée doivent toujours avoir la même priorité.
Service	Affiche le service pour lequel le chiffrement est limité. Si le chiffrement n'est pas limité à un service, il est affiché "N'importe quel service".
Action pour la règle	Affichage du mode de traitement des paquets IP par cette règle : pass signifie que les paquets IP sont transmis, deny signifie qu'aucun paquet IP n'est transmis.
Chiffrement nécessaire	Affichage du chiffrement. La procédure de cryptage est définie par le tunnel correspondant.
Etat de la règle	Indicateur d'état dans la règle. Plage de valeurs : activé/désactivé
Etat dans la pile IP	Affichage de l'état dans la pile IP. Plage de valeurs : Activer / Désactiver
Adresse source	
Type	Affichage du type pour l'adresse source. Plage de valeurs : Hôte, sous-réseau, plage d'adresses IP, nom DNS
Adresse (inférieure de la plage)	Affichage de l'adresse de source et de destination dans le format qui convient au type sélectionné. Le masque de saisie dépend du type d'adresse sélectionné. Lorsque n'importe quelle adresse IP peut être utilisée, il est affiché 0.0.0.0. Si l'adresse de destination indiquée est 0.0.0.0, pour l'envoi de paquets dans un tunnel, il faut alors désactiver NAT à l'interface avec le réseau de destination. Autre variante : une indication IP entre 0.0.0.1 et 255.255.255.254 est possible afin d'envoyer les paquets dans un tunnel.
Masque de sous-réseau / Adr. supérieur de la plage	Ce paramètre est défini si une plage d'adresses source/de destination doivent être définies pour la transmission
Adresse de destination	

Paramètres	Description
Type	Affichage du type pour l'adresse de destination. Plage de valeurs : Hôte, sous-réseau, plage d'adresses IP, nom DNS
Adresse (supérieure de la plage)	
Masque de sous-réseau / Adr. supérieur de la plage	Ce paramètre est défini si une plage d'adresses source/de destination doivent être définies pour la transmission
Tunnel pour le chiffrement	
Tunnel côté réception	Affichage du tunnel dans le sens réception auquel cette règle s'applique. On va chercher dans ce tunnel les paquets IP qui ont été reçus par le réseau. Affichage : pas d'affectation de tunnel (dans le cas où aucun tunnel n'a été affecté dans le sens réception).
Tunnel côté émission	Affichage du tunnel dans le sens émission auquel cette règle s'applique. On va chercher dans ce tunnel les paquets IP qui ont été reçus par le réseau. Affichage : pas d'affectation de tunnel (dans le cas où aucun tunnel n'a été affecté dans le sens émission).

27.3.2.20 Sécurité > VPN > Public Key Infrastructure (PKI)

Le serveur PKI correspond à un serveur qui peut établir, distribuer et contrôler des certificats numériques. Les certificats établis à l'intérieur d'une infrastructure PKI (Public Key Infrastructure) sont utilisés pour sécuriser la communication. A l'aide de la PKI-URL configurée par le serveur PKI, on tente de télécharger CRL en utilisant des certificats (signatures numériques).

Description des paramètres des onglets :

- **Afficher le serveur PKI**
- **Ajouter un serveur PKI**

Paramètres	Description
Nom du serveur PKI	Entrez pour le serveur un nom facilement reconnaissable.
Type de serveur PKI	Sélectionnez la tâche du serveur (possible : LDAP et Enrollment).
URL du serveur PKI	Inscrivez l'URL du serveur (par ex. LDAP://139.21.92.144:389).

27.3.2.21 Sécurité > SSL > Génération de certificats

L'accès administration se produit de manière cryptée via HTTPS, en utilisant le protocole TLS 1.2. Les certificats servent à authentifier la connexion. Par défaut, il est utilisé un certificat autosigné. Pour augmenter la sécurité, il est possible d'utiliser un certificat spécifique du client émis par un service de certification (CA). Le système de communication s'authentifie par rapport au client Admin à l'aide des certificats générés dans WBM ou importés. Un tel certificat peut être importé dans le navigateur comme certificat de confiance afin d'éviter les messages d'avertissement du navigateur en cas de liaison avec le serveur SSL.

Description des paramètres des onglets :

- **Générer le certificat CA**
- **Générer le certificat autosigné**

Paramètres	Description
Nom du certificat	Nom du certificat à générer.
Numéro de série du certificat	Numéro de série pour le certificat. Le numéro doit être un nombre entier positif
Type d'algorithme de signature	Algorithme de signature à utiliser Plage de valeurs : sha256RSA, sha512RSA
Longueur de la clé publique	Plage de valeurs, valeur par défaut : 2048
Début de la validité du certificat (GMT) Moment à partir duquel le certificat doit être valide. La date est interprétée comme heure GMT (Greenwich Mean Time).	
Jour, Mois, Année, Heure, Minute, Seconde	Unité pour l'indication du temps de validité du certificat
Fin de la validité du certificat (GMT) Moment à partir duquel le certificat cesse d'être valide. La date indiquée est une heure GMT (Greenwich Mean Time)	
Jour, Mois, Année, Heure, Minute, Seconde	Unité pour l'indication du temps de validité du certificat
Demandeur Affichage des données du demandeur de certificat suivant les conventions de la norme X.509 (par ex. DE pour l'Allemagne dans le champ Pays (C)). Les quatre champs doivent être complétés.	
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Autre nom de demandeur Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrées d'une adresse IP). La fenêtre de saisie dépend de la sélection du format. Si un autre format est sélectionné, il est possible de configurer plusieurs entrées SAN.	
Format du nom DNS	Cette information est généralement fournie en tant que Nom commun RDN dans le champ Objet du certificat principal
Autre format	Autres noms, donnés en tant que nom général
Extension Autre nom de l'objet	(en option) Plage de valeurs, valeur par défaut : nom DNS, adresse IP, E-mail, URI (identifiant uniforme de ressource), autres
Autre nom de demandeur	

Paramètres	Description
Type de point de distribution CRL	Plage de valeurs : nom DNS, adresse IP, E-mail, URI (identifiant uniforme de ressource), autres
Point de distribution CRL	Ici, il est possible (en option avec une URL) d'indiquer l'endroit à partir duquel les listes de verrouillage des certificats (CRL) sont distribuées

27.3.2.22 Sécurité > SSL > Gestion des certificats

Description des paramètres de l'onglet :

- **Afficher le certificat du fichier**

Paramètres	Description
Format PKCS#12	Si le certificat est enregistré dans un fichier PKCS#12, ce champ doit être activé.
Mot de passe de déchiffrement	Si le champ Format PKCS#12 a été activé, il faut que soit indiqué dans ce champ le même mot de passe que celui utilisé lors de la création du fichier.
Fichier avec le certificat	Indication du chemin et du nom de fichier du certificat. Si nécessaire cliquer sur Parcourir afin de définir l'emplacement d'enregistrement.

27.3.2.23 Sécurité > SSL > Gestion des certificats > Certificats de serveur

Description des paramètres des onglets :

- **Générer une demande de certificat (CSR)**
- **Importer le certificat de serveur (PKCS#12)**
- **Afficher le certificat**
- **Supprimer le certificat**
- **Exporter le certificat (X.509)**
- **Importer le certificat actualisé (X.509)**
- **Activer le certificat**

Paramètres	Description
Nom de la demande de certificat	Nom du certificat à générer.
Type d'algorithme de signature	Algorithme de signature à utiliser pour ce certificat Plage de valeurs : sha256RSA, sha512RSA
Longueur de la clé publique	Plage de valeurs : 2048
Demandeur Affichage des données du demandeur de certificat suivant les conventions de la norme X.509 (par ex. DE pour l'Allemagne dans le champ Pays (C)). Les quatre champs doivent être complétés.	
Pays (C)	Code de pays à deux caractères
Organisation (O)	La raison sociale complète de la société

Paramètres	Description
Unité organisationnelle (OU)	L'Unité organisationnelle correspond à la branche de l'entreprise qui commande le certificat
Nom général (CN)	Nom de domaine entièrement qualifié (FQDN)
Autre nom de demandeur Cette indication optionnelle fait la distinction entre le format du nom DN (indications comme pour demandeur) et l'autre format (par ex. entrées d'une adresse IP). La fenêtre de saisie dépend de la sélection du format. Si un autre format est sélectionné, il est possible de configurer plus d'une entrée SAN.	
Format du nom DNS	Cette information est généralement fournie en tant que Nom commun RDN dans le champ Objet du certificat principal
Autre format	Autres noms, donnés en tant que nom général
Extension Autre nom de l'objet	(en option) Plage de valeurs, valeur par défaut : nom DNS, adresse IP, E-mail, URI (identifiant uniforme de ressource), autres
Autre nom de demandeur	(en option)
Nom du certificat	Nom du certificat à importer.
Mot de passe de déchiffrement	Mot de passe qui a été utilisé pour la création du fichier. Plage de valeurs : 7 à 32 caractères
Fichier avec le certificat	Dans le champ **Fichier avec le certificat** il est possible d'entrer le certificat souhaité ou de le sélectionner à l'aide du champ Parcourir. Tout d'abord, il faut afficher l'**Empreinte digitale** du certificat, ensuite on peut effectuer l'importation.

27.3.2.24 Sécurité > Web

Description des paramètres de l'onglet :

- **Filtre d'accès Web**

Paramètres	Description
Clients Web	Uniquement en association avec UC Suite : activation et désactivation de l’accès Web depuis les téléphones mobiles et les applications mobiles (myPortal pour mobile/tablette, lanceur d’applications et applications tierces via un service Web). Information : Utilisation des clients Web avec UC Smart via le mode Expert > Applications > UC Smart > Paramètres de base
Accès via HTTPS	Seules les connexions chiffrées sont autorisées.
Accès via HTTP	Les connexions non chiffrées sont autorisées.
Enregistrer les données de connexion pour les appareils	Lorsque cette option est activée, il n'est pas nécessaire de saisir les identifiants de connexion à chaque démarrage de l'application.

27.3.2.25 Sécurité > Sécurité SQL

Description des paramètres de l'onglet :

- **Mot de passe accès SQL**

Paramètres	Description
Générer nouveau	Un mot de passe SQL chiffré, inconnu de l’utilisateur, est généré.
Activation par défaut	Le mot de passe SQL par défaut est activé.

27.3.3 Interfaces réseau

Dans **Interfaces réseau** sont regroupées des fonctions comme la configuration des différentes interfaces LAN. Les interfaces peuvent être configurées indépendamment les unes des autres.

27.3.3.1 Interfaces réseau > Carte mère > Nom d'hôte

Description des paramètres des onglets :

- **Modifier le nom de l'hôte**

Paramètres	Description
Nom d'hôte	Nom d'hôte du système de communication - choix libre. Exemple: `commsystem` Si le nom et l'adresse IP de la carte d'application sont placés dans un serveur DNS, il est possible de définir une désignation. Le nom de la carte d'application se compose du nom d'hôte et du nom de domaine. Exemple: `commsystem.mynet.home`

27.3.3.2 Interfaces réseaux > Carte mère > LAN 1 (WAN)

Description des paramètres des onglets :

- **Afficher le mode LAN 1**
- **Modifier l'interface LAN 1**
- **Modifier le ACD**

Paramètres	Description
Sélection du fournisseur d'accès Internet	Sélection permettant de déterminer le mode d'accès à un FAI (Fournisseur d’accès internet) via l'interface WAN.
Sélection du fournisseur d'accès Internet : Non configuré ou désactivé	L'interface WAN n'est pas utilisée.

Paramètres	Description
Sélection du fournisseur d'accès Internet : Type de connexion LAN TCP/IP	L'interface WAN est utilisée pour accéder à un FAI, qui est déjà configuré dans un routeur Internet externe. Le système de communication et le routeur Internet ne doivent pas nécessairement se trouver sur le même segment LAN, mais l'interface WAN doit être connectée au segment LAN du routeur Internet.
Sélection du fournisseur d'accès Internet : T-Online, T-DSL Business, ...	Le système de communication fonctionne comme un routeur Internet. L'interface WAN est utilisée pour accéder à un FAI préconfiguré.
Sélection du fournisseur d'accès Internet : Fournisseur PPPoE	Le système de communication fonctionne comme un routeur Internet. L'interface WAN est utilisée pour accéder à un FAI utilisant PPPoE. PPPoE est le protocole le plus couramment utilisé par les modems DSL.
Sélection du fournisseur d'accès Internet : Fournisseur PPTP	Le système de communication fonctionne comme un routeur Internet. L'interface WAN est utilisée pour l'accès à un FAI utilisant le protocole PPTP. Cette variante est courante en Autriche, par exemple.
Accès à l'internet via un routeur externe	L'accès à Internet se fait via un routeur externe. Cet indicateur est utilisé en interne par l'assistant de **Configuration Internet** et ne doit pas être modifié.
Configuration automatique de l'adresse (via DHCP)	Un serveur DHCP externe (éventuellement le serveur DHCP du routeur Internet) attribue une adresse IP au système de communication.
Accepter l'adresse IP du routeur par défaut	Le serveur DHCP externe communique l'adresse IP du routeur par défaut (par exemple, le routeur Internet) au système de communication.
Accepter l'adresse IP du serveur DNS	Le serveur DHCP externe communique l'adresse IP du serveur DNS au système de communication.
Accepter l'adresse IP du serveur SNTP	Le serveur DHCP externe communique l'adresse IP du serveur SNTP au système de communication.
Adresse IP	Adresse IP de l’interface LAN.
Masque de sous-réseau :	Masque de réseau du segment LAN.
Adresse MAC	Affiche l'adresse MAC de l'interface LAN.
Mode de liaison Ethernet	Mode de l'interface WAN.
Mode du liaison Ethernet : Auto	Commutation automatique entre les modes 100 et 1000 Mbps full duplex.
Mode du liaison Ethernet : 100HDX	100 Mbps, duplex intégral.
Mode du liaison Ethernet : 100FDX	100 Mbps, duplex intégral.
Mode du liaison Ethernet : 1000FDX	1000 Mbps, duplex intégral.
NAT	Le NAT (Network Address Translation) est activé. Cette tâche est généralement déjà prise en charge par le routeur externe.

Paramètres	Description
Contrôle de la bande passante pour les connexions vocales	Ce champ permet d'activer le contrôle de la bande passante pour les connexions vocales.
Bande passante pour les liaisons descendantes	Valeur de bande passante totale en kbit/s pour le téléchargement à partir du FAI.
Bande passante pour les liaisons montantes	Valeur de bande passante totale en kbit/s pour le transfert au FAI.
Bande passante utilisée pour la voix/le fax (%)	Pourcentage de la bande passante disponible pour les connexions voix/fax. Plage de valeurs, valeur par défaut : 0 - 100, 80
Balisage IEEE802.1p/q	Si cette case est cochée, un « type de service » est inclus dans les paquets Ethernet (couche 2) à des fins de priorisation L'option est désactivée par défaut.
IEEE802.1p/q VLAN ID	Entrez le numéro d'ID du VLAN si le commutateur utilisé a des problèmes avec la valeur par défaut « 0 ».
Classe QoS de la couche 2	
Données de signalisation	Classe de priorité pour l'établissement de la connexion. 0 = priorité la plus faible / 7 = priorité la plus élevée. Plage de valeurs, valeur par défaut : 0 - 7, 3
Charge utile fax/modem	Classe de priorité pour les données de fax et de modem de la connexion IP. 0 = priorité la plus faible / 7 = priorité la plus élevée. Plage de valeurs, valeur par défaut : 0 - 7, 5
Contrôle de réseau	Classe de priorité pour les données de contrôle du réseau (transfert de traps SNMP, par exemple). 0 = priorité la plus faible / 7 = priorité la plus élevée. Plage de valeurs, valeur par défaut : 0 - 7, 0
Charge utile vocale	Classe de priorité pour les données vocales de la connexion IP. 0 = priorité la plus faible / 7 = priorité la plus élevée. Plage de valeurs, valeur par défaut : 0 - 7, 5
Données d'accès à l'internet pour ...	
ID de connexion / Nom d'utilisateur / Numéro T-Online / Numéro de sous-utilisateur / Compte d'accès à Internet / DSL-Login ...	Données d'accès du fournisseur d'accès à Internet.
Mot de passe CHAP	Mot de passe pour l'accès au fournisseur d'accès à Internet.
Entrer à nouveau le mot de passe	Mot de passe pour l'accès au fournisseur d'accès à Internet.
Paramètres IP	
Adresse IP partenaire de la connexion PPP	Adresse IP du serveur FAI, si le FAI utilise une adresse IP statique.

Paramètres	Description
Adresse IP locale de la connexion PPP	Adresse IP attribuée par votre FAI pour l'accès à Internet.
Négociation de l'adresse IP	Sélection permettant de déterminer comment les partenaires de la connexion doivent négocier l'adresse IP lors de l'établissement de la connexion.
Négociation de l'adresse IP : adresse IP configurée	Seule l'adresse IP configurée est possible.
Négociation de l'adresse IP : accepter n'importe quelle adresse IP	Toute adresse proposée par le partenaire est acceptée.
Négociation de l'adresse IP : demande d'une nouvelle adresse IP	Une nouvelle adresse IP est demandée à chaque connexion.
Demande DNS	
Accès à l'internet avec demande de DNS	Le serveur DNS est déterminé automatiquement.
Adresse IP du serveur DNS primaire	Un serveur DNS spécial est sélectionné.
Paramètres PPP généraux	
Routeur par défaut	La connexion PPP créée ici est utilisée comme destination de routage.
Compression de l'en-tête IP	L'en-tête TCP est compressé. Les en-têtes UDP et RTP sont toujours compressés.
Envoi d'une demande d'écho LCP	Une demande d'écho LCP est envoyée. Cette fonction est utilisée pour vérifier si la connexion est toujours active.
Reconnexion PPP automatique	La connexion PPP est automatiquement rétablie après une coupure de la connexion (par exemple, dans le cas d'un accès ISP avec un forfait et une déconnexion forcée après 24 heures).
Paramètre PPTP	
Adresse IP locale de la connexion de contrôle	Adresse IP attribuée par votre FAI pour la connexion PPTP.
Adresse IP distante de la connexion de contrôle	Adresse IP du serveur de votre FAI pour la connexion PPTP.
Masque de sous-réseau distant de la connexion de contrôle	Masque de sous-réseau attribué par votre FAI pour la connexion PPTP.
Mise en attente courte	
Mise en attente courte	Le mode de fonctionnement « short hold » est activé pour la connexion PPP. La saisie suivante n'est possible que lorsque le mode « Short Hold » est activé.

Paramètres	Description
Temps de maintien court (sec)	Durée sans transmission de données après laquelle la connexion PPP doit être supprimée. Le délai d'attente court n'est déclenché que par les paquets sortants. Plage de valeurs, valeur par défaut : 10 - 9999, 60
Authentification	
Authentification du PPP	L'authentification PPP est activée. Le réglage doit être effectué conformément aux spécifications du FAI.
Nom d'utilisateur PPP	Nom d'utilisateur librement sélectionnable à utiliser pour l'authentification via PAP ou CHAP.
Mode d'authentification PAP	Activation et type d'authentification PAP pour la connexion PPP : Non utilisé, PAP Client, PAP Host.
Mot de passe PAP	Mot de passe pour l'authentification PAP.
Mode d'authentification CHAP	Activation et type d'authentification CHAP pour la connexion PPP : Non utilisé, CHAP Client, CHAP Hôte, CHAP Client et Hôte.
Mot de passe CHAP	Mot de passe pour l'authentification CHAP.
Compression des données	
Compression des données DEFLATE	Pour la compression des paquets de données PPP avec l'algorithme de compression DEFLATE.
Compression des données COMPRESS	Pour la compression des paquets de données PPP avec l'algorithme de compression COMPRESS.
Traduction d'adresse	
NAT	Le NAT (Network Address Translation) est activé. Les protocoles suivants sont pris en charge : TCP, UDP et ICMP (uniquement en mode passif).
Mappage d'adresses	seront abandonnés.
Paramètres du routeur	
Circuit à temps plein	Selon le modèle tarifaire, le circuit à temps plein (connexion permanente) au FAI peut être activé ou désactivé. Le circuit à temps plein doit être désactivé pour un modèle tarifaire basé sur le temps et activé pour un modèle tarifaire forfaitaire.
Temps de maintien court (sec)	Si le circuit à temps plein est désactivé (modèle tarifaire basé sur le temps), entrez la durée d'inactivité après laquelle la connexion doit être interrompue (par exemple, 60 secondes). Plage de valeurs, valeur par défaut : 10 - 9999, 60
Déconnexion forcée à (heure:min)	Si l'option Circuit à plein temps est activée (modèle tarifaire forfaitaire), entrez l'heure à laquelle la connexion Internet doit être désactivée (par exemple, 04:59).
Temps de connexion	Affiche le temps de connexion écoulé en jours-heures-minutes-secondes.
Paramètres QoS de l'interface	

Paramètres	Description
Bande passante pour les liaisons descendantes	Valeur de bande passante totale en kbit/s pour le téléchargement à partir du FAI.
Bande passante pour les liaisons montantes	Valeur de bande passante totale en kbit/s pour le transfert au FAI.
Contrôle de la bande passante pour les connexions vocales	Le contrôle de la bande passante permet d'éviter que les taux de transmission disponibles ne soient surchargés par les connexions vocales au sein d'une connexion multi-liaison. En d'autres termes, lorsque la compression de l'en-tête est active, un maximum de 5 connexions vocales est autorisé sur un canal B. Ce champ permet d'activer le contrôle de la bande passante pour les connexions vocales. Seules les connexions vocales dont les routes sont configurées dans la passerelle vocale sont prises en compte ici.
Bande passante utilisée pour la voix/le fax (%)	Pourcentage de la bande passante disponible pour les connexions voix/fax. Plage de valeurs, valeur par défaut : 0 - 100, 80

Description des paramètres des onglets :

- **Modifier le ACD**

Paramètres	Description
Temps de connexion	Affiche le temps de connexion écoulé en jours-heures-minutes-secondes.
Forcer la reconnexion à	Heure à laquelle la connexion doit être supprimée et rétablie.
Activer le ACD	Activer la déconnexion automatique pour éviter une déconnexion par le FAI à un moment inopportun.

27.3.3.3 Interfaces réseau > Carte mère > LAN 2

Description des paramètres des onglets :

- **Modifier l’interface LAN 2**

Paramètres	Description
Accès Internet via un routeur externe	L'accès à Internet se produit via un routeur externe.
Interface activée	L'interface LAN est activée.
Adresse IP	Adresse IP du système de communication.
Masque de réseau :	Masque réseau du segment LAN où se trouve le système de communication.
Adresse MAC	Affichage de l'adresse MAC du système de communication.
Mode liaison Ethernet	Mode de l'interface LAN.

Paramètres	Description
Mode liaison Ethernet : Auto	Commutation automatique entre 100 et 1000 Mbit/s ainsi que mode semiduplex et duplex intégral. Dans ce mode, il est possible d'activer la gestion de l'alimentation. Après avoir migré vers la version V2R3 ou une version ultérieure, vous devez appuyer sur la touche Appliquer située en haut de la liaison Ethernet souhaitée via la page d'interface réseau afin que sa valeur par défaut soit définie sur Auto. Sinon, les systèmes doivent être définis sur Auto ou sur 100 avant la migration.
Mode liaison Ethernet : 100HDX	100 MBit/s, semi-duplex. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.
Mode liaison Ethernet : 100FDX	100 Mbit/s, duplex intégral. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.
Mode liaison Ethernet : 1000FDX	1000 Mbit/s, duplex intégral. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.
IEEE802.1p/q-Tagging	Si cette case est cochée, il est indiqué dans les paquets Ethernet (couche 2) un "Type de Service" pour la priorisation. Par défaut, l'option est désactivée.
IEEE802.1p/q-VLAN-ID	Le numéro ID du VLAN ne doit être indiqué que si le commutateur utilisé a des problèmes avec la valeur par défaut "0".
Classe QoS de couche 2	
Données de signalisation	Classe de priorité pour l'établissement de la liaison. 0 = priorité la plus basse / 7= priorité la plus élevée. Plage de valeurs, valeur par défaut : 0 - 7, 3
Charge utile fax/modem	Classe de priorité pour les données fax et modem de la connexion IP. 0 = priorité la plus basse / 7= priorité la plus élevée. Plage de valeurs, valeur par défaut : 0 - 7, 5
Commande de réseau	Classe de priorité pour les données de la commande de réseau (par ex. transmission de traps SNMP). 0 = priorité la plus basse / 7= priorité la plus élevée. Plage de valeurs, valeur par défaut : 0 - 7, 0
Charge utile voix	Classe de priorité pour les données Voix. 0 = priorité la plus basse / 7= priorité la plus élevée. Plage de valeurs, valeur par défaut : 0 - 7, 5

27.3.3.4 Interfaces réseau > Carte mère > LAN 3 (Admin)

Description des paramètres des onglets :

- **Modifier l’interface LAN 3**

Paramètres	Description
Interface activée	L'interface LAN est activée.
Configuration automatique de l'adresse (via DHCP)	Un serveur DHCP attribue une adresse IP au système de communication.
Accepter Adresse IP of the Default Router	Le serveur DHCP externe communique au système de communication l'adresse IP du routeur par défaut (par ex. routeur Internet).
Accepter Adresse IP du serveur DNS	Le serveur DHCP externe communique au système de communication l'adresse IP du serveur DNS.
Accepter Adresse IP Adresse IP du routeur par défaut	Le serveur DHCP externe communique au système de communication l'adresse IP du serveur SNTP.
Adresse IP	Adresse IP de l'interface LAN.
Masque de réseau :	Masque de réseau du segment LAN.
Adresse MAC	Affichage de l'adresse MAC de l'interface LAN.
Mode liaison Ethernet	Mode de l'interface LAN.
Mode liaison Ethernet : Auto	Commutation automatique entre 100 et 1000 Mbit/s ainsi que mode semiduplex et duplex intégral.
Mode liaison Ethernet : 100HDX	100 MBit/s, semi-duplex.
Mode liaison Ethernet : 100FDX	100 Mbit/s, duplex intégral.
Mode liaison Ethernet : 1000FDX	1000 Mbit/s, duplex intégral.

27.3.3.5 Interfaces réseau > Carte mère > Serveur FTP

Description des paramètres des onglets :

- **Modifier les paramètres du serveur FTP**

Paramètres	Description
Valider le serveur FTP	Si la case est activée, le serveur FTP interne est validé.
Utilisateur de téléchargement 'Phone'	
Nom	Nom pour l'accès des téléphones IP au serveur FTP afin de pouvoir télécharger les mises à jour logicielles actuelles. Le nom ne peut pas être modifié.
Nouveau mot de passe	Mot de passe pour l'accès des téléphones IP au serveur FTP. Si le mot de passe prédéfini est modifié, il faut aussi modifier le mot de passe sur les téléphones IP.
Confirmer le mot de passe	Mot de passe pour l'accès des téléphones IP au serveur FTP.

Paramètres	Description
Utilisateur de téléchargement 'FTP_Admin'	
Nom	Nom pour l'accès de l'administrateur au serveur FTP. Le nom ne peut pas être modifié.
Nouveau mot de passe	Mot de passe pour l'accès de l'administrateur au serveur FTP.
Confirmer le mot de passe	Mot de passe pour l'accès de l'administrateur au serveur FTP.

27.3.3.6 Interfaces réseau > Carte mère > Mode DHCP

Description des paramètres des onglets :

- **Modifier le mode DHCP**

Paramètres	Description
Aucun DHCP	Si le champ option est activé, le serveur DHCP interne est arrêté.
Serveur DHCP	Si le champ option est activé, le serveur DHCP interne est en marche.
Agent relais DHCP	Si le champ option est activé, le système de communication joue le rôle d'agent relais DHCP. Les demandes DHCP des abonnés IP sont transmises du système de communication au serveur DHCP proprement dit. Le serveur DHCP et les abonnés IP ne doivent pas se trouver dans le même segment de réseau.

27.3.3.7 Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Paramètres globaux

Les données spécifiques au réseau sont transmises du serveur DHCP aux stations IP.

Description des paramètres des onglets ::

- **Modifier les Paramètres globaux**

Paramètres	Description
Activer du Serveur DHCP	Indique que le serveur DHCP interne est activé et que ses paramètres globaux peuvent être configurés. Ne peut être modifié.
Appareils Mitel/Unify uniquement	Indique que le serveur DHCP interne n'accepte que les demandes des périphériques Mitel et de l'Unify Phone. Si le client reçoit plusieurs réponses, par exemple du serveur DHCP d'OpenScape Business et d'un autre serveur du réseau, il préférera la réponse reçue d'OpenScape Business, s'il utilise des appareils compatibles : • OpenScape DeskPhone CP x00 avec la version logicielle V1R8.4.0 (HFA) / V1R11.6.0 (SIP) ou supérieure • OpenScape DeskPhone CP x10 avec la version logicielle V2R0.18.0 (HFA ou SIP) ou supérieure • Mitel MiVoice 69xx / 68xx (SIP)

Paramètres	Description
Masque de sous-réseau :	Le masque de sous-réseau définit la taille du sous-réseau. Exemple : `255.255.255.0`.
Adresse de diffusion	Avec l'adresse de diffusion, toutes les stations IP d'un réseau ou d'un sous-réseau peuvent être adressées par le serveur DHCP (en option). Exemple : `0.0.0.0`.
Passerelle par défaut	
Passerelle 1	Adresse IP sous laquelle la passerelle par défaut peut être atteinte. Si un routeur Internet est utilisé dans le réseau, le routeur Internet est la passerelle par défaut. Exemple : `192.168.1.1`. Si le système de communication est directement connecté à un modem Internet, le système de communication est la passerelle par défaut. Exemple : `192.168.1.2`.
Passerelle 2	Adresse IP sous laquelle une deuxième passerelle par défaut (routeur) peut être atteinte (en option).
Passerelle 3	Adresse IP sous laquelle une troisième passerelle par défaut (routeur) peut être atteinte (facultatif).
Serveur DNS	
Nom du domaine	Nom de domaine du réseau interne, max. 80 caractères, par exemple, `mynet.home` (en option).
Serveur 1	Adresse IP sous laquelle le serveur DNS peut être atteint. Si le système de communication est directement connecté à un modem Internet, la valeur par défaut `0.0.0.0` ne doit pas être modifiée. Le système de communication l'utilise pour se connecter automatiquement à un serveur DNS à partir d'Internet. Un serveur DNS externe peut également être saisi. Exemple : le serveur DNS du routeur Internet (`192.168.1.1)` ou un serveur DNS de l'Internet (`google-public-dns-a.google.com`).
Serveur 2	Adresse IP sous laquelle un deuxième serveur DNS peut être atteint (en option).
Serveur 3	Adresse IP sous laquelle un troisième serveur DNS peut être atteint (en option).
Durée de location en heures (0 infini)	Période de validité maximale en heures, 0 = durée de vie infinie (par défaut : 1 heure).
Activer la mise à jour dynamique du DNS	Si cette case est cochée, le serveur DNS peut être mis à jour dynamiquement. Par défaut : non activée. **Remarque :** Si l'option Mise à jour dynamique du DNS est activée, il est obligatoire de configurer le nom de domaine dans le champ **Nom de domaine** respectif du pool d'adresses IP.

Paramètres	Description
Utiliser le DLI interne	Si cette case est cochée, la DLI interne est utilisée. Si la case n'est pas cochée, les paramètres d'un serveur DLS externe s'affichent. Valeur par défaut : activée.
Serveur DLS externe	
Adresse IP	Adresse IP sous laquelle le serveur DLS externe est accessible.
Port	Port par lequel le serveur DLS externe peut être atteint.

27.3.3.8 Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Pools d'adresses IP

Description des paramètres des onglets ::

- **Afficher les pools d'adresses IP**
- **Ajouter le pool d'adresses IP**
- **Modifier le pool d'adresses IP**
- **Supprimer le pool d'adresses IP**

Paramètres	Description
Adresse de sous-réseau	L'adresse de sous-réseau définit la plage maximale d'adresses IP. Exemple : `192.168.1.0`.
Masque de sous-réseau :	Le masque de sous-réseau définit la taille du sous-réseau. Paramètre par défaut : `255.255.255.0`.
plage d'adresses	
Plage d'adresses 1	Limites inférieure et supérieure de la plage d'adresses IP du sous-réseau. Exemple : de `192.168.1.50` à `192.168.1.254`.
Plage d'adresses 2	Limites inférieure et supérieure d'une deuxième plage d'adresses IP dans le même sous-réseau (en option).
Plage d'adresses 3	Limites inférieure et supérieure d'une troisième plage d'adresses IP dans le même sous-réseau (en option).
Passerelle par défaut	
Passerelle 1	Adresse IP sous laquelle la passerelle par défaut peut être atteinte. Si un routeur Internet est utilisé dans le réseau, le routeur Internet est la passerelle par défaut. Exemple : `192.168.1.1`. Si le système de communication est directement connecté à un modem Internet, le système de communication est la passerelle par défaut. Exemple : `192.168.1.2`.
Passerelle 2	Adresse IP sous laquelle une deuxième passerelle par défaut (routeur) peut être atteinte (en option).
Passerelle 3	Adresse IP sous laquelle une troisième passerelle par défaut (routeur) peut être atteinte (facultatif).

Paramètres	Description
Adresse de diffusion	Avec l'adresse de diffusion, toutes les stations IP d'un réseau ou d'un sous-réseau peuvent être adressées par le serveur DHCP (en option). Valeur par défaut : `0.0.0.0`.
Nom du domaine	Nom de domaine du réseau interne, max. 80 caractères, par exemple, `mynet.home` (en option).
Serveur DNS	
Serveur 1	Adresse IP sous laquelle le serveur DNS peut être atteint. Si le système de communication est directement connecté à un modem Internet, la valeur par défaut `0.0.0.0` ne doit pas être modifiée. Le système de communication l'utilise pour se connecter automatiquement à un serveur DNS à partir d'Internet. Un serveur DNS externe peut également être saisi. Exemple : le serveur DNS du routeur Internet (`192.168.1.1)` ou un serveur DNS de l'Internet (`google-public-dns-a.google.com`).
Serveur 2	Adresse IP sous laquelle un deuxième serveur DNS peut être atteint (en option).
Serveur 3	Adresse IP sous laquelle un troisième serveur DNS peut être atteint (en option).
Sécurité avancée	
Option de relai	Un nombre hexadécimal configuré par l'administrateur pour une sécurité accrue. La valeur de ce champ est vide par défaut, et cette option ne sera pas prise en compte si elle n'est pas configurée.
Durée de location en heures (0 infini)	Période de validité maximale en heures, 0 = durée de vie infinie (par défaut : 1 heure).

27.3.3.9 Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Adresses IP statiques

Description des paramètres des onglets ::

- **Afficher l'adresse IP statique**
- **Ajouter l’adresse IP statique**
- **Modifier l’adresse IP statique**
- **Supprimer l'adresse IP statique**

Paramètres	Description
Nom d’hôte	Nom ou description de la station IP (par exemple, PC ou serveur) qui doit recevoir une adresse IP fixe. Exemple: `Serveur d'impression`.
Adresse IP	Adresse IP fixe souhaitée. Exemple: `192.168.1.10`.
Identifiant du client	Adresse MAC de la station IP ex. Périphérique RFP Mitel SIP-DECT.
Masque de sous-réseau :	Masque de réseau du sous-réseau. Exemple: `255.255.255.0`.

Paramètres	Description
Passerelle par défaut	
Passerelle 1	Adresse IP sous laquelle la passerelle par défaut peut être atteinte. Si un routeur Internet est utilisé dans le réseau, le routeur Internet est la passerelle par défaut. Exemple: `192.168.1.1`. Si le système de communication est directement connecté à un modem Internet, le système de communication est la passerelle par défaut. Exemple: `192.168.1.2`.
Passerelle par défaut 1	Adresse IP sous laquelle une deuxième passerelle par défaut (routeur) peut être atteinte (en option).
Passerelle par défaut 1	Adresse IP sous laquelle une troisième passerelle par défaut (routeur) peut être atteinte (facultatif).
Adresse de diffusion	Avec l'adresse de diffusion, toutes les stations IP d'un réseau ou d'un sous-réseau peuvent être adressées par le serveur DHCP (en option). Exemple: `0.0.0.0`.
Nom du domaine	Nom de domaine du réseau interne, max. 80 caractères, par exemple, `mynet.home` (en option).
Serveur DNS	
Serveur 1	Adresse IP sous laquelle le serveur DNS peut être atteint. Si le système de communication est directement connecté à un modem Internet, la valeur par défaut `0.0.0.0` ne doit pas être modifiée. Le système de communication l'utilise pour se connecter automatiquement à un serveur DNS à partir d'Internet. Un serveur DNS externe peut également être saisi. Exemple : le serveur DNS du routeur Internet (`192.168.1.1)` ou un serveur DNS de l'Internet (`google-public-dns-a.google.com`).
Serveur 2	Adresse IP sous laquelle un deuxième serveur DNS peut être atteint (en option).
Serveur 3	Adresse IP sous laquelle un troisième serveur DNS peut être atteint (en option).
Sécurité avancée	
Option de relai	Un nombre hexadécimal configuré par l'administrateur pour une sécurité accrue.
Durée de location en heures (0 infini)	Période de validité maximale en heures, 0 = durée de vie infinie (par défaut : 1 heure).

27.3.3.10 Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Derniers baux actifs

L'adresse IP attribuée par un serveur DHCP reste valable pour une station IP jusqu'à l'expiration de la « période de location », même si la station IP est

éteinte pendant cette période. Les dernières attributions actives sont affichées ici.

Description des paramètres des onglets ::

- **Afficher le bail**
- **Supprimer le bail**

Paramètres	Description
Adresse IP	Adresse IP attribuée à la station IP par le serveur DHCP.
Adresse MAC	Adresse MAC de la station IP à laquelle une adresse IP a été attribuée.
ID du client	ID client de la station IP. Si l'ID client n'est pas disponible, l'adresse MAC de la station IP est affichée.
Nom d'hôte	Nom ou numéro d'appel de la station IP à laquelle une adresse IP a été attribuée.
Début du bail	Heure de début de l'attribution. Une adresse IP est attribuée à la station IP à partir de ce moment.
Fin du bail	Heure de fin de l'attribution. Après cette période, la station IP doit envoyer une nouvelle demande d'adresse IP.

27.3.3.11 Interfaces réseau > Carte mère > Mode DHCP > Serveur DHCP > Toutes les locations

L'adresse IP attribué par un serveur DHCP demeure valide pour un abonnés IP tant que la "durée du leasing" le prévoit, même si entre-temps l'abonné IP est déconnecté. Toutes les affectations sont présentées ici.

Description des paramètres des onglets :

- **Afficher Lease**
- **Effacer Lease**

Paramètres	Description
Adresse IP	Adresse de l'abonné IP affectée par le serveur DHCP.
Adresse MAC	Adresse MAC de l'abonné IP auquel une adresse IP a été attribuée.
ID Client	ID Client de l'abonné IP. Si l'ID client n'est pas disponible, l'adresse MAC de l'abonné IP est indiquée.
Nom d'hôte	Nom ou numéro de téléphone de l'abonné IP auquel une adresse IP a été attribuée.
Démarrage de la Lease	Début de l'attribution. A partir de ce moment-là, une adresse IP a été attribuée à l'abonné IP.
Fin de la Lease	Fin de l'attribution. Ensuite, l'abonné IT lance une nouvelle demande d'adresse IP.

27.3.3.12 Interfaces réseau > Carte d'application > Nom d'hôte

Description des paramètres des onglets :

- **Modifier le nom de l'hôte**

Paramètres	Description
Nom d'hôte	Nom d'hôte de la carte d'application - choix libre. Exemple: `applboard` Si le nom et l'adresse IP de la carte d'application sont placés dans un serveur DNS, il est possible d'effectuer une résolution de nom. Le nom de la carte d'application se compose du nom d'hôte et du nom de domaine. Exemple: `applboard.mynet.home`

27.3.3.13 Interfaces réseau > Carte d'application > LAN 1

Description des paramètres des onglets :

- **Modifier l'interface LAN 1**

Paramètres	Description
Interface activée	Si cette case est cochée, l'interface LAN 1 de la carte d'application (application board) est activée.
Configuration automatique de l'adresse (via DHCP)	Si cette case est cochée, le serveur DHCP attribue automatiquement à l'interface LAN 1 l'adresse IP et le masque de réseau. De plus, il peut être décidé de reprendre également d'autres paramètres spécifiques du réseau depuis le serveur DHCP.
Accepter Adresse IP of the Default Router	Si cette case est cochée, le serveur DHCP reprend l'adresse IP du routeur par défaut.
Accepter Adresse IP du serveur DNS	Si cette case est cochée, le serveur DHCP reprend l'adresse IP du serveur DNS.
Accepter Adresse IP Adresse IP du routeur par défaut	Si cette case est cochée, le serveur DHCP reprend l'adresse IP du serveur SNTP.
Adresse IP	Adresse IP permettant de joindre la carte d'application (Application Board).
Masque de réseau :	Masque de réseau permettant de joindre la carte d'application.
Adresse MAC	Adresse MAC de la carte d'application (non modifiable).
Mode liaison Ethernet	Mode de l'interface LAN 1.
Mode liaison Ethernet : Auto	Commutation automatique entre 100 et 1000 Mbit/s ainsi que mode semiduplex et duplex intégral. Dans ce mode, il est possible d'activer la gestion de l'alimentation.
Mode liaison Ethernet : 100HDX	100 MBit/s, semi-duplex. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.
Mode liaison Ethernet : 100FDX	100 Mbit/s, duplex intégral. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.

Paramètres	Description
Mode liaison Ethernet : 1000FDX	1000 Mbit/s, duplex intégral. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.

27.3.3.14 Interfaces réseau > Carte d'application > LAN 2

Description des paramètres des onglets :

- **Modifier l'interface LAN 2**

Paramètres	Description
Interface activée	Si cette case est cochée, l'interface LAN 2 de la carte d'application (application board) est activée.
Adresse IP	Adresse IP permettant de joindre la carte d'application (Application Board).
Masque de réseau :	Masque de réseau permettant de joindre la carte d'application.
Adresse MAC	Adresse MAC de la carte d'application (non modifiable).
Longueur de paquet de données maxi. (octets)	Longueur de paquet maximum en octets qui doit s'appliquer au protocole IP. Les valeurs comprises entre 576 et 1500 sont autorisées.
Mode liaison Ethernet	Mode Interface LAN 2.
Mode liaison Ethernet : Auto	Commutation automatique entre le mode semiduplex et le duplex intégral. Dans ce mode, il est possible d'activer la gestion de l'alimentation.
Mode liaison Ethernet : 100HDX	100 MBit/s, semi-duplex. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.
Mode liaison Ethernet : 100FDX	100 Mbit/s, duplex intégral. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.
Mode liaison Ethernet : 1000FDX	1000 Mbit/s, duplex intégral. Dans ce mode, il n'est pas possible d'activer la gestion de l'alimentation.
IEEE802.1p/q-Tagging	Si cette case est cochée, le format Ethernet envoyé par la carte d'application est défini. Par défaut, l'option est désactivée.
IEEE802.1p/q-VLAN-ID	Numéro ID du VLAN, différent de la valeur par défaut "0" lorsque le commutateur utilisé a des problèmes avec la valeur par défaut "0".
Classe QoS de couche 2	
Données de signalisation	Classe de priorité pour l'établissement de la liaison. 0 = priorité la plus basse / 7= priorité la plus élevée.
Charge utile fax/modem	Classe de priorité pour les données fax et modem de la connexion IP. 0 = priorité la plus basse / 7= priorité la plus élevée.
Commande de réseau	Classe de priorité pour les données de la commande de réseau (par ex. transmission de traps SNMP). 0 = priorité la plus basse / 7= priorité la plus élevée.

Paramètres	Description
Charge utile voix	Classe de priorité pour les données voix de la connexion IP. 0 = priorité la plus basse / 7= priorité la plus élevée.

27.3.4 Routage

Le menu **Routage** permet de gérer les tables de routage. Dans les petits réseaux, l'administrateur peut gérer manuellement une table de routage sur chaque routeur. Dans les grands réseaux, cette tâche est automatisée au moyen d'un protocole qui distribue les données de routage dans le réseau.

27.3.4.1 Routing > IP Routing > Mainboard > Static Routes

Le système de communication ne prend en charge que les routes statiques. Les routes statiques connectent deux périphériques IP entre eux. Ils sont créés manuellement.

Selon l'application, il peut être nécessaire de définir différents itinéraires pour le système (carte mère).

Description des paramètres des onglets :

- **Afficher le tableau de routage statique**
- **Ajouter un itinéraire statique**
- **Modifier l'itinéraire statique**
- **Supprimer l'itinéraire statique**

Paramètres	Description
Index des itinéraires :	L'index de l'itinéraire est attribué automatiquement et n'est affiché qu'à titre informatif. Il ne peut pas être modifié.
Nom de l'itinéraire :	Nom ou description de l'itinéraire statique ; librement sélectionnable.
Réseau/hôte de destination :	Adresse IP du réseau de destination.
Masque de sous-réseau :	Masque de sous-réseau du réseau de destination.
Passerelle de route :	Adresse IP du routeur suivant sur cette route ou adresse IP de l'interface locale ou distante d'un homologue PSTN.

27.3.4.2 Routage > IP Routage > CarteMère > RouteurParDéfaut

Selon l'application, il peut être nécessaire de définir un routage par défaut différent pour le système (carte mère).

Description des paramètres des onglets :

- **Modifier le routeur par défaut**

Paramètres	Description
Routage par défaut via	Activer ou désactiver le routage IP via un routeur par défaut.
Aucune interface	Désactiver le routage IP via un routeur par défaut.
LAN	Activer le routage IP via un routeur par défaut.
Adresse IP du routeur par défaut	Adresse IP du routeur par défaut, si **le réseau local (LAN)** est sélectionné comme interface dans le champ **« Routage par défaut via »** . Exemple : adresse IP du routeur Internet, `192.168.1.1`.

27.3.4.3 Routage > Routage IP > Carte mère > Serveur DNS

Vous pouvez afficher l'adresse IP du serveur DNS Afficher et si nécessaire la modifier. Le paramétrage est nécessaire pour le Trunking avec adresses IP dynamiques.

Description des paramètres des onglets :

- **Modifier les paramètres DNS**

Paramètres	Description
Adresse IP du serveur DNS	Adresse IP à laquelle le serveur DNS est joignable. Si le système de communication est relié directement à un modem Internet, la valeur par défaut `0.0.0.0` ne doit pas être modifiée. Le système de communication se relie ainsi automatiquement à un serveur DNS de l'Internet. Il est également possible d'inscrire un serveur DNS. Exemple : Serveur DNS du routeur Internet (`192.168.1.1)` ou un serveur DNS de l'Internet (`google-public-DNS-a.google.com`). S'il s'agit d'un système OpenScape Business S, un redémarrage du système est nécessaire pour que les modifications soient applicables.

27.3.4.4 Routage > IP Routage > Application Board > Itinéraires statiques

Selon l'application, il peut être nécessaire de définir différents itinéraires pour le système (carte mère).

Description des paramètres des onglets :

- **Afficher le tableau de routage statique**
- **Ajouter un itinéraire statique**
- **Modifier l'itinéraire statique**
- **Supprimer l'itinéraire statique**

Paramètres	Description
Index des itinéraires :	L'index de l'itinéraire est attribué automatiquement et n'est affiché qu'à titre informatif. Il ne peut pas être modifié.
Nom de l'itinéraire :	Nom ou description de l'itinéraire statique ; sélectionnable librement (facultatif) Plage de valeurs : 35 caractères maximum

Paramètres	Description
Réseau/hôte de destination :	Adresse IP du réseau de destination.
Masque de sous-réseau :	Masque de sous-réseau du réseau de destination.
Passerelle de route :	Adresse IP du routeur suivant sur cette route ou adresse IP de l'interface locale ou distante d'un homologue PSTN.

27.3.4.5 Routage > IP Routage > Application Board > Routeur par défaut

Selon l'application, il peut être nécessaire de définir un routage par défaut différent pour le système (carte mère).

Description des paramètres des onglets :

- **Changer le routeur par défaut**

Paramètres	Description
Routage par défaut via	Activer ou désactiver le routage IP via un routeur par défaut.
Aucune interface	Désactiver le routage IP via un routeur par défaut.
LAN	Activer le routage IP via un routeur par défaut.
Adresse IP du routeur par défaut	Adresse IP du routeur par défaut, si le réseau local (LAN) est sélectionné comme interface dans le champ « Routage par défaut via ».

27.3.4.6 Routage > NAT

Vous pouvez présenter, ajouter, modifier et effacer une règle NAT pour la traduction d'adresse réseau. A l'aide du tableur NAT, vous pouvez facilement gérer facilement et d'une manière globale toutes les entrées NAT actuelles et supplémentaires pour la traduction d'adresse réseau.

Description des paramètres des onglets :

- **Ajouter NAT**
- **Tableur NAT**

Paramètres	Description
Règle NAT active	
Description	
Adresse IP locale	Adresse de destination locale dans LAN.
Port local	Numéro de port local du protocole configuré dans LAN.
Port global	Numéro de port du protocole configuré.
Protocole	Protocole de transport à utiliser. Le protocole de transport configuré s'applique aux indications d'adresse locales comme globales.

Paramètres	Description
Protocole : **TCP**	TCP (Transmission Control Protocol) TCP est un protocole fiable, orienté connexion, pour la transmission des paquets IP. Avant le début de la transmission, un canal virtuel est établi entre les deux extrémités de la liaison réseau. Sur ce canal, il est possible de transmettre des données dans les deux sens. TCP est principalement utilisé dans les secteurs suivants : WorldWideWeb, E-Mail et réseaux pair-à-pair. Il est également utilisé pour la signalisation d'appel dans la téléphonie IP ; en effet il possède la caractéristique de détecter les pertes de données lors de la transmission et de les éliminer automatiquement.
Protocole : **UDP**	UDP (User Datagram Protocol) UDP est un protocole simple, sans connexion, pour la transmission des paquets IP. Avant le début de la transmission, il n'est pas créé de canal virtuel vers le correspondant comme dans TCP, ce qui permet aux PC de commencer plus rapidement à échanger des données. Pour l'adressage des paquets voix, UDP envoie le numéro de port du service qui doit recevoir les données. Ce protocole est utilisé principalement dans le secteur DNS et pour la transmission de la voix en téléphonie IP. Comme, avec un protocole sans connexion, il n'est pas contrôlé si le correspondant reçoit vraiment les données, cela peut se traduire par des pertes lors de la transmission de la voix.

27.3.4.7 Routage > RTC

Avec ces paramètres, il est établi une connexion IP Remote (DFÜ) via le réseau téléphonique classique.

Description des paramètres des onglets :

- **Modifier les données RTC globales**

Paramètres	Description
Numéro du routeur (numéro interne)	Sélectionner la SDA du système Toutes les applications qui utilisent la fonction routeur peuvent être jointes depuis l'extérieur à l'aide de ce numéro SDA. Les partenaires de routage externes qui ne transmettent pas de numéro d'appel doivent utiliser d'autres numéros d'appel. Ces numéros de téléphone sont configurés comme MSN.
Répétition de la numérotation	
Nombre de répétitions	Tentatives de répétition à entreprendre par le système pour établir une connexion Plage de valeurs : 0 à 255
Pause de répétition de la numérotation (s)	Pause entre les répétitions de la numérotation, en secondes. Plage de valeurs : 1 - 1 000
Script	

Paramètres	Description
Identification 1 pour script	Première partie du nom de compte pour la connexion à un fournisseur Internet. Le fournisseur Internet transmet les entrées sur l'hôte, l'identification de l'utilisateur et un mot de passe, par ex. hôte=ERT005, utilisateur=KJUMBERT, mot de passe=123456. Les entrées sont les suivantes : identification 1 pour script : hôte:ERT005 - Identification 2 pour script: USER:KJUMBERT - Nouveau mot de passe pour script : PASSWORD:123456.
Identification 2 pour script	Deuxième partie du nom de compte lors de la connexion à des fournisseurs Internet.
Nouveau mot de passe pour script	Mot de passe pour la connexion à des fournisseurs Internet.

27.3.4.8 Routage > RTC > Protocole PPP

Description des paramètres des onglets :

- **Charger par HTTP**

Paramètres	Description
Charger	Le fichier journal PPP peut être chargé via HTTP. Suivant le paramétrage du navigateur, il est indiqué si le fichier journal téléchargé doit être enregistré ou bien être lu dans l'éditeur par défaut.

27.3.4.9 Routage > RTC > Partenaire RTC

Description des paramètres des onglets :

- **Ajouter un partenaire RTC**
- **Afficher le partenaire RTC**
- **Modifier le partenaire RTC**

Paramètres	Description
Nom du partenaire	Nom du partenaire RTC. Les partenaire RTC suivants sont disponibles : • RTC par défaut - non configurable • RTC Partenaire 1 : par défaut pour CLA, fonction reconfigurable • RTC Partenaire 2 : par défaut pour RNIS, fonction reconfigurable • RTC Partenaire 3 : nom et fonction librement configurables • RTC Partenaire 4 : nom et fonction librement configurables Plage de valeurs : 1 à 14 caractères
Type de connexion RTC	Configuration de la connexion RTC (sélection par défaut : activée).
Type de connexion RTC : Non affecté	Le partenaire RTC peut être préconfiguré. Ce paramétrage n'empêche pas toutefois l'établissement de la liaison via ce partenaire RTC.

Paramètres	Description
Type de connexion RTC : Activé	Partenaire RTC est activé. Ce paramétrage autorise l'établissement de la liaison via ce partenaire RTC.
Type de connexion RTC : Reprise DSL	Utilisation de l'accès DSL pour la connexion RTC (le routeur par défaut est l'accès DSL)
Paramètres IP	
Adresse IP du partenaire RTC	Adresse IP de l'ordinateur hôte de l'autre partie avec laquelle le RTC a établi une connexion.
Adresse IP de l'interface RTC locale	Adresse IP du système de communication local qui doit être utilisé pour la connexion RTC.
Négociation de l'adresse IP	Négociation de l'adresse IP entre les partenaires de la connexion lors de l'établissement de la liaison.
Négociation de l'adresse IP : Utiliser l'adresse IP configurée	Seule l'adresse IP configurée du partenaire RTC est acceptée.
Négociation de l'adresse IP : Accepter chaque adresse IP	Pas de négociation de l'adresse IP
Négociation de l'adresse IP : Demander une nouvelle adresse IP	L'adresse IP est négociée
Paramètres PPP généraux	
Routeur par défaut	Le partenaire RTC paramétré ici ne doit pas seulement être préconfiguré, mais il doit être utilisé comme destination de routage. Il ne peut y avoir qu'un routeur par défaut. Soit il s'agit d'un accès DSL soit du partenaire RTC configuré ici.
Accès Internet avec interrogation DNS	L'accès doit être utilisé comme accès Internet. Un seul accès Internet par système doit être activé (soit un partenaire RTC soi un accès DSL).
Entrée de service	Lors d'un appel au MSN du partenaire RTC, le contrôle de la numérotation doit être désactivé. L'entrée de service ne peut être activée que si le partenaire RTC dispose d'un numéro MSN et si une authentification PAP ou CHAP a été activée.
MSN/SDA (numéro interne)	Configuration du numéro MSN. Si le partenaire transmet son numéro de téléphone, celui-ci doit être configuré sinon l'appel est refusé. Par contre, si les numéros de téléphone du partenaire sont configurés mais que le partenaire n'en transmet aucun, la connexion est tout de même établie.
Canaux B	Nombre de canaux B utilisés. Plage de valeurs : 1 ou 2

Paramètres	Description
Rappel	Un appel est refusé et le partenaire est ensuite immédiatement rappelé. Cela empêche la sélection de postes distants non autorisés. La partie appelante doit transmettre le numéro d'appel dans le canal D de la liaison RNIS et autoriser la sélection par le système. Pour le partenaire RTC, ce numéro doit être configuré avec faisceau sortant. Si "Rappel" est activé, seules les connexion sortantes sont acceptées par ce partenaire. Si le poste distant est également une passerelle, et si le "Rappel" est également activé pour cette connexion, il n'est pas possible d'établir de connexion par ce qu'aucun des partenaire n'accepte l'établissement d'une liaison entrante. Si, dans une configuration incorrecte de ce type, seul "Rappel sans répétition de la numérotation" est activé, il est alors détecté et l'établissement d'une liaison permanente est empêché. Si Répétition de la numérotation est activée, le problème n'est pas détecté.
Poste distant V.34	Accepter un poste distant V.34 (par ex. un modem).
Reconnecter automatiquement PPP	La connexion PPP est rétablie automatiquement après une coupure de connexion (par ex. avec accès FAI avec forfait et coupure forcée au bout de 24 heures).
Envoyer une demande d'écho LCP	Une demande d'écho LCP est envoyée. Cette fonction sert à contrôler si la connexion est encore active.
Short-Hold	
Short-Hold	Le mode "Short Hold" est activé pour la connexion PPP. Les entrées suivantes sont uniquement possibles lorsque le mode Short-Hold est activé.
Durée Short-Hold (s)	Durée sans transmission de données à l'issue de laquelle la connexion PPP doit être coupée. Le timer Short-Hold est activé par les paquets sortants. Plage de valeurs : 10 à 9999
Analyse de l'horloge de taxation Short-Hold	Optimisation du mode Short-Hold avec prise en compte de l'impulsion de taxation. Pour les appels via PPP, il est effectué une évaluation de l'impulsion de taxation (évaluation des messages Facility avec éléments d'information AoC). Si le fournisseurs de services de téléphonie sur Internet ne donne aucune information sur la taxation,on utilise comme valeur par défaut du timeout 0 seconde.
Authentification	
Authentification PPP	L'authentification PPP est activée.
Nom d'utilisateur PPP	Nom d'utilisateur (choix libre) qui doit être utilisé lors de l'authentification PAP ou CHAP.
Mode d'authentification PAP	Activation et type d'authentification PAP pour la connexion PPP : non utilisé, client PAP, hôte PAP.
Mot de passe PAP	Mot de passe pour l'authentification PAP.
Mode d'authentification CHAP	Activation et type d'authentification CHAP pour la connexion PPP : non utilisé, client CHAP, hôte CHAP, client et hôte CHAP.
Mot de passe CHAP	Mot de passe pour l' authentification CHAP.
Compression d'en-tête	

Paramètres	Description
Compression de l'en-tête IP	La compression de l'en-tête IP/TCP ou IP/UDP/RTP est activée. La compression d'en-tête améliore la transmission des données dans les scénarios Voice-over-PPP. Tous les paquets Voix dont le numéro de port UDP est situé dans la plage réglée sont comprimés.
Compression de données	
Compression de données DEFLATE	Compression avec l'algorithme DEFLATE
Compression de données COMPRESS	Compression avec l'algorithme COMPRESS
Conversion d'adresse	
NAT	NAT (Network Adress Translation - traduction d'adresse réseau) est activée. Les protocoles ci-après sont supportés : TCP, UDP et ICMP (uniquement en mode passif).
Mappage d'adresses	Le mappage d'adresses est activé.
Paramètres QoS de l'interface	
Gestion de la bande passante pour les connexions vocales	Le contrôle de la bande passante empêche une surréservation du débit de transmission disponible par les connexion vocales à l'intérieur d'une connexion multilink, c.-à-d. lorsque la compression de l'en-tête est activée, on autorise au maximum 5 liaisons vocales (G.729 / 60ms ou G.723 / 60ms) sur un canal B. Ce champ active la gestion de la bande passante pour les connexions vocales. Dans ce cadre, seules sont prises en compte les liaisons vocales dont les routes ont été configurées dans la passerelle vocale.
Bande passante pour les connexions voix/fax (%)	Indication de pourcentage relatif à la bande passante disponible pour les connexions voix/fax. Plage de valeurs, valeur par défaut : 0 - 95, 80

Description des paramètres des onglets :

- **Ramener à la valeur par défaut**

Paramètres	Description
Appliquer	Les valeurs pour le partenaire RTC sont rétablies sur les valeurs à la livraison.

Description des paramètres des onglets :

- **Ajouter un numéro**
- **Modifier numéro**
- **Effacer un numéro**

Paramètres	Description
Numéro d'appel	Numéro de téléphone sous lequel le partenaire RTC peut être joint. Il doit être univoque au sein de la configuration globale et peut comporter jusqu'à 22 chiffres décimaux (0 à 9). Il est possible d'utiliser des traits d'union. Pour chaque partenaire RTC il est possible de configurer jusqu'à cinq numéros de téléphone. Lors de la transmission du numéro de téléphone, celui-ci est contrôlé et seuls sont acceptés les appels pour lequel il a été défini pour le numéro entrant un partenaire RTC disposant de l'autorisation d'appel correspondante.
Sens de l'appel	Etablissement de la connexion avec les numéros de téléphone indiqués plus haut.
Sens de l'appel : Verrouillé	Le numéro n'est pas utilisable.
Sens de l'appel : entrant	Le partenaire peut appeler, mais ne peut pas être appelé.
Sens de l'appel : sortant	Le partenaire peut être appelé, mais ne peut pas appeler.
Sens de l'appel : Entrant et sortant	Le partenaire peut être appelé et peut appeler.
Effacer	Le numéro de téléphone sélectionné est supprimé.

27.3.5 LCR

Dans **LCR** sont décrites les fonctions de LCR comme les discriminations, les plans de numérotation, les tables de routage et les règles de numérotation.

27.3.5.1 LCR > Flags LCR

Description des paramètres de l'onglet :

- **Modifier les flags LCR**

Paramètres	Description
Flags LCR	
Autoriser LCR	LCR est validé et donc la recherche automatique d'acheminement.
Réinitialiser les données LCR	
Effacement des données LCR configurées et initialisation avec données LCR standard	Si ce champ d'option est activé, les entrées LCR configurées (plans de numérotation, tables de routage, règles de numérotation) sont supprimées et remplacées par les entrées standard.

Conseil : Une configuration incorrecte du mode LCR risque de rendre impossibles ou de restreindre les connexions sortantes.

Concepts associés

Données abonnés à la page 130

27.3.5.2 LCR > Classes de service

Description des paramètres de l'onglet :

- **Modifier les classes de discrimination LCR**

Paramètres	Description
L'index	Liste d'index hiérarchique
Numéro de téléphone	Numéro de l'abonné
Nom	Nom de l'abonné
Groupe de discrimination	Chaque abonné est affecté à un groupe de discrimination (Classic Of Service COS). Par défaut, tous les abonnés sont inscrits avec la discrimination LCR maximale (15) Plage de valeurs : 1 à 15

Conseil : Un abonné ne peut occuper un chemin que si sa discrimination est égale ou supérieure à la discrimination LCR de la table de routage.

27.3.5.3 Plan de numérotation > LCR

Description des paramètres des onglets :

- **Modifier le plan de numérotation**
- **Afficher le plan de numérotation**

Paramètres	Description
Plan de numérotation	Le plan de numérotation est analysé afin de trouver des modèles correspondant aux chiffres composés. Le résultat est utilisé comme critère de sélection de la table de routage. Dans le même temps, le système vérifie si la classe de service de l'abonné correspond à cet itinéraire. Pour les connexions externes, chaque numéro d'appel, y compris l'indicatif (jusqu'à un maximum de 24 caractères, séparateurs de champs compris), est vérifié dans le plan de numérotation. Le plan de numérotation détermine ensuite une table de routage pour la station ; cette table est attribuée à la station pour l'établissement de la connexion. Jusqu'à 16 itinéraires sont créés via une seule table de routage. Le tableau des règles de numérotation définit comment les chiffres sélectionnés par la station sont convertis et composés par le système de communication.
Nom	La colonne Nom peut être utilisée pour attribuer un nom à chaque profil, par exemple, appel local, appel longue distance, international, etc. Selon la version du système de communication, la colonne Nom peut être affichée ou non. Il convient de choisir un nom significatif lors de l'attribution des noms. Plusieurs occurrences du même nom peuvent être utilisées. Les noms appropriés sont automatiquement attribués via l'assistant de règles de numérotation.

Paramètres	Description
chiffres composés	Ce système permet d'évaluer le numéro d'appel afin de rediriger vers la table de routage appropriée. Les délimiteurs de champs C et - ainsi que les espaces réservés X, N et Z peuvent être utilisés. Chiffres fixes 0 à 9 : délimiteurs de champs (évaluation selon la règle de numérotation) ; X : espace réservé pour un chiffre de 0 à 9 ; N : espace réservé pour un chiffre de 2 à 9 ; Z : espace réservé pour un ou plusieurs chiffres jusqu'à la fin de la numérotation ; C : tonalité simulée (peut être saisie 3 fois maximum).
Tableau de routage	La colonne « Table de routage » permet de spécifier la table de routage à utiliser pour le profil. La flèche renvoie à la définition de la table de routage correspondante. Plage de valeurs : de 1 à 254, dont 1 à 15 préréglées Si l' **équilibrage de charge** est actif, les routes requises doivent figurer dans la même table de routage.
Code d'accès	La case à cocher de cette colonne est sélectionnée/désélectionnée pour déterminer si la saisie d'un code de compte est obligatoire après le code de saisie (aux États-Unis : après la fin de la numérotation). Lorsque la case est décochée, le code de compte n'est pas requis tant que le plan de numérotation n'a pas été entièrement composé, s'il a été configuré pour l'itinéraire.
Restriction de péage	Lorsqu'ils sont sélectionnés, les chiffres composés sont soumis à des restrictions de péage (classe de service). Cela s'applique aussi bien aux réseaux qu'aux systèmes de communication autonomes. Grâce à cela, il est possible de supprimer individuellement les numéros d'appel soumis à la restriction d'interurbain. Si la restriction de péage doit être appliquée, les règles connues relatives aux listes autorisées/interdites s'appliquent.
Urgence	Si un numéro configuré comme numéro d'urgence (case à cocher de la colonne « urgence » sélectionnée) est composé et qu'aucune ligne libre n'est disponible, une ligne utilisée pour un numéro non urgent (case à cocher de la colonne « urgence » décochée) est déconnectée puis automatiquement libérée pour le numéro d'urgence.

27.3.5.4 LCR > Table de routage

Description des paramètres des onglets :

- **Modifier la table de routage**

Paramètres	Description
Tables de routage	A l'aide des tables de routage, il est affecté une action (sélection) aux numéros définis dans le plan de numérotation. Plage de valeurs : 254 tables de routage
L'index	La table de routage est analysée du haut vers le bas, par ordre hiérarchique. Le système vérifie si le faisceau est libre ou si l'abonné dispose de la classe de service LCR requise. Si c'est le cas, la numérotation est exécutée conformément à la règle de numérotation entrée dans la table de routage. Plage de valeurs : 1 à 16

Paramètres	Description
Route dédiée	Il est utilisé le faisceau qui a été attribué de manière fixe à l'abonné (par ex. lors de l'attribution du faisceau dans le cadre de la gestion multisite).
Faisceaux	Faisceau à prendre, voir "Lignes/Mise en réseau > Faisceaux" Valeur par défaut : nom du faisceau configuré dans le système
Règle de numérotation	Les règles de numérotation LCR permettent de convertir les numéros d'appel entrés en de nouvelles séquences de chiffres aléatoires pour un traitement supplémentaire. La conversion des chiffres permet d'accéder à divers opérateurs. Définition dans "Règle de numérotation". Plage de valeurs : 254 règles de numérotation
Dis. min.	La classe de discrimination mini. décrit la discrimination LCR dont doit disposer au moins l'abonné pour être en droit d'utiliser la route correspondante. On voit par ex. ici qu'un abonné ne peut utiliser qu'une ligne (carrier) définie et ne peut téléphoner qu'à certaines heures, tandis que d'autres abonnés disposent d'alternatives car ils peuvent choisir d'autres routes. La valeur de la classe de discrimination maximale est 15. Plage de valeurs : 1 à 15
Avertissement	Si la voie de communication principale de la table de routages est occupée, LCR choisit la voie de communication suivante (et éventuellement plus onéreuse) configurée dans le tableau. Cela peut être signalé à l'utilisateur par un signal acoustique et/ou optique. Plage de valeurs : néant, son, écran, écran + son
Passerelle dédiée	Le paramètre définit la manière dont le noeud du partenaire de destination est identifié dans une interconnexion de réseaux IP. Plage de valeurs : non, forcée, multi emplacement
Passerelle dédiée : **Non**	Le noeud partenaire est identifié à partir du numéro de destination.
Passerelle dédiée : **Forcé**	L'acheminement est réalisé nécessairement vers la passerelle qui, dans la colonne **ID noeud Passerelle**, est identifié par son ID de noeud.
Passerelle dédiée : **Multi-emplacement**	Détermination du noeud partenaire selon appelant : l'acheminement a lieu vers la passerelle qui a été affectée à l'appelant correspondant à l'aide de l'assistant Multigateway ou dans le masque de saisie **Abonnés** > **Modifier les données du poste de travail** > **ClientID du système secondaire**. Pour les appelants sans entrée correspondante, l'acheminement est réalisé vers la passerelle qui, dans la colonne **ID nœud Passerelle**, est identifié par son ID de nœud (par défaut).
ID nœud Passerelle	Indication de l'ID de nœud Passerelle pour la sélection **Forcée** ou **multi emplacement** du paramètre **Passerelle dédiée**.
Boutons	
Flèche bleue dans la colonne **Règle de numérotation**	Affiche la page avec les paramètres **Règle de numérotation**.

27.3.5.5 Règle de numérotation > LCR

Description des paramètres de l'onglet :

- **Modifier la règle de numérotation**

Paramètres	Description
	Les règles de numérotation LCR permettent de convertir les numéros d'appel entrés en de nouvelles séquences de chiffres aléatoires pour un traitement supplémentaire. La conversion des chiffres permet d'accéder à divers opérateurs. La règle de numérotation utilisée est déterminée par l'entrée dans la table de routage.
Nom de la règle	Nom librement défini de la règle de numérotation, certaines règles de numérotation sont prédéfinies Plage de valeurs : 16 caractères maxi.
Format de la règle de numérotation	Programme pour les chiffres à sélectionner Les différentes étapes du programme sont traitées de gauche à droite. Les caractères du code de programme correspondent aux fonctions suivantes :
A	Répéter les champs restants (envoyer). "A" provoque l'émission de tous les champs de chiffres suivants. Le point de référence est le dernier séparateur de champs dans le champ Chiffres composés dans le plan de numérotation. Si "A" est inscrit sans référence explicite, cela correspond à tous les chiffres qui suivent le code d'accès, c.-à-d. que "A" correspond à "E2A"
B	Utilisé pour la mise en réseau multi passerelle lorsque le numéro appelé de l'extérieur est du type TON (type de numéro) "unknown" afin d'assurer le routage vers le noeud multi passerelle. Afin que ce numéro de téléphone soit univoque, il est complété en National ou International conformément au type TON dans LCR. Cela est nécessaire lorsque les n° SDA ne sont pas univoques et doivent être configurés au format national ou international.
D (n)	composer une séquence de chiffres (1 à 25 chiffres). "D" peut apparaître plusieurs fois, en un endroit quelconque, dans la chaîne de caractères.
E (n)	Expédition du contenu du champ (1 à 10). "E" peut apparaître plusieurs fois, en un endroit quelconque, dans la chaîne de caractères. La position de "E" par rapport à (n) est libre. Un champ spécifique peut être appelé plusieurs fois, y compris successivement. "E" peut, à l'exception de "E1" (Access Code) est intégré dans d'autres paramètres quelconques. En numérotation par chevauchement (par opposition à la numérotation par blocs), le dernier élément de la règle de numérotation ne doit pas être E(n) mais E(n)A.
M (n)	code d'autorisation (1 à 16). Cette lettre ne doit pas se trouver en dernière position.
P (n)	P (n) peut être présent plus d'une fois dans la séquence et placé dans n'importe quelle position. P (n) peut être entouré par n'importe quel autre paramètre (1 à 60 fois l'unité de pause de l'ensemble du système).
S	Switch, commutation du type de numérotation de DC à DTMF (avec CONNECT, PROGRESS ou CALL PROC avec PI). "S" ne doit apparaître qu'une seule fois dans la chaîne de caractères, et ne doit pas se trouver en dernière position. Après "S", on ne doit plus utiliser le paramètre "C".

Paramètres	Description
C	"C" ne doit apparaître qu'une seule fois dans la chaîne de caractères. Les caractères suivants sont envoyés sans pause interchiffre et utilisés pour l'accès à l'opérateur pour les modes "Single Stage", "Two Stage", "DICS" et "PRI".
U	utilisation du type de numérotation Adresse SUB. "U" ne doit apparaître qu'une seule fois dans la chaîne de caractères et ne doit pas se trouver en dernière position. Les paramètres "S", "P", "M" et "C" ne doivent pas être utilisés après "U".
N (n) (uniquement pour les Etats-Unis!)	groupe SFG de réseau (1 à 5) ou numéro de bande (1).
L (uniquement pour les Etats-Unis!) :	"L" ne peut apparaître qu'à la fin de la séquence de caractères. "L" fait que l'appel est traité comme un appel d'urgence.
Type d'accès de l'opérateur réseau	Sélection de l'opérateur réseau concerné
Inconnu(e)	Aucune indication explicite sur un opérateur.
Fournisseur réseau principal	En cas de prise via l'opérateur principal, la sélection simple se fait par numérotation par blocs ou par la sélection de chiffres individuels dans le réseau public.
MCL Single Stage	Avec MCL Single Stage, l'opérateur souhaité est sélectionné à l'aide d'un préfixe puis le numéro est composé. La sélection est effectuée pour le RNIS dans le canal D ou bien sous forme de numérotation normale sur LR.
MCL Two Stage	Avec MCL Two Stage, l'opérateur souhaité est sélectionné à l'aide d'un préfixe. Après une phase de synchronisation, il est tout d'abord envoyé, sous forme de caractères DTMF, le code d'autorisation (également configurable) puis le numéro de destination. Pour la synchronisation par le temps, une pause comprise entre 2 et 12 s doit être programmée.
Réseau d'entreprise	Un réseau d'entreprise est directement raccordé à OpenScape Business. La fonction LCR détermine à partir du numéro composé par l'abonné la faisceau correspondant et achemine la communication soit via le faisceau du réseau public soit via le faisceau du réseau de l'entreprise.
Serveur de contrôle de numérotation	Dans ce type de LCR, l'opérateur souhaité est sélectionné avec un préfixe à l'aide d'un serveur DICS (Dial-In Control Server) ; le numéro d'appel et un code d'autorisation configurable sont transmis dans la sous-adresse. La sélection est opérée dans le canal D.
Primary Rate Interface (interface primaire) (Seulement pour Etats-Unis)	Avec l'interface primaire, la sélection de l'opérateur ou du Calling Service intervient dans le message de SETUP avec les éléments d'information Network Specific Facility, Operator System Access et Transit Network Selection.
Type	Type of Number [TON] ; ici il est possible pour chaque règle de numérotation de sélectionner dans la liste déroulante les types suivants de "Numéro de l'abonné appelé" : numéro de l'installation, indicatif du réseau local, indicatif national. L'entrée par défaut est "Inconnu". Le Type of Number est uniquement placé avec E.164, dans une mise en réseau ce paramètre est réglé sur "inconnu".

27.3.5.6 LCR > Multisite

Description des paramètres de l'onglet :

- **Modifier une plage**

Paramètres	Description
Préfixe du réseau local	Entrée de l'indicatif local du site (y compris zéro à gauche, par ex. `069` pour Francfort et `030` pour Berlin). Il est possible d'inscrire des préfixes locaux différents ou identiques.
Plage	Entrée du nom pour un site (par ex. les villes `Francfort` et `Berlin` correspondant aux préfixes locaux ou, lorsque les préfixes locaux sont les mêmes, les désignations de département `Service` et `Distribution`).
Route dédiée	Sélection du faisceau ou de l'enregistrement ITSP pour ce site.
Effacer	Supprime les entrées de site marquées.
Boutons	
Sauvegarder	Enregistre les modifications.

Description des paramètres de l'onglet :

- **Modifier abonnés/groupes**

Paramètres	Description
Plage	Sélection du site pour l'abonné ou pour le groupe.
Route dédiée	Sélection du faisceau ou de l'enregistrement ITSP pour l'abonné ou pour le groupe.
Rechercher	Recherche d'abonnés et de groupes ; pour cela, entrer le terme de recherche dans les champs de recherche **Numéro**, **SDA** ou **Nom**, puis appuyer sur la touche Retour. Tous les abonnés et groupes sont listés lorsque tous les champs de recherche sont vides et que vous appuyez ensuite sur la touche Retour. A l'aide de la sélection **Type**, il est possible d'afficher tous les types d'abonnés (par ex. **Clients SIP** ou **Clients TFA**).

27.3.6 Passerelle vocale

Le menu **Passerelle vocale** regroupe les fonctions pour la téléphonie IP.

27.3.6.1 Passerelle vocale > Paramètres SIP

Description des paramètres des onglets :

- **Modifier les paramètres SIP**

Paramètres	Description
Protocole de transport SIP	

Paramètres	Description
SIP via TCP	TCP (Transmission Control Protocol) TCP est un protocole de transport obligatoire pour SIP et il ne peut pas être désactivé ici.
SIP via UDP	UDP (User Datagram Protocol) UDP est le protocole de transport par défaut pour SIP, mais il peut être désactivé lorsqu'aucun point terminal, aucune jonction ou ITSP ne l'utilise. Il est fortement recommandé de le laisser actif.
SIP via TLS	TLS (Transport Layer Security) TLS est le protocole de transport sécurisé pour SIP et il ne peut pas être désactivé ici.
Registrar SIP	
Durée d'enregistrement (s)	L'intervalle (en secondes) auquel l'enregistrement d'un point terminal SIP doit être répété. La valeur de l'intervalle ne doit pas être trop élevée car l'enregistrement est utilisé pour déterminer si un point terminal est hors service. (La période d'enregistrement pour les jonctions ITSP est configurée dans les profils ITSP). Plage de valeurs, valeur par défaut : 10 - 86400, 120
RFC 3261 Valeurs d'horloge	
Délai d'expiration de transaction (ms)	Indique le temps d'attente (en millisecondes)avant nouvelle transmission d'une réponse Invite pour la source de temps de la spécification RFC 3261. Ce paramétrage concerne la transaction Client Invite. Plage de valeurs, valeur par défaut : 2000 - 64000, 32000
Temporisation de session SIP	
Utiliser RFC 4028	RFC 4028 définit une extension du protocole SIP (Session Initiation Protocol). Cette extension autorise une actualisation périodique des sessions SIP. Les agents utilisateur et les proxys peuvent utiliser l'actualisation pour déterminer si la session SIP est toujours active ou non. L'option de configuration ici est utilisée pour contrôler l'actualisation de la session sur l'interface de jonction (pour les ITSP, voir le profil correspondant).
Expirations de session (s)	Définit la durée d'un intervalle de session SIP. La valeur par défaut est "1800". La valeur configurée est utilisée pour les interfaces de jonction et ITSP. Plage de valeurs, valeur par défaut : 90 - 65535, 1800
SE minimum (s)	Définit la durée minimale autorisée d'un intervalle de session SIP. La valeur configurée est utilisée pour les interfaces de jonction et ITSP. Plage de valeurs, valeur par défaut : 90 - 65535, 90
DNS-Enregistrements	
Blocage heure pour destination(s) non joignable(s)	Cette temporisation est utilisée pour contrôler la liste noire de la pile SIP. Si un serveur SIP réglé par DNS n'est pas joignable, il sera bloqué pendant la durée choisie ici. La valeur par défaut est 60 secondes. Dans les cas où des serveurs redondants sont utilisés (par exemples des résultats DNS au sein de plusieurs serveurs), une valeur plus élevée est recommandée (par exemple 900).
Appels du fournisseur	

Paramètres	Description
Appels possibles au maximum par le fournisseur	Le nombre des communications simultanées via tous les fournisseurs activés est affiché ici. Cette valeur est configurée durant l'installation en fonction de la bande passante disponible et de la configuration de ITSP.

27.3.6.2 Passerelle vocale > Urgence SIP

Description des paramètres des onglets :

- Ajouter les informations de localisation d'urgence SIP

  L'information de localisation d'urgence SIP est utilisée dans le protocole SIP pour informer le destinataire d'un appel d'urgence de l'origine géographique de l'appel. Dans le protocole SIP, le format des informations d'identification de localisation est défini par les RFC4119 et RFC5139 (objet Location codé XML dans le corps MIME). Le protocole SIP Emergency permet de définir tous les champs définis dans les RFC pertinentes, alors que dans votre déploiement spécifique, seule une partie de ces données doit être configurée (par exemple, en Suisse, seul le champ NAM est utilisé pour définir un emplacement).
- Emplacement codé XML dans le corps MIME (RFC4119 et RFC5139)

  L'option actuelle ne nécessite de configuration que dans l'onglet **Ajouter un emplacement** . Les données nécessaires à la définition d'un emplacement sont fournies par votre fournisseur de services de téléphonie sur IP (ITSP).

Paramètres	Description
Nom d'identification de localisation	Le nom de l'identifiant de localisation.
Pays	Le pays est identifié par le code ISO 3166 à deux lettres.
A1	subdivisions nationales (État, région, province, préfecture)
A2	Comté, paroisse, arme à feu, district
A3	Ville, canton, shi
A4	division de la ville, arrondissement, district de la ville, quartier, chou
A5	Quartier, pâté de maisons
A6	Rue
PRD	Direction de la rue principale
COSSE	suffixe de rue final
STS	suffixe de rue
HNO	Numéro de maison, partie numérique seulement
HNS	suffixe du numéro de maison
LMK	Adresse emblématique ou adresse de prestige
LOC	Informations complémentaires sur l'emplacement
FLR	Sol

Paramètres	Description
NAM	Nom (occupant du domicile, de l'entreprise ou du bureau).
PC	Code Postal
CHAMBRE	Chambre
PLC	Lieu - type
PCN	Nom de la communauté postale
BOÎTE POSTALE	boîte postale
AJOUTER LE CODE	Code supplémentaire
SIÈGE	Siège (bureau, box, poste de travail)
RD	Route ou rue principale
RDSEC	Section de route
RDBR	Branche routière
RDSUBBR	sous-branche routière
PRM	Pré-modificateur de route
POM	Post-modificateur de route
Activer les paramètres avancés	Une fois activés, les champs de paramètres avancés peuvent être configurés.
BLD	Bâtiment (structure)
UNITÉ	Unité (appartement, suite)

- Numéro virtuel d'urgence (Belgique)

  Pour le fournisseur **Proximus** uniquement, l'option choisie est **Numéro virtuel d'urgence (Belgique)** . L'option actuelle nécessite une configuration dans l'onglet **Configuration générale** et dans l'onglet **Ajouter un emplacement** . Les données nécessaires à la définition d'un emplacement sont fournies par votre fournisseur de services de téléphonie sur IP (ITSP).

Paramètres de configuration générale	Description
Protocole d'identification de localisation d'urgence	Options : • Aucun identifiant de localisation • Dans From, PAI et PPI • Dans le cadre des PAI et PPI
Protocole d'identification des municipalités	Options : • Aucun identifiant de municipalité • Ajouter l'identifiant de la municipalité au numéro appelé
Code d'accès d'urgence	Nombre à 4 chiffres (ex. 1992)

Ajouter des paramètres de localisation	Description
Nom du lieu	Le nom de l'identifiant de localisation

Ajouter des paramètres de localisation	Description
Numéro virtuel d'urgence	Fourni par votre fournisseur de services de téléphonie sur IP
Identifiant de la municipalité	Code Postal

Remarque :

En cas **d'urgence SIP** , un emplacement **de site principal** par défaut doit être configuré. Il s'agit de l'emplacement système attribué automatiquement aux périphériques à emplacement statique.

27.3.6.3 Paramètres du codec > de la passerelle vocale

Description des paramètres des onglets :

- **Modifier les paramètres du codec**

Paramètres	Description
Codec	Les paramètres des codecs G.711 A-law, G.711 µ-law, G.729A et G.729AB peuvent être modifiés.
Codec : G.711 A-law	G.711 (loi A et loi µ) : encodage vocal à 56 ou 64 Kbps - très haute qualité vocale. La norme G.711 est également utilisée dans les réseaux fixes (ISDN). La méthode A-law est une technique de numérisation principalement utilisée en Europe pour les signaux audio analogiques dans le secteur des télécommunications.
Codec : G.711 µ-law	G.711 (loi A et loi µ) : encodage vocal à 56 ou 64 Kbps - très haute qualité vocale. La norme G.711 est également utilisée dans les réseaux fixes (ISDN). En Amérique du Nord et au Japon, on utilise la méthode de la loi µ, similaire à la loi A, mais non compatible. Pour communiquer, par exemple lors d'une conversation téléphonique entre l'Europe et les États-Unis, les données numériques doivent être traduites par des convertisseurs appropriés.
Codec : G.729A	Encodage vocal à 8 Kbps.
Codec : G.729AB	Encodage vocal à 8 Kbps. Les silences étaient comblés par des bruits de fond apaisants.
Priorité	Les codecs audio peuvent se voir attribuer des priorités entre 1 (élevée) et 4 (faible). La communication tente automatiquement d'utiliser le codec audio ayant la priorité la plus élevée disponible pour chaque connexion. L'utilisation d'un codec audio avec une faible compression vocale (bonne qualité vocale) augmente la charge du réseau. Dans le cas d'une téléphonie IP intensive, cela peut entraîner une diminution de la qualité vocale sur un réseau déjà surchargé par les transferts de données.
Détection d'activité vocale	Activer la détection d'activité vocale (VAD). Cela peut réduire la charge du réseau pendant les longues pauses vocales.

Paramètres	Description
Taille du cadre	Vous pouvez spécifier une taille de trame (taille de paquet IP) de 10 à 90 ms pour chaque codec. Ceci spécifie la fréquence d'échantillonnage à laquelle le codec audio divise le signal vocal en paquets IP. Bien qu'une valeur plus élevée (90 ms, par exemple) permette une meilleure relation entre la charge utile et la surcharge du paquet IP, elle augmente également le délai de transfert. Les valeurs ajustables dépendent des codecs. Pour la mise en réseau d'OpenScape Business avec OpenScape Voice via SIP-Q V2 : Cordless IP et OpenScape Mobile Connect ne prennent en charge qu'une taille de trame de 20 ms pour le codec G.711. Si l'un de ces deux produits est présent dans l'interconnexion, la taille de la trame doit être de 20 ms ici. Plage de valeurs, valeur par défaut : 10 - max. 90, 20
Canaux DSP améliorés	
Utilisez uniquement le G.711	Seuls les protocoles G.711 A-law et G.711 µ-law sont utilisés. Avec le G.711, moins de ressources DSP sont nécessaires, ce qui permet d'effectuer davantage d'appels simultanés.
T.38 Fax	
T.38 Fax	Définit si le protocole de télécopie T.38 doit être utilisé ou non. Pour les systèmes avec carte Booster et/ou serveur Booster : lorsque cette option est activée, la correction d'erreurs est effectuée dans le protocole T.38. Une fenêtre contextuelle s'affiche pour informer l'utilisateur qu'un redémarrage manuel du système est nécessaire.
Utiliser FillBitRemoval	Définit si les bits de remplissage doivent être supprimés lors de l'envoi et restaurés lors de la réception lors de l'utilisation du protocole de télécopie T.38. Cela permet d'économiser de la bande passante.
Max. Taille des datagrammes UDP pour la télécopie T.38 (octets)	Indique la taille maximale d'un datagramme UDP T.38 en octets. Plage de valeurs, valeur par défaut : 1 - 1472, 1472
Correction d'erreurs utilisée pour le fax T.38 (UDP)	Définit la méthode à utiliser pour la correction des erreurs. Valeurs : t38UDPFEC, t38UDPRedundancy Pour les systèmes avec carte Booster et/ou serveur Booster : lorsqu'une option est sélectionnée, une fenêtre contextuelle s'affiche pour informer l'utilisateur qu'un redémarrage manuel du système est nécessaire. Valeur par défaut : t38UDPRedundancy
T.30 Fax	
Activer le ECM	Pour les systèmes avec carte Booster et/ou serveur Booster : lorsque ce drapeau est activé, la correction d'erreurs est effectuée dans le protocole T.30. Une fenêtre contextuelle s'affiche pour informer l'utilisateur qu'un redémarrage manuel du système est nécessaire. Valeur par défaut : activé

Paramètres	Description
mode de compatibilité VoIP	Pour les systèmes avec carte Booster et/ou serveur Booster : cette option doit être activée si vous rencontrez des problèmes de transmission de fax sur les réseaux VoIP. Une fenêtre contextuelle s'affiche pour informer l'utilisateur qu'un redémarrage manuel du système est nécessaire. Valeur par défaut : désactivé
Divers	
ClearChannel	Un ClearChannel est un canal ouvert dans lequel les points d'extrémité sont responsables du protocole utilisé sur le canal. Ce paramètre détermine si la fonctionnalité d'interface ClearChannel doit être activée ou non.
Taille du cadre	Vous pouvez définir la fréquence d'échantillonnage dans ce champ. Les réglages possibles sont 10, 20, 30, 40, 50 et 60 millisecondes (ms). Plage de valeurs, valeur par défaut : 10 - 60, 20
RFC2833 La RFC2833 définit comment les signaux de tonalité sont transmis.	
Transmission des tonalités de fax/modem conformément à la RFC2833	Transmission hors bande (via signalisation SIP) ; mode de fonctionnement recommandé pour transmettre les tonalités en toute sécurité
Transmission des tonalités DTMF conformément à la RFC2833	Transmission hors bande (via signalisation SIP) ; mode de fonctionnement recommandé pour transmettre les tonalités en toute sécurité
Type de charge utile pour RFC2833	Une adaptation peut être nécessaire, selon le partenaire de communication. Plage de valeurs, valeur par défaut : 96 - 126, 98
Transmission redondante des tonalités RFC2833 conformément à la RFC2198	Contribue à améliorer la fiabilité de la transmission

27.3.6.4 Passerelle vocale > Paramètres du codec de destination

Pour certains partenaires de communication, il est possible de définir des priorités pour l'utilisation du codec audio.

Description des paramètres des onglets :

- **Ajouter les paramètres de codec de destination**

Paramètres	Description
Codec : G.711 loi A	G.711 (Loi A et Loi µ) : codage de la voix à 56 ou 64 kbit/s - très bonne qualité vocale. G.711 est utilisé dans le secteur du réseau fixe (RNIS). La loi A est une procédure de numérisation utilisée en priorité en Europe pour les signaux audio analogiques dans le secteur des télécommunications.

Paramètres	Description
Codec : G.711 loi µ	G.711 (Loi A et Loi µ) : codage de la voix à 56 ou 64 kbit/s - très bonne qualité vocale. G.711 est utilisé dans le secteur du réseau fixe (RNIS). En Amérique du Nord et au Japon, il est utilisé la procédure de la loi µ, similaire à la loi A, mais incompatible. Pour la communication, par ex.lors d'une communication téléphonique entre l'Europe et les Etats-Unis, il faut que les données numériques soient traitées par un convertisseur adapté.
Codec : G.729A	Codage de la voix à 8 kbit/s.
Codec : G.729AB	Codage de la voix à 8 kbit/s. Remplissage des pauses de la voix par un bruit de confort.
Priorité	Il est possible d'attribuer aux codecs audio des propriétés de 1 (élevée) à 4 (basse). Le système de communication essaie automatiquement, pour chaque liaison, d'utiliser un codec audio avec une priorité aussi élevée que possible. Lorsque l'on utilise un codec audio à faible compression de la voix (bonne qualité vocale), la charge pour le réseau est plus élevée. Dans le cadre d'une téléphonie IP intensive, cela peut se traduire par une détérioration de la qualité de la voix lorsque le réseau est déjà surchargé en raison du transfert de données.
Destination	
Type d'adresse de destination	Affichage du type de destination auquel est affectée la priorité du codec audio réglée.
Adresse IP	Adresse IP de la destination à laquelle doivent s'appliquer les priorités des codecs audios définies (par ex. noeud en réseau, serveur SIP)

27.3.6.5 Passerelle vocale > Fournisseur de services de téléphonie Internet

Description des paramètres des onglets :

- **Ajouter un fournisseur de services de téléphonie Internet**
- **Modifier le fournisseur de services de téléphonie Internet**
- **Supprimer le fournisseur de services de téléphonie par Internet**

Paramètres	Description
Modèle de base	Sélection d'un modèle vide (par défaut) ou d'une configuration d'exemple prédéfinie pour un fournisseur de services particulier. Cela peut être adapté aux besoins individuels et enregistré en tant que nouveau fournisseur de services informatiques (ITSP).
Nom du fournisseur	Nom souhaité du fournisseur de services de télécommunications (ITSP). Le fournisseur de services de télécommunications (ITSP) configuré apparaîtra dans la liste des ITSP sous ce nom.
Activer le fournisseur	Le fournisseur de services de téléphonie sur IP (ITSP) est activé.
Identifiant du fournisseur dans le système	Attribution d'une désignation unique au sein du système. Un maximum de 8 fournisseurs de services de télécommunications (ITSP) peuvent être actifs simultanément. Fourchette de prix : Fournisseurs 1 à 8

Paramètres	Description
Nom de domaine	Nom de domaine de la passerelle du fournisseur de services de téléphonie sur IP (ITSP) : souvent différent du nom de domaine web.
Protocole de transport	Protocole de transport souhaité. Vous pouvez sélectionner UDP ou TCP.
Sécurité des transports	Les valeurs possibles sont **traditionnelles (udp ou tcp)** pour un appel traditionnel utilisant udp/tcp ou **sécurisées (tls).** pour un appel sécurisé utilisant TLS. Valeur par défaut : **traditionnel (udp ou tcp)**
Sécurité des médias	Les valeurs possibles sont **RTP uniquement** (seul le profil AVP est pris en charge) ou **SDES uniquement** (seul le profil SAVP est pris en charge). Valeur par défaut : **RTP uniquement**
Registre des fournisseurs	
Utiliser le registraire	Doit être sélectionné si le coffre fonctionne avec l'enregistrement (par défaut = désactivé).
Adresse IP / Nom d'hôte	Nom d'hôte ou adresse IP du serveur d'enregistrement externe.
Port	Numéro de port du serveur d'enregistrement externe, par exemple 5060. Saisissez le port 00 si le fournisseur de services de téléphonie sur IP utilise DNSSRV.
Intervalle de réinscription chez le fournisseur (s)	Intervalle (en secondes) auquel l'enregistrement ITSP est répété. La valeur de l'intervalle ne doit pas être égale à 0 et ne doit pas être trop élevée car, lors de la répétition de l'enregistrement auprès du fournisseur de services de télécommunications, une coupure de connexion peut également être détectée et un autre itinéraire (via ISDN ou un autre fournisseur) peut être sélectionné si nécessaire. Valeur par défaut : 120 secondes
Proxy du fournisseur	
Adresse IP / Nom d'hôte	Nom de domaine ou adresse IP du serveur proxy (par exemple, sip-voice.de). L'inscription est obligatoire et est généralement identique à celle figurant dans le registre des fournisseurs.
Port	Numéro de port du serveur proxy (ex. : 5060). En règle générale, cela correspond au numéro de port du fournisseur. Saisissez le port 0 si le fournisseur de services de téléphonie sur IP utilise plusieurs serveurs et DNSSRV.
Proxy sortant du fournisseur	
Utiliser un proxy sortant	N'activez cette fonction que si le fournisseur de services de téléphonie sur IP utilise un proxy sortant différent du proxy du fournisseur. Désactivé par défaut.
Adresse IP / Nom d'hôte	Nom de domaine ou adresse IP du proxy sortant.
Port	Numéro de port du proxy sortant. Saisissez le port 0 si le fournisseur de services de téléphonie sur IP utilise plusieurs serveurs et DNSSRV.

Paramètres	Description
Proxy entrant du fournisseur	
Utiliser un proxy entrant	À configurer uniquement si le fournisseur de services de messagerie (ITSP) envoie éventuellement des requêtes depuis un deuxième serveur. Désactivé par défaut.
Adresse IP / Nom d'hôte	Nom de domaine ou adresse IP du deuxième serveur ITSP
Port	Numéro de port du deuxième serveur ITSP. Saisissez le port 0 si le fournisseur de services de téléphonie sur IP utilise DNSSRV.
Fournisseur STUN	
Utilisez STUN	À configurer uniquement si le fournisseur de services de téléphonie sur IP utilise un serveur STUN. Le paramètre système global sous la configuration STUN s'applique comme mode STUN pour tous les fournisseurs de services de télécommunications (par défaut = désactivé).
Adresse IP / Nom d'hôte	Nom d'hôte ou adresse IP du serveur STUN.
Port	Numéro de port STUN du serveur STUN.
Données étendues du fournisseur SIP	
Afficher les données étendues du fournisseur SIP	L'activation de cette option permet d'accéder à des paramètres de configuration supplémentaires pour contrôler la pile SIP et adapter le contenu des champs d'en-tête SIP.
CLIP / CLIR	Le système offre différents paramètres pour contrôler le format des champs d'en-tête SIP en fonction des besoins du trunk natif. Le contenu des champs d'en-tête suivants, qui décrivent la source d'un appel, peut être contrôlé : • De : DisplayPart <sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>
CLIP sortant dans En-tête - partie d'affichage	Paramètres possibles : • Omettre - le champ est omis • Indicatif d'appel - le numéro configuré pour une station. Vous pouvez définir quel numéro est utilisé dans les « paramètres d'itinéraire ». • Compte - le nom d'utilisateur attribué au tronc natif • nom d'affichage
CLIP sortant dans l'en-tête From - partie utilisateur :	Paramètres possibles : • Numéro d'appel • Compte

Paramètres	Description
En-tête sortant - partie domaine/ hôte :	Modifiez la partie domaine/hôte de l'URI pour qu'elle corresponde à l'adresse IP du système. Ce paramètre affecte la partie hôte des trois champs d'en-tête : From:, PAI et PPI. Paramètres possibles : • Nom de domaine • Adresse IP locale • Adresse IP publique
Déviation : L'expéditeur contient le numéro d'appelant d'origine :	Si un appel sortant est établi grâce au renvoi d'appel, le système peut fournir des informations sur l'appelant initial. Si cette option est activée, le système envoie le nom de l'appelant d'origine (A-Ext) dans le champ d'en-tête From:, sinon il envoie le numéro de la station de transfert.
Détournement : PAI contient le numéro d'appelant d'origine	Si un appel sortant est établi grâce au renvoi d'appel, le système peut fournir des informations sur l'appelant initial. Si cette option est activée, le système envoie le nom de l'appelant d'origine (A-Ext) dans le champ d'en-tête P-Asserted-Id, sinon il envoie le numéro de la station de transfert. En activant cette option, le système envoie l'identifiant de l'appelant d'origine dans les champs d'en-tête P-Asserted_ID: et P-Preferred-ID:.
CLIP sortant dans l'en-tête P-Asserted-Id - partie affichage :	Paramètres possibles : • Omettre - le champ est omis • Indicatif d'appel - le numéro configuré pour une station. Vous pouvez définir quel numéro est utilisé dans les « paramètres d'itinéraire ». • Compte - le nom d'utilisateur attribué au tronc natif • nom d'affichage
CLIP sortant dans l'en-tête P-Asserted-Id - partie utilisateur :	Paramètres possibles : • Omettre - le champ est omis • Numéro d'appel • Compte
CLIP sortant dans l'en-tête P-Preferred-Id - partie affichage :	Paramètres possibles : • Omettre - le champ est omis • Indicatif d'appel - le numéro configuré pour une station. Vous pouvez définir quel numéro est utilisé dans les « paramètres d'itinéraire ». • Compte - le nom d'utilisateur attribué au tronc natif • nom d'affichage
CLIP sortant dans l'en-tête P-Preferred-Id - partie utilisateur :	Paramètres possibles : • Omettre - le champ est omis • Numéro d'appel • Compte

Paramètres	Description
CLIP sortant dans l'en-tête Diversion - partie affichage :	Paramètres possibles : • Omettre - le champ est omis • Indicatif d'appel - le numéro configuré pour une station. Vous pouvez définir quel numéro est utilisé dans les « paramètres d'itinéraire ». • Compte - le nom d'utilisateur attribué au tronc natif • nom d'affichage
CLIP sortant dans l'en-tête Diversion - partie utilisateur :	Paramètres possibles : • Omettre - le champ est omis • Numéro d'appel • Compte
CLIP sortant dans l'en-tête History-Info - partie utilisateur :	Paramètres possibles : • omettre • numéro d'appel
En-tête CLIR sortant - partie affichage :	Paramètres possibles : • Omettre • Numéro d'appel • Compte • **De la part d'Anonyme <sip: ...@...>**
En-tête CLIR sortant - partie utilisateur :	Paramètres possibles : • Numéro d'appel • Compte • Entièrement anonyme **De : ...<sip:anonymous@anonymous.invalid>** • Utilisateur anonyme **De : ... <sip:anonymous@...>**
En-tête de confidentialité sortant CLIR	Paramètres possibles : • Omettre • Identifiant **Confidentialité : identifiant** • Utilisateur **Confidentialité : utilisateur** • ID de l'utilisateur **Confidentialité : utilisateur ; identifiant**
Prise en charge COLP/TIP pour les appels sortants :	En ISDN, la fonction COLP (Connect Line Identification Presentation) a été introduite. Dans le protocole SIP, cette fonctionnalité est parfois appelée TIP (Termination Identification Presentation). RFD3324 (section 5.) définit un mécanisme pour transporter l'identité de la partie acceptante (C) dans le champ d'en-tête P-Asserted-Identity de la réponse 200 OK : Paramètres possibles : • COLP a soutenu • COLP non pris en charge
formatage de la cote	

Paramètres	Description
Appel entrant - Numéro de l'appelé :	Ce drapeau fait référence à l'adresse de destination d'un appel. Par défaut, cette valeur est extraite de la **partie utilisateur** du champ **d'en-tête À :** . Paramètres possibles : • Ligne de demande **INVITE sip : +498970070@...** • Pour afficher l'en-tête **À : +498970070 <sip:+** • En-tête de la partie utilisateur **À : <sip: +498970070@...** • partie d'affichage de l'en-tête P-Called-Party-Id **ID de l'appelant : +498970070 <sip:..** • En-tête P-Called-Party-Id partie utilisateur **ID de l'appelant : <sip : +498970070@..**
Appel entrant - Numéro de l'appelant :	Cet indicateur fait référence à l'adresse source d'un appel. Par défaut, le système retire l'appelant de la partie utilisateur de l'en-tête From. Paramètres possibles : • automatique • À partir de la partie d'affichage de l'en-tête **De : +498970070 <sip:+** • Partie utilisateur de l'en-tête **De : <sip: +498970070@...** • partie d'affichage de l'en-tête P-Asserted-Id **P-Asserted-ID: +498970070 <sip:..** • En-tête P-Asserted-Id partie utilisateur **P-Asserted-ID: <sip: +498970070@..** En mode automatique, le système effectue d'abord une recherche dans la partie utilisateur de l'identifiant P-Asserted-Identity, si elle est présente. Si l'en-tête P-Asserted-Identity est absent, c'est la partie utilisateur du champ d'en-tête From qui est prise en compte.
Appel entrant - Type de numéro (appelant) :	Paramètres possibles : • automatique • international
Appel entrant - Type de numéro (appelé) :	Paramètres possibles : • automatique • international • national

Paramètres	Description
Appel sortant - Type de numéro (appelant) :	Paramètres possibles : • automatique • international • national
Appel sortant - Type de numéro (appelé) :	Paramètres possibles : • automatique • international • national
Correspondance du numéro de fournisseur :	Paramètres possibles : • dans tous les cas • Appels entrants uniquement (si configuré) • désactivé
CLIP sans prise en charge du dépistage :	Paramètres possibles : • non pris en charge • CLIP dans From / numéro de confiance dans PAI • Prise en charge – Aucun traitement spécial • CLIP dans From / Numéro DID dans PAI
Numéro d'appel avec préfixe international/national :	Paramètres possibles : • Non • Oui
Numéro appelé au format E164 :	Paramètres possibles : • Non • Oui
Optimisation de l'itinéraire :	Paramètres possibles : • non autorisé • autorisé • autorisé (adresse IP locale dans le contact)
MEX pris en charge :	Paramètres possibles : • Non • Oui
L'URI de contact contient :	Ce paramètre est utilisé pour configurer le contenu de la partie utilisateur de l'URI de contact. **Contact : sip:UserPart@HostPart:port** Paramètres possibles : • Numéro d'appel : la partie utilisateur de l'URI Contact contient le numéro d'appel • AOR d'enregistrement : l'URI de contact contient la partie account=user de l'enregistrement.

Paramètres	Description
Port TCP utilisé dans l'URI de contact :	Ce paramètre sert à configurer le port TCP utilisé dans la partie hôte de l'URI de contact. **Contact : sip:UserPart@HostPart:port** Paramètres possibles : • ephem.src-port : Par défaut, le port source TCP éphémère est utilisé. • Port du serveur SIP : Le port du serveur SIP est utilisé dans l'URI de contact
Inscription	
L'adresse IP du contact enregistré est incluse :	Paramètres possibles : • adresseIP locale • nom de domaine
ContactUriWithProtocol :	activer/désactiver
Enregistrement BNC (SIPconnect) :	Paramètres possibles : • inscription normale • Inscription au BNC
Intervalle de réenregistrement après échec (s) :	
Mode de réenregistrement :	Paramètres possibles : • continu • SIPConnect
Réinscription après un échec d'appel :	Paramètres possibles : • L'échec d'appel n'est pas un échec d'enregistrement • L'échec d'appel est un échec d'enregistrement
Sécurité	
Mode UDP :	Paramètres possibles : • UDP symétrique • UDP asymétrique
Sélection par les pairs approuvée :	Paramètres possibles : • Faire confiance uniquement aux serveurs configurés • Serveurs de confiance reçus dans les réponses SIP
Divers	
Charge utile directe :	Pour une connexion directe avec un fournisseur de services de messagerie (ITSP), ce paramètre DOIT être défini sur false. Si un SBC externe est utilisé devant OpenScape Business, ce paramètre est défini sur vrai.

Paramètres	Description
Éviter la renégociation des médias :	Pour une connexion directe avec un fournisseur de services de messagerie (ITSP), ce paramètre DOIT être défini sur vrai. Si le paramètre de gestion des médias « Charge utile directe » est défini sur « vrai », ce paramètre est sans effet (par exemple, lorsqu'un SBC externe est utilisé devant le système métier OpenScape).
Attribut de changement de direction :	Paramètres possibles : • conserver l'attribut • passer à sendrecv
Attribut de suppression du silence :	Paramètres possibles : • soutenu • non pris en charge
Extension Mediasec :	Paramètres possibles : • soutenu • non pris en charge
Filtre SDP :	Paramètres possibles : • Défaut • Profil de compatibilité • Ouvrir
Utiliser l'authentification URI de la route :	La valeur True définit le comportement d'utilisation de l'URI de route au lieu de l'URI de requête dans l'en-tête d'autorisation (Proxy) pour INVITE ou INFO (pas pour REGISTER). L'URI de requête sera utilisée lorsqu'aucune URI de route n'est présente. Pour les fournisseurs de services de télécommunications (ITSP), ce paramètre DOIT être défini sur vrai.
Ignorer 100 Rel:	Ignorez le champ d'en-tête « Supported: 100rel » s'il est reçu dans l'INVITE. Étant donné que 100rel peut interférer avec l'interfonctionnement avec les abonnés non-SIP, ce paramètre DOIT être défini sur vrai.
Support 100rel	Lorsque cette option est activée, le système ajoutera un en-tête 100rel pris en charge dans l'invitation sortante. Cela permettra au fournisseur de services de télécommunications d'envoyer des réponses provisoires fiables, suivies de messages UPDATE. Ce paramètre est utilisable sans restriction pour la famille de cartes mères et les serveurs OpenScape Business V3.
UtiliserViaRPort :	Si la valeur est définie sur true, le paramètre rport est ajouté à l'en-tête Via. *Via : SIP/2.0/UDP 192.168.138.1:5060 ; rapport ;* Si la valeur est « false », aucun paramètre rport n'est ajouté à l'en-tête Via. *Via : SIP/2.0/UDP 192.168.138.1:5060 ;*

Paramètres	Description
MISE À JOUR Prise en charge :	Si la valeur est « true », la méthode UPDATE est utilisée en fonction du contenu du champ d'en-tête Allow. Si UPDATE n'est pas défini dans le champ d'en-tête Allow reçu, la pile SIP n'envoie jamais de requête UPDATE. Si la valeur est définie sur false, la méthode UPDATE ne sera jamais utilisée (une nouvelle invitation sera utilisée à la place). Pour les fournisseurs de services informatiques (ITSP), ce paramètre DOIT être défini sur vrai (valeur par défaut).
Soutien d'urgence EVN	**Paramètres possibles :** • activé uniquement avec le fournisseur **Proximus** • désactivé chez tout autre fournisseur
Prise en charge de l'en-tête P-Early-Media :	Paramètres possibles : • non pris en charge • soutenu
Prise en charge du minuteur de session :	Paramètres possibles : • inactif • rappel sur la politique de télétravail
Délai d'envoi de la réponse automatique 183 (s) :	Avec cette minuterie, une réponse provisoire (183) est déclenchée après le délai d'attente si aucune information de progression n'est disponible du système. Ceci est nécessaire car certaines plateformes n'arrêtent pas les minuteurs de supervision lorsqu'elles reçoivent un code 100 (par exemple, Broadsoft). Aucune réponse automatique n'est envoyée ; toutes les réponses sont déclenchées par le système. Délai d'attente de 1 à 10 secondes, le minuteur est démarré à la réception d'une requête INVITE de l'ITSP. À l'expiration du délai, une réponse 183 est envoyée par la pile SIP. 0 (par défaut)
UDP-Maintien en vie :	Paramètres possibles : • UdpKeepAliveON • UdpKeepAliveOFF • Options d'envoi en direct
Intervalle de maintien en vie pour OPTIONS (s) :	Ce paramètre définit l'intervalle d'envoi des options SIP. 60 (par défaut)
Échec de la réinscription via OPTIONS :	Paramètres possibles : • NoRegisterOnFailure • Inscription en cas d'échec
Réponse à OPTIONS :	Paramètres possibles : • Réponse complète • Sans corps
Boutons	

Paramètres	Description
Redémarrez le fournisseur de services informatiques (ITSP).	Lance une nouvelle inscription auprès du fournisseur de services de téléphonie sur IP (possible uniquement avec un fournisseur de services de téléphonie sur IP activé).

Description des paramètres des onglets :

- **Modifier la configuration STUN**

Paramètres	Description
Mode STUN	Ce paramètre s'applique globalement à tous les fournisseurs de services de téléphonie sur IP, à condition que STUN soit activé pour eux. La nécessité du protocole STUN dépend de l'infrastructure du fournisseur de services de téléphonie sur IP et du routeur Internet utilisé. STUN n'est pas nécessaire si le fournisseur de services de téléphonie sur IP (ITSP) résout le problème de traversée NAT sur son propre réseau. STUN garantit que l'adresse IP accessible publiquement est utilisée dans les messages SIP au lieu de l'adresse IP interne.
Mode STUN : Toujours	STUN est toujours actif.
Mode STUN : Automatique	Le type NAT du routeur par rapport à Internet est vérifié automatiquement. Si nécessaire, l'étourdissement est activé. Si aucune étourdissement n'est requis ou possible, la fonction STUN est désactivée. Il s'agit du paramètre par défaut recommandé.
Mode STUN : Utiliser une adresse IP statique	Si le fournisseur de services de téléphonie sur IP (ITSP) exige une authentification IP statique, une adresse IP statique (adresse IP publique) est requise dans le modem DSL ou le routeur Internet. L'adresse IP statique et le port doivent également être spécifiés.
Mode STUN : Utiliser une adresse IP statique, une adresse IP publique	Adresse IP statique du modem DSL ou du routeur Internet.
Mode STUN : Utiliser une adresse IP statique et un port SIP public	Port du modem DSL ou du routeur Internet.
Mode STUN : Routeur préservant les ports	Si aucun des modes STUN mentionnés ci-dessus ne fonctionne, essayez ce mode. Certains modems et routeurs Internet ne modifient pas le port RTP pour le NAT et nécessitent ce mode pour fonctionner correctement.
Type NAT détecté	Si un fournisseur de services de messagerie (ITSP) est actif, le type de NAT sera affiché ici.
Serveur STUN par défaut	
Adresse IP / Nom d'hôte	Adresse IP ou nom d'hôte du serveur STUN (par exemple, `stun.serviceprovider.com`). Ce serveur STUN est utilisé pour SIP@Home lorsqu'aucun fournisseur de services de téléphonie sur IP (ITSP) n'est utilisé ou si l'ITSP utilisé ne propose aucun serveur STUN.
Port	Port du serveur STUN (ex. : `3478`)

Description des paramètres des onglets :

- **Détection du type NAT**

Paramètres	Description
Activation automatique	Permet la détection automatique du type NAT.
Démarrage de la détection du type NAT	Lance manuellement la détection du type NAT.

Description des paramètres des onglets :

- **Ajouter une station de téléphonie Internet**
- **Modifier la station de téléphonie Internet**
- **Supprimer la station de téléphonie Internet**

Paramètres	Description
Station de téléphonie Internet	Données d'accès du compte attribué par le fournisseur de services de téléphonie sur IP. Selon le fournisseur de services de téléphonie sur IP (ITSP), différentes désignations sont utilisées à cet effet, par exemple : utilisateur SIP, identifiant SIP, etc. Vous devrez peut-être également saisir ici le numéro de client ITSP. Si l'authentification IP statique est utilisée, le numéro PABX doit être saisi ici.
Nom de l'autorisation	Nom d'autorisation attribué par le fournisseur de services de téléphonie sur IP (ITSP). Cela correspond souvent à l'abonné à la téléphonie par Internet.
Mot de passe	Mot de passe attribué par le fournisseur de services de téléphonie sur IP. Selon le fournisseur de services de téléphonie sur IP (ITSP), différentes appellations sont utilisées à cet effet, par exemple : mot de passe, mot de passe SIP, etc.
Confirmez le mot de passe	Mot de passe attribué par le fournisseur de services de téléphonie sur IP. Selon le fournisseur de services de téléphonie sur IP (ITSP), différentes appellations sont utilisées à cet effet, par exemple : mot de passe, mot de passe SIP, etc.

Description des paramètres des onglets :

- **Ajouter une entrée MSN**
- **Modifier l'entrée MSN**
- **Supprimer l'entrée MSN**
- **Supprimer toutes les entrées MSN**

Paramètres	Description
Numéro de téléphone de téléphonie Internet / **Numéro de téléphone de téléphonie Internet** / **Numéro de téléphone de téléphonie Internet**	(Unique) Numéro d'appel attribué par le fournisseur de services de téléphonie sur IP.
Numéro d'appel interne (**DID**)	Numéro d'appel interne attribué.

Paramètres	Description
Entrée par défaut	L'activation en tant qu'entrée par défaut permet aux utilisateurs qui ne possèdent pas leur propre numéro de téléphone de téléphonie Internet de passer des appels via ce numéro. Cette option est disponible uniquement pour un numéro MSN. (Appels vocaux uniquement, pas de fax)
Station de téléphonie Internet / **Station de téléphonie Internet**	Affiche la station de téléphonie Internet

Description des paramètres des onglets :

- **Ajouter la plage DID**
- **Modifier la plage DID**
- **Supprimer la plage DID**

Paramètres	Description
Numéro PABX	Numéro de tête attribué par le fournisseur de services de téléphonie sur IP (sans le numéro DID)
Bande d'appel direct entrant de … à	Plage de numéros DID attribués par le fournisseur de services de téléphonie sur IP
Début de la plage de numéros d'appel internes	Premier numéro interne à partir duquel une attribution automatique de numéros d'appel est souhaitée.
Attribuer automatiquement la bande d'appel direct entrant aux stations	Si cette option est sélectionnée, les numéros DID sont automatiquement attribués par ordre croissant aux numéros d'appel internes, et les entrées MSN correspondantes sont générées.

27.3.6.6 Passerelle vocale > Mise en réseau > Noeud

Description des paramètres des onglets :

- **Ajouter un nœud réseau**
- **Modifier le nœud réseau**
- **Supprimer le nœud réseau**

Paramètres	Description
ID de nœud	Uniquement pour configuration manuelle sans assistant par ex. avec numérotation ouverte : entrée d'un numéro de noeud qui est univoque dans l'interconnexion de réseaux.
Adresse IP	Uniquement pour configuration manuelle sans assistant par ex. avec numérotation ouverte : adresse IP du noeud
Surveillance de noeud	La sélection de la surveillance des noeud se traduit par un contrôle périodique de la communication avec le noeud. Il faut toutefois que la surveillance de noeud soit aussi active dans l'autre noeud.

Paramètres	Description
Niveau de sécurité du codage des nœuds	Le choix "Sécurisé" entraîne le chiffrement de la communication vocale avec le noeud. Pour cela, il faut de plus effectuer un paramétrage dans le système "Signaling et Payload Encryption (cryptage de la signalisation et de la charge utile)". Plage de valeurs : traditionnel, sécurisé

27.3.6.7 Passerelle vocale > Mise en réseau > Routage

Description des paramètres des onglets :

- **Ajouter un numéro**
- **Supprimer tous les numéros d'abonnés**

Paramètres	Description
ID de nœud	Sélection du numéro de noeud
Numéro de téléphone	Uniquement pour configuration manuelle, sans assistant, par ex. avec numérotation ouverte : indication de l'indicatif permettant de joindre le noeud.

27.3.6.8 Passerelle vocale > SIPQ-Interconnexion

L'interconnexion SIP-Q est utilisée pour définir les paramètres de deux routes SIP-Q externes possibles. Tout serveur SIP externe tel qu'OpenScape 4000 ou OpenScape Voice peut être connecté via ces routes. Des exemples pertinents sont inclus dans les modèles existants.

Description des paramètres des onglets :

- **Ajouter une interconnexion SIPQ**
- **Modifier l'interconnexion SIPQ**
- **Supprimer l'interconnexion SIPQ**

Paramètres	Description
Modèle de base	Modèle à utiliser comme base.
Nom	Nom du serveur SIP externe (nom du modèle).
Activer le coffre	La connexion au serveur SIP externe est activée. Valeur par défaut : désactivé
Identifiant du tronc dans le système	Sélection entre deux interconnexions SIPQ externes.
Nom de domaine distant	Nom d'hôte ou adresse IP du serveur SIP externe. La valeur est généralement identique à la valeur à **l'adresse IP / nom d'hôte** .
Serveur SIP	
Adresse IP / Nom d'hôte	Nom d'hôte ou adresse IP du serveur SIP externe.

Paramètres	Description
Port	Port SIP du serveur SIP externe. Plage de valeurs : 0 ou 1024 à 65535, valeur par défaut : 5060
Transport sécurisé	Lorsqu'il est connecté à OpenScape 4000 ou à OpenScape Voice, la signalisation SIP chiffrée peut être activée (fonction de chiffrement de la signalisation et de la charge utile). Valeur par défaut : désactivé
Registre SIP	
Registre des fournisseurs d'utilisation	Le serveur SIP externe nécessite un enregistrement. Valeur par défaut : désactivé
Adresse IP / Nom d'hôte	Nom d'hôte ou adresse IP du serveur d'enregistrement.
Port	Numéro de port du serveur d'enregistrement. Plage de valeurs : 0 ou 1024 à 65535, valeur par défaut : 5060
Intervalle de réenregistrement (s)	Intervalle (en secondes) auquel l'enregistrement est répété. Plage de valeurs : de 30 à 86 400, valeur par défaut : 300
Proxy sortant/Proxy entrant	
Utiliser un proxy sortant/ entrant du fournisseur	Activation du proxy sortant : Certains scénarios de redondance (par exemple, avec OpenScape Branch Proxy) nécessitent la gestion de la signalisation SIP via un proxy sortant. Activation du proxy entrant : Dans certains scénarios de redondance (par exemple, avec OpenScape Voice), la signalisation entrante provient d'un serveur SIP distinct (proxy entrant). Valeurs par défaut : désactivé dans les deux cas
Adresse IP / Nom d'hôte	Nom d'hôte ou adresse IP du proxy sortant ou entrant.
Port	Numéro de port du proxy sortant ou entrant. Plages de valeurs : 0 ou 1024-65535

Description des paramètres des onglets :

- **Ajouter un utilisateur d'interconnexion SIPQ**
- **Modifier l'utilisateur d'interconnexion SIPQ**
- **Supprimer l'utilisateur d'interconnexion SIPQ**

Paramètres	Description
ID de l'utilisateur	Saisie de l'identifiant utilisateur pour accéder au serveur SIP.
Nom de l'autorisation / **Domaine**	Saisie du nom d'autorisation ou du domaine pour l'accès au serveur SIP.
Mot de passe	Saisie du mot de passe d'accès au serveur SIP.
Confirmez le mot de passe	Répétition du mot de passe pour accéder au serveur SIP.

27.3.6.9 Passerelle vocale > Ligne réseau du serveur SIP natif

Les paramètres des 10 routes SIP natives externes possibles sont définis ici. Tout serveur SIP externe peut être connecté via ces routes.

Description des paramètres des onglets :

- **Ajouter une ligne réseau du serveur SIP natif**
- **Modifier une ligne réseau du serveur SIP natif**
- **Supprimer une ligne réseau du serveur SIP natif**

Paramètres	Description
Modèle de base	Modèle à utiliser comme base.
Nom de la ligne réseau	Nom du serveur SIP externe (nom du modèle).
Activer la ligne réseau	La connexion au serveur SIP externe est activée. Valeur par défaut : désactivé
Identifiant de la ligne réseau dans le système	Choix de 10 connexions SIP natives externes. Les éléments grisés sont occupés par des ITSP déjà configurés (8 ITSP maximum possibles - dans ce cas, il reste 2 connexions SIP natives).
Nom de domaine distant	Nom d'hôte ou adresse IP du serveur SIP externe. La valeur est généralement identique à celle de l' **adresse IP / nom d'hôte**. Exemple: Le **nom de domaine distant** configuré est utilisé dans la partie Host des champs From et PAI/PPI-header (voir ci-dessous) : De : sip : +49...@DomainName P-Asserted-Identity: sip: +49...@DomainName
Protocole de transport	Sélection du protocole UDP ou TCP.
Sécurité du transport	Sélection entre UDP ou TCP traditionnel et TLS sécurisé.
Sécurité des médias	Sélection entre RTP uniquement, SDES uniquement et DTLS-SRTP. DTLS-SRTP est un protocole qui combine le Datagram Transport Layer Security (DTLS) avec le Secure Real-time Transport Protocol (SRTP) pour fournir un flux de média crypté et authentifié sur Internet. **Remarque :** Dans les nouveaux déploiements (à partir de V3R4), DTLS-SRTP est le protocole par défaut. Le passage à DTLS-SRTP à partir de RT seul ou SDES seul nécessite un redémarrage du tronc pour qu'il prenne effet. **Remarque :** Des paramètres de pare-feu restrictifs peuvent entraîner des problèmes sporadiques ou permanents de charge utile vocale. Dans ce cas, désactivez l'option DTLS-SRTP.
Serveur SIP	

Paramètres	Description
Adresse IP / Nom de l'hôte	Nom d'hôte ou adresse IP du serveur SIP externe.
Port	Port SIP du serveur SIP externe. Valeur par défaut : 5060, entrer le port 0 si l'ITSP utilise DNSSRV
Enregistrement SIP	
Utiliser l'enregistrement	Doit être sélectionné si la liaison fonctionne avec l'enregistrement (par défaut = désactivé)
Adresse IP / Nom de l'hôte	Nom d'hôte ou adresse IP du serveur d'enregistrement externe
Port	Port du serveur d'enregistrement externe valeur par défaut : 5060, entrer le port 0 si DNSSRV est utilisé
Intervalle de réenregistrement	Intervalle auquel un enregistrement est répété (valeur par défaut = 600)
Serveur STUN	
Utiliser STUN	Doit être sélectionné si la ligne réseau fonctionne avec STUN (par défaut = désactivé)
Adresse IP / Nom de l'hôte	Nom d'hôte ou adresse IP du serveur STUN
Port	Port du serveur STUN
Données SIP étendues	
Afficher les données SIP étendues	En activant cet indicateur, des paramètres de configuration supplémentaires sont disponibles pour contrôler la pile SIP et adapter le contenu des champs d'en-tête SIP
CLIP / CLIR	Le système fournit divers paramètres pour contrôler le format des champs d'en-tête SIP en fonction des besoins de la ligne réseau native Le contenu des champs d'en-tête suivants, qui décrivent la source d'un appel, peut être contrôlé : • De : DisplayPart <sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>
CLIP sortant dans l'en-tête De - partie affichage	Paramètres possibles : • Omettre - le champ est omis • Numéro d'appel - numéro configuré pour une station. Vous pouvez définir le numéro utilisé dans les "paramètres d'acheminement" • Compte - le nom d'utilisateur attribué à la ligne réseau native • afficher un nom
CLIP sortant dans l'en-tête De - partie utilisateur :	Paramètres possibles : • Numéro d'appel • Compte

Paramètres	Description
Sortant de l’en-tête - partie domaine/hôte :	Modifier la partie domaine / hôte de l'URI pour qu'elle soit remplie par l'adresse IP du système. Ce paramètre affecte la partie hôte des trois fichiers d'en-tête De :, PAI et PPI Paramètres possibles : • nom du domaine • adresse IP locale • adresse IP publique
Déviation : De l’option contient le numéro de l'appelant d'origine :	Si un appel sortant est établi en raison d'un renvoi d'appel, le système peut fournir des informations sur l'appelant d'origine. Si la valeur est vraie, le système envoie le numéro de l'appelant d'origine (A-Ext) dans le champ d'en-tête De : sinon il envoie le numéro de la station de renvoi.
Déviation : PAI contient le numéro de l'appelant d'origine	Si un appel sortant est établi en raison d'un renvoi d'appel, le système peut fournir des informations sur l'appelant d'origine. Si la valeur est "vraie", le système envoie le numéro de l'appelant d'origine (A-Ext) dans l'en-tête P-Asserted-Id, sinon il envoie le numéro de la station de réacheminement. Si ce drapeau est activé, le système envoie l'appelant d'origine dans le champ d'en-tête P-Asserted_ID : et P-Preferred-ID :.
CLIP sortant dans l'en-tête P-Asserted-Id - partie affichage :	Paramètres possibles : • Omettre - le champ est omis • Numéro d'appel - numéro configuré pour une station. Vous pouvez définir le numéro utilisé dans les "paramètres d'acheminement" • Compte - le nom d'utilisateur attribué à la ligne réseau native • afficher un nom
CLIP sortant dans l'en-tête P-Asserted-Id - partie utilisateur :	Paramètres possibles : • Omettre - le champ est omis • Numéro d’appel • Compte
CLIP sortant dans l'en-tête P-Preferred-Id - partie affichage :	Paramètres possibles : • Omettre - le champ est omis • Numéro d'appel - numéro configuré pour une station. Vous pouvez définir le numéro utilisé dans les "paramètres d'acheminement" • Compte - le nom d'utilisateur attribué à la ligne réseau native • afficher un nom
CLIP sortant dans l'en-tête P-Preferred-Id - partie utilisateur :	Paramètres possibles : • Omettre - le champ est omis • Numéro d’appel • Compte

Paramètres	Description
CLIP sortant dans l'en-tête Déviation - partie affichage :	Paramètres possibles : • Omettre - le champ est omis • Numéro d'appel - numéro configuré pour une station. Vous pouvez définir le numéro utilisé dans les "paramètres d'acheminement" • Compte - le nom d'utilisateur attribué à la ligne réseau native • afficher un nom
CLIP sortant dans l'en-tête Déviation - partie utilisateur :	Paramètres possibles : • Omettre - le champ est omis • Numéro d'appel • Compte
CLIP sortant dans l'en-tête Histoire-Info - partie utilisateur :	Paramètres possibles : • omettre • numéro d'appel
CLIR sortant dans l'en-tête De - partie affichage :	Paramètres possibles : • Omettre • Numéro d'appel • Compte • Anonyme **De : Anonyme <sip: ...@...>**
CLIR sortant dans l'en-tête De - partie utilisateur :	Paramètres possibles : • Numéro d'appel • Compte • Pleinement anonyme**De: ...<sip:anonymous@anonymous.invalid>** • Utilisateur anonyme **De: ... <sip:anonymous@...>**
En-tête de vie privée sortante CLIR	Paramètres possibles : • Omettre • Id **Vie privée : id** • Vie **Privée de l'utilisateur : utilisateur** • Utilisateur, id **Vie privée : utilisateur;id**
COLP / TIP pris en charge pour les appels sortants :	La fonction COLP (Connect Line Identification Presentation) a été introduite dans le RNIS. Dans SIP, cette fonction est parfois appelée TIP (Termination Identification Presentation). RFD3324 (section 5.) définit un mécanisme pour transporter l'identité de la partie acceptante (C) dans le champ d'en-tête P-Asserted-Identity de la réponse 200 OK : Paramètres possibles : • COLP pris en charge • COLP non pris en charge
Formation du numéro d'appel	

Paramètres	Description
Appel entrant - Numéro de l'appelé :	Cet indicateur fait référence à l'adresse de destination d'un appel. Par défaut, cette adresse est tirée de la **partie utilisateur** du champ **À: en-tête**. Paramètres possibles : • Ligne de requête **INVITER sip: +498970070@...** • À la partie d'affichage de l'en-tête **À : +498970070 <sip:+** • À la partie utilisateur de l'en-tête **À : <sip: +498970070@...** • Partie affichage de l'en-tête P-Called-Party-Id **P-Called-Party-ID: +498970070 <sip:..** • Partie utilisateur de l'en-tête P-Called-Party-Id **P-Called-Party-ID: <sip: +498970070@..**
Appel entrant - Numéro de l'appelant :	Cet indicateur fait référence à l'adresse source d'un appel. Par défaut, le système retire le numéro de l'appelant de la partie utilisateur de l'en-tête De. Paramètres possibles : • automatique • De la partie affichage de l'en-tête **De : +498970070 <sip:+** • De la partie utilisateur de l'en-tête **De : <sip: +498970070@...** • Partie affichage de l'en-tête P-Asserted-Id **P-Asserted-ID: +498970070 <sip:..** • Partie utilisateur de l'en-tête P-Asserted-Id **P-Asserted-ID: <sip: +498970070@..** En mode automatique, le système recherche d'abord dans la partie utilisateur du champ P-Asserted-Identity, s'il est présent. Si aucune P-Asserted-Identity n'est présente, la partie utilisateur du champ d'en-tête De : est prise en compte.
L'URI de contact contient :	Ce paramètre est utilisé pour configurer le contenu de la partie utilisateur de l'URI de contact **Contact: sip:UserPart@HostPart:port** Paramètres possibles : • Numéro d'appel : la partie utilisateur de l'URI de contact contient le numéro d'appel • AOR d'enregistrement : l'URI de contact contient la partie compte=utilisateur de l'enregistrement.

Paramètres	Description
Port TCP utilisé dans l'URI de contact :	Ce paramètre permet de configurer le port TCP utilisé dans la partie hôte de l'URI de contact **Contact: sip:UserPart@HostPart:port** Paramètres possibles : • ephem.src-port: Par défaut, le port tcp src éphémère est utilisé • Port du serveur SIP : Le port du serveur SIP est utilisé dans l'URI du contact

Description des paramètres des onglets :

- **Ajouter un utilisateur de ligne réseau du serveur SIP natif**
- **Modifier un utilisateur de ligne réseau du serveur SIP natif**
- **Supprimer un utilisateur de ligne réseau du serveur SIP natif**

Paramètres	Description
ID utilisateur	Entrée de l'ID de l'utilisateur pour l'accès au serveur SIP.
Nom d'autorisation	Entrée du nom d'autorisation pour l'accès au serveur SIP.
Mot de passe	Entrée du mot de passe pour l'accès au serveur SIP.
Confirmer le mot de passe	Répétition du mot de passe pour l'accès au serveur SIP.

27.3.7 Abonnés

Le menu **Abonnés** regroupe les fonctions pour tous les abonnés. Ce sont notamment les noms et numéros d'appel des abonnés, mais aussi la programmation des touches.

27.3.7.1 Station > Station > UP0 Stations

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station.
A FAIT	Numéro DID de la station.
Prénom	Prénom librement choisi pour la station. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour la station. Plage de valeurs : max. 32 caractères.

Paramètres	Description
Afficher	Nom de la station librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Plage de valeurs : 16 caractères maximum
Nom	Nom de la station librement choisi. Plage de valeurs : 16 caractères maximum
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis). Plage de valeurs : max. 16 chiffres
Actif	Indique si la station est opérationnelle.
Type d'appareil	Affiche l'appareil associé à l'abonné.
Numéro d'appel fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de sites internes doit être saisi ici.
Numéro de fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de l'extérieur doit être saisi ici.
Accéder	Affiche l'interface physique à laquelle le périphérique est connecté.
Urgence SIP	Emplacement d'urgence SIP d'une station.
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **« Numéro d'appel »**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

Description des paramètres des onglets :

- **Maître/Esclave UP0**

  Cet onglet n'apparaît que pour OpenScape Business X8, car les ports esclaves sont gérés dynamiquement dans ce système. Pour OpenScape Business X1/X5, les ports esclaves sont attribués statiquement (c'est-à-dire qu'ils sont fixes).

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station.
A FAIT	Numéro DID de la station.
Nom	Nom de la station librement choisi. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
Accéder	Affiche l'interface physique à laquelle le périphérique est connecté.
Ajouter une zone d'esclaves	Si cette case est cochée, un port esclave est pré-affecté au port maître sélectionné. Après avoir enregistré la sélection avec **Appliquer** , le numéro d'appel, le numéro DID et le nom du téléphone du système esclave peuvent être configurés à l'avance. Lorsque le téléphone du système esclave est ensuite connecté à l'adaptateur esclave du téléphone du système maître, il se voit attribuer le port esclave précédemment sélectionné. Si le téléphone du système esclave est connecté sans port esclave prédéfini, le prochain port disponible (à partir du port 384) est automatiquement utilisé.
Supprimer la zone esclave	Si cette case est cochée, la préconfiguration du téléphone du système esclave est supprimée. Si un téléphone du système esclave est déjà connecté à l'adaptateur esclave du téléphone du système maître, la case à cocher est grisée et la préconfiguration ne peut pas être supprimée.
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

Description des paramètres des onglets :

- **Informations sur l'appareil**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station.

Paramètres	Description
Nom	Nom de la station.
Type d'appareil	Affiche le type de périphérique associé à la station.
Version actuelle du logiciel	Version logicielle du périphérique associé (le cas échéant).
Version matérielle	Version matérielle du périphérique associé (le cas échéant).
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

27.3.7.2 Clients IP > de > la station

Description des paramètres des onglets :

- **Modifier l'abonné**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station.
A FAIT	Numéro DID de la station.
Prénom	Prénom librement choisi pour la station. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour la station. Plage de valeurs : max. 32 caractères.
Afficher	Nom de la station librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans trémas ni caractères spéciaux.
Taper	Type de station.
Type : **Sans port**	Ce numéro d'appel n'est pas encore attribué à une station.
Type : **Client système**	Un client système est une station IP capable d'utiliser toutes les fonctionnalités du système de communication via CorNet-IP (anciennement appelé client système HFA).
Type : **Utilisateur RAS**	Un utilisateur RAS (utilisateur du service d'accès à distance) bénéficie d'un accès Internet au réseau IP via la connexion RNIS. Cela permet la maintenance et la gestion des licences à distance du système de communication.

Paramètres	Description
Type : **Client SIP**	Un client SIP est une station IP qui utilise le protocole SIP. Il ne peut accéder qu'à des fonctionnalités limitées du système de communication via SIP.
Type : **Utilisateur Desk Share**	Un utilisateur Deskshare est un utilisateur IP qui peut se connecter à un autre téléphone de système IP (connexion mobile) et ensuite utiliser ce téléphone comme son propre téléphone (y compris le numéro d'appel).
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis).
Actif	Indique si la station est opérationnelle.
Numéro d'appel fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de sites internes doit être saisi ici.
Numéro de fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de l'extérieur doit être saisi ici.
Urgence SIP	Emplacement d'urgence SIP d'une station.
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **Rechercher** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **Numéro d'appel**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

Description des paramètres des onglets :

- **Informations sur l'appareil**

Notez que le tri est strictement alphabétique pour toutes les colonnes. Il n'y a pas de tri numérique spécifique à une colonne pour certains types de données tels que **l'adresse IP** ou **la version actuelle du logiciel**.

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station.

Paramètres	Description
Afficher	Nom de la station.
Type d'appareil	Affiche le type de périphérique associé à la station.
Adresse IP	Adresse IP du périphérique associé ; lien direct vers le serveur WBM du téléphone IP
Adresse MAC	Adresse MAC du téléphone associé
Version actuelle du logiciel	Version logicielle du périphérique associé (le cas échéant).
Version matérielle	Version matérielle du périphérique associé (le cas échéant).
Port PC	Si cette option est activée, le port Ethernet du PC est mis en marche sur tous les téléphones du système actifs. Par défaut : désactivé
Paramètres du codec	Si cette option est activée, la priorisation des codecs suivante s'applique à tous les téléphones du système : G.729 - G.711 - G.722 Si cette option est désactivée, la priorisation des codecs suivante s'applique : G.722 - G.711 - G.729 **Remarque :** Le CP100 ne prend pas en charge le G.722. Par défaut : désactivé
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

Description des paramètres des onglets :

- **Passerelle secondaire**

Paramètres	Description
Numéro d'appel	Numéro d'appel interne de la station.
Nom	Nom de la station.
NodeId	Chaque nœud d'un système en réseau doit se voir attribuer un identifiant de nœud unique. Cela permet d'identifier de manière unique chaque nœud d'un système en réseau.
téléphonie de secours	Indique si la fonction est activée.
Appel de secours n°	Numéro d'appel de la station qui sera utilisé en cas de panne.

Paramètres	Description
Appel de secours sans numéro DID	Numéro d'appel interne de la station qui sera utilisé en cas de panne.

Description des paramètres des onglets :

- **Hébergement de secours**

Paramètres	Description
Numéro d'appel	Numéro d'appel interne de la station.
Nom	Nom de la station.
ID du nœud principal	L'identifiant unique du nœud sur lequel la station est initialement configurée.
Appel de secours n°	Numéro d'appel de la station qui sera utilisé en cas de panne.
Appel de secours sans numéro DID	Le numéro d'appel interne de la station qui sera utilisé en cas de panne.

27.3.7.3 Station > Station > Stations analogiques

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station. **Remarque :** Les numéros d'appel commençant par un astérisque (*) ne peuvent pas être utilisés comme destinations de fax.
A FAIT	Numéro DID de la station.
Prénom	Prénom librement choisi pour la station. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour la station. Plage de valeurs : max. 32 caractères.
Afficher	Nom de la station librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans trémas ni caractères spéciaux.
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis). Plage de valeurs : max. 16 chiffres

Paramètres	Description
Actif	Indique si la station est opérationnelle.
Type d'appareil	Affiche l'appareil associé à l'abonné.
Numéro d'appel fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de sites internes doit être saisi ici.
Numéro de fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de l'extérieur doit être saisi ici.
Accéder	Affiche l'interface physique à laquelle le périphérique est connecté.
Urgence SIP	Emplacement d'urgence SIP d'une station.
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **« Numéro d'appel »**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

27.3.7.4 Station > Station > Stations ISDN

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station.
A FAIT	Numéro DID de la station.
Prénom	Prénom librement choisi pour la station. Plage de valeurs : max. 32 caractères.

Paramètres	Description
Nom de famille	Nom de famille librement sélectionnable pour la station. Plage de valeurs : max. 32 caractères.
Afficher	Nom de la station librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis). Plage de valeurs : max. 16 chiffres
Actif	Indique si la station est opérationnelle.
Type d'appareil	Affiche l'appareil associé à l'abonné.
Numéro d'appel fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de sites internes doit être saisi ici.
Numéro de fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de l'extérieur doit être saisi ici.
Accéder	Affiche l'interface physique à laquelle le périphérique est connecté.
Urgence SIP	Emplacement d'urgence SIP d'une station.
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **« Numéro d'appel »**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

27.3.7.5 Station > Station > DECT Stations > SLC Numéro d'appel

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station.
A FAIT	Numéro DID de la station.
Prénom	Prénom librement choisi pour la station. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour la station. Plage de valeurs : max. 32 caractères.
Afficher	Nom de la station librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis). Plage de valeurs : max. 16 chiffres
Actif	Indique si la station est opérationnelle.
Type d'appareil	Affiche l'appareil associé à l'abonné. Les stations de base sont indiquées comme stations S0.
Accéder	Affiche l'interface physique à laquelle le périphérique est connecté.
Urgence SIP	Emplacement d'urgence SIP d'une station.
Paramètres	Affichage par défaut pour toutes les stations ; ne modifiez pas les paramètres
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **« Numéro d'appel »**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

27.3.7.6 Station > Station > DECT Stations > DECT

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station.
A FAIT	Numéro DID de la station.
Prénom	Prénom librement choisi pour la station. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour la station. Plage de valeurs : max. 32 caractères.
Afficher	Nom de la station librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis). Plage de valeurs : max. 16 chiffres
Actif	Indique si la station est opérationnelle.
Type d'appareil	Affiche l'appareil associé à l'abonné. Les stations DECT sont indiquées comme Comfort-PP.
Numéro d'appel fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de sites internes doit être saisi ici.
Numéro de fax	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de l'extérieur doit être saisi ici.
Accéder	Affiche l'interface physique à laquelle le périphérique est connecté.
Urgence SIP	Emplacement d'urgence SIP d'une station.
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	

Paramètres	Description
Flèche bleue dans la colonne **« Numéro d'appel »**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

27.3.7.7 Station > Station > Ports IVM/EVM > EVM

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne du port de messagerie vocale.
A FAIT	Numéro DID du port de messagerie vocale, le cas échéant.
Prénom	Prénom librement sélectionnable pour le port de messagerie vocale. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour le port de messagerie vocale. Plage de valeurs : max. 32 caractères.
Afficher	Nom librement choisi pour le port de messagerie vocale. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
Clip/Lin	Séquence de chiffres à afficher au destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis).
Actif	Indique si le port de messagerie vocale est opérationnel.
Type d'appareil	Pour l'EVM, les stations S0 sont affichées.
Accéder	Affiche le port interne de la messagerie vocale.
Urgence SIP	Emplacement d'urgence SIP d'une station.
Type de station	« PhoneMail » doit être sélectionné pour l'EVM ; « Standard » doit être défini pour le standard automatique de l'entreprise.
Paramètres	Affichage par défaut pour tous les ports de messagerie vocale ; ne modifiez pas les paramètres (par exemple, la « langue » ne correspond pas à la langue des annonces de messagerie vocale).

Paramètres	Description
Recherche	Vous pouvez également afficher les ports de messagerie vocale sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les ports de messagerie vocale correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les ports de messagerie vocale seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **« Numéro d'appel »**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

27.3.7.8 Station > Station > Stations virtuelles

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Numéro d'appel interne de la station virtuelle.
A FAIT	Numéro DID de la station virtuelle.
Prénom	Prénom librement choisi pour la station. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour la station. Plage de valeurs : max. 32 caractères.
Afficher	Nom de la station librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
Taper	Station vide ou virtuelle (affichage fixe pour l'accès aux personnes à mobilité réduite)
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis).
Actif	Indique si la station virtuelle est opérationnelle.

Paramètres	Description
Urgence SIP	Emplacement d'urgence SIP d'une station.
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **« Numéro d'appel »**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

27.3.7.9 Paramètres de > la > station

Description des paramètres des onglets :

- **Modifier les paramètres de la station**

Paramètres	Description
Stations - ...	
Taper	Type de station.
Numéro d'appel	Numéro d'appel interne de la station.
Prénom	Prénom librement choisi pour la station. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour la station. Plage de valeurs : max. 32 caractères.
Afficher	Nom de la station librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
numérotation directe entrante	Numéro DID de la station.
Type d'appareil	Affiche l'appareil associé à l'abonné.

Paramètres	Description
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis). Plage de valeurs : max. 16 chiffres
Accéder	Affiche l'interface physique à laquelle le périphérique est connecté.
Provisionnement des appareils	Ce menu est uniquement visible pour les stations SIP et les valeurs suivantes sont disponibles : • **Norme** (valeur par défaut) • **Mitel SIP DECT Device** (Le périphérique SIP spécifique est utilisé pour le Mitel SIP DECT). **Remarque :** L'option **Mitel SIP DECT Device** n'est prise en charge que sur le matériel V3 et les systèmes OSBiz S.
Configuration Mitel SIP DECT : ce menu n'est visible que lorsque **Mitel SIP DECT Device** est sélectionné sous **Provisionnement des périphériques**.	
ÉPINGLE	Le code PIN de l'appareil.
Verrouillage à clé activé	Activer (Oui) ou désactiver (Non) le verrouillage de la touche de l'appareil.
code PIN de verrouillage à clé	Le code PIN de la serrure à clé.
Temps de verrouillage des clés	Le délai d'activation du verrouillage.
Afficher l'annuaire personnel	Choisissez si le répertoire personnel est visible (Oui) ou non (Non).
Fax	
Numéro d'appel	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de sites internes doit être saisi ici.
numérotation directe entrante	Si une boîte de fax a été configurée (par exemple, avec les clients UC myPortal for Desktop ou myPortal for Outlook), le numéro de fax auquel l'abonné peut recevoir des messages fax provenant de l'extérieur doit être saisi ici.
Mobilité	
Taper	Type de station : • Station de mobilité • Station virtuelle • Station SFB • Station externe de confiance : type de station virtuelle à utiliser pour créer un utilisateur externe de confiance

Paramètres	Description
Numéro d'appel de la station externe mobile/Sfb/ de confiance	Uniquement pour les clients SIP et les utilisateurs mobiles : pour le service à numéro unique, ce numéro est utilisé pour l'authentification de l'accès DISA via le service mobile. Saisissez le numéro de téléphone mobile associé à l'abonné ainsi que le préfixe de numérotation (c'est-à-dire le code CO), par exemple 0017312345678). **Remarque :** Le champ **Numéro d'appel du terminal externe de confiance** est obligatoire. Si vous appliquez la configuration alors que le champ **Numéro d'appel du terminal externe de confiance** est vide, une alerte s'affiche, vous informant que « *Le numéro d'appel du terminal externe de confiance ne doit pas être vide !* ». En outre, après avoir cliqué sur **OK** pour la première alerte, une deuxième alerte s'affiche, vous informant que « *L'entrée n'a pas pu être traitée, veuillez vérifier* ».
ID de fonctionnalité Web	L'identifiant de fonctionnalité Web définit comment l'abonné doit se connecter au client Web mobile (nom d'utilisateur). Choix entre « non » (entrée mobile uniquement) et « automatique » (numéro d'appel interne de l'abonné) ou sélection du numéro de poste du client ou du téléphone dans la liste déroulante.
Paramètres	
Type de station	Type de périphérique connecté (liste déroulante)
Type de terminal : **Standard**	Téléphones système ou téléphones analogiques
Type de terminal : **Fax**	Télécopieur, par exemple, aucune dérogation possible
Type de terminal : **Haut-parleur**	Pour la pagination via le port a/b
Type de terminal : **répondeur**	Uniquement pour les systèmes analogiques : si un répondeur est connecté à cette interface, ce paramètre permet de prendre en charge un appel provenant du répondeur depuis n'importe quel appareil, même si le répondeur a déjà accepté l'appel. Pour ce faire, le terminal doit être programmé avec l'indicatif interne de la station analogique. Outre sa sélection pour les répondeurs automatiques, cette option doit également être sélectionnée pour les ports virtuels où aucun équipement physique n'a été installé. Cela empêche le système de communication de vérifier l'état de fonctionnement du port. Uniquement pour les ports virtuels : si un poste sans accès a été configuré comme un type de répondeur dans Manager E, le port doit également être configuré comme un port virtuel. Sinon, elle ne sera pas visible comme station dans le WBM.
Type de terminal : **P.O.T. MW LED**	Pour les téléphones analogiques standard (RTC = Téléphone fixe) avec voyant de message en attente Pas pour nous
Type de terminal : **Abonnés avec boucle d'impulsion**	Lors de l'utilisation d'un dispositif à boucle pulsée avec la fonction d'ouverture de porte

Paramètres	Description
Type de terminal : **Modem**	Il n'est pas possible de remplacer l'appel avec ce paramètre. Il est destiné aux modems.
	Lorsqu'un poste de fax ou de modem est supprimé (c'est-à-dire que le numéro d'appel et le DID sont supprimés), le type de poste doit également être réinitialisé à la valeur par défaut (standard).
Langue	Langue pour la commande du menu de l'appareil (téléphone système).
Signalisation d'appel interne	Chaque station peut se voir attribuer ici l'une des huit sonneries internes possibles. Cela signifie qu'en plus de la sonnerie externe, une sonnerie interne est également attribuée ici et transmise ultérieurement pour les appels internes. Valeur par défaut : Anneau de type 1
Signalisation d'appel externe	Vous pouvez sélectionner ici trois types de sonneries différents pour signaler les appels externes : – Téléphones téléphoniques : Sonnerie 1 = Appel externe (ex. : double sonnerie), Sonnerie 2 = Appel externe CO 2 (ex. : triple sonnerie), Sonnerie 3 = Appel externe CO 3 (ex. : sonnerie courte/longue/courte) – Téléphones analogiques pour l'Allemagne : Sonnerie 1 = Appel externe, Sonnerie 2 = Rappel automatique, Sonnerie 3 = Sonnerie de porte – Téléphones analogiques pour les autres pays : Sonnerie 1 = Appel externe, Sonnerie 2 = Appel externe, Sonnerie 3 = Appel externe Valeur par défaut : Anneau de type 1
Classe de service (LCR)	Un abonné ne peut s'emparer d'une route que si son COS est supérieur ou égal au COS LCR dans la table de routage, c'est-à-dire qu'un abonné avec un COS de 7 ne peut pas s'emparer d'une route avec un COS de 8. Par défaut, tous les abonnés sont inscrits avec la classe de service LCR maximale (15). Valeur par défaut : 15
Mode ligne d'assistance	Sélection des options de la ligne d'assistance téléphonique
Mode hotline: **désactivé**	Désactive la fonction d'assistance téléphonique.
Mode hotline : **Tempo**	L'appel à la ligne d'assistance téléphonique a lieu après un délai prédéfini (délai d'alarme de décrochage), voir Téléphonie/Paramètres de base/Système/Interception - Ligne d'assistance téléphonique
Mode hotline : **Hotline**	Active la fonction d'assistance téléphonique. Dès que vous décrochez le combiné, la connexion avec la ligne d'assistance est établie immédiatement (voir Téléphonie/Paramètres de base/Système/Interception - Standardiste - Ligne d'assistance).
Ligne d'assistance téléphonique	Pour plus d'informations sur la sélection des destinations des lignes d'assistance téléphonique, consultez la section Téléphonie/Paramètres de base/Système/Interception - Ligne d'assistance téléphonique
Hotline: **néant**	Aucune destination définie
Hotline : **Chiffres 1 à 6**	Pour plus de détails sur les destinations des lignes d'assistance téléphonique, consultez la section Téléphonie/Paramètres de base/Système/Interception - Ligne d'assistance téléphonique

Paramètres	Description
Sécurité de la charge utile (pour les clients du système IP)	Activer ou désactiver le chiffrement des conversations téléphoniques (SPE). Pour ce faire, toutes les stations concernées doivent avoir la fonction SPE activée. Valeur par défaut : activé
Sécurité des données (pour téléphones TDM/ analogiques)	Indique si le terminal spécifique est sécurisé ou non du point de vue de l'infrastructure, car la sécurité de la charge utile ne fonctionne que pour les téléphones IP. Si ce paramètre est activé et que l'indicateur système de support SPE est activé, il est indiqué si le chemin de connexion entre cette station et une station IP est crypté ou non. Si le paramètre est désactivé, aucune information n'est affichée. Valeur par défaut : désactivé
Protocole MWI	Sélection du protocole MWI pour les stations analogiques. Disponible uniquement pour SLMAVx (OpenScape Business X8), 4SLAV embarqué et SLAVx OpenScape Business X5.
Protocole MWI : Comtel3	Protocole Comtel 3 sélectionné. Valeur par défaut.
Protocole MWI : Haute tension	Protocole haute tension sélectionné. Disponible uniquement pour SLMAVx (OpenScape Business X8).
Boutons	
>	Passe à la station suivante. Si les stations correspondant au terme de recherche saisi dans les champs **de recherche** ont été préalablement filtrées, il est possible de se déplacer uniquement entre ces stations spécifiques.
<	Recule d'une station.

Description des paramètres des onglets :

- **Modifier les drapeaux de la station**

Paramètres	Description
Stations - ...	
Taper	Type de station.
Numéro d'appel	Numéro d'appel interne de la station.
Nom	Nom de la station.
drapeaux de gare	
Remplacer la classe de service sur	Lorsque cet indicateur est activé, l'abonné peut s'immiscer dans (c'est-à-dire remplacer) la connexion en cours d'un abonné interne. Les abonnés concernés sont avertis de la surcharge par un signal sonore et un message affiché. Valeur par défaut : Désactivé

Paramètres	Description
Désactiver le mode Ne pas déranger	Lorsque ce paramètre est activé, les règles suivantes s'appliquent : lorsqu'un abonné appelle une station pour laquelle le mode « Ne pas déranger » a été activé, il peut désactiver ce mode. Au bout de cinq secondes, l'appel est signalé à la station appelée. Si l'option est désactivée, la fonction « Ne pas déranger » ne peut pas être désactivée. Les abonnés qui appellent une station pour laquelle le mode « Ne pas déranger » est activé entendent une tonalité d'occupation. Valeur par défaut : Désactivé
FWD externe autorisé	Lorsque cette option est activée, l'abonné peut activer le renvoi d'appel vers une destination externe. Les frais occasionnés par l'exécution d'un renvoi d'appel externe sont imputés à l'abonné qui a activé le renvoi d'appel. Valeur par défaut : Activé
Prévention des appels vocaux	Lorsque ce drapeau est activé, la station peut être appelée directement. Cela permet d'établir un appel interne sans décrocher le combiné. Le haut-parleur de la station appelée s'active automatiquement. Valeur par défaut : Activé
Classe de service DISA	Lorsque ce drapeau est activé, les abonnés externes peuvent activer ou désactiver des fonctions du système de communication via DISA (Direct Inward System Access) et établir des connexions externes sortantes comme n'importe quel autre abonné interne. Cela inclut également l'activation et la désactivation du renvoi d'appel, la fonction « Ne pas déranger » et le code de verrouillage, par exemple. Valeur par défaut : Désactivé
Transit autorisé via Hook-on	Lorsque cette option est activée, l'abonné peut transférer un appel externe à un autre abonné externe en raccrochant. Exemple : L'abonné est le contrôleur de la conférence et raccroche : s'il reste d'autres abonnés internes dans la conférence, l'abonné interne participant depuis le plus longtemps devient automatiquement le contrôleur de la conférence. S'il ne reste que des participants externes à la conférence, celle-ci est interrompue et toutes les connexions sont coupées. Valeur par défaut : Désactivé
Réinitialisation du verrouillage téléphonique du système	Lorsque cette option est activée, l'abonné peut réinitialiser le code de verrouillage individuel des autres abonnés internes au code par défaut. Valeur par défaut : Désactivé
CLIP analogique (uniquement pour appareils analogiques)	Lorsque ce drapeau est activé, le numéro de téléphone de l'appelant s'affiche sur l'écran du poste analogique. En prérequis, le téléphone analogique de l'abonné doit prendre en charge la fonction CLIP (présentation de l'identification de l'appelant). Valeur par défaut : Activé

Paramètres	Description
accès MCID	Lorsque cette option est activée, l'abonné peut faire identifier les appelants externes malveillants via le central téléphonique RNIS. Au préalable, la fonction « Trace call » (identification des appels malveillants, MCID) doit avoir été demandée et activée par l'opérateur réseau. Une fois la fonction « Traçage d'appel » activée par l'opérateur réseau, il convient de noter ce qui suit : pour chaque appel entrant depuis le central RNIS, la libération de la connexion vers le poste appelé est retardée pendant une période de temporisation spécifique après que l'appelant a raccroché. Ce délai d'attente permet à la station appelée d'activer la fonction « Traçage de l'appel ». La disponibilité des liaisons RNIS s'en trouve quelque peu réduite. Valeur par défaut : Désactivé
Inscription dans l'annuaire téléphonique	Lorsque cette option est activée, le nom et le numéro de l'abonné seront affichés dans le répertoire système (y compris ODS). Valeur par défaut : Activé
Modifier le numéro de téléphone	Lorsque cette option est activée, l'abonné peut modifier les chiffres du numéro d'appel saisi via le clavier avant la transmission des chiffres. Cela nécessite un téléphone système avec écran. Valeur par défaut : Désactivé
Aucun appel groupé sur les lignes occupées	Lorsque cette option est activée, les conditions suivantes s'appliquent : le statut de la station sur laquelle la sonnerie de groupe est programmée (c'est-à-dire la station principale) détermine si la sonnerie de groupe se déclenche ou non. Si la station principale est libre, toutes les stations du groupe sont immédiatement appelées. Si la fonction d'appel en attente est activée sur le poste principal : tous les postes inclus dans le groupe sont appelés après un délai de 5 secondes. Si le poste principal ne peut pas recevoir d'appel ou si l'appel en attente est inactif : la sonnerie groupée n'a pas lieu. Valeur par défaut : Désactivé
Services/numérotation associés	Numérotation associée : lorsque cette option est activée, l'abonné peut composer un numéro pour le compte d'un autre abonné interne comme si ce poste composait lui-même le numéro. Services associés : lorsque cette option est activée, l'abonné peut contrôler des fonctionnalités pour le compte d'un autre abonné interne comme si cette station contrôlait elle-même ces fonctionnalités. Cela inclut par exemple l'activation et la désactivation du renvoi d'appel, de la sonnerie de groupe et du code de verrouillage. Valeur par défaut : Désactivé
Rejet d'appel en attente	Lorsque cette option est activée, les abonnés qui sont en communication ne sont pas informés des autres appels entrants par une tonalité d'appel en attente ou un message affiché. Valeur par défaut : Activé

Paramètres	Description
Appel discret	Lorsque cette option est activée, l'abonné peut discrètement rejoindre un appel vocal existant d'un autre abonné interne. Il ou elle peut surveiller discrètement l'appel et parler avec l'abonné interne sans que l'autre partie n'entende cette conversation. Cela n'est possible que dans le cas d'un appel à deux. Les appels discrets ne sont pas possibles lors des consultations ou des conférences. Valeur par défaut : Désactivé
Verrouillage d'appel discret	Lorsque ce drapeau est activé, la station ne peut pas être appelée discrètement. Valeur par défaut : Désactivé
Activation de fonctionnalités basée sur DTMF	Concerne uniquement les stations Mobility Entry : ce drapeau doit être activé pour pouvoir activer des fonctionnalités pendant un appel (c'est-à-dire en mode conversation). Le récepteur de code reste actif. (Attention : ressources limitées) Valeur par défaut : Désactivé
casque	Lorsque ce drapeau est activé, la station peut être équipée d'un casque audio qui se branche sur la connexion du combiné. L'activation de cette option permet à l'utilisateur d'accepter un appel en appuyant sur un bouton du casque du téléphone système sans décrocher le combiné. Lorsqu'un casque est connecté à la ligne téléphonique du système, il est automatiquement reconnu par le système de communication ; aucune autorisation n'est nécessaire dans ce cas. Lorsque ce paramètre est activé, les appels ne peuvent pas être raccrochés en appuyant sur la touche haut-parleur ; une touche de déconnexion doit être programmée pour que les appels puissent être raccrochés. Valeur par défaut : Désactivé
Dernière boîte aux lettres de destination active	Si ce paramètre est activé et que le correspondant n'est pas disponible, l'appel est transféré vers la messagerie vocale de substitution et le numéro de l'appelant s'affiche sur le téléphone de substitution. Valeur par défaut : Désactivé
Appel prioritaire/immédiat. Mise en attente.	Lorsque ce drapeau est activé (Priorité d'appel/appel en attente avec tonalité immédiate), les appels transitant par ce poste sont signalés avec une priorité plus élevée aux partenaires. La priorité est définie comme étant identique à celle des appels externes. Autrement dit, les appels prioritaires sont donc mis en file d'attente avant les appels internes existants, mais après les appels externes existants. Notez que les premiers appels en cours (et non les appels en attente) ne sont généralement jamais déplacés, quel que soit leur type de sonnerie. Si la même priorité doit également être définie pour un appel interne dans un autre nœud, l'indicateur de station « Priorité d'appel/attente d'appel avec tonalité immédiate » (Zone : Indicateurs de circuit, Priorité d'appel/attente d'appel avec tonalité immédiate) doit également être défini pour la jonction correspondante. Si cette option est activée, l'appelant entend immédiatement une sonnerie au lieu d'une tonalité d'occupation. Cela n'a aucun impact sur la signalisation acoustique. Les appels prioritaires sont toujours signalés comme des appels internes. Cette fonctionnalité est importante pour les connexions de messagerie téléphonique. Valeur par défaut : Désactivé

Paramètres	Description
Enregistrement vocal	Si l'option est activée, l'abonné peut activer l'enregistrement vocal pendant un appel. De plus, l'option **« Ton d'avertissement pendant l'enregistrement vocal »** sous « Indicateurs » permet de spécifier si un tonalité d'avertissement doit être émise au démarrage de l'enregistrement vocal. De plus, un périphérique d'enregistrement en direct approprié doit être configuré dans PhoneMail. Valeur par défaut : Désactivé
Compresser les données d'affichage	Lorsque cette option est activée, les données d'affichage sont compressées pour améliorer les performances. Si l'affichage sur un terminal UP0/E change, le système de communication ne met à jour que les données qui diffèrent de l'affichage précédent. Si une application (par exemple, Smartset/TAPI) est connectée via un adaptateur RS 232 (adaptateur de données ou de contrôle), cette fonction doit être désactivée. L'indicateur doit être désactivé pour les applications qui obtiennent les informations du numéro d'appel à partir de l'écran du téléphone (c'est-à-dire une sortie non compressée avec le numéro d'appel au lieu d'une sortie compressée avec le nom). Les noms ne sont généralement affichés que lorsque l'option « Affichage de l'appelant uniquement » sous « Afficher le nom/numéro d'appel » est désactivée. Valeur par défaut : Activé
Déverrouillage de porte DTMF	Si cette option est activée, la station peut ouvrir une porte avec la signalisation par code DTMF/MFV lorsqu'un relais de porte est connecté au port correspondant. Valeur par défaut : Désactivé
Connexion automatique, CSTA (uniquement pour les téléphones SIP OpenStage)	Lorsque cette option est activée, les conditions suivantes s'appliquent : le mode haut-parleur est activé sur le téléphone SIP associé lors de la numérotation ou de la réception d'appels via myPortal ou myAttendant. Les informations contenues dans la documentation du téléphone SIP doivent être respectées, car des paramètres supplémentaires peuvent être nécessaires sur le téléphone SIP pour une utilisation correcte de la fonctionnalité. Lorsque cette option est désactivée, l'établissement de l'appel n'a lieu qu'après avoir décroché le combiné. Valeur par défaut : Activé
Désactiver le microphone mains libres	Si ce drapeau est activé, le microphone mains libres ne peut pas être utilisé. Cette option n'est prise en charge que par les téléphones OpenStage. Valeur par défaut : Désactivé
Présentation forcée des nombres	Si cette option est activée, le numéro de téléphone de l'appelant s'affiche sur l'écran du correspondant au lieu de son nom. Valeur par défaut : Désactivé
Utilisation (pour certains pays uniquement)	Cette liste déroulante peut être utilisée pour configurer le courant de sortie des interfaces d'une carte analogique (en mA, par exemple 27 mA pour la Chine).
Mode de fonctionnement	Dans cette liste déroulante, un mode de fonctionnement peut être sélectionné pour la ligne d'abonné.

Paramètres	Description
Liste des appels manqués	Lorsque cette option est activée, la liste des appels manqués est activée pour l'abonné sur son téléphone (uniquement pour les téléphones avec écran). Les appels restés sans réponse de l'abonné sont horodatés (heure et date) et ajoutés à une liste triée chronologiquement. Seuls les appels comportant un numéro de téléphone ou un nom sont enregistrés. Si un abonné appelle plusieurs fois, seul l'horodatage de l'appel est mis à jour et le compteur d'appels de cet appelant est incrémenté.
Signalisation centrale occupée	Ce drapeau doit être activé (voir aussi les fonctionnalités QSIG) pour les abonnés qui ont une signalisation occupée sur un système de communication centralisé. Ne s'applique pas aux États-Unis. La mise en œuvre de la signalisation centralisée d'occupation est conditionnée par un nombre maximal de 100 stations par nœud.
Affichage du texte d'urgence	Si cette option est activée, un texte d'urgence configurable s'affiche sur l'écran du téléphone en mode urgence.
Supervision des appels	Lorsque cette option est activée, l'abonné peut surveiller silencieusement (c'est-à-dire écouter) la conversation de tout abonné interne. Le microphone de la personne qui écoute est automatiquement coupé. L'abonné surveillé n'est pas averti par un signal sonore ou un message affiché. Lorsque vous commencez et terminez la supervision d'un appel, il est possible que la conversation soit interrompue pendant deux secondes maximum. Valeur par défaut : Désactivé
Boutons	
>	Passe à la station suivante. Si les stations correspondant au terme de recherche saisi dans les champs **de recherche** ont été préalablement filtrées, il est possible de se déplacer uniquement entre ces stations spécifiques.
<	Recule d'une station.

Description des paramètres des onglets :

- **Modifier les données client du point de travail**

Paramètres	Description
Stations - ...	
Taper	Type de station.
Numéro d'appel	Numéro d'appel interne de la station.
Nom	Nom de la station.
Paramètres	
Message d'état	Réservé aux clients système : cet indicateur active le mécanisme de « maintien de la connexion » pour les téléphones système. Si un téléphone système tombe en panne, par exemple, il est signalé comme inactif après quatre minutes. Cette option ne doit pas être activée lors de la configuration d'un téléphone système en tant que client résidentiel ou lors de l'utilisation de la fonction « Mise en attente courte ». La désactivation de cette option réduit le trafic de messages entre le système de communication et les téléphones du système.

Paramètres	Description
Authentification active	Si vous souhaitez que le client IP puisse s'identifier auprès du système de communication à l'aide d'un mot de passe, l'authentification doit être activée et un mot de passe défini. C’est un avantage notamment pour les clients qui ne sont pas connectés au réseau local interne, mais qui se connectent depuis l’extérieur. Pour les clients SIP uniquement : vous devez saisir un mot de passe. Le même mot de passe doit être utilisé sur l'appareil.
Nouveau mot de passe	Mot de passe pour l'authentification. Pour les clients SIP uniquement : si un mot de passe a déjà été défini pour l’appareil, ce même mot de passe doit être utilisé lors de l’application pour maintenir l’enregistrement de l’appareil.
Confirmez le mot de passe	Mot de passe pour répéter l'authentification.
Identifiant/nom d'utilisateur SIP	Uniquement pour les clients SIP : nom d’utilisateur librement sélectionnable pour l’authentification de l’abonné SIP, par exemple « SIP-120 ». La valeur définie ici doit également être saisie sur le téléphone SIP.
Royaume	Uniquement pour les clients SIP : noms librement sélectionnables pour la zone associée, par exemple « OSBIZ-SIP ». Cette valeur doit être identique pour tous les clients SIP. La valeur définie ici doit également être saisie sur le téléphone SIP.
Adresse IP fixe	Pour les clients SIP uniquement : la saisie d’une adresse IP fixe garantit qu’un seul client SIP peut se connecter au système avec cette adresse IP. Si cette option est activée, l'adresse IP et le numéro d'appel sont vérifiés. Si cette option n'est pas activée, seul le numéro d'appel est vérifié.
Adresse IP	Uniquement pour les clients SIP : adresse IP du client SIP (par exemple, l’adresse IP du téléphone SIP).
Taper	Uniquement pour les clients système : un client IP mobile (option mobile) n’est pas attribué de façon permanente à un téléphone IP. Le numéro d'appel d'un client IP mobile peut être utilisé par un abonné pour se connecter à n'importe quel terminal IP (qui le permet) via la procédure de connexion (*9419) (à condition que l'option Mobile bloqué ne soit pas activée).
Type : **Mobile**	Uniquement pour les clients système : aucun périphérique IP n’est attribué de manière permanente à l’abonné. Cette fonctionnalité n'est prise en charge qu'à partir du troisième port de station.
Type : **Non mobile**	Uniquement pour les clients système : le numéro d’appel est attribué de manière permanente au périphérique IP de l’abonné. Lors de l'utilisation d'un téléphone WLx, l'option Non mobile doit être sélectionnée avant d'enregistrer le téléphone WLx auprès du système de communication.
Type : **Non mobile et bloqué**	Réservé aux clients système : un abonné ne peut pas se connecter à ce périphérique IP avec un client système mobile.
Bloqué pour l'utilisateur Deskshare	Uniquement pour les clients du système : ce téléphone système peut être partagé par plusieurs abonnés (partage de bureau).

Paramètres	Description
Identifiant du système secondaire	Ce paramètre a deux fonctions différentes : 1. Pour toutes les stations : définit la passerelle multi-sites attribuée à la station. 2. Uniquement pour les clients système : si l'indicateur « Urgence » a été défini (sous « Stations/Clients IP/Passerelle secondaire ») pour les systèmes en réseau, l'ID du nœud du système de basculement pour les clients système peut être saisi ici.
Inscription Internet auprès du SBC interne	Active la fonctionnalité SIP@Home. Cela permet à un téléphone SIP externe compatible STUN de s'enregistrer auprès d'OpenScape Business via Internet et d'être ainsi utilisé comme téléphone interne.
Boutons	
>	Passe à la station suivante. Si les stations correspondant au terme de recherche saisi dans les champs **de recherche** ont été préalablement filtrées, il est possible de se déplacer uniquement entre ces stations spécifiques.
<	Recule d'une station.

Description des paramètres des onglets :

- **Modifier le groupe/CFW**

Paramètres	Description
Stations - ...	
Taper	Type de station.
Numéro d'appel	Numéro d'appel interne de la station.
Nom	Nom de la station.
Transfert d'appel	
Destination du jour	Affiche les destinations de renvoi d'appel pour les appels externes entrants pendant la journée (voir l'assistant Téléphonie utilisateur/Renvoi d'appel).
Destination nocturne	Affiche les destinations de renvoi d'appel pour les appels externes entrants pendant la nuit (voir l'assistant Téléphonie utilisateur/Renvoi d'appel).
Destination interne	Affiche les destinations de renvoi d'appel pour les appels internes entrants (voir l'assistant Téléphonie utilisateur/Renvoi d'appel).
Classe de service	
Jour	Chaque abonné peut se voir attribuer une classe de service pour la journée. Il existe 15 classes de service parmi lesquelles choisir (voir Téléphonie/Classes de service).
Nuit	Chaque abonné peut se voir attribuer une classe de service pour la nuit. Il existe 15 classes de service parmi lesquelles choisir (voir Téléphonie/Classes de service).
Prise d'appel	

Paramètres	Description
Groupe	Chaque poste peut être affecté à un groupe de prise d'appel. Vous pouvez choisir parmi 32 groupes de prise d'appel (120 avec OpenScape Business S ; voir aussi Appels entrants / Prise d'appel).
Boutons	
>	Passe à la station suivante. Si les stations correspondant au terme de recherche saisi dans les champs **de recherche** ont été préalablement filtrées, il est possible de se déplacer uniquement entre ces stations spécifiques.
<	Recule d'une station.

27.3.7.10 Applications UC > de > la station

Les fonctionnalités des solutions de communications unifiées UC Smart et UC Suite sont présentées ici. Il est recommandé de configurer les paramètres de base sous « Configuration > Installation de base > Installation de base > Modifier les numéros d'appel et de fonction préconfigurés ».

Selon la solution UC utilisée, différentes fonctions sont affichées.

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Numéro d'appel du service
A FAIT	Numéro DID du service
Prénom	Prénom librement choisi pour le service. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement choisi pour le service. Plage de valeurs : max. 32 caractères.
Afficher	Nom du service librement choisi. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
Taper	Selon la solution UC : UC Smart : MeetMe / Conférence Suite UC : Standard automatique / Fax / Fax du centre de contact / Stationnement / MeetMe / Conférence / Groupe de fax

Paramètres	Description
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé au lieu du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis). **Remarque :** Le format CLIP n'est pas pris en charge pour la télécopie UC. Il n'est pris en charge que pour les télécopies analogiques.
Actif	Indique si le service est opérationnel.
Urgence SIP	Emplacement d'urgence SIP d'une station.
Recherche	Vous pouvez également afficher les services sélectionnés en saisissant un terme de recherche dans les champs **Rechercher** et en appuyant sur la touche Entrée. Les services correspondant à la recherche s'affichent. Si tous les champs **Rechercher** sont vides et si la touche Entrée est appuyée, tous les services seront de nouveau listés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **Numéro d'appel**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

27.3.7.11 Abonnés > Abonnés > Profils / Modèles

Il est possible de configurer ici des profils utilisateur (Paramètres d'abonné, Drapeaux abonnés, Groupes/Renvoi tempo.), ce qui permet de disposer d'une configuration de base pour un grand nombre d'utilisateurs à la fois.

Description des paramètres des onglets :

- **Modifier tous les profils**

Paramètres	Description
Profils	Affichage du numéro du profil.
Nom	Entrée d'un nom de profil quelconque.

Description des paramètres des onglets :

- **Afficher tous les profils utilisateur**

Paramètres	Description
Profils	Affichage du numéro du profil.
Nom	Affichage du nom du profil.
N° d'appel du membre	Affichage du n° interne du membre du profil.
Nom du membre	Affichage du nom du membre de profil.

Description des paramètres des onglets :

- **Ajouter/Supprimer profil Membre**

Paramètres	Description
Profils - ...	Affichage du numéro du profil.
Nom	Affichage du nom du profil attribué.
Profils membres	
Sélection	Liste des abonnés disponibles dans le système.
Membres	Liste des abonnés affectés au profil.
Boutons	
Ajouter	Reprendre dans la liste des membres du profil les abonnés sélectionnés.
Effacer	Effacer de la liste des membres du profil les abonnés sélectionnés.

Description des paramètres des onglets :

- **Importer/Exporter profil**

Paramètres	Description
Charger le profil via HTTP	
Nom de fichier distant (système de fichiers PC)	Chargement d'un fichier profil déjà existant au format XML
Exporter le profil via HTTP	
Nom de fichier	Affichage du nom du fichier dans lequel le profil est édité (format XML)
Action	Téléchargement du profil
Boutons	
Réinitialiser les valeurs par défaut	Les valeurs de profil de tous les abonnés affectés à ce profil sont réinitialisées à la valeur par défaut.

Description des paramètres des onglets :

- **Importer/Exporter tous les profils**

Paramètres	Description
Charger tous les profils via HTTP	

Paramètres	Description
Nom de fichier distant (système de fichiers PC)	Chargement d'un fichier profil déjà existant Dans ce fichier, il est aussi possible d'enregistrer plusieurs profils.
Exporter tous les profils via HTTP	
Nom de fichier	Affichage du nom du fichier où les profils sont enregistrés.
Action	Téléchargement des profils dans un fichier de profils.
Boutons	
Réinitialiser les valeurs par défaut	Les valeurs de profil de tous les profils et abonnés attribués sont réinitialisées à la valeur par défaut.

Description des paramètres des onglets :

- **Modifier les paramètres de l'abonné: voir Abonnés > Abonnés > Paramètres d'abonné**
- **Modifier les flags abonné: voir Abonnés > Abonnés > Paramètres d'abonné**
- **Modifier les groupes de renvoi: voir Abonnés > Abonnés > Paramètres d'abonné**

27.3.7.12 Abonnés > Abonnés > Numéros SDA

Il est affiché ici un aperçu des numéros SDA configurés avec les abonnés correspondants.

Description des paramètres des onglets :

- **Afficher les extensions SDA**

Paramètres	Description
Numéro	Affichage du numéro de l'abonné.
Nom	Affichage du nom de l'abonné.
SDA	Affichage du numéro SDA de l'abonné.
(d'autres champs peuvent être affichés)	

27.3.7.13 Entrée pour les personnes à mobilité réduite > de > la gare

Il est recommandé de configurer les utilisateurs mobiles via l'assistant « Téléphonie utilisateur > Intégration des téléphones mobiles ».

Description des paramètres des onglets :

- **Station de changement**

Paramètres	Description
Appelez le numéro	Saisie du numéro de poste interne de l'utilisateur Mobility (par exemple, 777). Ce numéro d'appel interne ne doit pas avoir déjà été attribué.
A FAIT	Saisie du numéro DID interne de l'utilisateur Mobility. Ce numéro DID interne ne doit pas avoir déjà été attribué.
Prénom	Prénom librement sélectionnable pour l'utilisateur Mobility. Plage de valeurs : max. 32 caractères.
Nom de famille	Nom de famille librement sélectionnable pour l'utilisateur Mobility. Plage de valeurs : max. 32 caractères.
Afficher	Nom librement choisi pour l'utilisateur Mobility. Par défaut, il est créé à l'aide des paramètres Prénom et Nom de famille en fonction de l'algorithme d'affichage du nom. Nombre de caractères maximum : 16, sans tréma ni caractères spéciaux.
Taper	Affiche le type d'utilisateur de la mobilité.
Type d'appareil	Affiche le type de téléphone système associé au fichier image.
Clip/Lin	Séquence de chiffres à afficher chez le destinataire appelé à la place du numéro réel pour les appels sortants (par exemple, pour les services d'urgence E911 aux États-Unis). Valeurs possibles : 16 chiffres maximum.
Accéder	Affiche l'interface physique à laquelle le périphérique est connecté.
Numéro d'appel mobile	Saisie du numéro de téléphone portable. L'entrée doit inclure le préfixe de numérotation sortante initial (c'est-à-dire le code CO), par exemple 0016012345678.
ID de fonctionnalité Web	L'identifiant de fonctionnalité Web définit comment l'abonné doit se connecter au client Web mobile (nom d'utilisateur). Choix entre « non » (utilisateur de Mobility Entry) et « automatique » (numéro d'appel interne de l'abonné ou de Mulap) ou sélection du numéro de poste du client ou du téléphone dans la liste déroulante.
Recherche	Vous pouvez également afficher les abonnés sélectionnés en saisissant un terme de recherche dans les champs **de recherche** et en appuyant sur la touche Entrée. Les abonnés correspondant aux termes de recherche sont affichés. Si vous laissez tous les champs **de recherche** vides et appuyez sur la touche Entrée, tous les abonnés seront à nouveau affichés.
Articles par page	Sélection permettant de déterminer si 10, 25, 50 ou 100 éléments doivent être affichés par page.
Boutons	
Flèche bleue dans la colonne **Numéro d'appel**	Affiche la page contenant les onglets **Modifier les paramètres de la station** , **Modifier les indicateurs de la station** , **Modifier les données client du point de travail** et **Modifier le groupe/CFW** .
>	Passe à la page suivante.
<	Recule d'une page.
>|	Se déplace à la fin de la liste.
|<	Se place en tête de liste.

Description des paramètres des onglets :

- **Passerelle secondaire**

  Uniquement pour les systèmes en réseau (multi-sites)

Paramètres	Description
Numéro d'appel	Numéro d'appel interne de l'utilisateur mobile.
Nom	Nom de l'utilisateur mobile.
ID du nœud	Saisie de l'identifiant du nœud via lequel l'abonné mobile est accessible de l'extérieur.

27.3.7.14 Abonné > Abonné > Utilisateur SfB

Description des paramètres des onglets :

- **Modifier un abonné**

Paramètres	Description
N° d'appel	Entrée du numéro de téléphone interne de l'abonné Skype for Business Client Mobility (par ex. 777). Ce numéro interne ne doit pas encore être attribué.
SDA	Numéro SDA du client Skype for Business.
Prénom	Prénom (au choix) de l'abonné. Plage de valeurs : 16 caractères maxi., sans inflexions ou caractères spéciaux.
Nom	Nom de famille (au choix) de l'abonné. Plage de valeurs : 16 caractères maxi., sans inflexions ou caractères spéciaux.
Afficher	Nom (au choix) de l'abonné. Par défaut, la création a lieu avec les paramètres de prénom et de nom, en fonction de l'algorithme d'affichage du nom. Plage de valeurs : 16 caractères maxi., sans inflexions ou caractères spéciaux.
Type	Affiche le type d'utilisateur Mobility, qui sera toujours Abonné SfB dans ce cas.
Numéro d'appel SfB	Numéro d'appel client Skype Entreprise.
Rechercher	Vous pouvez aussi afficher des abonnés sélectionnés en saisissant le terme de recherche dans les champs **Rechercher** et en validant avec la touche Retour. Les abonnés correspondant au terme de recherche sont affichés. Si tous les champs **Rechercher** sont vides et si la touche Retour est enfoncée, tous les abonnés sont de nouveau listés.
Eléments par page	Sélectionnez l'affichage de 10, 25, 50 ou 100 entrées par page.
Boutons	

Paramètres	Description
Flèche bleue dans la colonne **N° d'appel**	Appelle la page comportant les onglets **Modifier les Paramètres de l'abonné**, **Modifier les indicateurs abonné**, **Modifier les données du poste de travail Client** et **Modifier les groupes de renvoi**.
>	Saute à la page suivante.
<	Saute à la page précédente.
>|	Saute à la fin de la liste.
|<	Saute au début de la liste.

27.3.7.15 Abonnés > Abonnés > Vue d'ensemble des abonnés

Liste tous les abonnés du système de communication, avec tri par numéro de téléphone (par défaut). Cliquer sur un autre titre de colonne trie la colonne sélectionnée dans l'ordre ascendant, un nouveau clic effectue un tri dans l'ordre descendant.

Description des paramètres des onglets :

- **Modifier l'abonné**

Paramètres	Description
Numéro	Numéro interne de l'abonné.
SDA	Numéro SDA de l'abonné
Prénom	Prénom (au choix) de l'abonné. Plage de valeurs : 32 caractères maxi.
Nom	Nom de famille (au choix) de l'abonné. Plage de valeurs : 32 caractères maxi.
Afficher	Nom (au choix) de l'abonné. Par défaut, la création a lieu avec les paramètres de prénom et de nom en fonction de l'algorithme d'affichage du nom. Plage de valeurs : 16 caractères maxi., sans inflexions ni caractères spéciaux
Type d'équipement	Affichage du type d'abonné.
Activé	Indique si l'abonné est opérationnel.
Accès	Affichage de l'interface physique à laquelle le terminal est raccordé.
Rechercher	Vous pouvez aussi afficher des abonnés sélectionnés en saisissant le terme de recherche dans les champs **Rechercher** et en validant avec la touche Retour. Les abonnés correspondant au terme de recherche sont affichés. Si tous les champs **Rechercher** sont vides et si la touche Retour est appuyée, tous les abonnés sont de nouveau listés.
Eléments par page	Sélectionner l'affichage de 10, 25, 50 ou 100 entrées par page.
Boutons	

Paramètres	Description
Flèche bleue dans la colonne **Numéro**	Appelle la page comportant les onglets **Modifier les Paramètres de l'abonné**, **Modifier les indicateurs abonné**, **Modifier les données du poste de travail Client** et **Modifier les groupes de renvoi**.
>	Saute à la page suivante.
<	Saute à la page précédente.
>|	Saute à la fin de la liste.
|<	Saute au début de la liste.

27.3.7.16 Abonné > Programmation des touches

Description des paramètres des onglets :

- **Programmation des touches**

  La programmation des touches est uniquement supportée pour les téléphones UP0 et les clients HFA. La fonction de recherche (par les champs Numéro, SDA, Prénom, Nom de famille, Affichage et Type d'équipement) est disponible.

Paramètres	Description
Liste de sélection	Sélection du téléphone des abonnés.
Changement niveau	Si une touche avec la fonction "Changement niveau" a été paramétrée, il est possible de programmer ici le deuxième niveau.
Téléphone	Un clic sur la zone touche du téléphone ouvre la configuration actuelle des touches.
Champ de touche	Affichage de la fonction de la touche (identification des touches)
Touche	Sélection de la fonction souhaitée

Description des paramètres des onglets :

- **Reprendre la configuration des touches**

Paramètres	Description
Reprise de la configuration de touche à partir d'un abonné	Sélection de l'abonné dont la configuration de touche doit être reprise pour les abonnés sélectionnés.
Tous les abonnés	Reprendre la configuration de touche pour tous les abonnés.
Champ de sélection	Reprise de la configuration de touche uniquement pour les abonnés sélectionnés
Abonnés	Affichage des numéros internes et du nom de l'abonné.
Type d'équipement	Affichage du type de téléphone de l'abonné. Le type d'équipement ne peut pas être modifié pour les abonnés déjà actifs.

Paramètres	Description
Copier le type d'équipement à partir du poste	Sélection de l'abonné dont le type d'équipement doit être repris pour les abonnés sélectionnés.
vers le(les) poste(s) suivant(s)	Sélection du ou des postes dans lesquels le type d'équipement sera copié. Le filtrage par type d'équipement de l'abonné est disponible.

27.3.8 Cordless

Dans **Cordless** figurent les fonctions de la solution cordless intégrée pour l'exploitation de téléphones cordless (téléphones DECT) sur le système de communication. Ici est réalisée la configuration des stations de bas et des téléphones DECT (abonnés internes avec fonctionnalités HFA).

27.3.8.1 Cordless > Dans l'ensemble du système

Description des paramètres des onglets :

- **Modifier les données dans l'ensemble du système**

Paramètres	Description
Données CMI	
Identifiant système	Entrée de l'identifiant système DECT hexadécimal à 8 positions. Celui-ci est fourni lors de l'acquisition du système DECT. Il est configuré de la manière suivante : Chiffre 1 : E/ARC (Access Right Code) Chiffres 2.-5. : EIC (Equipment Installer's Code) Chiffres 6.-7 : (FPN Fixed Part Number) Chiffre 8 : (FPS Fixed Part Subscriber)
Bande fréq.	Choix de la bande de fréquences en fonction du pays. Il est affiché par défaut la bande de fréquences correspondant à l'identification du pays.
Codage parole	Affichage du codec voix pour l'ensemble du système (loi a, loi µ).
Chiffrement	Le cryptage est le chiffrement des données au niveau de l'interface radio ; il peut être activé ou désactivé. Par défaut : actif
Fenêtre enreg.	Horaires d'ouverture de la fenêtre pour la connexion des téléphones DECT. Ouverture de la fenêtre de connexion avec entrée sur un téléphones système de l'indicatif *94 2 19970707 et du mot de passe. Ensuite, les numéros des téléphones DECT à inscrire sont entrés dans la fenêtre de connexion. Par défaut : 10 minutes

Paramètres	Description
Traitement de l’écho Dans **Lignes** > **Paramètres/Flags généraux** Traitement d'écho réglé pour les utilisateurs mobiles, vous pouvez désactiver ces paramètres pour l'ensemble du noeud. Le paramétrage est réalisé après le réglage de la ligne des communications. Il faut pour chaque cas tester la possibilité d'amélioration offerte par une désactivation générale ou une activation spécifique à la ligne.	
Suppresseur d’écho activé	Le suppresseur d'écho (ES) active en fonction du niveau d'émission du téléphone DECT un affaiblissement dans le sens réception du téléphone DECT. Lorsque le suppresseur d'écho est activé, cela peut provoquer des bruits parasites forts étant donné que le signal de réception est affaibli de manière supplémentaire. Cela rend la compréhension plus difficile. En mode **Désactivé**, le faisceau réception du téléphone DECT ne bénéficie pas d'un affaiblissement lorsque le niveau d'émission du téléphone DECT est élevé. Sur un réseau analogique, lorsque l'environnement est bruyant, ce paramétrage assure une meilleure compréhension entre les correspondants sur les téléphones DECT. Par défaut : Automatique
Annuleur d’écho	L'annuleur d'écho (EC) élimine les retours de signal non souhaitées qui sont provoquées par une conversion 4/2 fils (termineur) dans le réseau fixe. Lorsque l'annuleur d'écho est activé sans écho, il peut se produire des erreur car l'annuleur d'écho essaie de s'adapter à un écho qui n'existe pas. En mode **Désactivé** l'activation de ce paramètre est impossible et l'annuleur d'écho (Echo Canceller) est toujours désactivé. Par défaut : Automatique
Echo artificiel activé	A l'aide de l'acheminement Artificial Echo (AE) (écho artificiel), le signal voix en provenance du réseau fixe est renvoyé à l'abonné distant avec un amortissement de 24 dB. Cela peut être nécessaire afin de donner dans certains cas (liaison internationale par ex.) une certaine précharge à un annuleur d'écho ajouté. En mode **Désactivé** l'activation de ce paramètre est impossible et l'Echo artificiel (Artificial Echo) est toujours désactivé. Par défaut : Automatique
PP Deviation Control	Lors des connexions VoIP à l'aide de téléphones DECT, il se produit souvent des échos. Pour éliminer/réduire ces échos, la fonction "PP Deviation Control" peut être activée. Cette fonction agit sur tous les mobiles DECT raccordés au système de communication. Pour un combiné, l'activation ou la désactivation n'est opérationnelle qu'après arrêt et remise en marche. En mode **Désactivé**, la suppression d'écho n'est pas opérante et il peut donc se produire des phénomènes d'écho sur les liaisons VoIP avec des mobiles DECT. Par défaut : désactivé
Mode ECO	
Mode ECO	Le mode ECO peut être activé pour tous les téléphones DECT sur l'ensemble du système. Dans ce cas, soit la puissance d'émission des téléphones DECT est abaissée d'une valeur fixe (statique), soit chaque téléphone DECT adapte de manière autonome sa puissance d'émission à la puissance du signal reçu (adaptatif). Par défaut : désactivé
Mode ECO : **Désactivé**	Le mode ECO est désactivé dans l'ensemble du système.

Paramètres	Description
Mode ECO : **Activé**	Le mode ECO (statique) est activé dans l'ensemble du système. La puissance d'émission des téléphones DECT est abaissée d'une valeur fixe.
Mode ECO : **Evolutif**	Le mode ECO (adaptatif) est activé dans l'ensemble du système. Chaque téléphone DECT individuel adapte de manière autonome sa puissance d'émission à la force du signal reçu. En cas de handover (transfert automatique intercellulaire), la commutation se fait tout d'abord sur la puissance d'émission élevée et ensuite, elle est réduite en fonction de la réception.

27.3.8.2 Cordless > SLC

Description des paramètres des onglets :

- **Modifier les téléphones DECT**

Paramètres	Description
Numéro	Numéro du téléphone DECT.
SDA	Numéro SDA du téléphone DECT.
Nom	Nom du téléphone DECT.
Activé	Etat de connexion du téléphone DECT: Vert : téléphone DECT actif. Rouge : interrupteur de cartes activé pour téléphone DECT déclaré. Jaune : le téléphone DECT a été automatiquement déconnecté en raison de la modification du PIN. Gris : aucun téléphone DECT n'a encore été déclaré sur ce port.
Code mobile	Code PIN pour la connexion du téléphone DECT. Le code mobile doit être univoque pour l'ensemble du système.
Accès	Nom, numéro et emplacement de la ligne de prolongation S_0.
Emplacement	Affichage de l'emplacement des modules SLC enfichés.
Boutons	
Effacer	Le téléphone DECT est sorti du système. Dans ce cadre, le numéro de téléphone, le n° SDA et le nom sont supprimés et la licence TDM User correspondante est libérée.

Description des paramètres des onglets :

- **Ajouter téléphones DECT**

Paramètres	Description
Identifiant système	Si le système de communication ne fait pas partie d'une interconnexion de réseaux (ID de noeud = 0), l'identifiant système est prédéfini avec 1. Si le système de communication fait partie d'une interconnexion de réseaux (ID de noeud > 0), l'identifiant système doit être identique à l'ID de noeud (**Cordless** > **Multi SLC** > **Identifiant système**).

Paramètres	Description
Emplacement	Affichage du module SLC enfiché.
N° SLC	Numéro ID univoque dans l'ensemble du système pour le module SLC. Plage de valeurs : 1-15,17-31,33-47,...,127. Les multiples de 16 ne sont pas autorisés.
Nombre de téléphones	Nombre des téléphones DECT déjà configurés de ce module SLC.
SLC Numéro	Numéro de téléphone univoque dans l'ensemble du système pour la ligne de prolongation S_0.
Accès	Nom, numéro et emplacement de la ligne de prolongation S_0.
Ajouter téléphones DECT	
Nombre de téléphones	Si le nombre des téléphones DECT est inférieur à la taille admissible dans le système (en fonction de la version) un nombre supplémentaire de téléphones DECT peut être ajouté pour ce module SLC. Les nouveaux téléphones DECT ajoutés sont présentés dans l'onglet **Modifier les téléphones DECT**.

27.3.8.3 Cordless > Multi-SLC

Description des paramètres des onglets :

- **Modifier Multi-SLC**

Paramètres	Description
N° SLC	Numéro ID univoque dans l'ensemble du système pour le module SLC. Plage de valeurs : 1-15,17-31,33-47,...,127. Les multiples de 16 ne sont pas autorisés.
ID de nœud	Affichage de l'ID de noeud (si configuré). Si le système de communication fait partie d'une interconnexion de réseaux, il est présenté ici tous les modules SLC configurés de l'interconnexion de réseaux.
SLC Numéro	Numéro de téléphone univoque dans l'ensemble du système pour la ligne de prolongation S_0 du module SLC.

27.3.8.4 Cordless > Station de base

Description des paramètres des onglets :

- **Modifier stations de base**

Paramètres	Description
Emplacement	Affichage de l'emplacement où le module SLC est inséré dans la station de base. Pour la carte mère (SLUC), l'emplacement 2 est indiqué.

Paramètres	Description
Type	Type de station de base. Avec un module SLC, le type est seulement présenté ; avec SLUC il est possible de sélectionner le type. Si le type est modifié de **Libre** en **Station de base**, il est automatiquement préconfiguré 16 téléphones DECT et une ligne de mise en réseau SLC.
Type : **Station de base**	Station de base en marche.
Type : **Libre**	Aucune station de base en marche.
Nom	Nom de la station de base.
Niveau	Niveau de la station de base. Plage de valeurs : 50 % et 100 %; valeur par défaut : 100%
État	Etat de la station de base.
Maître	Avec un module SLC, il est affiché les ports auxquels les stations de base sont raccordées. Avec SLUC tous les ports avec les terminaux raccordés sont présentés.

27.3.9 Appels entrants

Le menu **Appels entrants** regroupe les fonctions pour la gestion des appels (Call Management, CM). Ce sont notamment les paramètres pour les groupes et le renvoi temporisé.

27.3.9.1 Appels entrants > Groupes/Groupes de recherche

Pour la configuration initiale des appels de groupe et des groupes de recherche, il est recommandé d'utiliser l'assistant **Appel de groupe / Groupe de recherche**.

Description des paramètres des onglets :

- **Modifier les numéros d'appel de groupe**
- **Afficher les groupes utilisés**
- **Afficher tous les membres du groupe**
- **Ajouter un groupe**
- **Supprimer un groupe**
- **Modifier les paramètres du groupe**
- **Afficher les membres**
- **Ajouter un membre**
- **Modifier l'ordre des membres**
- **Vérifier les MULAP de base**
- **Vérifier les préférences MULAP**

Paramètres	Description
Index	Numéro consécutif attribué par le système de communication.

Paramètres	Description
Numéro d'appel	Numéro de téléphone de l'appel de groupe, du groupe de recherche, du MULAP de base, du MULAP exécutif ou du groupe de messagerie vocale
SDA	Numéro SDA de l'appel de groupe, du groupe de recherche, du MULAP de base, du MULAP exécutif ou du groupe de messagerie vocale
Prénom	Prénom librement sélectionnable pour l'appel de groupe, le groupe de recherche, le MULAP de base, le MULAP exécutif ou le groupe de messagerie vocale. Plage de valeurs : 16 caractères maxi., sans inflexions ni caractères spéciaux
Nom	Nom librement sélectionnable pour l'appel de groupe, le groupe de recherche, le MULAP de base, le MULAP exécutif ou le groupe de messagerie vocale. Plage de valeurs : 16 caractères maxi., sans inflexions ni caractères spéciaux
Afficher	Nom de l'appel de groupe, du groupe de recherche, du MULAP de base, du MULAP exécutif ou du groupe de messagerie vocale Par défaut, la création a lieu avec les paramètres de prénom et de nom en fonction de l'algorithme d'affichage du nom.
Type	Définition du type de groupe Valeur par défaut : Groupe Pour plus d'informations, voir : Tableau : Options de type
Type de sonnerie	Définit la signalisation acoustique des appels externes entrants vers le groupe Valeur par défaut : 1 Sur les téléphones analogiques, seul le paramètre par défaut est possible. Les modifications n'ont pas d'influence.
Type de sonnerie : 1	Deux sonneries
Type de sonnerie : 2	Sonnerie à trois tons
Type de sonnerie 3	Sonnerie courte/longue/courte
Annuaire téléphonique	Lorsque cet indicateur est activé (Afficher Oui), le numéro d'appel du groupe apparaît dans l'annuaire interne. Valeur par défaut : Activé
Mulap en tant que membre du groupe	Lorsque cet indicateur est activé, le groupe MULAP peut être ajouté en tant que membre dans Groupes.
Membre du groupe	
Groupe	Numéro (index) du groupe
Membre	Numéro (index) du membre au sein du groupe
Numéro d'appel	Numéro d'appel du membre du groupe
Nom	Nom du membre du groupe
Paramètres	Paramètres activés du membre du groupe

Paramètres	Description
Paramètre : M	Maître (M) : MULAP de base : Le membre est le maître du MULAP de base. MULAP exécutif : Le membre dispose de fonctions exécutives.
Paramètre : R	Appel acoustique (R) : MULAP de base et MULAP exécutif : Les appels entrants sont signalés par un signal acoustique.
Paramètre : A	Saisie automatique sortante (A) : MULAP de base : La ligne MULAP de base est automatiquement sélectionnée pour un appel lorsque vous décrochez le combiné. MULAP exécutif : La ligne MULAP exécutif est automatiquement sélectionnée pour un appel lorsque vous décrochez le combiné.
Paramètre : K	Pas d'acceptation automatique des appels entrants (K) : MULAP de base et MULAP exécutif : Pour accepter l'appel entrant, il faut appuyer sur la touche MULAP.
Paramètre : P	Libération automatique de la confidentialité (P) : MULAP de base et MULAP exécutif : Vous pouvez libérer la ligne MULAP occupée pour une conférence en appuyant sur la touche MULAP.
Touche MULAP configurée	Indique si une touche MULAP a été configurée pour le membre du groupe.
Acheminement	Pour un membre externe du groupe, l’itinéraire est affiché.
Groupe	
Contrôle de cohérence	Les collisions possibles dues au chevauchement des maîtres des MULAP de base ou à la saisie automatique des MULAP de base sont affichées.

Tableau 63 : Options de type

Paramètres	Description
Toutes les conversions de type de groupe sont autorisées sans suppression des membres du groupe, à l'exception des types de groupe MULAP. **Remarque :** Si un groupe de type *Groupe*, *Groupe de recherche linéaire*, *Groupe de recherche cyclique* ou *Messagerie vocale* a un groupe MULAP comme membre, la conversion en groupe *RNA* ou *groupe d'attente d'appel* n'est pas autorisée. **Remarque :** Si un membre du groupe configure le transfert d'appel (*1) vers un autre *groupe de recherche*, *groupe d'attente d'appel* et *groupe RNA*, l'appel n'est pas acheminé. Ceci est interdit afin d'éviter les boucles d'appel. Pour les appels directs vers la station, le transfert est valide. Pour les membres des *groupes cycliques*et *linéaires (groupes de recherche)*, cela est autorisé, *1 vers n'importe quelle destination fonctionne, sauf pour la messagerie vocale.	
Type : Groupe de recherche linéaire	Un appel entrant est toujours signalé en premier lieu au premier membre d'un groupe de recherche. La suite de la signalisation est effectuée en fonction de l'ordre dans lequel les membres sont entrés dans le tableau des groupes.
Type : Groupe de recherche cyclique	Un appel entrant est toujours signalé en premier au membre qui suit l'abonné qui a répondu au dernier appel. La suite de la signalisation est effectuée en fonction de l'ordre dans lequel les membres sont entrés dans le tableau des groupes.
Type : Groupe	Appel de groupe de type Groupe : Les appels entrants sont signalés simultanément chez tous les membres du groupe disponibles. Les membres du groupe disponibles sont les abonnés qui ne sont pas occupé. Chez les membres du groupe occupés, un appel en attente est signalé immédiatement par un bip d'avertissement. Si un abonné raccroche, l'appel continue à être signalé chez tous les membres du groupe (bip d'avertissement chez les abonnés occupés).
Type : RNA	Appel de groupe de type RNA : Les appels entrants sont signalés simultanément chez tous les membres du groupe. Si un membre du groupe est occupé, l'ensemble de l'appel de groupe est marqué comme occupé (seuls les membres occupés sont signalés pour l'appel entrant). Les appelants du groupe reçoivent la tonalité occupée.
Type : MULAP de base	Les appels entrants sont signalés visuellement sur tous les téléphones associés au MULAP (Multiple Line Appearance) de base. L'abonné peut également définir si les appels entrants doivent également être signalés acoustiquement pour chaque membre individuel. Le statut du MULAP de base passe à occupé et les autres appelants entendent le signal d'occupation lorsqu'ils répondent à un appel. Le numéro de téléphone du MULAP de base est affiché sur l'écran de l'appelé pour les appels sortants via la ligne MULAP de base.

Paramètres	Description
Type : MULAP exécutif	Vous pouvez configurer des MULAP exécutifs si vous souhaitez utiliser des fonctions exécutives et de secrétariat restreintes. Si un appelant compose le numéro de téléphone MULAP exécutif, l'appel est signalé visuellement sur tous les téléphones appartenant au MULAP exécutif. Les appels entrants sont également signalés acoustiquement pour les membres disposant de fonctions de secrétariat.
Type : Appel en attente	Appel de groupe de type Appel en attente : Les appels entrants sont signalés simultanément chez tous les membres du groupe disponibles. Les membres du groupe disponibles sont les abonnés qui ne sont pas occupé. Un appel est signalé par une tonalité d'occupation pour les membres du groupe qui sont occupés.
Type : Boîte vocale	Groupe de messagerie vocale : Un groupe de messagerie vocale permet à un groupe spécifique d'abonnés d'accéder aux messages vocaux. Lorsqu'un appel est passé au numéro d'appel d'un groupe de messagerie vocale, l'appel est envoyé directement à la boîte vocale (c'est-à-dire la messagerie vocale) du groupe et non aux membres du groupe. Une fois qu'un message vocal a été laissé dans la boîte vocale du groupe, il est transféré vers les boîtes vocales de tous les membres. Tous les membres reçoivent le message vocal simultanément. Lorsqu'un membre supprime un message vocal, celui-ci est également supprimé des boîtes vocales de tous les membres et de la boîte vocale du groupe. Les messages vocaux personnels de tous les membres ne sont pas affectés par cette opération.

27.3.9.2 Appels entrants > Membres du groupe

Description des paramètres des onglets :

- **Modifier le membre**
- **Effacer le membre**

Paramètres	Description
Groupe	Numéro (Index) du groupe
Membre groupe	Numéro (Index) du membre du groupe
Numéro de téléphone	Numéro de téléphone du membre du groupe
Prénom	Prénom (au choix) du membre du groupe. Plage de valeurs : 16 caractères maxi., sans inflexions ni caractères spéciaux
Nom	Nom de famille (au choix) du membre du groupe. Plage de valeurs : 16 caractères maxi., sans inflexions ni caractères spéciaux
Nom	Nom du membre du groupe Par défaut, la création a lieu avec les paramètres de prénom et de nom en fonction de l’algorithme d’affichage du nom.
Nom MULAP	Nom du groupe MULAP (Multiple Line Appearance). Il s’agit du nom MULAP affiché sur l’écran du téléphone lorsque ce groupe Team est appelé. Le nom MULAP est le même pour tous les membres du groupe Team du même type.

Paramètres	Description
N° d'appel MULAP	Numéro de groupe MULAP
Master (M)	MULAP de base : par activation de ce flag, un membre devient le maître d'un MULAP de base. Si un maître active un renvoi d'appel, celui-ci s'applique à tous les membres (téléphones) du MULAP de base. MULAP Chef : grâce à l'activation de cet indicateur, un membre reçoit des fonctions de chef. Lorsque le combiné est décroché, il y a automatiquement appel par la ligne MULAP chef. Les appels entrants par le numéro MULAP chef sont signalés exclusivement de façon optique.
Sonnerie acoustique (R)	MULAP de base et MULAP chef : Lorsque ce flag est activé, les appels entrants sont signalés de manière acoustique. Valeur par défaut : activé pour tous les maîtres d'un MULAP de base. Active tous les membres avec fonction Chef d'un MULAP chef.
Prise automatique sortante (A)	MULAP de base : lorsque le flag est activé, l'appel a lieu automatiquement sur la ligne MULAP de base lorsque le combiné est décroché. MULAP Chef : lorsque ce flag est activé, l'appel a lieu automatiquement sur la ligne MULAP chef lorsque le combiné est décroché. Valeur par défaut : activé pour tous les maîtres d'un MULAP de base. Active tous les membres avec fonction Chef d'un MULAP chef.
Pas de prise d'appel automatique entrante (K)	MULAP de base et MULAP chef : Lorsque ce flag est activé, il n'est pas possible de prendre l'appel entrant en décrochant le combiné. Vous pouvez uniquement répondre à un appel entrant en appuyant sur la touche MULAP. Valeur par défaut : Désactivé
Autorisation conférence automatique (P)	MULAP de base et MULAP chef : Lorsque ce flag est activé, une pression sur la touche MULAP valide la ligne MULAP pour la conférence. Chez tous les autres participants, la validation est signalée par le clignotement de la touche MULAP. Pour rejoindre la conférence, appuyez sur la touche MULAP. Valeur par défaut : Désactivé
Touche MULAP configurée	MULAP de base : lorsque ce flag est activé, une touche MULAP est configurée sur le téléphone correspondant. L'appui sur la touche provoque une prise sortante par la ligne MULAP de base. Le numéro MULAP de base apparaît sur l'écran de l'appelé. MULAP Chef : lorsque ce flag est activé, une touche MULAP est configurée sur le téléphone correspondant. Vous pouvez appuyer sur la touche pour configurer un appel sortant via la ligne MULAP chef. Le numéro MULAP chef s'affiche sur l'écran de la personne appelée. Valeur par défaut : Activé
Faisceaux	Pour un membre de groupe externe, la voie est affichée.
Type	Définition du type de groupe

27.3.9.3 Gestion des appels > Team/Top

Lors de la première configuration des groupes Team et Top, il est recommandé d'utiliser les assistants **Configuration Team** et **Chef/Secrétaire**.

Description des paramètres des onglets :

- **Afficher tous les groupes Team/Top**
- **Afficher les groupes Team/Top utilisés**
- **Ajouter un groupe Team/Top**
- **Modifier le groupe Team/Top**
- **Effacer le groupe Team/Top**
- **Modifier le groupe Team/Top**
- **Afficher tous les membres du groupe Team/Top**
- **Ajouter un membre Team/Top**
- **Modifier le membre Team/Top**
- **Effacer le membre Team/Top**
- **Afficher les boîtes Fax**
- **Ajouter une boîte Fax**

Paramètres	Description
L'index	Numéro consécutif, attribué par le système de communication.
Prénom	Prénom (au choix) du groupe Team/Top. Plage de valeurs : 16 caractères maxi., sans inflexions ni caractères spéciaux
Nom	Nom de famille (au choix) du groupe Team/Top. Plage de valeurs : 16 caractères maxi., sans inflexions ni caractères spéciaux
Nom	Nom du groupe Team/Top Par défaut, la création a lieu avec les paramètres de prénom et de nom en fonction de l'algorithme d'affichage du nom.
Type	Définition du type de groupe
Type : Team	Un groupe Team offre plusieurs fonctions d'équipe pratiques. Les numéros de téléphone de tous les membres d'une équipe ont été programmés sur les touches MULAP (touches de ligne). Chaque membre de l'équipe a donc accès à toutes les lignes (pour l'interception d'appel, par exemple) et peut téléphoner simultanément sur plusieurs lignes.
Type : Haut	Un groupe Top offre des fonctions Chef/Secrétaire conviviales (fonction Top) pour jusqu'à trois chefs et jusqu'à trois secrétaires.
Équipe en tant que membre du groupe	Cet indicateur peut être configuré uniquement lorsque des membres du groupe Team possèdent le même type de poste, ce qui crée un seul groupe MULAP sous ce groupe Team. Lorsque cet indicateur est activé, le groupe MULAP peut être ajouté en tant que membre dans les groupes.
Assignation des touches sur Team	Définition de la configuration des touches MULAP des membres du groupe Team
Assignation des touches sur Team : sur la 1ère/2ème console	Lorsque cet indicateur est activé, les touches MULAP sont automatiquement configurées sur le premier ou le deuxième appareil supplémentaire (touche Module ou BLF) du téléphone Team.

Paramètres	Description
Assignation des touches sur Team : sur les 1ères touches libres	Lorsque cet indicateur est activé, les touches MULAP sont automatiquement configurées sur les premières touches libres du téléphone Team.
Assignation des touches sur Top	Définition de la configuration des touches MULAP des membres du groupe Top
Assignation des touches sur Top : sur la 1ère/2ème console	Lorsque cet indicateur est activé, les touches MULAP sont automatiquement activées sur le premier ou le deuxième appareil supplémentaire (touches Module ou BLF) du téléphone Top.
Assignation des touches sur Top : sur les 1ères touches libres	Lorsque cet indicateur est activé, les touches MULAP sont automatiquement configurées sur les premières touches libres du téléphone Top.
Membre groupe	
Groupe	Numéro (Index) du groupe
Membres	Numéro (Index) du membre à l'intérieur du groupe
Type	Définition du type de membre
N° d'appel	Numéro de téléphone du membre du groupe (modifie un groupe MULAP en ** Numéro d’appel et est accessible en interne sous ce ** Numéro d’appel.)
Nom	Nom du membre du groupe
N° d'appel MULAP	Numéro de groupe MULAP
N° SDA MULAP	Numéro SDA du groupe MULAP
Nom MULAP	Nom de groupe MULAP. Il s’agit du nom MULAP affiché sur l’écran du téléphone lorsque ce groupe Team est appelé. Le nom MULAP est le même pour tous les membres du groupe Team du même type.
Type de sonnerie	Définition de la signalisation acoustique des appels externes entrants du groupe Valeur par défaut : 1 Sur les téléphones analogiques, seul le paramètre par défaut est possible. Les modifications n'ont pas d'influence.
Type de sonnerie : 1	Double tonalité d'appel
Type de sonnerie : 2	Sonnerie à trois tons
Type de sonnerie : 3	Sonnerie courte/longue/courte
Annuaire	Lorsque l'indicateur est activé (affichage Oui) il apparaît le numéro d'appel du groupe dans le répertoire interne. Valeur par défaut : Activé

Paramètres	Description
Master (M)	Groupe Team : grâce à l'activation de ce paramètre, un membre devient le maître du groupe Team. Si un maître active un renvoi d'appel, cette fonction s'applique à tous les membres (téléphones) du groupe Team. Groupe Top : grâce à l'activation de cet indicateur, un membre reçoit des fonctions de chef. Lorsque le combiné est décroché, la ligne MULAP chef est automatiquement sélectionnée pour l'appel. Les appels entrants via le numéro MULAP chef associé sont par défaut uniquement indiqués avec un signal visuel.
Sonnerie acoustique (R)	Groupe Team et Groupe Top : Lorsque ce flag est activé, les appels entrants sont signalés de manière acoustique. Valeur par défaut : Activé pour tous les membres d'un groupe Team. Activé pour tous les membres d'un groupe Top disposant de la fonction Secrétaire.
Prise automatique sortante (A)	Groupe Team et Groupe Top : Lorsque ce flag est activé, lorsque le combiné est décroché, l'appel a lieu automatiquement par la ligne MULAP de ce membre. Valeur par défaut : Activé
Pas de prise d'appel automatique entrante (K)	Groupe Team et Groupe Top : Lorsque ce flag est activé, il n'est pas possible de prendre l'appel entrant en décrochant le combiné. Vous pouvez uniquement répondre à un appel entrant en appuyant sur la touche MULAP. Valeur par défaut : Désactivé
Autorisation conférence automatique (P)	Groupe Team et Groupe Top : Lorsque ce flag est activé, une pression sur la touche MULAP valide la ligne MULAP pour la conférence. Chez tous les autres participants, la validation est signalée par le clignotement de la touche MULAP. Pour rejoindre la conférence, appuyez sur la touche MULAP. Valeur par défaut : Désactivé
Touche MULAP configurée	Groupe Team : lorsque ce flag est activé, une touche MULAP est configurée sur le téléphone correspondant. Appuyez sur la touche pour configurer un appel sortant via la ligne MULAP du maître. Le numéro du poste MULAP du maître s'affiche sur l'écran de la personne appelée. Groupe Top : lorsque ce flag est activé, une touche MULAP est configurée sur le téléphone correspondant. Vous pouvez appuyer sur la touche pour configurer un appel sortant via la ligne MULAP chef. Le numéro MULAP chef s'affiche sur l'écran de la personne appelée. Valeur par défaut : désactivée pour tous les membres d'un groupe Team. Activé pour tous les membres d'un groupe Top.
Type MULAP	Définition du type MULAP
Type MULAP : MULAP de base	Les appels entrants sont indiqués par un signal visuel sur tous les téléphones associés au MULAP de base. Pour chaque membre, il est possible d'indiquer également si les appels entrants doivent être aussi signalés de façon acoustique. Après la réception de l'appel, le MULAP de base est occupé et les autres appelants entendent la tonalité d'occupation. Pour les appels entrants par la ligne MULAP de base, le numéro MULAP de base apparaît sur l'écran des appelés.

Paramètres	Description
Type MULAP : MULAP Chef	Tous les membres d'un MULAP chef peuvent être joints sous le numéro MULAP chef et sous leurs numéros de poste personnels.
N° d'appel Fax	Numéro de la boîte fax du membre du groupe
SDA Fax	Numéro SDA de la boîte Fax du membre du groupe

27.3.9.4 Appels entrants > Interception d'appel

Description des paramètres des onglets :

- **Modifier le nom des groupes d'interception**
- **Afficher les abonnés du groupe**
- **Affecter les abonnées au groupe**

Paramètres	Description
Groupe	
Groupe	Numéro (Index) du groupe d'interception Plage de valeurs : 1 à 32 (120 pour OpenScape Business S)
Nom	Nom du groupe d'interception
Abonnés	
N° d'appel	Numéro d'abonné de l'abonné interne
Nom	Nom de l'abonné interne
Affectation au groupe X	Lorsque l'indicateur est activé, l'abonné et affecté au groupe d'interception X.
Groupe	Groupe d'interception qui est affecté à ces abonnés.

27.3.9.5 Appels entrants > UCD

Description des paramètres de l'onglet :

- **Modifier les paramètres UCD**

Paramètres	Description
Flags UCD	
Libérer application UCD	Lorsque le flag est activé, la fonctionnalité de distribution des appels (UCD - Uniform Call Distribution) est validé pour l'ensemble du système. Valeur par défaut : Activé
Agents toujours disponibles	Lorsque le flag est activé, tous les agents UCD sont des agents toujours disponibles. Un agent disponible de manière durable demeure ensuite disponible pour les appels, fax et e-mails, même s'il n'a pas répondu à un appel, un fax ou un e-mail. Valeur par défaut : Désactivé

Paramètres	Description
Postraitement	
Temps de postraitement (cycles)	La définition du délai de post-traitement automatique se fait, pour tous les agents UCD, par cycles d'appels, c'est-à-dire par paliers de 5 secondes. Pendant la durée du post-traitement, un agent est temporairement exempté de la distribution des appels afin qu'il puisse réaliser des opérations de post-traitement pour l'appel qui vient de s'achever. Valeur par défaut : 0
Priorite sur appels internes	
Priorite interne	Définition de la priorité sur l'ensemble du système pour appels internes à l'aide de 10 niveaux de priorité (1 = élevé, 10 = bas). Valeur par défaut : 10
Priorite sur appels externes	
Slot / Ligne	Affichage du module, de l'emplacement d'enfichage (slot) et du numéro de la ligne (du canal B). Pour les appels externes, l'affectation de priorité se fait en fonction de la ligne (par canal B), qu'il s'agisse de lignes IP ou TDM.
Priorité	Définition de la priorité pour les appels externes qui arrivent par la ligne concernée (canal B). La définition est réalisée à l'aide de 10 niveaux de priorité (1 = élevé, 10 = bas). Valeur par défaut : 1

Description des paramètres des onglets :

- **Afficher les groupes UCD**
- **Modifier le groupe UCD**

Paramètres	Description
Numéro d'appel	Numéro de téléphone du groupe UCD
MSN	Numéro SDA du groupe UCD
Nom	Nom du groupe UCD
Cycles de sonnerie primaire	Définition du cycle de sonnerie primaire : L'indication se fait en cycles de sonneries, c'est-à-dire par paliers de 5 secondes. Vous paramétrez le temps pendant lequel un appel reste en file d'attente s'il n'est pas pris par l'agent qui se trouve à l'état Disponible depuis le plus de temps. Ensuite, l'appel est transféré à l'agent disponible suivant. Valeur par défaut : 3 Cycles
Distribution 2 (cycl. sec.)	Définition du cycle de sonnerie secondaire : L'indication se fait en cycles de sonneries, c'est-à-dire par paliers de 5 secondes. Vous paramétrez le temps pendant lequel un appel reste en file d'attente s'il n'est pas pris par l'agent disponible suivant. Valeur par défaut : 3 Cycles

Paramètres	Description
Appels en attente	Définition du nombre maximum des appels en attente : Si le nombre maximum d'appels en attente est dépassé, les autres appels peuvent être acheminés à une destination de débordement (une destination externe, un autre groupe UCD, un abonné interne ou un groupe). Valeur par défaut : 10 (valeur par défaut du dernier groupe UCD : 72)
AICC	Définition de l'Automatic Incoming Call Connection AICC. Le paramétrage s'applique à tous les agents d'un groupe UCD que le téléphone de l'agent soit équipé d'un casque ou pas. Valeur par défaut : Non
AICC : Oui	Les agents de ce groupe UCD peuvent accepter les appels entrants sans opérations supplémentaires. L'agent est averti par un bip dans le casque de l'arrivée d'un appel, qui lui est automatiquement et immédiatement transféré.
AICC : Non	Les agents de ce groupe UCD ne doivent pas prendre les appels entrants sans les opérations habituelles (par exemple en décrochant le combiné).
Changement annonce	Définition des changements d'annonce possibles Valeur par défaut : une fois
Changement annonce : individuel	Les appelants figurant dans la file d'attente entendent une annonce unique.
Changement annonce : Cyclique	La dernière et l'avant-dernière annonces dans la configuration sont répétées de façon cyclique.
Temps débordement	Définition du délai de débordement en secondes : Si un appel en attente n'est pas pris par l'application UCD dans le délai de débordement, l'appel continue à être traité par le système de communication grâce aux indications de la Gestion des appels. Ce paramétrage a un intérêt uniquement si une application UCD externe est raccordée. Valeur par défaut : 600
Retard annonce	Définition du retard de l'annonce en secondes : une fois ce délai écoulé, l'appelant qui est dans la file d'attente entend une annonce. Valeur par défaut : 0

Description des paramètres de l'onglet :

- **Modifier les paramètres du groupe UCD**

Paramètres	Description
Index de dest.	Pour chaque groupe UCD, il est possible de définir jusqu'à sept destinations (Index 1 à 7) pour les annonces. Les annonces des destinations sont diffusées à l'appelant l'une après l'autre dans la file d'attente.
Annonce	Annonce pour l'index de destination correspondant.

Paramètres	Description
Temps d'attente	L'annonce peut être cyclique (9 cycles maxi. de 5 s = 45 s) ou diffusée en continu. Une fois cette période de temps écoulée, il est diffusé à l'appelant l'annonce de l'index suivant dans la file d'attente (pas dans en **continu**). Valeur standard : en continu

Description des paramètres de l'onglet :

- **Ajouter/Effacer Membres du groupe UCD**

Paramètres	Description
Sélection	Liste de tous les ID d'agents UCD Les ID d'agent UCD ne correspondent pas aux numéros d'appel dans le système de communication.
Membres	Liste des ID d'agents UCD du groupe UCD sélectionné
Boutons	
Ajouter	Ajoute au groupe UCD les ID d'agents UCD marqués.
Effacer	Efface dans le groupe UCD les ID d'agents UCD marqués.

Description des paramètres de l'onglet :

- **Affecter les abonnés**

Paramètres	Description
ID d'agent	Liste des ID d'agents UCD du groupe UCD sélectionné.
Abonnés	Liste des abonnés qui peuvent être affectés aux ID d'agents UCD du groupe UCD.

27.3.9.6 Appels entrants > Renvois d’appels

Description des paramètres des onglets :

- **Tables d'acheminement - Définition**

Paramètres	Description
Table d’acheminement	Sélection de la table d’acheminement à traiter. Plage de valeurs : 1 à 740
Modifier le renvoi temporisé Pour retrouver plus rapidement une destination d’appel, vous pouvez entrer un ou plusieurs chiffres dans les champs **Dest 1 - Dest 4**. Ensuite, vous êtes directement redirigé vers l’entrée de la liste qui commence par la séquence de chiffres saisie. L’entrée d’une séquence de lettres est également possible.	
Dest 1 - 4 : **Pas d’entrée**	La destination de l’appel est sautée.

Paramètres	Description
Dest 1 - 4 : **Destination externe**	Faisceau et numéro de téléphone externe avec code d'accès CO.
Dest 1 - 4 : *** Abonné appelé**	Abonnés appelés
Dest 1 - 4 : **** Défini(e) par l'utilisateur**	Destination du renvoi d'appel après tempo (si paramétré).
Dest 1 - 4 : **#9 Recherche système**	Abonné suivant disponible (à l'exclusion du poste Chef).
Dest 1 - 4 : **#201 - #260**	Distribution d'appels (groupe UCD).
Dest 1 - 4 : **#801 - #817**	Équipement d'annonces.
Dest 1 - 4 : 100, 101, ...	Numéro de téléphone d'un abonné ou d'un groupe (par ex. boîte vocale)
Renvoi temporisé après	Durée à l'issue de laquelle un appel est transféré à la destination suivante. Avec les groupes UCD, le renvoi d'appel suit le mécanisme des cycles d'appel primaire et secondaire (voir Groupes UCD). Plage de valeurs : 5/10/15/...75 s, valeur par défaut : 15 s
Renvois temporisés	En cas d'occupation, l'appel est immédiatement transmis à la destination d'appel suivante. Valeur par défaut : activé
Sonnerie	
Destination de la seconde sonnerie	Abonné interne supplémentaire auquel l'appel est également signalé ou actionneur (relais) d'un module actionneurs/capteurs pour un réveil central.
Type de seconde sonnerie	L'appel peut être signalé à l'abonné immédiatement ou bien à l'issue du délai défini pour le renvoi temporisé. Valeur par défaut : Immédiatement

Description des paramètres des onglets :

- **Table d'acheminement - Affectation**

Paramètres	Description
Numéro	Numéro de l'abonné ou du groupe.
Nom	Nom de l'abonné ou du groupe.
Type	Type d'abonné, par ex. U_{P0}, client système, AB, RNIS, SIP.
jour	Numéro de la table d'acheminement pour appels externes entrants durant le temps de travail (circuit de jour) Valeur par défaut : 14
Nuit	Numéro de la table d'acheminement pour appels externes entrants lorsque le circuit de nuit est activé Valeur par défaut : 15

Paramètres	Description
Interne	Numéro de table d'acheminement pour appels internes entrants Valeur par défaut : 16
Rechercher	Si un terme de recherche a été entré dans les champs **Numéro de téléphone** ou **Nom** puis si l'on appuie sur la touche Return, tous les résultats contenant le terme de recherche sont affichés. Par exemple, si vous entrez `521` comme numéro d'appel, les résultats qui s'affichent sont `+495213535` et `+498967521` ou si vous entrez `co` comme nom, les résultats `Collins`, `Mcoin` et `Branco` s'afficheront. Toutes les entrées sont affichées lorsque rien n'a été saisi dans tous les champs de recherche et que vous appuyez ensuite sur la touche Retour.

Description des paramètres des onglets :

- **Membres de la table d'acheminement**

Paramètres	Description
Afficher tous les membres de la liste d'appel de destination	Pour la table d'acheminement sélectionnée, tous les abonnés ou groupes qui utilisent cette table d'acheminement sont affichés.

Description des paramètres des onglets :

- **Copie listes dest. appel**

Paramètres	Description
Table d'acheminement	Choix de la table d'acheminement à laquelle les abonnés doivent être affectés. Plage de valeurs : 1 à 740
jour	Table d'acheminement pour appels externes entrants durant le temps de travail (circuit de jour)
Nuit	Table d'acheminement pour appels externes entrants lorsque le circuit de nuit est activé
Interne	La table d'acheminement est pour les appels internes entrants
Tables d'acheminement	
Sélection	Liste de tous les abonnés.
Membres	Liste des abonnés auxquels est affectée la table d'acheminement.
Boutons	
Ajouter	Les abonnés marqués sont repris de la fenêtre Sélection et placés dans la fenêtre Membres.
Effacer	Les abonnés marqués sont effacés dans la fenêtre Membres.

27.3.10 Lignes/Routage

Le menu **Lignes/Routage** regroupe les fonctions pour les lignes réseau et les faisceaux.

27.3.10.1 Lignes/Routage > Lignes

Description des paramètres des onglets :

- **Afficher toutes les lignes**
- **Modifier le faisceau**

Paramètres	Description
Ligne	Affichage des lignes réseau physiques raccordées au système de communication.
Box-Em-Pt-Li ou Box/ Emplacement/Port/Ligne	Affichage du type de module ainsi que du numéro d'emplacement et de port (port physique) pour le raccordement de la ligne au système de communication.
Indicatif	Affichage ou configuration de l'indicatif d'appel. Lors de la saisie de ce numéro, le système de communication occupe la ligne correspondante. On utilise ce numéro pour tester la ligne ou pour programmer une touche de ligne. Si des applications CSTA sont utilisées, la valeur de ce paramètre doit être définie.
Faisceaux	Affichage ou Sélection de la voie attribuée à la ligne (néant ou Gpe Lign 1 à Gpe lign 12). Si la valeur "Aucune" a été réglée pour une ligne active, le système se comporte de manière instable. De plus, le système peut certes recevoir un appel sur cette ligne, mais il lui est impossible de le transférer.
État	Affichage de l'état de la ligne. Une ligne inactive est identifiée par une étoile.
Type	Affichage du type de ligne. Les lignes inactives sont désignées par "No Port".

Description des paramètres des onglets :

- **Acheminement LR toutes les lignes**

Paramètres	Description
Ligne	Affichage des lignes réseau physiques raccordées au système de communication.
Box-Em-Pt-Li ou Box/ Emplacement/Port/Ligne	Affichage du type de module ainsi que du numéro d'emplacement et de port (port physique) pour le raccordement de la ligne au système de communication.
Jour Numéro	Affichage du numéros attribué au service de jour
Jour Nom	Affichage du nom du numéro d'appel attribué au service de jour
Nuit Numéro	Affichage du numéros attribué au service de nuit
Nuit Nom	Affichage du nom du numéro d'appel attribué au service de nuit

Description des paramètres des onglets :

- **Ajouter une ligne**

Paramètres	Description
Nombre	Nombre des lignes à ajouter.

Description des paramètres des onglets :

- **Changer de direction**

Paramètres	Description
Ligne	Affiche le numéro de la ligne.
sortant	Des appels sortants peuvent être passés sur la ligne. **Remarque :** Il est possible de passer des appels d'urgence même si l'indicateur est désactivé.
entrant	Les appels entrants peuvent être reçus sur la ligne.

Description des paramètres des onglets :

- **Modifier la ligne**
- **Effacer la ligne**

Paramètres	Description
Ligne	Affichage du numéro de ligne.
Box/Emplacement/Port/ Ligne	Affichage du port physique de la ligne (Box/Emplacement/Port/Ligne).
Indicatif	Affichage ou saisie de l'indicatif d'appel.
Faisceaux	Affichage ou Sélection de la voie attribuée à la ligne (néant ou Gpe Lign 1 à Gpe lign 12).
Acheminement LR	
Jour Numéro	Numéro de téléphone pour connexion entrante sans sélection directe, le jour.
Nuit Numéro	Numéro de téléphone pour connexion entrante sans sélection directe, la nuit.

Description des paramètres des onglets :

- **Modifier les flags RNIS**

Paramètres	Description
Protocole : Description	Chaque entrée pour un modèle de protocole se compose de Interface, Protocole et Info suppl. : Raccordement de base S0 2B+D via interface S0, Raccordement de base BRI 2B+D via interface U2B1Q (Etats-Unis), Raccordement primaire multiplex S2 30B+D, Raccordement primaire multiplex T1 23B+D (Etats-Unis)
Logique/Physique	Mode de comptage logique ou physique des canaux
Slave B-channel neg : Master	Réglage maître/esclave dans la couche 3. Pour les connexions, un côté doit être défini comme esclave et l'autre comme maître.
Up B-channel alloc : Down	Définition du mode de comptage de canal B (doit être le même dans les deux systèmes)
S0 S0 Format CHI : S2M	Format de protocole CHI, à définir comme S0 (format court) ou S2M (format long)

Paramètres	Description
Asymétrique/symétrique/	Utilisation symétrique ou asymétrique des éléments de protocole L3
Automatique/fixé	Gestion automatique ou Affectation fixe de la symétrie
Longueur 1 CR : 2	Longue de référence format de protocole Call
Signalisation d'alarme	Utilisez la signalisation d'alarme dans le protocole de couche 3
Horloges de protocole	Utilisez la temporisation couche 3
Démarrage rapide de PRI	Utilisez la procédure PRI-Quickstart
IE_TNS	Utilisez l'élément d'information Transit Network Selection
IE_OSA	Utilisez l'élément d'information Open Service Access
CIDL	Utilisez la signalisation de l'ID Call and Link dans la mise en réseau
Côté utilisateur/Côté réseau	Définition du protocole Couche 2. Sur la partie opposée, configuration miroir nécessaire
Réseau/abonné	Définition du protocole Couche 2. Sur la partie opposée, configuration miroir nécessaire
PP/PMP	Définition Point à Point ou Point Multipoint, uniquement pertinent pour S0
Actif en permanence	Couche 2 active en permanence
Activer le contrôle TEI	Activer le contrôle TEI
Côté utilisateur/Côté réseau	Définition du protocole Couche 1. Sur la partie opposée, configuration miroir nécessaire
PP/PMP	Définition du protocole Couche 1. Même configuration nécessaire des deux côtés
Type bus S : L	bus court/long (portées)
Actif en permanence	Définition du protocole Couche 1. Même configuration nécessaire des deux côtés
Vérification de CRC4	Définition du protocole Couche 1, pertinente uniquement pour S2M, même configuration des deux côtés
Communication de CRC4	Définition du protocole Couche 1, pertinente uniquement pour S2M, même configuration des deux côtés

Description des paramètres des onglets :

- **Modifier le canal B**

Paramètres	Description
Canal B	Affichage du numéro de canal B.
Sortant	Sur le canal B effectuer un appel téléphonique sortant.
Entrant	Sur le canal B on peut effectuer un appel téléphonique entrant.

Description des paramètres des onglets :

- **Modifier la direction**

Paramètres	Description
Ligne	Affichage du numéro de ligne.
Sortant	Des appels sortants peuvent être passés sur la ligne.
Entrant	Les appels entrants peuvent être reçus sur la ligne.

27.3.10.2 Groupe > de troncs/tronçons de routage

Description des paramètres des onglets :

- **Changer d'itinéraire**

Paramètres	Description
Nom de la route	Nom de la route. Le nom saisi remplace le numéro d'itinéraire par défaut dans la liste des itinéraires.
Codes de saisie	Les codes d'affectation pour chaque itinéraire sont saisis ici. Les codes de routage saisis doivent être exempts de collisions, tant entre eux qu'au sein du plan de numérotation d'appel complet du système de communication. Utilisez le bouton Vérifier pour tester les collisions. Le code de saisie est le code qui permet au système de commutation de fournir une ligne à la station qui a composé ce code. Les codes de saisie ne fonctionnent que si le LCR n'a pas été activé. Si l' **équilibrage de charge** est actif, le code de saisie doit être identique sur tous les itinéraires utilisés.
Code CO (2e code de tronc)	Un deuxième code de jonction (code CO) est défini si le système de communication est un sous-système d'un autre système de communication ou s'il est mis en réseau avec plusieurs autres systèmes de communication. Cela ne concerne que les routes réseau (type de route = PABX). Dans ce cas, le deuxième code de tronc est le code de saisie pour le système principal. Au sein d'un réseau, les codes de prise de contrôle du tronc, les codes de prise de contrôle de la route et le deuxième code CO doivent être configurés de manière uniforme. La valeur par défaut en Allemagne est 0.
Emplacement de la passerelle	
Code du pays	Affiche le code pays de l'emplacement de la passerelle. Configurer via Paramètres de base/Passerelle/Emplacements de la passerelle
indicatif régional	Affiche l'indicatif régional de l'emplacement de la passerelle. Configurer via Paramètres de base/Passerelle/Emplacements de la passerelle
Numéro PABX	Affiche le numéro PABX de l'emplacement de la passerelle. Configurer via Paramètres de base/Passerelle/Emplacements de la passerelle
Numéro de station du système - entrée	
Code du pays	Utilisé pour l'analyse des chiffres des appels entrants. Indicatif de pays sans zéros non significatifs (ex. : 1 aux États-Unis, 49 en Allemagne)

Paramètres	Description
indicatif régional	Utilisé pour l'analyse des chiffres des appels entrants. Indicatif régional sans zéros non significatifs (ex. : 89 pour Munich)
Numéro PABX	Utilisé pour l'analyse des chiffres des appels entrants. Numéro PABX (numéro de téléphone central de l'entreprise, par exemple, 777)
Numéro de localisation	Utilisé pour l'analyse numérique des numéros de téléphone publics pour les appels sortants. Vérifie les informations de numérotation pour déterminer si le numéro de destination appelé se trouve dans son propre système.
Numéro de station du système - sortant Information : Toute modification des numéros PABX sortants doit être coordonnée avec les opérateurs de réseau. (Extrait non filtré)	
Code du pays	Utilisé pour l'identification de l'appelant lors des appels sortants. L'indicatif du pays sans les zéros non significatifs (par exemple, 1 aux États-Unis, 49 en Allemagne) est transmis au réseau. Si aucun numéro PABX sortant n'est saisi, le numéro PABX entrant est automatiquement utilisé.
indicatif régional	Utilisé pour l'identification de l'appelant lors des appels sortants. L'indicatif régional spécifié ici (sans zéros non significatifs, par exemple 89 pour Munich) est transmis au réseau. Si aucun numéro PABX sortant n'est saisi, le numéro PABX entrant est automatiquement utilisé.
Numéro PABX	Utilisé pour l'identification de l'appelant lors des appels sortants. Le numéro PABX spécifié ici (numéro de téléphone central de l'entreprise, par exemple 777) est transmis au réseau. Si aucun numéro PABX sortant n'est saisi, le numéro PABX entrant est automatiquement utilisé.
Supprimer la station Numéro d'appel	L'activation de cette option supprime le numéro DID de l'identification de l'appelant.
Route de débordement	
Route de débordement	Si toutes les lignes de l'itinéraire configuré sont occupées, un débordement vers un autre itinéraire peut être défini. La voie de débordement ne s'applique que lorsque LCR est désactivé.
Transmission numérique	
Transmission numérique	Le type de transmission numérique est déterminé ici pour l'itinéraire sélectionné et est affiché sous forme de texte statique (par exemple, table de routage 6 : envoi en bloc) sous Paramètres | Routage au moindre coût | Plan de numérotation après avoir sélectionné la table de routage (voir la liste déroulante Table de routage).
Transmission numérique : Chiffre par chiffre	Les chiffres sont transmis en synchronisation avec la numérotation.

Paramètres	Description
Transmission numérique : envoi en bloc	Lors de la transmission de chiffres par bloc (numérotation par bloc par itinéraire), les chiffres composés sont mis en mémoire tampon par le système de communication. La numérotation n'a lieu que lorsqu'un délai s'est écoulé après la composition du dernier chiffre, lorsque le code de fin de numérotation # a été saisi ou si une correspondance exacte est trouvée dans la règle de numérotation. Aux États-Unis, dans le cas du PRI, la numérotation par blocs vers le central téléphonique est obligatoire. Le LCR doit être activé pour pouvoir sélectionner la transmission numérique en bloc. Le type de transmission de chiffres est automatiquement défini sur transmission de chiffres en bloc dans la table de routage si au moins une route de la table de routage LCR est configurée avec la transmission de chiffres en bloc.
Numéro de poste mobile (MEX)	
Numéro MEX	Si le fournisseur de services de téléphonie sur IP utilisé prend en charge la fonction « Extension mobile (MEX) », le numéro MEX (8 positions, uniquement des chiffres) fourni par le fournisseur de services de téléphonie sur IP doit être saisi ici. Cette fonctionnalité ne peut être utilisée qu'avec une connexion téléphonique Internet DID (de type SIP comme ISDN). Il permet d'intégrer les téléphones mobiles/smartphones au système de communication. L'utilisateur du téléphone mobile peut être joint via le service One Number sous un seul numéro de téléphone, qui est également communiqué à l'autre partie. Lorsqu'un abonné passe un appel avec son téléphone portable, c'est son numéro de bureau qui est affiché à son interlocuteur, de sorte que son numéro de téléphone portable reste inconnu. De plus, les autres abonnés internes peuvent vérifier le statut de présence de ces abonnés même s'ils sont actuellement en communication sur leur téléphone portable.
Utilisateur externe de confiance	
Utilisateur externe de confiance	Utilisateur pouvant être affecté à une plateforme de collaboration externe telle que MS Teams pour passer des appels téléphoniques.

Description des paramètres des onglets :

- **Modifier les paramètres de routage**

Paramètres	Description
Indicateurs de routage	
Répétition des chiffres sur	Lorsqu'un itinéraire sortant est utilisé avec la répétition des chiffres activée, le code de routage est envoyé avant le numéro d'appel. Ceci s'applique uniquement si LCR est désactivé (voir Paramètres | Routage au moindre coût).
Analyse de la deuxième tonalité / Surveillance des lignes	L'analyse de la deuxième tonalité alerte le système de communication afin de détecter une tonalité supplémentaire. Cette fonctionnalité est utilisée avec les applications de systèmes de communication en tandem. Cette évaluation dépend du pays, par exemple, en Belgique après 2000 et en France après 2016 ou 2019. Cela n'est pas pertinent en Allemagne. Cela ne concerne que les opérateurs de réseau qui envoient une deuxième tonalité pour les appels internationaux.

Paramètres	Description
Intercepter par direction	Ce drapeau est nécessaire pour le réseau QSIG. Lorsque ce drapeau est activé, le système de communication vérifie si une demande de déroutement a été reçue par la station distante ou si le système de communication a mis en œuvre une commutation directe vers la position d'interception centrale. La station distante reçoit un message indiquant si un détournement doit être mis en œuvre pour cet appel. Si l'interception est activée pour une route, tous les appels transférés vers cette route sont interceptés à ce point d'interception. Pour mettre en œuvre cette fonctionnalité, les numéros de jour et de nuit doivent être configurés pour chaque itinéraire (voir Attribution de sonnerie par ligne). De plus, une position d'interception ne doit pas être saisie pour le service jour/nuit (voir Interception/Agent).
Service audio 3,1 kHz terminé.	Pour tous les appels sortants sur ISDN, le service Over. utilise par défaut une fréquence audio de 3,1 kHz. Il s'agit du type de transmission standard pour les appels sortants sur une ligne de réseau numérique à intégration de services (RNIS). Une connexion entre le système de communication et un central téléphonique numérique via un modem analogique doit être identifiée comme un service de données. Ce paramètre doit être activé pour éviter les problèmes lors du fonctionnement du télécopieur. Dans certains cas, un opérateur de réseau peut ne pas prendre en charge le service de transmission audio 3,1 kHz. Cela peut entraîner l'échec de la transmission de fax vers certains numéros de téléphone externes. Une solution possible consiste à désactiver l'indicateur **audio Over. service 3,1 kHz** .
Ajouter un préfixe de direction entrant	Lorsque cette option est activée sur les téléphones du système avec prise d'appel entrante, l'affichage du numéro d'appel est complété par le code de routage.
Ajouter un préfixe de direction sortant	Lorsque cette option est activée lors d'une saisie sortante, l'affichage du numéro d'appel est complété par le code d'accès. Information : la modification de ce paramètre affecte l'identification de l'appelant et doit donc être coordonnée avec les opérateurs de réseau. (Extrait non filtré)
Numéro d'appel avec préfixe international/ national	Si cette option est activée, l'indicatif national ou international du numéro de téléphone (par exemple, 02302…, 00492302…) doit être ajouté comme préfixe pour le fournisseur de services de téléphonie sur IP (ITSP). Par défaut : activé
Sonnerie de retour vers CO	Si cette option est activée, une tonalité de retour d'appel sera envoyée au central ISDN lors d'un appel entrant. Il s'agit d'un protocole de traitement spécial requis par les fournisseurs Global One et Sovintel.
Segmentation	Cette zone définit le comportement du système lors de l'envoi de messages ISDN dans lesquels la longueur maximale des données utilisateur de couche 2 (260 octets) est dépassée.
Segmentation : Oui	Le message à envoyer est divisé en segments de 260 octets et envoyé individuellement. Le système de communication récepteur doit prendre en charge la segmentation, collecter et organiser les segments individuels en un message.

Paramètres	Description
Segmentation : Non	La segmentation n'est pas nécessaire, car la couche 2 sous-jacente peut transporter des messages de n'importe quelle longueur.
Segmentation : Tronquer le message	Le message à envoyer est tronqué à moins de 260 octets en éliminant les parties les moins importantes (comme les noms, par exemple) puis envoyé.
Désactiver UUS par itinéraire	La signalisation utilisateur-à-utilisateur (UUS) peut être désactivée avec cet indicateur. Cela supprime la transmission du nom et du numéro de téléphone de la station A dans l'élément UUI (informations utilisateur-utilisateur, UUI) pour le renvoi d'appel externe (FWD ext.). Ce paramètre doit être désactivé manuellement pour Telefonica.
Utilisez toujours le DSP	Si cette option est activée, la connexion au fournisseur de services de téléphonie sur Internet n'est possible que via un DSP (processeur de signal numérique). Si cet indicateur n'est pas activé, une connexion Direct Payload est établie avec le fournisseur de services de téléphonie Internet. Ce paramètre doit être activé pour la route du réseau OpenScape Voice. Ce drapeau ne peut pas être activé dans le cas de transmissions de fax (T.38) via un périphérique externe (par exemple, Mediatrix 4102).
Nom dans CO	Ce drapeau est configuré pour les CO qui prennent en charge le nom de l'appelant.
saisie du tronc analogique	Ici, différents horaires peuvent être sélectionnés pour déterminer le moment où la numérotation commence lors de l'utilisation de lignes analogiques commutées (MSI). Si aucune pause n'est définie, le système de communication attend de reconnaître une tonalité. Note pour le Brésil : lors de l'utilisation de la signalisation DTMF à partir de terminaux analogiques en conjonction avec des lignes analogiques et une sortie d'impulsions numériques après détection de tonalité, des problèmes peuvent survenir avec la restriction d'interurbain lorsque l'indicatif du pays est défini sur le Brésil. Dans ce cas, les signaux DTMF provenant des terminaux analogiques vont directement aux lignes analogiques (la procédure 1A n'est pas utilisée). De ce fait, les signaux DTMF composés avant la réception de la tonalité sont perdus. Par conséquent, dans de tels cas, le routage au moindre coût (LCR) doit être activé pour que la méthode de numérotation et la restriction de péage fonctionnent correctement sur l'appareil.
Pause d'appel interurbain	La pause d'appel CO détermine la période de temps qui s'écoule avant qu'un appel ne soit considéré comme terminé une fois que l'utilisateur a raccroché. Cette option s'applique uniquement aux lignes MSI. Pour un appel interurbain avec, par exemple, 1 seconde de communication et 4 secondes d'arrêt, une pause de 6 secondes doit être configurée. Dans certains centres d'appel, cependant, une pause de sonnerie de 10 secondes est appliquée. Dans de tels cas, une pause de 13 secondes doit être programmée sur les appels interurbains. Sinon, aucun renvoi d'appel ne peut être mis en œuvre. Aux États-Unis, ce cycle consiste en deux secondes de marche, deux secondes d'arrêt, pour un total de six secondes. L'option de six secondes est celle par défaut, vous n'aurez donc pas besoin d'effectuer de modifications ici. Plage de réglage : 2 à 13 secondes.
Type de saisie	Ce champ spécifie les critères qui s'appliquent si le système de communication doit s'emparer d'une ligne sortante.

Paramètres	Description
Type de crise : cyclique	Le système de communication entame sa recherche cyclique d'une ligne libre avec le numéro de ligne suivant, en fonction de la dernière ligne sortante saisie sur cet itinéraire.
Type de crise : linéaire	Le système de communication commence toujours sa recherche par le numéro de ligne le plus bas attribué à cet itinéraire.
Type d'itinéraire	Il existe deux options pour le type d'itinéraire. Le type de routage peut être configuré soit en CO (Central Office), soit en PABX (Private Automatic Branch Exchange).
Type d'itinéraire : CO	Les lignes affectées à cet itinéraire sont soumises à des restrictions de péage. Lorsque LCR est actif, la restriction d'appel est régulée par le plan de numérotation (colonne COS).
Type d'itinéraire : PABX	La restriction de péage n'est appliquée que s'il existe un deuxième code CO attribué à cet itinéraire. Lorsque LCR est actif, la restriction d'appel est régulée par le plan de numérotation (colonne COS). Le type d'itinéraire influe également sur le texte par défaut du nom de l'itinéraire (voir Itinéraires) ainsi que sur la procédure utilisée pour reconnaître la tonalité sur les lignes MSI.
Non et type, sortant	L'administrateur peut configurer séparément le « numéro PABX entrant » et le « numéro PABX sortant », divisés en parties pour l'indicatif du pays, l'indicatif régional et le numéro PABX (= numéro de connexion sur le réseau local). Ceci est nécessaire pour la mise en œuvre de la fonctionnalité « CLIP sans filtrage ». Si aucun numéro PABX sortant n'a été configuré, le système de communication utilisera toujours les données du paramètre « Numéro PABX entrant ». En cas de saisie entrante sur une ligne RNIS, le système de communication tronque le numéro PABX (aligné à gauche) du numéro de téléphone reçu et interprète la partie restante comme le numéro d'appel direct entrant. Pour les informations de numéro d'appel vers le réseau téléphonique public commuté (RTPC), le système de communication insère automatiquement le numéro PABX (ou la partie définie dans la configuration) comme partie initiale du numéro d'appel. Ceci ne s'applique pas aux informations de numérotation (adresse de destination). Les numéros d'appel des stations internes transmis à la station distante peuvent être composés comme suit :
Non. et type, sortant : Inconnu	numéro DID uniquement (paramètre par défaut)
Non. et type, sortant : Numéro PABX	Numéro PABX + numéro DID
Non. et type, sortant : indicatif régional	+ Indicatif régional + Numéro PABX + Numéro DID
Non. et type, sortant : Code du pays	Indicatif de pays + Indicatif régional + Numéro PABX + Numéro DID
Non. et type, sortant : Interne	Uniquement pour les systèmes en réseau : les préfixes numériques ne peuvent pas être ajoutés pour les plans de numérotation fermés. Les préfixes des numéros d'appel sont supprimés ici.

Paramètres	Description
Type de numéro d'appel	Les paramètres de la zone « N° et type, appels sortants » affectent également les appels provenant d'un poste dans un système partenaire (un nœud en réseau). Grâce à ce paramétrage, le numéro de l'appelant reçu du nœud du réseau et transmis au central téléphonique est étendu pour l'itinéraire sortant.
Type de numéro d'appel : Interne	Dans ce cas, seul le numéro d'appel interne est transmis. Si la destination est une station externe, soit aucun numéro n'est transmis, soit seul celui de la console de l'opérateur l'est. Le numéro d'appel interne peut être affiché lorsque la destination est une station interne sur un autre nœud.
Type de numéro d'appel : numérotation directe entrante	Dans ce cas, seul le numéro DID est transmis. Le numéro d'appel interne n'est pas fourni pour affichage sur les destinations internes des autres nœuds. Les informations relatives à l'appel sont suffisantes pour les destinations externes.
Type de numéro d'appel : Interne / DID	Ce paramètre est utile pour la mise en réseau. Le numéro d'appel interne et le numéro d'appel DID sont tous deux transmis à la station de destination. Si un poste interne est appelé au sein du réseau, le numéro d'appel interne de l'appelant peut être affiché pour ce poste. Si le poste de destination interne a activé le renvoi d'appel vers une destination externe, par exemple un numéro DID peut également être transmis dans ce cas.
Déroutement	
Changer d'itinéraire	Lorsque cette option est activée, il est également possible d'acheminer les informations du canal D via d'autres itinéraires. Cette option permet d'effectuer des itinéraires alternatifs via d'autres routes. Cette option ne peut être activée que lorsque le plan de numérotation des appels est sans ambiguïté (numérotation fermée ou codes de saisie uniques au sein d'un réseau). Le système effectuant la requête doit également prendre en charge cette fonctionnalité.). Si le réacheminement est mis en œuvre, le réacheminement avec changement d'itinéraire actif doit également être configuré pour l'itinéraire correspondant. Cette option est uniquement disponible pour le réseau CorNet NQ et doit être activée de la même manière dans les deux systèmes de communication en réseau.
Optimisation active de l'itinéraire	Pour optimiser l'utilisation du canal B, le renvoi d'appel peut être effectué sur la base du protocole conformément à la spécification « Renvoi d'appel/ Réacheminement partiel ». Si le réacheminement partiel est rejeté, la commutation directe est utilisée.
Optimisation de la route active : Non	Lorsque vous sélectionnez cette option, le réacheminement est désactivé. Pour le renvoi d'appel, la connexion est toujours établie via deux canaux B.
Réacheminement actif : Si l'itinéraire est connu	Lorsque vous sélectionnez cette option, le réacheminement n'est actif que si l'itinéraire est connu et si une procédure de « prise de contact » réussie a lieu entre les deux systèmes de communication en réseau.
Optimisation de la route active : Toujours	Si l'établissement de l'appel entrant emprunte le même itinéraire que l'itinéraire de destination du transfert d'appel, l'appel sera rejeté (fonction de déviation d'appel utilisée) par le système de communication si cette option est activée. Dans le cas des systèmes en réseau, cette option doit toujours être activée de la même manière dans les deux systèmes de communication en réseau.

Description des paramètres des onglets :

- **Modification de paramètre spéciale**

Paramètres	Description
Plan de numérotation Définit le paramètre de plan de numérotation dans les messages sortants	
Numéro de l'appelé	Contrôle système = défini par le système ; plan de numérotation RNIS, plan de numérotation privé, plan de numérotation inconnu = préréglé manuellement
Tous les autres	Ex. : numéro de l'appelant, numéro de redirection, etc. Contrôle système = défini par le système. Plan de numérotation RNIS, plan de numérotation privé, plan de numérotation inconnu = préréglage manuel
Site	Le paramètre Site (emplacement) détermine comment le paramètre Emplacement est défini dans l'élément d'information Q931 CAUSE et Indicateur de progression. Contrôle système = défini par le système ; il est également possible de paramétrer manuellement le système en sélectionnant « Réseau et station privés » ou « Station toujours active ».
COLP	Si cette option est activée, le numéro de l'appelé sera affiché à l'appelant en cas de connexion entrante externe via un central téléphonique. L'appelant peut voir si l'appel a été transféré ou pris en charge par quelqu'un d'autre. Cette fonctionnalité doit également être activée par le bureau central. Si l'indicateur est activé et qu'un appel entrant externe est transféré ou intercepté, le numéro d'appel mis à jour est signalé au CO dans le message de connexion émis par le système de communication. Si la fonction COLP est activée dans le CO, le numéro d'appel mis à jour est également affiché pour l'appelant. Information : Ce paramètre n'affecte pas l'affichage du numéro d'appel pour les connexions sortantes externes.
Notification d'envoi	Ce message sert à transmettre des informations sur l'état de la connexion actuelle. Le message peut être envoyé aussi bien du côté du réseau que du côté de l'abonné pour informer l'autre partie (réseau ou abonné) d'une interruption de connexion, par exemple, ou que le renvoi d'appel est actif. Si la fonction de notification n'est pas prise en charge par le CO, le message de notification peut être supprimé en réinitialisant cet indicateur. Si cette option est activée, un message « Notifier » est transmis si un appel est en attente ou en attente, par exemple. L'envoi de notifications n'est évalué que dans les protocoles DSS1, NI1 et MCI. Dans les protocoles SIP-Q, CorNet-NQ et QSIG, la notification est toujours envoyée.
sans clip	Si cette option est activée, les informations relatives à l'appelant seront supprimées pour les appels sortants sur une ligne BRI ou PRI sur le réseau public. Ce paramètre peut être activé ou désactivé pour chaque itinéraire. De plus, la station a la possibilité de supprimer les informations de l'appelé pour chaque appel, via un code d'accès ou le menu téléphonique du système.
Aucun accusé de réception de configuration.	Si cette option est activée, le message d'accusé de réception de la configuration envoyé par le système de communication au bureau central est supprimé. Pertinent pour les CO spéciaux. Exemple : les CO Fetex150 de Fujitsu.

Paramètres	Description
aucune information sur la division	Si cet indicateur est activé, le signal d'information LEG de redirection standard (numéro d'appel de la partie redirigeante) n'est pas envoyé au CO. Le DIV. Les informations LEG doivent être supprimées en cas de problème lors du renvoi d'appel externe (CF ext.).
Envoi terminé	Si cette option est activée, le système affichera l'information facultative « Tous les chiffres envoyés » une fois que tous les chiffres composés auront été transmis.
Appel interne comme appel externe	Si cette option est activée, les appels internes au réseau sont signalés acoustiquement de la même manière que les appels externes.
Sans CCNR	Si cet indicateur est activé, un appel ISDN entrant avec CCNR (Call Completion on No Reply) est signalé afin que le système puisse accepter une demande de rappel. Cela signifie que l'appelant peut demander à être rappelé si la station ne répond pas. Dans certains cas, le message n'est pas pris en charge par le fournisseur ISDN. Dans ce cas, l'interrupteur doit être activé pour empêcher le système d'envoyer du CCNR.
Avec équilibrage de charge	Si cette option est activée, toutes les routes d'équilibrage de charge seront actives. Pour les appels sortants, les lignes principales sont sélectionnées de manière cyclique parmi les itinéraires désignés pour l'équilibrage de charge dans la table de routage LCR.

Remarque : La fonctionnalité **d'équilibrage de charge** est réservée à certains fournisseurs de services de télécommunications après sa mise en service officielle.

27.3.10.3 Lignes/Routage > Fonctionnalités QSIG

Dans un réseau composé de plusieurs systèmes de communication, les informations de connexion (données GEZ) émises dans les installations secondaires sont envoyées à un système de communication défini du réseau. A cet effet, il convient de configurer dans chaque système de communication le numéro d'appel du système de destination (numéro d'appel du poste central de saisie) auquel les données doivent être envoyées.

Description des paramètres des onglets :

- **Modifier les fonctionnalités QSIG**

Paramètres	Description
Données de la propre installation	

Paramètres	Description
N° système	Ces données permettent d'identifier son propre système de communication dans le réseau. Ces données sont valables pour la signalisation d'occupation centrale tout comme pour le routage des données de connexion. Dans un réseau composé de plusieurs systèmes de communication, chaque système possède un numéro d'installation univoque. Lorsque le système de communication est mis en réseau avec de tels systèmes, et que l'on souhaite utiliser les fonctionnalités QSIG, le numéro de système doit alors également être administré ici pour des raisons de compatibilité. Plage de valeurs : 1 à 255
Numéro de groupe	Dans les systèmes de communication, il est possible d'organiser les abonnés en groupes, qui reçoivent ensuite un numéro de groupe univoque. Dans le système de communication, il n'existe pas de groupement de cette sorte. Pour des raisons de compatibilité, il convient malgré tout d'administrer ici également les numéros de groupe. Plage de valeurs : 1 à 40
Signalisation de tonalité occupée pour toute l'installation	
N° install. syst. de dest.	Ces données définissent un système de communication qui dispose de la signalisation d'occupation centrale. Il peut aussi bien s'agir de l'installation principale que d'une installation secondaire. Numéro d'installation du système de communication qui est paramétré pour la signalisation occupé centrale. Plage de valeurs : 1 à 255
N° du syst. de dest.	Numéro du système de communication qui est paramétré pour la signalisation d'occupation centrale. Entrez ici uniquement le numéro de l'installation (pas de l'abonné). Dans le plan de numérotation LCR veuillez tenir compte du fait que ce numéro d'installation doit être entré sans suffixe ! Exemple: le numéro d'appel du système de destination est 999. L'entrée du plan de numérotation doit être -999 (et non -999xxx, et non -999Z).
Routage des données de taxation	
N° du syst. de dest.	Ces données définissent un système de communication qui dispose de la saisie centrale des données de connexion. Il peut aussi bien s'agir de l'installation principale que d'une installation secondaire. Numéro de téléphone du système de communication, paramétré comme service central de saisie (voir aussi la remarque sur le n° d'appel des systèmes de destination, un peu plus haut).

27.3.10.4 Lignes/Routage > Affecter le MSN

Description des paramètres des onglets :

- **Afficher le MSN**
- **Modifier le MSN**

Paramètres	Description
MSN	Affichage ou entrée des MSN (numéro de connexion multiposte).
Ligne	Affichage de l'affectation de la ligne où MSN est activé.

27.3.10.5 Lignes/Routage > Paramètres RNIS

La fréquence d'horloge de référence (ISDN Clock) assure la synchronisation des déroulements sur les lignes d'un réseau défini ou à l'intérieur du central. Normalement, le système de communication recherche automatiquement la ligne qui sert de fréquence de référence pour tous les systèmes de communication à l'intérieur d'un réseau ou d'un central. Si la ligne de fréquence d'horloge de référence est défaillante, il faut alors paramétrer une ou plusieurs lignes pour fournir la fréquence d'horloge de référence.

Le système de communication sélectionne la ligne selon la séquence suivante :

1) Numéros autorisés
2) Ligne réseau S_{2M}
3) Ligne réseau S_0
4) Ligne interautomatique S_{2M} (uniquement configuration esclave)
5) Ligne interautomatique S_0

Description des paramètres des onglets :

- **Horloge RNIS**

Paramètres	Description
L'index	Les positions reflètent les priorités 1-4 (pour Numéros autorisés) ou 1-16 (pour Numéros interdits).
Listes des numéros autorisés	Si la liste des numéros autorisés contient des entrées, la sélection automatique de ligne du système de communication est mise hors service. Les ports RNIS inscrits dans la liste Numéros autorisés (4 maxi. possibles) sont utilisés en premier lors de la recherche de la ligne de fréquence d'horloge de référence.
Listes des numéros interdits	Les ports RNIS inscrits dans la liste Numéros interdits (16 maxi. possibles) sont sautés lors de la recherche de la ligne de fréquence d'horloge de référence.

27.3.11 Discriminations

Dans **Classes de discrimination**, les fonctions correspondant aux autorisations des lignes réseau sont regroupées. Elles règlent l'accès des abonnés aux connexions externes, éventuellement payantes.

27.3.11.1 Classes de service > Abonnés

Description des paramètres de l'onglet :

- **Afficher tous les abonnés**

Paramètres	Description
N° tél., **Numéro de téléphone**	Numéro de l'abonné.
Nom	Nom de l'abonné.
Jour	Groupe de discrimination sélectionné pour le jour.
Nuit	Groupe de discrimination sélectionné pour la nuit.
Discriminations Jour	Sélection du groupe de discrimination Jour La sélectionné effectuée fait référence à la table **Discriminations Jour** qui sert à associer le groupe de discrimination à la discrimination à proprement parler.
Discriminations Nuit	Sélection du groupe de discrimination Nuit La sélectionné effectuée fait référence à la table **Discriminations Nuit** qui sert à associer le groupe de discrimination à la discrimination à proprement parler.

Remarque : Les textes des groupes de classes de service sont générés en fonction de l'assistant de **Configuration de base** > **Indicatif de pays du système**.

27.3.11.2 Classes de service > Jour : Groupes de discrimination

Description des paramètres des onglets :

- **Modifier noms**
- **Modifier le groupe de discrimination**
- **Jour : Afficher les membres du groupe**

Paramètres	Description
Groupe de discrimination	Nom choisi librement pour les groupes de discrimination 1 à 15. Attribution de discrimination réseau par faisceau (groupe de lignes) respectivement pour Jour et Nuit. Lors de la configuration des abonnés, l'accès aux numéros externes peut être limité par l'attribution de groupes de discrimination.
Classe de discrimination	Affectation des discriminations pour les différents groupes de discrimination pour service Jour. Toutes les restrictions ne sont opérationnelles que sur les lignes d'un faisceau de type réseau
Groupe de discrimination : Interne	L'abonné peut uniquement téléphoner en interne. Valeur par défaut : Par défaut dans groupe de discrimination 1
Groupe de discrimination : Appels entrants	L'abonné peut uniquement recevoir des appels externes. Valeur par défaut : Par défaut dans groupe de discrimination 2
Groupe de discrimination : Numéros autorisés	L'abonné n'est autorisé à composer que les numéros externes définis dans la liste des numéros autorisés. Si aucun numéro n'est inscrit, l'abonné bénéficie de la catégorie Appels entrants uniquement. Valeur par défaut : Par défaut dans groupe de discrimination 4

Paramètres	Description
Groupe de discrimination : Numéros interdits	L'abonné n'est pas autorisé à composer les numéros externes définis dans la liste des numéros interdits. Si aucun numéro n'est inscrit, l'abonné bénéficie de la catégorie Accès total au réseau. Valeur par défaut : Par défaut dans groupes de discrimination 3, 5, 6
Groupe de discrimination : Aucune limitation	L'abonné peut recevoir des communications entrantes et effectuer des appels sortants sans aucune restriction. Valeur par défaut : Par défaut dans groupes de discrimination 7 à 15
Afficher les membres du groupe	Affichage du numéro et du nom des membres dans le groupe de discrimination sélectionné.

27.3.11.3 Classes de service > Nuit Groupes de discrimination

Description des paramètres des onglets :

- **Modifier noms**
- **Modifier le groupe de discrimination**
- **Nuit : Afficher les membres du groupe**

Paramètres	Description
Groupe de discrimination	Nom choisi librement pour les groupes de discrimination 1 à 15. Attribution de discrimination réseau par faisceau (groupe de lignes) respectivement pour Jour et Nuit. Lors de la configuration des abonnés, l'accès aux numéros externes peut être limité par l'attribution de groupes de discrimination.
Classe de discrimination	Affectation des discriminations pour les différents groupes de discrimination pour service Nuit. Toutes les restrictions ne sont opérationnelles que sur les lignes d'un faisceau de type réseau
Groupe de discrimination : Interne	L'abonné peut uniquement téléphoner en interne. Valeur par défaut : Par défaut dans groupe de discrimination 1
Groupe de discrimination : Appels entrants	L'abonné peut uniquement recevoir des appels externes. Valeur par défaut : Par défaut dans groupe de discrimination 2
Groupe de discrimination : Numéros autorisés	L'abonné n'est autorisé à composer que les numéros externes définis dans la liste des numéros autorisés. Si aucun numéro n'est inscrit, l'abonné bénéficie de la catégorie Appels entrants uniquement. Valeur par défaut : Par défaut dans groupe de discrimination 4
Groupe de discrimination : Numéros interdits	L'abonné n'est pas autorisé à composer les numéros externes définis dans la liste des numéros interdits. Si aucun numéro n'est inscrit, l'abonné bénéficie de la catégorie Accès total au réseau. Valeur par défaut : Par défaut dans groupes de discrimination 3, 5, 6
Groupe de discrimination : Aucune limitation	L'abonné peut recevoir des communications entrantes et effectuer des appels sortants sans aucune restriction. Valeur par défaut : Par défaut dans groupes de discrimination 7 à 15

Paramètres	Description
Afficher les membres du groupe	Affichage du numéro et du nom des membres dans le groupe de discrimination sélectionné.

27.3.11.4 Classes de service > Listes des numéros autorisés

Description des paramètres des onglets :

- **Afficher les numéros abrégés**
- **Ajouter un numéro**

Paramètres	Description
Liste 1-6	Afficher/Ajouter/Modifier/Effacer un numéro de téléphone autorisé. La liste des numéros autorisés comprend les numéros que l'abonné peut appeler. Il est possible de créer jusqu'à 6 listes de numéros autorisés. La 1e liste de numéros autorisés peut comporter 100 entrées, les autres 5 listes chacune jusqu'à 10 entrées.
Numéro de téléphone	Les numéros d'appel individuels peuvent comporter jusqu'à 26 positions (chiffres 0 à 9 ainsi que les caractères * et #). Il n'est pas nécessaire d'indique le numéro d'appel complet. Par exemple, pour donner l'autorisation aux abonnés de composer tous les numéros 0800xxx (gratuits), il suffit d'inscrire ici 0800. Comme les listes concernent uniquement les communications externes sortantes, l'indicatif de prise de ligne n'a pas besoin d'être indiqué dans les numéros inscrits.

27.3.11.5 Classes de service > Listes des numéros interdits

Description des paramètres des onglets :

- **Afficher les numéros abrégés**
- **Ajouter un numéro**
- **Modifier le filtre d’analyse**

Paramètres	Description
Liste 1-6	Afficher/Ajouter/Modifier/Effacer un numéro de la listes des numéros interdits. La liste des numéros interdits comprend les numéros de téléphone que l'abonné ne peut pas appeler. Il est possible de définir jusqu'à 6 listes des numéros. La 1e liste des numéros interdits peut contenir 50 entrées, les autres 5 listes chacune jusqu'à 10 entrées.
Numéro de téléphone	Les numéros d'appel individuels peuvent comporter jusqu'à 26 positions (chiffres 0 à 9 ainsi que les caractères * et #). Il n'est pas nécessaire d'indique le numéro d'appel complet. Pour par exemple empêcher que les abonnés ne sélectionnent les numéros en 0900xxx (payants), il faut entrer ici uniquement 0900. Le caractère # placé en tête dans un numéro interdit empêche de contourner le contrôle de la numérotation pour les téléphones système qui occupent une ligne réseau analogique avec numérotation MF et veulent basculer sur MF en cours de numérotation. Comme les listes concernent uniquement les communications externes sortantes, le code d'accès CO n'a pas besoin d'être indiqué dans les numéros inscrits.

Paramètres	Description
Modifier le filtre d’analyse A l'aide d'un filtre d'analyse, vous pouvez, pour une liste des numéros interdits quelconque, déterminer quels sont les chiffres qui doivent être comparés avec la listes des numéros interdits correspondante. Le système de communication masque la plage de numéros définis avant l'évaluation de la numérotation.	
Du chiffre ... **Au chiffre**	Dans cette plage de numéro (1-25) à l'intérieur du numéro de téléphone, le filtre d'analyse est activé.
Caractère	L'interdiction des caractères * et # permet à l'abonné de contourner le contrôle de la numérotation en entrant ces caractères.

27.3.11.6 Classes de service > Liste noire

Description des paramètres des onglets :

- **Afficher la liste**
- **Ajouter un numéro**

Paramètres	Description
Numéro d’appel	Les numéros d'e téléphone peuvent comporter jusqu'à 25 chiffres, qui peuvent inclure les numéros 0 à 9 ainsi que le caractère +. Le caractère '+' fait référence au préfixe international configuré dans le système et doit être entré à la première position. Le premier caractère de chaque entrée peut être '+' ou n'importe quel chiffre. Les numéros de téléphone sont triés numériquement dans la liste noire. Les entrées de la liste noire doivent être saisies au format international (par exemple, 004989) ou au format international canonique (par exemple, +4989).
Bloquer les appels anonymes	L'activation de cet indicateur bloque les appels sans numéro d'origine ou avec un numéro d'origine existant, mais une présentation restreinte.
Fonction Liste noire activée	L'activation de cet indicateur bloque les numéros de téléphone ajoutés. La fonction de liste noire est basée uniquement sur le numéro de l'appelant (initiateur de l'appel) donné par le fournisseur de service.

27.3.11.7 Classes de service > Renvoi de nuit

Description des paramètres de l'onglet :

- **Modifier renvoi de nuit**

Paramètres	Description
Abonnés autorisés pour renvoi de nuit	Si certains abonnés doivent avoir la possibilité de placer le système de communication en mode Nuit, ces abonnés doivent figurer dans la liste des abonnés autorisés pour le renvoi de nuit. Il est possible d'inscrire au maximum 5 abonnés. Valeur par défaut : 100
Abonnés	Liste de tous les abonnés intégrés dans le système de communication.

Paramètres	Description
Abonnés autorisés	Liste des abonnés autorisés à activer le mode Nuit.
Ajouter >>	Ajoute l'abonné sélectionné aux abonnés autorisés.

27.3.11.8 Classes de service > Affectation à un groupe VBZ

Description des paramètres des onglets :

- **Modifier l'affectation groupe**
- **Affectation Ligne au groupe**
- **Plage de numérotation abrégée du groupe**

Paramètres	Description
Affectation à un groupe VBZ	Affectation d'un groupe VBZ (1-64) à un abonné. Grâce à l'affectation du groupe VBZ, vous attribuez un groupe VBZ aux différents abonnés du système de communication. Lors du codage de la matrice de connexion, vous pouvez utiliser ces groupes et définir ainsi les communications possibles entre les différents abonnés. Par défaut, tous les abonnés sont affectés au groupe de connexion VBZ 1. Ainsi tous les abonnés ont un accès sans restriction aux autres abonnés. Plage de valeurs : 1 - 64
Affectation Ligne au groupe	Affectation d'une ligne au groupe VBZ. A l'aide de l'affectation de groupes VBZ, vous affectez aux différentes lignes du système de communication un groupe VBZ. Lors du codage de la matrice de connexion, vous pouvez utiliser ces groupes et déterminer quels abonnés peuvent accéder à quelles lignes. Par défaut, toutes les lignes réseau sont affectées au groupe VBZ 1. Ainsi, tous les abonnés ont un accès sans restriction à toutes les lignes, entrantes comme sortantes. Plage de valeurs : 1 - 64
Plage de numérotation abrégée du groupe	Il est attribué à chaque groupe VBZ une plage de n° abrégés (KWZ). Si un abonné quelconque sélectionne une numérotation abrégée, on détermine le groupe VBZ correspondant pour savoir si cet abonné est autorisé à choisir cette numérotation abrégée. Si ce numéro abrégé est bien situé dans la plage des numéros abrégés correspondant à ce groupe VBZ, le choix est alors confirmé. Si le numéro abrégé ne correspond pas à la plage affectée, un message d'erreur est édité. Les plages de numéros abrégés peuvent se recouper dans les groupes de matrices de connexion. Il n'est toutefois pas autorisé d'inscrire des numéros abrégés individuels dans les groupes VBZ et d'inscrire plusieurs plages de numéros abrégés dans un groupe VBZ. Sont admis par exemple VBZ 1 : 0-99; VBZ 2 : 50-150; VBZ 3 : 200-500. Ne sont pas admis par exemple VBZ 1 : 0, 5, 10; VBZ 2 : 50-100, 300-500. Plage de valeurs : 0-7999

27.3.11.9 Classes de service > Matrice VBZ

Description des paramètres des onglets :

- **Modifier la matrice de connexions**

Paramètres	Description
Matrices de connexions	Si vous souhaitez traiter une possibilité de connexion entre deux groupes de restriction de trafic cliquez dans le champ au croisement de ces groupes de restriction de trafic, dans la matrice de connexions. Cliquez de nouveau dans le champ afin de valider ou de bloquer les possibilités de connexion dans une direction, dans l'autre direction ou dans les deux directions. Pour qu'il soit possible d'utiliser une matrice de connexion, il faut tout d'abord affecter chaque abonné à un groupe. Dans le paramétrage par défaut, tous les abonnés et toutes les lignes sont affectés au groupe 1. Une fois qu'il a été défini un accès sans restriction pour le groupe 1, chaque abonné peut accéder, dans le cadre du paramétrage par défaut, à tous les autres abonnés et à toutes les lignes.
Quadrillage	Dans la matrice, il est affiché une liste de groupes horizontalement sur le bord supérieur et une autre liste verticalement sur le bord gauche. Aux points de contact se trouve chaque fois une case. La flèche figurant dans la case correspondante indique la relation entre un groupe et l'autre. Un champ vide indique qu'aucune connexion n'est possible. Une matrice de connexion où aucune flèche n'est inscrite se traduit par un blocage total du système de communication.
Interdire tout	La matrice de connexion empêche la circulation entre abonnés/lignes à l'intérieur d'une groupe (partie d'installation) et entre les groupes.
Autoriser tout	La matrice de connexion autorise la circulation entre abonnés/lignes à l'intérieur d'une groupe (partie d'installation) et entre les groupes.
Uniquement en interne dans le groupe	La matrice de connexion autorise la circulation uniquement entre abonnés/ lignes à l'intérieur d'une groupe (partie d'installation).

27.3.11.10 Classes de service > Renvoi de nuit automatique

Description des paramètres des onglets :

- **Afficher tous les jours**
- **Modifier le jour**

Paramètres	Description
Lundi, Mardi, Mercredi, Jeudi, Vendredi, Samedi, Dimanche, Jour spécial	Jour paramétré à l'aide du calendrier. Le calendrier englobe la semaine complète (Lundi à Dimanche) ainsi que les jours spéciaux. Les jours spéciaux sont des jours fériés ou des jours particuliers comme les congés de l'entreprise.
Zone	Le calendrier d'une journée peut être subdivisé en 4 zones max. (intervalles de temps). Ces zones peuvent être définies séquentiellement et sans écart, c'est-à-dire que le temps de fin du premier intervalle peut être identique au temps de début du second intervalle, par exemple. Toutefois, un intervalle ne peut pas avoir le même temps de début et de fin. La durée minimale d'un intervalle est de 15 minutes. Plage de valeurs : 1 - 4
Début	Heure de début pour la zone. Lorsque le premier intervalle d'une journée débute à 0h00, l'heure de départ entrée doit être 00h00.

Paramètres	Description
Fin	Heure de fin pour la zone. Si le dernier intervalle d'une journée se termine à 24h00 (12 pm), l'heure de fin indiquée doit être 23h59 (11h59).
Nuit Numéro	Numéro de téléphone de nuit pour la zone. S'il n'est pas inscrit de numéro pour le numéro de Nuit, le système a recours au renvoi de nuit par ligne. Les destinations correspondantes sont réglées dans **Lignes/Mises en réseau** > **modifier la ligne** > **Acheminement Li**. Les heures qui sont inscrites par le renvoi de nuit automatique s'appliquent à toutes les lignes.
OK	La zone est organisée.
Effacer	La zone définie est effacée.
Service de copie	Vous pouvez copier les zones configurées pour un ou plusieurs jours en choisissant le jour que vous souhaitez, pour le jour spécial en sélectionnant le flag concerné, tous à tous en sélectionnant **Cocher tout**. Lorsque vous cliquez sur **Appliquer**, les paramètres de zone pour les jours sélectionnés seront écrasés et remplacés par les zones configurées pour le jour courant.

27.3.11.11 Classes de service > Jours spéciaux

Description des paramètres de l'onglet :

- **Modifier les jours spéciaux**

Paramètres	Description
jour	Lorsque l'on sélectionne la date dans le calendrier, celle-ci est automatiquement inscrite ici.
Nom	Nom de ce jour spécial(par ex. lundi de Pentecôte)

27.3.12 Connexions

Les fonctions relatives à la connexion, telles que la musique d'attente (MoH), la configuration des annonces ou la connexion d'un interphone d'entrée comme ouvre-porte aux ports du système (faisceaux), sont regroupées sous **Connexions**.

27.3.12.1 Connexion > Musique d'attente

Description des paramètres des onglets :

- **Modifier la musique d'attente**

Paramètres	Description
Type de MOH	Le paramètre Type de MOH vous permet de choisir parmi trois options possibles. La musique pour cette fonction peut être fournie en interne ou en externe.

Paramètres	Description
Type de MOH : Pas de musique d'attente	Si cette option est sélectionnée, la fonction de musique d'attente sera complètement désactivée. Cela ne s'applique pas lorsqu'un appel externe est transféré par un transfert avant réponse ; l'appelant entend alors la sonnerie.
Type de MOH : MOH sans sonnerie	Si cette option est sélectionnée, dans le cas d'un transfert non masqué, l'appelant entendra la musique d'attente pendant le transfert, ainsi que pendant que l'appel est transféré par le correspondant et que la connexion externe sonne à la destination transférée.
Type de MOH : MOH avec sonnerie	Si cette option est sélectionnée, dans le cas d'un transfert non masqué, l'appelant entendra la musique d'attente pendant le transfert. Dès que l'appel est transféré par le correspondant et que la connexion externe sonne à la destination transférée, l'appelant entend une sonnerie. L'option MOH avec sonnerie doit toujours être activée dans un système de réseau afin d'offrir au client un environnement uniforme. |Si l'appelant accède au système par l'intermédiaire d'un fournisseur de services de téléphonie sur Internet (ITSP), cette option ne s'applique pas et l'appelant entend la musique d'attente pendant le transfert.

Accès et activation du type via le Manager E.

Le format d'entrée pour la musique d'attente est un fichier wave avec PCM et 16 bits. Les fréquences d'échantillonnage prises en charge sont 8, 22,05, 24, 32, 40, 44,1 et 48 kHz en mono ou en stéréo. Le format préféré est PCM, 16 bits, 8 kHz, mono. Il est recommandé d'utiliser le format d'entrée préféré et de limiter la longueur des fichiers d'ondes à environ 2 minutes. Il est possible de régler une MOH pour le jour et un autre pour la nuit. Une réinitialisation est nécessaire.

27.3.12.2 Connexions > PhoneMail

Description des paramètres des onglets :

- **Modifier PhoneMail**

Paramètres	Description
Accès à la boîte vocale pour le rappel	Définir le **Numéro d'appel** et le **Nom** du périphéhrique.
Périphérique d'enregistrement en direct	Définir le **Numéro d'appel** du péripéhrique.

27.3.12.3 Annonces > équipements auxiliaires

Description des paramètres des onglets :

- **Modifier les annonces**

Paramètres	Description
Fichier WAVE	Vous pouvez sélectionner ici le fichier WAVE (.wav) pour une annonce spécifique (voir Configuration > Annonces > Charger vers la passerelle).
Accéder	La connexion est définie via Access. Ici, vous pouvez sélectionner le port (analogique SLA ou EVM) auquel cet appareil est connecté. **Conseil :** Les ports analogiques configurés comme ports d'annonce doivent se voir attribuer la valeur « Répondeur », sous **Mode expert** > **Serveur téléphonique** > **Station** > **Stations analogiques** > **Modifier** > **Type d'extension**, comme décrit dans Paramètres de la station. Les destinations externes peuvent être utilisées pour adresser des dispositifs d'annonce situés sur un autre nœud du système. Pour ce faire, le dispositif d'annonce est identifié comme externe. Le numéro d'appel d'un port d'annonce dans un autre nœud du système est saisi ici. **Conseil :** Cette liste d'équipements fait référence au paramètre **Annonce**, sous **Mode expert** > **Serveur de téléphonie** > **Appels entrants** > **UCD** > **Modifier les paramètres du groupe UCD**, comme décrit dans Appels entrants > UCD. Si vous sélectionnez **Destination externe**, les deux champs suivants apparaissent : • **Route** (groupes de faisceaux) • **Numéro d'appel** (périphérique)

Paramètres	Description
Taper	Vous pouvez sélectionner l'un des types d'annonces suivants dans le menu déroulant : • **Aucun** : L'équipement d'annonce n'est pas connecté. • **Annonce** : Permet la connexion d'un seul périphérique d'annonce externe via des ports SLA ou des cartes EVM. L'annonce diffusée par le dispositif d'annonce activé doit avoir un début et une fin fixes. Cet appareil ne doit pas transférer l'appel après la fin de l'annonce (aucune destination de commutation ne doit être saisie). Le port du périphérique d'annonce correspondant est saisi sous **Accès**). Équivalent à **démarrer/arrêter** pour les périphériques de destination externes. • **Musique d'attente** : Une annonce ou une musique est répétée en continu. Les appels en attente peuvent également être connectés pendant la diffusion de la musique ou de l'annonce. La connexion est possible soit via des ports SLA, soit via des cartes EVM. Le port du périphérique d'annonce correspondant est saisi sous **Accès**. Équivalent à **continu** pour les périphériques de destination externes. • **Musique interne** : Active la musique d'attente interne au système dans le système de communication. Pour cette option, **Aucun** doit être saisi sous **Accès**. La musique d'attente externe (configuration Manager E) est audible si elle est définie comme destination dans le système de communication. Les entrées sous **Accès** n'ont aucun effet sur l'une ou l'autre variante. • **PC multimédia** : Ce paramètre est prédéfini. Le PC multimédia ou l'application de contrôle détermine si l'appelant entend l'annonce depuis le début ou s'il est connecté à une annonce en cours.
Mode	Vous pouvez choisir l'une des deux options suivantes : • **démarrer/arrêter** : lecture unique • **continu** : lecture en continu

Remarque : L'assistant **Musique d'attente / Annonces** peut également être utilisé pour configurer les **Annonces**. Pour plus d'informations, consultez Comment configurer les annonces.

27.3.12.4 Connexion > Ouvre-porte

Description des paramètres des onglets :

- **Modifier l'ouvre-porte**

Paramètres	Description
Station	Sélection du numéro de téléphone / port de connexion du téléphone d'entrée. Le type de port de la station doit être P.O.T ou Port N°.
Destination	Sélection du numéro de téléphone / port de connexion de la destination de la sonnerie du téléphone d'entrée. Un numéro de station ou un numéro de groupe peut être spécifié comme destination de sonnerie à laquelle une sonnerie spéciale est émise lorsque le bouton de la sonnette est actionné. L'appel est signalé conformément aux algorithmes de transfert d'appel définis dans « Paramètres - Appels entrants ».

Paramètres	Description
Ouvre-porte	Active la fonction ouvre-porte. En activant cet indicateur, un ouvre-porte connecté au TFE-S peut être activé pour les stations.
DTMF	L'activation de cet indicateur permet d'activer l'ouvre-porte à distance à l'aide d'un émetteur DTMF.
FWD	L'activation de cet indicateur permet le transfert externe de la destination de la sonnerie du téléphone d'entrée.

27.3.12.5 Connexions > SmartVM

Description des paramètres des onglets :

- **Modifier boîtes de messageries SmartVM**

Paramètres	Description
N° boîte vocale	Entrée des numéros de téléphone de boîte de messagerie. Une boîte vocale est identifiée à partir du numéro boîte vocale. Lorsqu'on attribue une mailbox à un abonné, il est obligatoire d'affecter à cette mailbox le numéro déjà attribué à l'abonné.
Nom	Affichage du nom de la boîte de messagerie. Le nom correspond au nom de l'abonné (s'il est disponible). Dans le cas d'un groupe, c'est le nom du groupe qui est affiché.
Message d'accueil	Sélection du message d'accueil. L'utilisation des entrées proposées est fonction du menu téléphone choisi (TUI). Avec OSO TUI seul le message d'accueil 1 est supporté avec les boîtes de messagerie standard.
Message d'accueil : **Message d'accueil 4**	Le choix des messages d'accueil 1-4 est fonction du type de boîte de messagerie : Boîte de messagerie standard : message d'accueil 1 ou 2 (avec OSO TUI uniquement message d'accueil 1) Boîte de messagerie de diffusion : message d'accueil 1, 2, 3 ou 4
Message d'accueil : **Jour/ Nuit**	Le message d'accueil est fonction du mode Jour/Nuit : Message d'accueil 1 Jour / Message d'accueil 2 Nuit
Message d'accueil : **Type d'appel**	Uniquement pour boîte de messagerie standard : le message d'accueil est fonction de l'état de l'abonné : Appel non accepté - Message d'accueil 1 / Occupé - Message d'accueil 2
Message d'accueil : **Néant**	Il n'est pas diffusé de message d'accueil. La boîte de messagerie demeure toutefois active, par ex. pour un transfert de l'appel vers le poste de renvoi.

Paramètres	Description
Enregistrement	Si ce flag est activé, la boîte de messagerie est une boîte de messagerie standard. Elle ne peut plus être une boîte vocale de diffusion. Si le flag est désactivé (par défaut), la boîte de messagerie n'est pas en mesure d'enregistrer un message. L'abonné peut activer l'enregistrement lors de la première interrogation de sa boîte de messagerie. Cela permet de garantir qu'aucun message ne peut être enregistré avant la première mise en service par l'abonné. Par défaut :Activé
Standard automatique	Si ce flag est activé, la boîte de messagerie est une boîte de messagerie de diffusion (AutoAttendant). Elle ne peut plus être une boîte de messagerie standard. 100 boîtes vocales maximum peuvent être configurées comme postes opérateurs. En cas de remplacement d'une boîte vocale standard par un standard automatique, tous les messages enregistrés sur la boîte vocale sont effacés. Par défaut : désactivé
Réinitialisation mot de passe	Si ce flag est activé, le mot de passe de la boîte de messagerie est rétabli sur `123456`. Lors de l'accès suivant à sa boîte de messagerie, l'abonné devra modifier son mot de passe. Par défaut : désactivé

Description des paramètres des onglets :

- **Modifier les paramètres SmartVM**

Paramètres	Description
Paramètres généraux	
long. max. des n° de boîte vocale	Longueur maximale des numéros boîte vocale. Plage de valeurs : 2 - 16 positions; valeur par défaut : 3 positions
Longueur max. du message (min)	Longueur maxi. de la durée d'enregistrement d'un message. Plage de valeurs : 1 ou 2 minutes; valeur par défaut : 2 minutes
Limitation de la longueur des numéros	Pour les communications sortantes lancées par SmartVM (standard automatique, post-sélection et standard automatique, numérotation abrégée), seuls des numéros ne dépassant pas la longueur indiquée peuvent être composés. Lorsque des numéros de téléphone plus longs sont paramétrés, l'établissement de la connexion n'est pas effectuée. Par défaut, la limitation de la longueur des numéros d'appel correspond à celle de la boîte de messagerie (longueur des numéros d'appel internes), de telle sorte que seule la composition de numéros internes est permise. Plage de valeurs : 2 à 30, valeur par défaut : 3
Dest. gén. renv. fax	Indiquer ici la destination vers laquelle SmartVM doit renvoyer normalement les fax entrants. Si aucun poste de renvoi Fax n'est indiqué, les fax entrants sont refusés. Plage de valeurs : 16 chiffres

Paramètres	Description
Langue standard	Choix de la langue du guide utilisateur. Cela s'applique à toutes les boîtes de messagerie. Si le guide utilisateur n'est pas disponible dans la langue souhaitée, la langue est alors convertie en anglais-Royaume-Uni (enuk).
Interface utilisateur du téléphone	Choix de la structure du menu téléphone de la boîte vocale (Telefone User Interface, TUI). Le choix s'applique à toutes les boîtes de messagerie.
Telephone User Interface (TUI) : **SmartVM**	SmartVM TUI, EVM TUI (par défaut).
Telephone User Interface (TUI) : **OSO**	OSO TUI, similaire à UC Suite TUI.
Ordre de l'annonce de date	uniquement visible avec SmartVM TUI : Paramétrage de la séquence des annonces pour message, date de réception, et numéro de l'appelant (si connu).
Ordre de la communication d'interphone de date : **Date après message**	uniquement visible avec SmartVM TUI : Message -- Date d'enregistrement -- Numéro de l'appelant (si connu).
Ordre de la communication d'interphone de date : **Date avant message**	uniquement visible avec SmartVM TUI : Date d'enregistrement -- Numéro de téléphone de l'appelant (si connu) -- Message. Pour les messages des abonnés internes, on applique les règles suivantes : Nom de l'abonné interne (s'il y en a) -- Date d'enregistrement -- Numéro de l'appelant (si connu) -- Message.
Quantité de messages par boîte de messagerie	Nombre maxi. de messages par boîte de messagerie. Plage de valeurs : 0 à 100, valeur par défaut : 30
Désactivation EVM	Si ce flag est activé, la SmartVM est désactivée. Par défaut : désactivé
Autoriser le rappel à partir de MV uniquement en direction des numéros connus	Lorsque l'utilisateur externe A appelle l'utilisateur B, l'appel est renvoyé vers sa boîte vocale, l'utilisateur externe A laisse un message vocal, l'utilisateur B appelle la SmartVM, saisit son mot de passe et appuie sur la touche 8 en écoutant le message. Appuyer sur cette touche permet de rappeler l'utilisateur B. Lorsque ce flag est activé, le rappel se produit si le numéro de l'utilisateur B fait partie des numéros connus. Les numéros connus sur les numéros de téléphone portable et domicile/externe des détails du profil de la gestion des utilisateurs (Applications-UC Smart-Gestion des utilisateurs) Par défaut :Activé
Comportement AA VP Paramétrage pour indiquer si le standard automatique doit ou non diffuser automatiquement des annonces dans certains cas.	

Paramètres	Description
VP Avant transfert	Si ce flag est activé, dans le cas "VP Avant libération", l'annonce ci-après est diffusée : "Patientez, vous allez être mis en communication..." Par défaut : désactivé
VP Transfert résultat	Si ce flag est activé, dans le cas "Résultat transfert VP", une des annonces ci-après est diffusée : "Le numéro d'abonné n'existe pas." "L'abonné est occupé." "L'abonné ne répond pas." Par défaut :Activé
VP Vidage mémoire	Si ce flag est activé, dans le cas "Renvoi VP", une des annonces ci-après est diffusée : "Vous êtes mis en relation avec l'opérateur. Veuillez patienter." "Vous êtes mis en relation avec la boîte vocale de l'abonné." "Patientez, vous allez être mis en communication..." Par défaut :Activé
VP Avant libération	Si ce flag est activé, dans le cas "VP Avant libération", une des annonces ci-après est diffusée : "Veuillez rappeler ultérieurement." "Merci. Au revoir." "Le numéro de la boîte vocale n'est pas valide." Par défaut :Activé

Description des paramètres des onglets :

- **Modifier les paramètres de standard automatique**

Paramètres	Description
Numéro d'appel	Numéro de téléphone du standard automatique (AutoAttendant) (par défaut : 352).
Renvoi après annonce	Si ce flag est activé, il est réalisé, après le message d'accueil, le renvoi de l'appel vers le poste de renvoi (par ex. poste opérateur). Pendant le passage de l'annonce d'accueil, il n'est pas possible de composer un numéro abrégé. Par défaut : désactivé
Pas de surnumérotation	Si ce flag est activée, l'appelant ne peut être renvoyé vers d'autres destinations qu'en composant des numéros abrégés. L'appelant ne peut pas sélectionner un numéro de téléphone à plusieurs positions. Par défaut : désactivé

Description des paramètres des onglets :

- **Modifier numérotation abrégée/vidage mémoire Jour**

- **Modifier numérotation abrégée/vidage mémoire Nuit**
- **Modifier numérotation abrégée/vidage mémoire 3**
- **Modifier numérotation abrégée/vidage mémoire 4**

Paramètres	Description
Sélectionner	Sélection d'un abonné interne (1e moitié de la liste) ou d'une boîte vocale (2e moitié de la liste) comme destination de la numérotation abrégée ou poste de renvoi.
Action	Affichage des 10 numéros abrégés possibles et du poste de renvoi.
Numéro d'appel	Numéro de l'abonné sélectionné ou de la boîte vocale sélectionnée.
Nom	Nom de l'abonné sélectionné ou de la boîte vocale sélectionnée.
Type	Sélection du type de numéro de téléphone.
Type : **Numéro d'appel**	Ici, l'abonné sélectionné est appelé à l'aide du numéro abrégé correspondant.
Type : **Boîte vocale**	Ici, la boîte vocale sélectionnée est appelée à l'aide du numéro abrégé correspondant.

27.3.13 Charge utile

Le menu **Charge utile** regroupe les fonctions pour l'affichage et la configuration des types de ports et des protocoles.

27.3.13.1 Charge utile > Equipements

Description des paramètres des onglets :

- **Afficher les Paramètres d'équipement généraux**
- **Ramener les Paramètres d'équipement à la valeur par défaut**

Paramètres	Description
Passerelle globale de type G.711	Equipements est le terme collectif pour les abonnés, les fonctionnalités et fonctions qui ont besoin de canaux. Il est affiché le type de codec de la passerelle globale, le nombre maximum des canaux B disponibles et sous licence ainsi que le nombre maximum des clients LAN sur un canal pour la musique d'attente (les appareils en surplus ne sont pas commutés).
Nombre maxi. de canaux B du matériel	
Nombre de clients LAN sur un canal MoH	

La réinitialisation des paramètres d'équipement nécessite un redémarrage du système de communication.

27.3.13.2 Charge utile > Media Stream Control (MSC)

Description des paramètres des onglets :

- **Modifier les paramètres de gigue MSC**

Paramètres	Description
	La gestion du flux des médias (MSC) surveille et gère les flux de médias sont guidés à travers le système de communication. Elle veillent à la commutation des données de média entre les réseaux, via les passerelles (TDM/IP).
Statistiques de trafic (SNMP uniquement)	Nécessaire pour l'accès aux données des statistiques Per-Call du sytème via SNMP.
Intervalle de génération de paquets RTCP (s)	Intervalle de rapport en secondes pour les paquets RTCP (Real-time Transport Control Protocol) pour négocier et respecter les paramètres de qualité de service (QoS) grâce à l'échange périodique de messages de commande entre émetteur et destinataire. Plage de valeurs : 5 à 10, valeur par défaut : 5

Description des paramètres des onglets :

- **Ramener les paramètres MSC à la valeur par défaut**

Paramètres	Description
Ramener les paramètres MSC à la valeur par défaut	Rétablir tous les paramètres MSC d'origine

27.3.13.3 Charge utile > Modules matériels

Administration des modules DSP du système de communication

Description des paramètres des onglets :

- **Afficher tous les modules matériels**
- **Modifier les paramètres DSP**
- **Modifier les paramètres de gigue DSP**

Paramètres	Description
Type de matériel	Affichage des DSP utilisés dans le système de communication (Digital Signal Processor). Sont possibles : • **Embarqué** = DSP intégré de la carte mère • **OCCB X-1** = DSP d'un sous-module OCCB (OCCB1 ou OCCB3)
Version de firmware	Version actuelle du firmware de chaque DSP
Version de l'API	Version actuelle de l'API (Application Programming Interface) de chaque DSP
Général	
Adresse IP	Adresse IP du module DSP (modifiable dans le cas où l'adresse IP est déjà attribuée.) ***Remarque:*** Le dernier octet de l'adresse IP ne peut pas être .1 (xxx.xxx.xxx.1)
Port	Numéro de port du module DSP
Affichage de l'État	Permet d'identifier la disponibilité des DSP Valeur par défaut : Message d'état

Paramètres	Description
Annuleur d'écho	Lorsque le flag est activé, le couplage audio (Echo) est supprimé lors des transmissions vocales. Valeur par défaut : Activé
Signalisation hors la bande MF	Lorsque le flag est activé, les signaux MF sont transmis dans un canal de signalisation séparé (Outband). Valeur par défaut : Désactivé
Paramètres fax	
Nombre de paquets redondants	Définition du nombre des paquets de redondance : plus cette valeur est élevée et plus la transmission fax est protégée contre les pertes de paquets. Le désavantage avec les grandes valeurs est l'augmentation de la bande passante nécessaire. Valeur par défaut : 2
Gigue de réseau maximum (hex ms)	Définition de la gigue réseau maximale en millisecondes : plus la valeur est élevée et plus la variance du temps de parcours des paquets de données sur les résaux est importante. Sont autorisées exclusivement des valeurs hexadécimales, avec des chiffres de 0 à 9 et de A à F. Autant que possible, il ne faut apporter aucune modification à ce paramètre. Valeur par défaut : 00C8
Dépassement du délai Détection de tonalité Fax/ Modem (s)	Définition du temps en secondes pour la reconnaissance des tonalités fax durant une connexion : la commutation sur le protocole fax T.38 est ainsi garantie. Une fois écoulé le temps indiqué ici, aucune tonalité fax n'est plus reconnue. La valeur 0 signifie que la reconnaissance des tonalités est activée pendant toute la durée de la connexion. Valeur par défaut : 0
Gigue DSP	
Type de tampon de gigue	Définition du type de tampon de gigue Valeur par défaut : Evolutif
Type de tampon de gigue : Statique	Le délai moyen du tampon de gigue demeure toujours le même.
Type de tampon de gigue : Evolutif	Le tampon de gigue adapte le délai moyen à la situation à la réception des données. On tente de réduire le délai au minimum et de perdre aussi peu de paquets de données que possible.
Délai moyen pour la voix (ms)	Définition du temps en millisecondes correspondant au maintien moyen dans le tampon de gigue d'un paquet d'une transmission vocale basée sur IP. ***INFO :*** Dans le cas du **type de tampon de gigueEvolutif** la valeur définie ici est seulement une valeur initiale. Valeur par défaut : 40

Paramètres	Description
Délai maxi. pour la voix (ms)	Définition de la durée maximale en millisecondes du retard de la voix **Type de tampon de gigue Statique :** il faut indiquer le nombre de millisecondes que peut représenter le délai réel mesuré lors de la réception des paquets IP pour la transmission vocale avant que le tampon de gigue n'intervienne dans le flux de données avec un effet régulateur. Dans le tampon de gigue adaptatif, 80 est une valeur recommandable pour la plupart des environnements. **Type de tampon de gigue Evolutif** : il faut indiquer le nombre maxi. de millisecondes que peut représenter le délai moyen pour la voix. Si le délai réel mesuré est plus important, des paquets sont perdus. Dans le tampon de gigue adaptatif, 120 est une valeur recommandable pour la plupart des environnements. ***Remarque:*** cette valeur doit toujours être supérieure à la valeur spécifiée dans le champ « Délai moyen pour la voix (ms) ». Valeur par défaut : 120
Délai mini. pour la voix (ms)	Définition de la durée minimale en milliseconde du délai pour la voix **Type de tampon de gigue Evolutif** : il faut indiquer le nombre mini. de millisecondes que peut représenter le délai moyen pour la voix. Le délai moyen sera dans tous les cas supérieur ou égal à cette valeur. Valeur par défaut : 20
Perte de paquet / Préférence de délai	Il est définit la relation entre perte de paquets et délai de circulation des paquets de données **Type de tampon de gigue Evolutif** : Il faut indiquer une valeur entre 0 et 8. La valeur dépend de la question suivante : dans le cas de délais élevée faut-il accepter la perte de paquets ou plutôt un délai encore plus élevé. La valeur 0 correspond à des pertes de paquets minimale, avec le désavantage de délais de circulation. La valeur 8 correspond à un délai minimum avec le désavantage de possibles pertes de paquets. Une valeur recommandable pour la plupart des environnements est 4. Valeur par défaut : 4
Délai moyen pour les données (ms)	Définition du retard moyen des données, en millisecondes Il faut indiquer le nombre de millisecondes durant lesquelles un paquet de données doit être maintenu en moyenne dans le tampon de gigue lors de la tranmission des données. Une valeur recommandable pour la plupart des environnements est 60. Valeur par défaut : 60

Paramètres	Description
Délai maxi. pour les données (ms)	Définition du retard maximum des données, en millisecondes Il faut indiquer le nombre de millisecondes possible pour le retard effectivement mesuré à la réception des paquets IP, avant que le tampon de gigue exerce son effet régulateur. Une valeur recommandable pour la plupart des environnements est 200. ***INFO :*** Les valeurs plus élevées (à partir de 2000 env.) n'ont pas d'influence. Dès qu'un paquet a été entièrement réceptionné dans le tampon, il le quitte. Les valeurs inférieures à 100 ms sont possibles, mais ne sont absolument pas recommandées dans la pratique. Valeur par défaut : 200

27.3.14 Statistiques

Le menu **Statistiques** regroupe les fonctions d'affichage des statistiques.

27.3.14.1 Statistiques > Statistiques de la passerelle > Carte mère > Statistiques d’équipements

Description des paramètres des onglets :

- **Afficher les statistiques SCN**
- **Afficher les statistiques LAN**

Paramètres	Description
Type d'équipement	Affichage des composantes LAN et SCN (Switched Circuit Network) disponibles.
Ressources actuellement occupées	Affichage des ressources actuellement occupées d’une composante (canaux configurés et utilisés).
Total	Affichage du total des ressources actuellement occupées.
Actualisation automatique	L’affichage est actualisé toutes les 60 secondes.
Secondes jusqu'à la prochaine actualisation	Affichage d’une temporisation avec indication du temps restant, débutant à 60 secondes.
Abonnés DDS1	Dès qu’un téléphone mobile se déplace dans la zone d’un autre emplacement de commutation radio ("carte sans fil de localisation"), une connexion d’extension est commutée via une connexion DSS1 initiée par la carte sans fil. Ainsi, l’abonné DSS1 fait référence au nombre de téléphones mobiles ou de connexions DSS1 établis dans le commutateur.
Langue HFA / Mise en réseau IP	Cette composante SCN indique le nombre de canaux DSP occupés lorsque les communications passerelle sont établis.
Musique d’attente	Lorsque la fonction Interfonctionnement DMC est active dans un réseau IP, les connexions passerelle sont établies sur des canaux DMC. Du point de vue de l’utilisateur, un canal DMC est un canal passerelle qui fournit une connexion passerelle.

Paramètres	Description
SIU	L'unité de signalisation (SIU) réserve un canal DSP utilisé pour détecter ou générer des tonalités système, comme les tonalités DTMF
DMC	Affichage d'une temporisation avec indication du temps restant, débutant à 60 secondes.
H.323 (RTP)	Affiche les ressources utilisées en cas d'appel vocal.
Fax T.38	Affiche les ressources utilisées en cas de connexion fax.
PPP	Affiche les ressources utilisées en cas de raccordement système.

27.3.14.2 Statistiques > Statistiques de la passerelle > Carte mère > Statistiques MSC

Description des paramètres des onglets :

- **Afficher les statistiques globales**

  Les statistiques MSC sont des statistiques sur le flux de média qui circule via des processeurs de signal numériques entre IP et TDM (Media Stream Control). Les statistiques globales MSC donnent un aperçu sur les données statistiques concernant toutes les communications enregistrées. Elles donnent des indications sur les paquets RTP/TCP envoyés et non envoyés, sur les paquets reçus et non reçus et sur le nombre des octets envoyés et reçus.

Description des paramètres des onglets :

- **Afficher les statistiques d'appels individuels**

  Les statistiques d'appel individuel MSC fournissent une liste en forme de tableau pour chaque connexion avec passage par processeurs de signal numérique, pour les données de connexion et pour les paramètres utilisés. Elle sort aux experts pour analyser les défauts.

27.3.14.3 Statistiques > Statistiques SNMP

Description des paramètres des onglets :

- **Afficher le tableau des statistiques**
- **Afficher les statistiques**

Paramètres	Description
Statistiques Tableaux if	Détails saisis dans SNMP à propos des différentes interfaces (if = interface) dans le système de communication, par exemple interfaces Ethernet.
Statistiques IP	Détails et erreurs relatifs au routage IP
Statistiques TCP	Détails et erreurs relatifs au protocole TCP
Statistiques UDP	Détails et erreurs relatifs au protocole UDP

27.3.14.4 Statistiques > Statistiques de téléphonie > Textes système

Description des paramètres des onglets :

- **Afficher les textes système**

Paramètres	Description
Langues disponibles	Affichage des langues disponibles dans le système de communication pour les affichages du téléphone

27.3.14.5 Statistiques > Statistiques de téléphonie > Agents UCD

Description des paramètres des onglets :

- **Afficher les agents UCD**

Paramètres	Description
Nombre d'agents UCD	
Total	Nombre total des agents UCD connecté au système de communication
Disponible	Nombre des agents UCD disponibles
Statut des agents UCD	
Numéro de téléphone	Numéro de téléphone de l'agent UCD
Nom	Nom de l'agent UCD
ID	ID de l'agent UCD
Groupe UCD	Groupe UCD qui est affecté à l'agent UCD.
État	Etat de l'agent UCD

27.3.14.6 Statistiques > Statistiques de téléphonie > Etat de la ligne

Description des paramètres des onglets :

- **Afficher l’état de la ligne**

Paramètres	Description
Date	Date de l'interrogation de l'état ou de la dernière modification d'état de la ligne
Heure	Heure de la demande d'état ou de la dernière modification d'état de la ligne
Slot / Port	Affichage du module, de l'emplacement de montage (slot) et de l'interface (port) ou de l'interface LAN
Faisceaux	Affichage du nom de l’itinéraire, pour obtenir un meilleur conseil sur l’ITSP auquel appartient une ligne.
N° ligne	Code de ligne

Paramètres	Description
Commentaire	Etat de la ligne(il est affiché le dernier état de la ligne) Les états de ligne suivants sont possibles : • **Idle** (ligne à l'état de repos) • **Alerting** (appel présenté) • **Connecté à** (connexion avec le numéro d'appel affiché) • **Ligne verrouillée** • **Ligne hors service**

27.3.14.7 Statistiques > Statistiques de téléphonie > Renvois

Description des paramètres des onglets :

- **Afficher les renvois**

Paramètres	Description
Renvoi d'appel	
État	Etat du renvoi d'appel : • **désactivé** (aucun renvoi d'appel activé) • Lorsque un renvoi d'appel est activé, le type de renvoi et la destination de renvoi sont présentés.
Destinataire du renvoi de	Indication précisant si l'abonné est la destination de renvoi d'un renvoi programmé par un autre abonné. Il est affiché le numéro de téléphone et le nom de l'abonné effectuant le renvoi.
Pilotage	
Abonnés inclus	Numéro de téléphone et nom des abonnés pilotés
Pilotage de	Indication précisant si l'abonné est la destination de pilotage d'un autre abonné. Il est affiché le numéro de téléphone et le nom de l'abonné effectuant le pilotage.

27.3.14.8 Statistiques > Statistiques de téléphonie > Abonnés

Description des paramètres des onglets :

- **Afficher les Paramètres de l'abonné**
- **Afficher les fonctionnalités activées**

Paramètres	Description
Numéro de téléphone	Numéro de l'abonné
Nom	Nom de l'abonné
N° SDA	Numéro SDA de l'abonné
Type d'équipement	Type de téléphone, par exemple OpenStage 60

Paramètres	Description
Clip/Lin	Location Identification Number LIN Uniquement pour les Etats-Unis, le Canada : avec le service d'appel d'urgence étendu E911, outre le numéro d'appel, des informations relatives à la localisation géographique de l'appelant sont transmises à l'émission de l'appel d'urgence. De plus, il est affecté un numéro LIN à chaque raccordement d'abonné avec n° SDA valide.
Accès	Pour les téléphones analogiques et $U_{P0/E}$, affichage du module, de l'emplacement de montage et du numéro de raccordement. En plus, affichage du type (maître ou esclave) pour les téléphones $U_{P0/E}$. Pour les téléphones IP, affichage de l'interface LAN, du type et du numéro
Paramètres	
Type d'abonné	Type de poste, par exemple Par défaut ou Fax Valeur par défaut : Standard
Langue	Réglage de la langue sur le téléphone
Signalisation des appels internes	Type de sonnerie pour la signalisation des appels internes Valeur par défaut : Type de sonnerie 1
Signalisation des appels externes	Type de sonnerie pour la signalisation des appels externes Valeur par défaut : Type de sonnerie 1
Classe de discrimination (LCR)	Classe de service de l'abonné pour Least Cost Routing Valeur par défaut : 15
Type de licence	Type de licence de l'abonné
Caractéristiques	
Ne pas déranger	Etat de la fonctionnalité Ne pas déranger Valeur par défaut : Désactivé
Texte d'absence	Etat de la fonctionnalité Texte d'absence Valeur par défaut : Désactivé
Code verrouillage	Etat de la fonctionnalité Code verrouillage Valeur par défaut : Désactivé
Activation masquage du N° SDA	Etat de la fonctionnalité Masquage du numéro d'appel Valeur par défaut : Désactivé
Pilotage	Etat de la fonctionnalité Pilotage Valeur par défaut : Désactivé
Désactivation sonnerie poste	Etat de la fonctionnalité Appel sans sonnerie / Repos Valeur par défaut : Désactivé

Paramètres	Description
Groupement	Etat de la fonctionnalité Groupe de recherche/Appel de groupe Valeur par défaut : Désactivé
Avertissement sans tonalité	Etat de la fonctionnalité Avertissement sans tonalité Valeur par défaut : Désactivé
Réponse sur appel interphone	Etat de la fonctionnalité Réponse sur appel interphone Valeur par défaut : Désactivé
Autoriser l'avertissement	Etat de la fonctionnalité Autoriser l'avertissement Valeur par défaut : Désactivé
Renvoi après temporisation	Etat de la fonctionnalité Renvoi après temporisation Valeur par défaut : Désactivé
Renvoi	Etat de la fonctionnalité Renvoi d'appel Valeur par défaut : Désactivé

27.4 Applications

Dans **Applications** sont regroupées les fonctions de configuration du serveur d'application pour les Unified Communications et les Web Services.

27.4.1 Sélection de l'application

Dans **Sélection de l'application** sont regroupées les fonctions de sélection de la solution utilisée pour les Unified Communications.

27.4.1.1 Sélection de l'application

Description des paramètres des onglets :

- **Sélection de l'application**

Paramètres	Description
Sélectionnez les packages d'applications	Choix de suites logicielles avec UC Smart ou avec UC Suite.
Sélection de l'application	Affichage des composants pris en charge, en fonction du package d'application sélectionné, y compris l'adresse IP du serveur utilisé.

27.4.2 Intégration d’Active Directory Service

Les fonctions pertinentes pour l’intégration d’Active Directory sont regroupées sous **Intégration d’Active Directory Service**.

27.4.2.1 Intégration d’Active Directory Service

Description des paramètres des onglets :

- **Intégration d’Active Directory Service**

Paramètres	Description
Type de synchronisation	Le type de synchronisation peut avoir les valeurs suivantes : • **Libre** Aucune synchronisation de l’utilisateur avec le service Active Directory. • **sda** Synchronisation automatique de l’utilisateur avec Active Directory. Le numéro SDA est utilisé comme clé de synchronisation. • **forcé** Synchronisation manuelle de l’utilisateur avec un utilisateur d’Active Directory. Avec la synchronisation forcée, il est possible de synchroniser un utilisateur d’Active Directory avec plusieurs utilisateurs d’OpenScape Business. • **mulap_member** L’utilisateur synchronisé automatiquement est membre du groupe MULAP.
Rechercher	Les champs vides en haut de l’écran peuvent être utilisés pour chercher un utilisateur spécifique lorsque tous les utilisateurs ne rentrent pas dans l’écran. Une recherche « commence par » est effectuée dans les champs **Prénom**, **Nom**, **Nom d’affichage** et **SDA**, . Une recherche « contient » est effectuée dans le champ **Utilisateur d’Active Directory**. Pour initier la recherche, appuyer sur le bouton **Rechercher**.
Modifier	Vous pouvez utiliser ce bouton pour configurer la synchronisation de l’utilisateur spécifié. Les actions disponibles lorsque vous sélectionnez **Modifier** correspondent aux boutons suivants, qui s’affichent.
Enregistrer les données	Vous pouvez sélectionner un utilisateur d’AD spécifique et forcer la synchronisation avec l’utilisateur d’OpenScape Business spécifique. Vous pouvez de cette manière synchroniser différents numéros SDA pour le même utilisateur d’AD.
Réinitialiser	Essayez de synchroniser l’utilisateur d’OpenScape Business avec tout utilisateur d’Active Directory. Cette action peut être utilisée, par exemple, si la synchronisation de l’utilisateur s’est arrêtée.
Ne pas synchroniser	Arrêtez la synchronisation de l’utilisateur d’OpenScape Business spécifié. Les données déjà synchronisées pour l’utilisateur ne sont pas supprimées, mais la synchronisation avec AD est interrompue.

27.4.3 UC Smart

Dans **UC Smart** sont regroupées les fonctions Unified Communications.

27.4.3.1 UC Smart > Configuration de base

Description des paramètres des onglets :

- **Configuration de base**

Paramètres	Description
Activer / Verrouiller UC Smart	
Actif(ve)	UC Smart et UC Suite ne peuvent pas être simultanément opérationnels. (Après activation, d'autres paramètres sont affichés)
Activer / désactiver CloudService	
Actif(ve)	Cet indicateur contrôle l'état de la fonctionnalité CloudService. Notez que l'activation de la fonctionnalité CloudService entraînera un redémarrage de WebServices.
Paramètres d'accès	
HTTP	Les clients UC Smart peuvent pas principe accéder de manière cryptée au système via HTTPS ou de manière non cryptée via HTTP (non recommandé). La sélection est effectuée dans l'application. C'est à ce niveau qu'est attribuée la classe de discrimination pour un protocole ou pour les deux.
HTTPS	
Règles concernant le mot de passe	
L'utilisateur doit entrer un mot de passe sûr	Directive sur le mot de passe pour les clients UC Smart. Le mot de passe par défaut doit être modifié lors de la première connexion et respecter la règle sélectionnée ici (voir bouton avec point d'exclamation). Le mot de passe est enregistré dans le client, sinon il est demandé lors de chaque démarrage du client.
Enregistrer les données de connexion dans le terminal	Les données de connexion sont en plus enregistrées sur le téléphone.
Mot de passe UC Smart initial pour l'ensemble du système	Le mot de passe initial, pour l'ensemble du système, s'applique à tous les utilisateur UC Smart configurés qui ne se sont pas encore connecté à UC Smart ou qui n'ont pas encore modifié leur mot de passe initial. Il doit être ensuite attribué un mot de passe individuel à chaque utilisateur concerné. ***INFO*** : L'attribution d'un mot de passe UC Smart initial, pour l'ensemble du système, représente un risque pour la sécurité, en particulier s'il n'est pas attribué rapidement un mot de passe personnel à chaque utilisateur individuel. Ou bien, il est recommandé d'attribuer des mots de passe individuels initiaux pour chaque utilisateur.
Heures de bureau	
Heure de début	Vous pouvez configurer les Heures de bureau en sélectionnant deux valeurs dans les listes déroulantes Heure de début et Heure de fin. Les heures de bureau par défaut sont comprises entre 08h00 et 20h00.
Heure de fin	
Présence	
Masquer l'état de maladie	Vous pouvez masquer l'option d'état de présence « Maladie » aux utilisateurs de clients UC.

27.4.3.2 UC Smart > Gestion des utilisateurs

Description des paramètres des onglets :

- **Gestion des utilisateurs**

Paramètres	Description
Utilisateurs	Liste de tous les abonnés existants, l'abonné sélectionné doit disposer d'une licence UC User
Paramètres	
Utilisateurs	Affichage des numéros de téléphone internes de l'utilisateur.
Nom	Affichage du nom de l'abonné.
Mot de passe	Il est possible de définir ici le mot de passe de l'utilisateur de UC Smart Client.
Langue	Langue de UC Smart Assistant
L'utilisateur doit attribuer un nouveau mot de passe	(uniquement affichage)
Accès UC Smart Assistant	Classe de discrimination pour accès à UC Smart Assistant par l'utilisateur
Configuré comme abonné Mobility	(uniquement affichage)
Licence de messagerie vocale	(uniquement affichage)
Services associés	(uniquement affichage)
Détails du profil	
Numéro de téléphone mobile	Numéro de téléphone mobile de l'abonné au format canonique (par ex. `+49 173 1234567`).
Numéro privé / externe	Numéro de téléphone supplémentaire de l'abonné au format canonique (par ex. `+49 89 987654321`).
Adresse e-mail	Adresse e-mail de l'abonné.
Messagerie vocale à e-mail	Activation/Désactivation de la notification par e-mail lors de la réception d'un nouveau message vocal.
Visibilité de l'état Présence	Configuration pour déterminer si l'état Présence doit-il être visible pour les abonnés internes et externes ou être uniquement visible pour les abonnés ou ne jamais être visible.
Informations sur la licence	Affichage des licences disponibles dans le système pour l'application concernée

27.4.3.3 UC Smart > État

Description des paramètres des onglets :

- **État**

Paramètres	Description
Serveur d'application	Affichage de l'état du serveur d'application UC Smart intégré.
Liaisons actives	Affichage du nombre des liaisons actives par UC Smart Client.

27.4.4 OpenScape Business, UC Suite

Dans **OpenScape Business UC Suite** figurent des fonctions Unified Communications, par ex. Conférences, Départements et Groupes, Configuration du répertoire externe, Calendrier des congés et Calendrier, Centre de contacts et Paramètres serveur pour UC Suite.

27.4.4.1 OpenScape Business, UC Suite

Paramètres	Description
OpenScape Business UC Suite	Configuration de UC Suite, y compris les clients myPortal, myAgent, myAttendant et myReports, messages Voix et Fax ainsi que conférences.

27.4.4.2 OpenScape Business UC Suite > Répertoire utilisateur

Si vous souhaitez modifier votre prénom et votre nom de famille, demandez à l'administrateur. Sinon, les modifications ne seront pas conservées après une synchronisation. La synchronisation à lieu quand les systèmes redémarrent ou que les paramètres sont modifiés par l'administrateur.

Un abonné membre d'un groupe MULAP n'est pas affiché dans le répertoire utilisateur. Si l'abonné est membre d'un groupe de recherche, il est affiché dans le répertoire utilisateur.

Paramètres	Description
Rechercher	Recherche d'un utilisateur UC Suite.
Icône de l'état de présence	L'administrateur peut modifier le statut de présence de chaque utilisateur et définir la date et l'heure de son retour au format jour-mois-année (JJ/MM/AA) et 24 heures (HH:MM) respectivement. Une illustration en gris signifie qu'il n'y a pas de connexion avec UC Suite. **Remarque :** Chaque membre d'un groupe de recherche est considéré comme utilisateur du répertoire système et est affiché de façon grisée.

Paramètres	Description
Modifier	Modifier les paramètres de l'utilisateur de l'UC Suite sélectionné. **Remarque :** En raison d'un problème connu de compatibilité du navigateur, l'organisation de la fenêtre **Modifier l'utilisateur** peut différer en utilisant Firefox. L'organisation est normale sous IE/Chrome/Edge.
Réinitialiser l'utilisateur	Les paramètres d'un utilisateur sont replacées aux valeurs par défaut. Cela supprime ses messages vocaux, ses annonces personnalisées de la boîte vocale, ses entrées journal, ses conférences programmées, ses e-mails et ses messages Fax. **Remarque :** Dans ce cas, le mot de passe par défaut est défini sur 4 caractères (1234).
Abonné déverrouillé	Les utilisateurs verrouillés (par ex. à la suite de plusieurs saisies erronées du mot de passe) peuvent être débloqués ici, affichage de l'icône du cadenas. L'administrateur peut être informé du verrouillage par le système, via e-mail.
Données personnelles	Données personnelles de l'utilisateur
Données personnelles : Mes données personnelles	Nom de connexion, Mot de passe, Nom, Poste, Prénom, Numéro de boîte vocale, Numéro de fax, Numéro de l'assistant(e), Adresse e-mail, Département, Numéro mobile, Numéro externe 1/2, Numéro à domicile (au format canonique, par ex.: +49 89 700798765). Le mot de passe est valide pour UC Suite Clients.
Données personnelles : Ma photo	Escalade automatique Formats de fichiers pris en charge : BMP, JPG/JPEG/JFIFI, PNG. Taille maximale du fichier: 10 Mo
Données personnelles : Niveau utilisateur	Réglable uniquement par l'administrateur du centre de contacts : si l'agent doit être disponible de manière durable, cochez la case **Agent disponible de manière durable**. L'agent demeure ensuite disponible pour les appels, fax et e-mails, même s'il n'a pas répondu à un appel, un fax ou un e-mail. Lorsqu'un utilisateur est configuré en tant qu'agent, les droits de l'agent sont définis en sélectionnant la classe de service appropriée pour cet agent (c'est-à-dire le niveau d'autorisation en tant qu'agent, superviseur ou administrateur), dans la liste déroulante **Niveau**. Un agent avec le niveau d'autorisation Superviseur ou Administrateur dispose d'autorisations élargies.
Mes Préférences	Paramètres spécifiques utilisateur du client.
Mes Préférences : Apparence	Couleurs de peau de l'interface utilisateur ; langue de l'interface utilisateur ; utilisation ou non de traypop classique.
Mes Préférences : Notifications	Paramètres pour la fenêtre contextuelle.
Mes Préférences : Présence	Paramètres pour le statut de présence.

Paramètres	Description
Mes Préférences : Connexion Outlook	Gérez les rendez-vous du calendrier : reprise de l'état Présence dans le calendrier Outlook Intégration calendrier : gestion de l'état à l'aide des rendez-vous Outlook/iCal (le premier mot de passe de la ligne de l'objet gère l'état Présence)
Mes Préférences : Touches de raccourci	Définition des touches de raccourci pour les fonctions d'appel.
Mes Préférences : Divers	Réinitialisation automatique du statut de présence sur « Bureau » après la fin d'un rendez-vous, activation de l'enregistrement des journaux des clients, définition de la méthode de transfert, période de conservation des entrées du journal (valeur maximale de 30 jours), programmation des touches de fonction du téléphone, activation de la recherche en direct et inclusion des contacts LDAP dans la recherche en direct des annuaires, spécification d'un message de réponse.
Règles d'appel	Règles pour les appels entrants
Règles d'appel : Destinations de renvoi	Définition des destinations de renvoi pour chaque état Présence (Renvoi d'appel en fonction de l'état)
Règles d'appel : Moteur de règles	Définition de règles d'appel complexes en fonction de l'état Présence (renvoi d'appel basé sur une règle)
Communications	Traitement des messages spécifiques de l'utilisateur
Communications : Paramètres de messagerie vocale	L'enregistrement de messages vocaux est possible dans l'état Présence correspondant ; réglage de la langue de la messagerie vocale Valeur par défaut : désactivé
Communications : Notification MV	Service de notification pour nouveaux messages vocaux - adresse e-mail, voir propres données personnelles. Condition : configuration du mailserver et de la propre adresse mail dans Servicecenter > Renvoi e-Mail. "Sortant" génère un appel User-Outcall vers le numéro indiqué (format canonique). Numéro SMS voir propres données personnelles. Contenu du SMS voir modèles.
Communications : Notification fax	Service de notification pour nouveaux messages fax - adresse e-mail, voir propres données personnelles. Condition : configuration du mailserver et de la propre adresse mail dans Servicecenter > Renvoi e-Mail. L'option « Outbound » génère un appel sortant de l'utilisateur vers le numéro de téléphone spécifié (en format canonique), soit pendant les heures ouvrables uniquement, soit 24 heures par jour. Numéro SMS voir propres données personnelles. Contenu du SMS voir modèles.
Communications : Notifications d'appel manqués	Service de notification des nouveaux appels manqués - voir l'adresse e-mail de Mes données personnelles. Condition : configuration du mailserver et de la propre adresse mail dans Servicecenter > Renvoi e-Mail.
Profils MV	Profil pour standard automatique personnel
Occupé(e), Pas de réponse, Réunion, Maladie, Pause, Absent, Congé, Déjeuner, À domicile	Un appelant peut, en composant un chiffre de 0 à 9, être dirigé vers une destination de renvoi ou enregistrer un message. Condition : disposer d'une annonce par état Présence.

Paramètres	Description
Profils : Sauter le message d'accueil dynamique	L'annonce automatique de l'état Présence est sauté, à la place l'appelant n'entend que l'annonce du nom puis du standard automatique personnel
Sensibilité	Paramètres pour assurer la confidentialité
Sensibilité : Sécurité et accès	Libération des messages vocaux pour myAttendant ; consultation de la boîte vocale à partir du propre téléphone sans mot de passe ; permettre aux autres utilisateurs de voir à qui vous parlez et de copier votre présentation BLF.
Sensibilité : Visibilité de l'état de présence	Définition de la visibilité du propre état Présence pour les utilisateurs internes
Sensibilité : État de présence de boîte vocale	Annonce concernant votre état Présence pour appelants externes. Saisie des numéros de téléphone internes à verrouiller ; il est possible d'utiliser des jokers.
myAttendant	Affichage uniquement pour les abonnés avec licence myAttendant
myAttendant : Messages LAN	Modules de texte pour messages instantanés de myAttendant, saisie libre, sélection dans la fenêtre de chat du client
myAttendant : SDA	Entrée de numéros SDA ; lorsque myAttendant est utilisé pour plusieurs sociétés, il est possible d'afficher une fenêtre "Pour"
myAttendant : Communications	Saisie d'un numéro interne pour le renvoi d'appel en cas d'urgence ou de non-acceptation (Renvoi non surveillé) par myAttendant (pour les États-Unis)

27.4.4.3 OpenScape Business UC Suite > Départements

Description des paramètres des onglets :

- **Départements**

Paramètres	Description
Nom du département	Les départements regroupent les abonnés dans un répertoire interne en fonction de leur appartenance organisationnelle. Il est ainsi possible par ex. d'effectuer une affectation automatique des utilisateurs aux départements, dans myAttendant.
Groupement	(numérotation interne, sans autre signification)
Ajouter	Ajouter un nouveau département.
Modifier	Modifier un département sélectionné.
Supprimer	Supprimer les départements sélectionnés.

27.4.4.4 OpenScape Business UC Suite > Groupes

Un groupe Boîte vocale (groupe Répondeur) peut permettre à un groupe défini d'abonnés d'accéder aux messages vocaux. Ce numéro du groupe Boîte vocale

n'appelle pas les membres de ce groupe, mais joint directement la boîte vocale (le répondeur) du groupe.

Un groupe Fax (groupe Boîte Fax) peut permettre à un groupe défini d'abonnés d'accéder aux messages Fax. Le numéro du groupe Fax permet d'accéder directement à la boîte Fax du groupe.

Les groupes Favoris vous permettent de créer des groupes avec des contacts et d'attribuer ces derniers aux utilisateurs.

Description des paramètres des onglets :

- **Groupes messagerie vocale**
- **Groupe Fax**
- **Groupes Favoris**

Tableau 64 :

Paramètres	Description
Groupes Boîte vocale	
Modifier	Modifier le groupe Boîte vocale sélectionné
Supprimer	Supprimer les groupes Boîte vocale sélectionnés
Groupes Boîte vocale	Nom du groupe Boîte vocale
Pilote	Numéro de téléphone du groupe Boîte vocale
Type	Type de groupe Boîte vocale
Nombre d'utilisateurs	Nombre des membres du groupe Boîte vocale
Nombre de messages	Nombre des nouveaux messages vocaux dans le groupe Boîte vocale
Utilisateurs	Membres du groupe Boîte vocale
Groupe Fax	
Modifier	Modifier le groupe Fax sélectionné
Groupe Fax	Nom du groupe Fax
Pilote	Numéro de téléphone du groupe Fax
Nombre d'utilisateurs	Nombre des membres du groupe Fax
Nombre de fax	Nombre des nouveaux messages fax dans le groupe Fax
Multi-utilisateurs	S'il s'agit d'un groupe Fax, **Oui** s'affiche. Sinon, **Non** s'affiche.
Groupes Favoris	
Ajouter	Ajouter un nouveau groupe Favoris

Paramètres	Description
Modifier	Modifier le groupe Favoris sélectionné
Supprimer	Supprimer les groupes Favoris sélectionnés
Nom du groupe	Nom du groupe Favoris
Nombre de contacts	Nombre de contacts qui ont été ajoutés au groupe
Modifiable	Sélectionnez cette option pour autoriser l'utilisateur à modifier le groupe Favoris.

27.4.4.5 OpenScape Business UC Suite > Modèles

Description des paramètres des onglets :

- **Fournisseur SMS**

Paramètres	Description
Ajouter	Ajoutez un nouveau modèle. Entrez le nom du modèle et le nom de l'auteur. Dans le champ Destinataire, Objet ou Corps, il est possible d'ajouter des jokers, sélectionnés dans « Champs VSL ».
Modifier	Modifiez le modèle sélectionné Modifiez le nom du modèle et le nom de l'auteur. Modifiez également les champs Destinataire, Objet et Corps. Dans le champ Destinataire, Objet ou Corps, il est possible d'ajouter des jokers, sélectionnés dans « Champs VSL ».
Supprimer	Supprimez le modèle sélectionné.
Paramétrer comme valeur par défaut	Définissez le modèle sélectionné par défaut.

27.4.4.6 OpenScape Business UC Suite > Répertoire externe

Description des paramètres des onglets :

- **Répertoire externe**

Paramètres	Description
Ajouter	Ajout manuel de différents contacts au répertoire externe. Les caractères doivent correspondre au format UTF-8
Modifier	Modifier un contact sélectionné du répertoire externe.
Supprimer	Supprimer les contacts sélectionnés du répertoire externe

Description des paramètres des onglets :

- **Importer répertoire externe**

Paramètres	Description
Importer de	Indiquez si l'importation des informations de contacts sera effectuée à partir d'un fichier local ou à partir d'un dossier Windows public.
Chargement du fichier	Cliquez sur **Choisir un fichier** pour sélectionner le fichier à charger dans le système.
Dossier Windows public	Entrez le **Nom de fichier**, le **Nom d'utilisateur**, le **Domaine**, le **Mot de passe** du dossier Windows public à charger dans le système, puis cliquez sur **Test** pour le tester.
Options	Cette fenêtre offre différentes options concernant le formatage du fichier csv qui va être importé. Il existe également une option permettant d'effacer les données existantes avant d'exécuter l'importation. Enfin, une autre option permet d'indiquer la méthode de traitement des doublons lors d'une importation.

Description des paramètres des onglets :

- **Exporter le répertoire externe**

Paramètres	Description
Exporter vers	Choisissez où le fichier exporté sera enregistré, localement ou dans un dossier Windows public.
Dossier Windows public	Entrez le **Nom de fichier**, le **Nom d'utilisateur**, le **Domaine**, le **Mot de passe** du dossier Windows public à charger dans le système, puis cliquez sur **Test** pour le tester.

27.4.4.7 Configuration des fournisseurs externes > d'OpenScape Business UC Suite

Description des paramètres des onglets :

- **Fournisseurs LDAP**

Paramètres	Description
Ajouter / Modifier / Supprimer	Ajouter, modifier ou supprimer les données d'accès du serveur LDAP.
Nom	Nom de ce répertoire hors ligne externe
Serveur / Adresse du serveur	Nom DNS ou adresse IP du serveur LDAP.
Port	Numéro de port du serveur LDAP externe
Nom d'utilisateur	Nom d'utilisateur pour accéder au serveur LDAP distant.
Mot de passe	Mot de passe pour accéder au serveur Exchange distant.
Nom distinctif de base LDAP	Nom distinctif de base LDAP, par exemple, dc=exemple-pour-un-domaine, dc=net.
TLS	Autoriser uniquement l'utilisation de connexions sécurisées au serveur LDAP.

Paramètres	Description
Titre, **Prénom**, **Nom**, **Professionnel 1**, **Professionnel 2**, **Tél. domicile**, **Mobile**, **Société**, **Tél. société**, **Adresse postale**, **Nom de l'État ou de la province**, **Nom du pays**, **Code postal**, **E-mail**, **Radiomessagerie**, **N° Fax** et **Ville**	Lors de la configuration d'un annuaire hors ligne externe, l'administrateur peut adapter le mappage des champs aux noms du serveur LDAP utilisé. Les champs supprimés sont ignorés lors de la recherche de noms par numéro de téléphone. La recherche s'effectue toujours avec les 4 derniers chiffres du numéro de téléphone précédés d'un caractère générique. Vous pouvez désactiver la recherche de noms à partir des numéros de téléphone pour les appels entrants. Saisissez le nom de champ correspondant du serveur LDAP dans chaque cas. **Remarque :** Le mappage des champs LDAP dépend du nom du champ correspondant, via l'utilisation d'un serveur LDAP externe.

Description des paramètres des onglets :

- **Échange PST**

Paramètres	Description
Ajouter / Modifier / Supprimer	Ajouter, modifier ou supprimer les données d'accès du serveur Exchange. Dans un environnement Microsoft, le serveur Active Directory (ADS) ou le serveur Exchange fait également office de serveur LDAP.
Nom	Nom de ce répertoire externe hors ligne.
Méthode d'authentification	Méthode d'authentification à utiliser pour accéder au serveur Exchange distant. Vous pouvez choisir entre **Basic**, **OAuth 2.0 EWS** et **OAuth 2.0 Graph**.
Serveur / Adresse du serveur	Nom DNS ou adresse IP du serveur Exchange.
Nom d'utilisateur	Nom d'utilisateur pour accéder au serveur Exchange distant.
Mot de passe	Mot de passe pour accéder au serveur Exchange distant. Visible uniquement si la méthode d'authentification sélectionnée est **Basique** .
ID du locataire , **ID de l'application** , **Secret client** , **Étendue**	**ID du locataire** , **ID de l'application** et **secret client** correspondant à l'application enregistrée dans Azure AD pour l'intégration d'annuaire Exchange. Vous pouvez les obtenir auprès de votre administrateur Azure AD. **Portée** requise par l'application (facultatif). Valeur par défaut : https://outlook.office365.com/.default Visible uniquement si la méthode d'authentification sélectionnée est **OAuth 2.0** .

Description des paramètres des onglets :

- **Intégration du calendrier Exchange**

Paramètres	Description
Intégration du calendrier Exchange	L'intégration du calendrier permet la création automatique de rendez-vous Outlook sous Windows lorsque l'utilisateur est absent. Si les rendez-vous Outlook ne doivent pas être stockés dans le fichier PST local de l'utilisateur, mais sur le serveur Exchange, les données d'accès requises doivent être saisies ici.
Activer l'intégration du calendrier Exchange	Activez l'intégration du calendrier Exchange
Méthode d'authentification	Méthode d'authentification à utiliser pour accéder au serveur Exchange distant. Vous pouvez choisir entre **Basic**, **OAuth 2.0 EWS** et **OAuth 2.0 Graph**.
Serveur	Des informations sur l'utilisation des différents serveurs Microsoft Exchange sont disponibles dans le wiki des experts Unify à l'adresse suivante : `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server` .
Nom d'utilisateur	Nom d'utilisateur pour accéder au serveur Exchange distant.
Mot de passe	Mot de passe pour accéder au serveur Exchange distant. Visible uniquement si la méthode d'authentification sélectionnée est **Basique** .
ID du locataire , **ID de l'application** , **Secret client** , **Étendue**	**ID du locataire** , **ID de l'application** et **secret client** correspondant à l'application enregistrée dans Azure AD pour l'intégration du calendrier Exchange. Vous pouvez les obtenir auprès de votre administrateur Azure AD. **Portée** requise par l'application (facultatif). Visible uniquement si la méthode d'authentification sélectionnée est **OAuth 2.0** .

27.4.4.8 Suite de communications unifiées OpenScape Business > Centre de contact

Description des paramètres des onglets :

- **Calendrier**
- **File d'attente**
- **Niveau de service**
- **Priorités des appelants VIP**
- **Liste d'appels VIP**
- **Agents privilégiés**
- **Pauses du centre de contact**
- **Résumé simple**
- **Résumé multiple**
- **Liaisons de file d'attente**

Calendrier

Un planning est utilisé pour définir comment les appels entrants doivent être traités certains jours et à des heures précises. Pour chaque file d'attente, un calendrier peut être défini avec des règles (vecteurs de contrôle d'appel ou CCV) pour déterminer comment les appels entrants doivent être traités à des dates et à des heures spécifiques. Un planning, à son tour, doit avoir au moins une règle (appelée vecteur de contrôle d'appel ou CCV) qui lui est attribuée. Les règles déterminent comment les appels entrants destinés à une file d'attente doivent être traités pendant la période à laquelle s'applique le

planning. Ces règles s'appliquent uniquement aux appels et non aux fax et aux courriels.

Pour plus d'informations sur la configuration des planifications, consultez la procédure de configuration.

Paramètres	Description
Calendrier	Nom du programme
File d'attente	Nom de la file d'attente à laquelle la planification est affectée.
Groupe de chasse	Identifiant du groupe de recherche du groupe UCD, qui a été configuré lors de la configuration de base du centre de contact.
Calendrier	
Nom du programme	Nom du programme
CCV par défaut	Affiche la règle par défaut de la planification, qui s'applique à une file d'attente 24 heures sur 24 et 365 jours par an lorsqu'elle est attribuée. Si des règles différentes doivent être appliquées à certains moments (pauses, week-ends, jours fériés, vacances, etc.), celles-ci peuvent être attribuées au planning en tant que règles d'exception (Exception CCV).
Files d'attente	
Nom de la file d'attente	Nom de la file d'attente à laquelle cette planification est affectée.
File d'attente active	Indique si la file d'attente est active ou inactive.
Exceptions	
CCV	Nom de la règle d'exception (exception CCV). Les règles d'exception définissent la manière dont doivent être traités les appels entrants reçus pendant certaines périodes exceptionnelles (pause, week-end, jour férié, vacances, etc.). Les horaires des jours fériés prévalent sur les autres horaires et règles de la file d'attente.
Description	Texte descriptif de la règle d'exception
Taper	Type de règle d'exception
Date de début	Date d'entrée en vigueur de la règle d'exception
Date de fin	Date de fin de la règle d'exception
Heure de début	Il est temps de commencer le contrôle des exceptions
Fin des temps	Il est temps d'en finir avec la règle de l'exception.
Se produit	La fréquence à laquelle la règle d'exception est programmée

File d'attente

Les files d'attente sont la base d'un centre de contact. Les appels, fax et courriels destinés à une file d'attente peuvent être traités, en fonction du niveau de compétence des agents, des priorités et des délais d'attente. Des annonces peuvent être diffusées aux personnes en attente d'appel.

Pour plus d'informations sur la configuration des files d'attente, consultez la procédure de configuration.

Paramètres	Description
File d'attente	Nom de la file d'attente
File d'attente active	Indique si la file d'attente est active ou inactive.
Groupe de chasse	Identifiant du groupe de recherche du groupe UCD, qui a été configuré lors de la configuration de base du centre de contact.
Paramètres généraux	
Nom de la file d'attente	Nom de la file d'attente
File d'attente active	Définition de l'état de la file d'attente
File d'attente active : Inactive	La file d'attente n'est pas active.
File d'attente active : Active	La file d'attente est active.
Groupe de chasse	Identifiant du groupe de recherche du groupe UCD, qui a été configuré lors de la configuration de base du centre de contact.
Commutateur téléphonique	Affiche l'entrée CSP
Calendrier	Affiche l'horaire assigné
Nombre d'alarmes en file d'attente	numéro de seuil d'alarme Si le nombre d'appels en attente dans la file d'attente dépasse le nombre spécifié ici, le symbole de la file d'attente pour l'agent passe du vert à l'orange. Valeur par défaut : 0 appels
Heure d'alarme de la file d'attente	délai de seuil d'alarme en secondes Si le temps d'attente pour un appel en file d'attente spécifié ici dépasse le temps indiqué ici, l'élément correspondant dans la liste des appels du centre de contact pour les agents passe au rouge. Valeur par défaut : 0 seconde
Délai d'attente pour l'appel manqué	Délai d'attente de l'appel manqué expiré en secondes Si un appel reste sans réponse après le délai indiqué ici, il est transféré au prochain agent disponible. Valeur par défaut : 10 secondes
Seuil d'appel abandonné	Valeur seuil pour les appels abandonnés en secondes L'heure spécifiée ici détermine si un appel abandonné est inclus ou non dans les statistiques. Les appels abandonnés après l'expiration du délai imparti sont inclus dans les statistiques. Valeur par défaut : 0 seconde

Paramètres	Description
Affichage contextuel activé	Lorsque cette option est activée, une fenêtre contextuelle permettant d'afficher et de saisir les données client apparaît dans myAgent pour les appels entrants. Des fenêtres contextuelles sont nécessaires pour accepter et exécuter les rappels, ainsi que pour recevoir les fax et les courriels. Valeur par défaut : Désactivé **Remarque :** L'option de notifications via **myAgent** > **Configuration** > **Notifications** > **L'application Pop up sur les appels entrants** est remplacée par l'activation du screen pop via **WBM** > **Mode Expert** > **OpenScape Business UC Suite** > **Centre de Contact** > **File d'attente** > **Paramètres généraux** > **Pop up d'écran activé**.
Mode de synthèse	Définition du mode de récapitulation
Mode de récapitulation : pas de récapitulation	Aucune raison de clôture ne peut être définie pour la file d'attente.
Mode de récapitulation : Récapitulation simple	Une ou plusieurs raisons de clôture peuvent être définies pour la file d'attente.
Mode de récapitulation : récapitulation multiple	Une ou plusieurs raisons de clôture peuvent être définies pour la file d'attente, puis classées en groupes et sous-groupes.
Délai d'attente de Screenpop	Délai d'expiration de l'écran contextuel en secondes Si la valeur est définie sur 0, il n'y aura pas de délai d'expiration pour l'affichage de l'écran. Si le champ est laissé vide, la valeur précédemment attribuée est utilisée. Valeur par défaut : 20 secondes
Priorités	Si un agent est affecté à plusieurs files d'attente, la priorité de la file d'attente peut être utilisée pour définir si les appels destinés à une file d'attente de priorité plus élevée doivent être transmis à cet agent en priorité sur les appels destinés aux autres files d'attente.
Mode de profondeur de file d'attente	Définition du mode de profondeur de file d'attente
Mode de profondeur de la file : Statique	Si le mode de profondeur de file d'attente est défini sur Statique, WLS et la taille de la profondeur de file d'attente peuvent être configurés.
Mode de profondeur de la file : Néant	Si la profondeur de la file d'attente est définie sur « Aucune », le paramètre WLS peut être configuré et affecte également la configuration UCD, mais le paramètre « Taille de la profondeur de la file d'attente » ne peut pas être défini.
Pilotes de file d'attente	
Pilotes de fax entrants	Numéros de téléphone (pilotes) pour les fax entrants Les fax envoyés à ces numéros de téléphone seront alors ajoutés à la file d'attente et traités comme des appels entrants.

Paramètres	Description
Service de messagerie entrante	Adresses électroniques pour les courriels entrants Les courriels envoyés à ces adresses sont mis en file d'attente et traités comme des appels entrants.
Ajouter	Ajouter un nouveau service de messagerie entrante
Modifier	Modifier un service de messagerie entrant sélectionné
Retirer	Supprimer le service de messagerie entrant sélectionné
Méthode d'authentification	Méthode d'authentification à utiliser pour accéder au service de messagerie entrante Vous pouvez choisir entre **Basic**, **OAuth 2.0 EWS** et **OAuth 2.0 Graph**.
Serveur	Nom DNS ou adresse IP du service de messagerie entrant
Port	Numéro de port du service de messagerie entrante
Nom d'utilisateur	Nom d'utilisateur pour accéder au service de messagerie entrante
Mot de passe	Mot de passe pour accéder au service de messagerie entrante Modifiable uniquement si la méthode d'authentification sélectionnée est de **Base**.
Utilise des connexions SSL	Activez ou désactivez l'utilisation des connexions SSL en fonction de la configuration du service de messagerie entrante.
ID du locataire , **ID de l'application** , **Secret client** , **Étendue**	**ID du locataire**, **ID de l'application** et **Secret du client** correspondant à l'application qui a été enregistrée dans Azure AD pour les files d'attente d'e-mails. Vous pouvez les obtenir auprès de votre administrateur Azure AD. **Portée** requise par l'application (facultatif). Valeur par défaut : https://outlook.office365.com/.default Visible uniquement si la méthode d'authentification sélectionnée est **OAuth 2.0** .
Divers	
Adresse e-mail de retour	Adresse électronique de l'expéditeur pour les courriels envoyés L'adresse électronique indiquée ici est affichée au destinataire lorsqu'un courriel est envoyé par un agent.
Routage intelligent des appels	Lorsque cette option est activée, les appels entrants sont automatiquement transférés à l'agent avec lequel l'appelant était en contact en dernier lieu. Préalablement, aucun agent préféré ne doit avoir été défini pour l'appelant. Valeur par défaut : Désactivé

Niveau de service

Le niveau de service peut être utilisé pour évaluer le taux de réponse de la file d'attente. Ceci est réalisé en comparant le temps d'attente des appelants dans la file d'attente avec des valeurs cibles, qui peuvent être spécifiées individuellement pour chaque file d'attente ici.

Pour chaque appel à une file d'attente appropriée, le niveau de service est déterminé après l'appel et enregistré dans la base de données. Le niveau de service peut être évalué par les agents ayant le niveau d'autorisation d'un superviseur ou d'un administrateur à l'aide de l'application myAgent.

Pour plus d'informations sur la définition des valeurs cibles du niveau de service, consultez la procédure de configuration.

Paramètres	Description
File d'attente	Nom de la file d'attente
File d'attente active	Indique si la file d'attente est active ou inactive.
Groupe de chasse	Identifiant du groupe de recherche du groupe UCD, qui a été configuré lors de la configuration de base du centre de contact.
Niveau de service	L'axe horizontal indique le temps d'attente dans la file d'attente par intervalles de 10 secondes, et l'axe vertical indique la valeur cible du niveau de service sous forme de pourcentage. Les points rouges indiquent les valeurs cibles pour la qualité de la commutation dans la file d'attente. Des évaluations de la qualité peuvent ensuite être effectuées en comparant ces valeurs cibles aux temps d'attente réels des appelants dans la file d'attente.

Priorités des appelants VIP

La priorité des appelants VIP peut être définie individuellement pour chaque file d'attente afin de spécifier si les appelants figurant sur la liste d'appels VIP doivent bénéficier d'un traitement préférentiel.

Les valeurs de priorité des appelants VIP peuvent être définies librement, en fonction du temps d'attente des appelants dans une file d'attente. Cela détermine le niveau de préférence accordé aux appelants VIP par rapport aux appelants normaux.

Lorsqu'un client VIP active le rappel d'un agent (en enregistrant un message vocal avec une demande de rappel), c'est le rappel de l'agent qui est conservé dans la file d'attente à la place de celui du client VIP. La priorité accordée aux appelants VIP ne s'applique pas ici.

Pour plus d'informations sur la définition de la priorité des appelants VIP, consultez la procédure de configuration.

Paramètres	Description
File d'attente	Nom de la file d'attente
File d'attente active	Indique si la file d'attente est active ou inactive.
Groupe de chasse	Identifiant du groupe de recherche du groupe UCD, qui a été configuré lors de la configuration de base du centre de contact.
Priorité d'appel VIP	L'axe horizontal indique le temps d'attente dans la file d'attente par intervalles de 30 secondes, et l'axe vertical indique la priorité des appelants normaux qui ne sont pas inscrits dans le répertoire de la liste d'appels VIP. Les points rouges indiquent la priorité des appelants normaux par rapport aux appelants VIP.

Liste d'appels VIP

Les appelants déjà inscrits dans le système de communication (annuaire externe) peuvent être ajoutés à la liste d'appels VIP. De plus, il est possible de saisir des modèles de numéros d'appel. Un modèle de numéro d'appel se compose d'une séquence spécifique de chiffres et d'un caractère générique (espace réservé). Il peut ainsi être utilisé pour transférer tous les employés d'une entreprise sur la liste d'appel VIP, par exemple.

Pour plus d'informations sur la configuration de la liste d'appels VIP, consultez la procédure de configuration.

Paramètres	Description
File d'attente	Nom de la file d'attente
File d'attente active	Indique si la file d'attente est active ou inactive.
Groupe de chasse	Identifiant du groupe de recherche du groupe UCD, qui a été configuré lors de la configuration de base du centre de contact.
Liste d'appels VIP	Affiche les appelants et les modèles de numéros d'appel inclus dans la liste d'appels VIP. Vous pouvez ajouter, modifier ou supprimer des appelants et des modèles de numéros d'appel de la liste d'appels VIP. Plus la barre de défilement est déplacée vers la droite pour un appelant ou un modèle de numéro d'appel, plus sa priorité est élevée par rapport aux autres appelants ou modèles de numéros d'appel contenus dans la liste d'appels VIP.

Agents privilégiés

Chaque appelant peut se voir attribuer un ou plusieurs agents privilégiés au sein d'une file d'attente. Dans de tels cas, le système de communication tente d'abord de transférer l'appelant et ses demandes de rappel vers un agent de son choix. Si plusieurs agents préférés ont été spécifiés, une priorité (séquence) peut être définie pour déterminer l'ordre dans lequel ces agents sont connectés.

Si aucun agent privilégié n'est disponible, l'appel est transféré à tout agent disponible.

Pour plus de détails sur la définition des agents préférés, consultez la procédure de configuration.

Paramètres	Description
File d'attente	Nom de la file d'attente
File d'attente active	Indique si la file d'attente est active ou inactive.
Groupe de chasse	Identifiant du groupe de recherche du groupe UCD, qui a été configuré lors de la configuration de base du centre de contact.

Paramètres	Description
Agents privilégiés	Affiche les agents préférés pour chaque appelant indiqué dans la liste des clients. Vous pouvez ajouter, supprimer et modifier la priorité d'un agent. Si plusieurs agents préférés ont été définis pour un appelant, la position dans la liste indique la priorité par rapport aux autres agents préférés. Plus un agent est haut placé dans la liste, plus sa priorité est élevée.
Afficher uniquement les clients ayant des relations avec un agent.	Lorsque cette option est activée, seuls les appelants pour lesquels au moins un agent préféré a été défini sont affichés dans la liste des clients. Valeur par défaut : Désactivé

Pauses du centre de contact

Afin de permettre à chaque agent de prendre une pause définie, des pauses de différentes durées peuvent être définies dans les centres de contact. Les pauses des centres de contact sont disponibles à l'échelle du système et peuvent être sélectionnées par un agent via myAgent selon les besoins.

Pour plus de détails sur la définition des interruptions du centre de contact, consultez la procédure de configuration.

Paramètres	Description
Ajouter	Ajouter une nouvelle interruption au centre de contact
Modifier	Modifier une pause du centre de contact sélectionnée
Retirer	Supprimer la coupure du centre de contact sélectionnée
Nom	Nom de la pause du centre de contact
Durée	Durée de la pause du centre de contact (en minutes)
Actif	Indique si la pause du centre de contact est active ou inactive.

Résumé simple

Une ou plusieurs raisons de regroupement peuvent être définies ici pour les files d'attente avec le mode de regroupement « Regroupement simple ».

Les motifs de clôture peuvent être utilisés pour attribuer les appels entrants à des catégories spécifiques (commandes, réclamations, service, etc.). L'attribution est effectuée par un agent après la fin de l'appel (pendant les heures de travail) en saisissant le motif de clôture approprié via myAgent.

Pour plus de détails sur la définition des raisons de clôture, consultez la procédure de configuration.

Paramètres	Description
Ajouter	Ajouter un nouveau résumé simple
Modifier	Modifier un résumé simple sélectionné
Retirer	Supprimer le wrapper simple sélectionné
File d'attente	Nom de la file d'attente pour laquelle un encapsulage simple a été configuré.

Paramètres	Description
Description	Texte descriptif en guise de conclusion.

Résumé multiple

Pour les files d'attente avec le mode de regroupement « Regroupement multiple », une ou plusieurs raisons de regroupement peuvent être définies ici, puis classées en groupes et sous-groupes.

Les motifs de clôture peuvent être utilisés pour attribuer les appels entrants à des catégories spécifiques (commandes, réclamations, service, etc.). L'attribution est effectuée par un agent après la fin de l'appel (pendant les heures de travail) en saisissant le motif de clôture approprié via myAgent.

Pour plus de détails sur la définition des raisons de clôture, consultez la procédure de configuration.

Paramètres	Description
File d'attente	Nom de la file d'attente configurée pour l'encapsulation multiple. Les groupes et sous-groupes déjà définis pour cette file d'attente sont affichés.
Description	Texte descriptif en guise de conclusion.

Liaisons de file d'attente

Les liaisons de files d'attente servent à affecter des agents à une ou plusieurs files d'attente.

Pour plus d'informations sur l'affectation des agents aux files d'attente, consultez la procédure de configuration.

Paramètres	Description
File d'attente	Nom de la file d'attente
File d'attente active	Indique si la file d'attente est active ou inactive.
Groupe de chasse	Identifiant du groupe de recherche du groupe UCD, qui a été configuré lors de la configuration de base du centre de contact.
Cession d'agent (contraignante)	
Extension	Affichage du numéro de poste de l'utilisateur
Nom	Affichage du nom de l'utilisateur.
Agent	Agent affecté à la file d'attente.
Taper	Type d'agent Les options suivantes sont possibles : • Agent principal : cet agent reçoit les appels quelle que soit la charge de la file d'attente. • Agent de débordement : cet agent ne reçoit les appels que lorsque la file d'attente est saturée.

Paramètres	Description
Niveau de compétence	Affiche le niveau de compétence en pourcentage Le niveau de compétence détermine la répartition des appels entre les agents en attente. Lors de la répartition des appels, la priorité est donnée aux agents les plus compétents. Dans les cas où tous les agents ont le même niveau de compétence, l'agent inactif depuis le plus longtemps reçoit l'appel.
Activer le rappel de l'agent	Lorsque cette option est activée, l'agent reçoit les demandes de rappel sous forme de messages vocaux.
Temps de travail	Temps de travail automatique en secondes
Dépassement de capacité après quelques secondes dans la file d'attente	Uniquement pour l'agent de débordement : durée du débordement en secondes Lorsque le délai de débordement est écoulé, l'appel est redirigé vers un agent de débordement.
Débordement après les appels en file d'attente	Uniquement pour l'agent de débordement : nombre d'appels Les appels qui dépassent ce nombre maximal sont redirigés vers un agent de débordement.

27.4.4.9 OpenScape Business UC Suite > Calendriers

Description des paramètres des onglets :

- **Modifier/Ajouter**

Paramètres	Description
Standard automatique	Configuration de la fonction Standard automatique de UC Suite (Company AutoAttendant)
Calendrier	Nom du calendrier
File d'attente	Nom de la file d'attente à laquelle le calendrier est affecté.
Groupement	Numéro de téléphone du groupe UCD qui a été défini lors de la configuration de base du centre d'appels.
Modifier / Ajouter / Supprimer	Modifier ou supprimer la règle sélectionnée, ou ajouter une nouvelle règle (ouvre l'éditeur de règles)
Nom du calendrier	Le calendrier peut être enregistré sous un nom librement choisi. Il est recommandé de donner un nom qui a un sens dans le contexte.
CCV par défaut	Un calendrier doit comporter au moins une règle (Call Control Vector CCV). Les règles définissent pour la période concernée la manière dont les appels entrants sont traités. Les règles s'appliquent uniquement aux appels et non aux fax et e-mails. Les règles sont créées à l'aide de l'éditeur de règles graphique (Editeur de CCV) en associant des objets CCV prédéfinis. Plusieurs modèles normalisés prédéfinis sont disponibles et peuvent être modifiés à loisir pour être adaptés à des besoins spéciaux.

Paramètres	Description
Files d'attente	Il est recommandé de n'activer qu'une file d'attente par calendrier (cocher une seule fois).
Nom de file d'attente	La file d'attente peut être enregistrée sous un nom librement choisi. Il est recommandé de donner un nom qui a un sens dans le contexte.
File d'attente active	La file d'attente peut être activée ou désactivée.
Calendrier	Sélection du calendrier correspondant
Pilote	Numéro de téléphone du port virtuel correspondant dans le système de communication.
Exceptions	Un calendrier avec une règle par défaut s'applique, après affectation à une file d'attente, 24 h sur 24 et 365 jours par an. Si à certains moments (pause, weekend, jours fériés, congés, etc.) d'autres règles s'appliquent, celles-ci peuvent être programmées dans le calendrier correspondant en tant que règles exceptionnelles (Exceptions-CCV). Il est ainsi possible de définir par exemple comment les appels entrants sont traités durant la période de congés. Les calendriers de congés sont prioritaires par rapport à d'autres calendriers et règles.
CCV	Sélection de la règle d'exception (exception CCV)
Description	Entrée libre d'une description pour le calendrier d'exceptions
Type	Dans un intervalle de temps de un ou plusieurs jours / Dans un intervalle de temps / de dates librement définissable / Plans de congés pour une plage de dates.
Date de début	Début de l'exception (date)
Date de fin	Fin de l'exception (Date)
Heure de début	Début de l'exception (heure)
Heure de fin	Fin de l'exception (Heure)
(Jour ouvré)	L'exception peut s'appliquer à un ou plusieurs jours de la semaine
Se produit	La fréquence à laquelle l'exception est programmée

27.4.4.10 OpenScape Business UC Suite > Chargement du fichier

Description des paramètres des onglets :

- **Gestionnaire de fichiers audio**

Paramètres	Description
Destination de téléchargement	Application pour laquelle la nouvelle annonce est utilisée
Destination de téléchargement : Standard automatique	Annonce pour le standard automatique

Paramètres	Description
Destination de téléchargement : Profils	Annonces pour tous les utilisateurs ou pour des utilisateurs individuels de UC Suite
Destination de téléchargement : Message d'accueil de la boîte vocale	Message d'accueil Boîte vocale pour tous les utilisateurs ou pour des utilisateurs individuels de UC Suite La durée maximale d'enregistrement du message d'accueil de la messagerie vocale est de 1 minute.
Destination de téléchargement : Mes. accueil Groupe MV	Message d'accueil pour une boîte vocale de groupe
pas de touche pour : téléchargeur	L'annonce est disponible pour téléchargement sous forme de fichier PCM, aux caractéristiques suivantes : 8 kHz, 16 bits, mono. La longueur du nom du fichier audio est de 30 caractères au maximum.
Enregistreur	L'annonce est enregistrée par le téléphone d'un poste
Fichier son	
Télécharger	Annonces téléchargées.
Effacer	Effacer les annonces téléchargées.
Renommer	Renommer les annonces téléchargées.
Enregistreur	
Nom de fichier	Indication du nom de fichier de l'annonce à enregistrer.
Poste	Sélection du téléphone à l'aide duquel l'annonce sera enregistrée.
Appeler	Appelle le téléphone devant servir à enregistrer l'annonce.
Lire	Diffuse l'annonce enregistrée.
Enregistrer	Démarre l'enregistrement de l'annonce.

Description des paramètres des onglets :

- **Chargement de la page de garde du fax centralisé**

Paramètres	Description
Chargement de la page de garde du fax centralisé	
Fichier Ocp	Page de garde Fax disponible comme fichier .ocp
Nom	Nom de la page de garde Fax centrale
Description	Description pour la page de garde Fax centrale
Charger	Chargement du fichier de la page de garde Fax centrale
Modifier	Modification du fichier de la page de garde Fax centrale sélectionnée
Supprimer	Suppression du fichier de la page de garde Fax centrale sélectionnée
Paramétrer comme valeur par défaut	Définition du fichier de la page de garde Fax centrale sélectionnée comme la valeur défaut

Paramètres	Description
Nom de fichier	Indication du nom de fichier de l'annonce à charger.
Date de création	Date de création du fichier de la page de garde Fax centrale

27.4.4.11 OpenScape Business UC Suite > Conférences

Description des paramètres des onglets :

- **Conférences**

Paramètres	Description
Nom	Nom de la conférence (attribué par l'utilisateur)
Propriétaire	Nom de l'utilisateur qui a lancé la conférence
Prochain planifié	Prochaine heure de début planifiée
Actif	
Nombre de membres	Nombre des participants à la conférence, y compris le directeur de conférence
Afficher	Participants à la conférence sélectionnée
Effacer	Supprimer les conférences sélectionnées

27.4.4.12 Liste des sites > OpenScape Business UC Suite

Description des paramètres des onglets :

- **Liste des sites**

Paramètres	Description
Nom du site	Sites du système de communication en réseau (voir Paramètres de base > Propriétés de la passerelle)
Adresse du site	Adresse IP du système de communication
Site Port	Port du serveur
Liaisons IP du site	Liaisons IP du site, si disponibles
Statut en ligne	État de la connexion du système de communication sur le site

27.4.4.13 Serveur > OpenScape Business UC Suite

Description des paramètres des onglets :

- **Paramètres généraux**
- **Enregistrement en direct**
- **Enregistrement**

- **Notifications**
- **Entretien**
- **Messagerie vocale**
- **Cartographie des cartes de contact**

Paramètres	Description
Heures de bureau	
Heure de début	Début des heures de bureau quotidiennes (heures ouvrables) Paramétrage du statut de présence des clients UC Valeur par défaut : 07:00 **Remarque :** La valeur saisie doit être au format 24 heures (HH:MM).
Fin des temps	Fin des heures de bureau quotidiennes (heures ouvrables) Paramétrage du statut de présence des clients UC Valeur par défaut : 19:00 **Remarque :** La valeur saisie doit être au format 24 heures (HH:MM).
Longueur du mot de passe	
Longueurs	Longueur du mot de passe pour les clients UC. La valeur minimale est de 6. ***La modification de la longueur du mot de passe provoque la réinitialisation des mots de passe de tous les utilisateurs.*** Valeur par défaut : 6
Numéro d'appel de la position d'interception	
Objectif	Numéro d'appel de la position d'interception ***Il faut*** inscrire le numéro du poste d’interception configuré dans le système de communication.
Messagerie instantanée	
Désactiver la messagerie instantanée	Lorsque ce paramètre est activé, l'envoi de messages instantanés est impossible. Valeur par défaut : Désactivé
Extensions analogiques	
Mode utilisateur analogique	Définit la manière dont les stations analogiques sont affichées dans le répertoire interne Valeur par défaut : Afficher tout
Mode utilisateur analogique : Tout afficher	Toutes les stations analogiques sont affichées dans le répertoire interne

Paramètres	Description
Mode utilisateur analogique : Afficher uniquement le nom	Seules les stations analogiques ayant un nom sont affichées dans le répertoire interne.
Mode utilisateur analogique : non affiché	Aucune station analogique n'est affichée dans le répertoire interne.
Extension	
Longueur intérieure maximale	Nombre maximal de chiffres pour les numéros d'appel internes Valeur par défaut : Longueur maximale de toutes les extensions internes.
Longueur externe minimale	Nombre minimum de chiffres pour les numéros d'appel externes Valeur par défaut : Longueur d'extension interne maximale +1. Si sa valeur est inférieure à 4, elle est fixée à 4.
Transfert	
Répondeur automatique normal SST	Lorsque ce paramètre est activé, l'appel sera transféré, que le destinataire soit libre, occupé ou indisponible. Valeur par défaut : Activé
Journal	
Autoriser la suppression des écritures de journal	Ce paramètre autorise ou interdit à un utilisateur de supprimer ou non une entrée de journal.
Masquer les appels « Ouverts » dans le journal	Masque le bouton **Ouvrir** sous Journal.
Format fax	
Utiliser le format PDF comme format de fax	Si l'option est activée, le fax reçu peut être enregistré au format PDF ; sinon, il est enregistré au format TIFF.
Serveur d'annuaire	
Fournisseur externe lent	Cette option améliore le temps de réponse du clic droit sur un e-mail. De plus, lorsqu'elle est activée, les recherches de contacts sont exécutées uniquement dans le répertoire parent Exchange et non dans les sous-répertoires.
Durée de la vérification	Un chiffre de 4 à 8 doit être saisi pour définir la longueur des numéros CLI pour la recherche dans LDAP dans myPortal pour ordinateur et myPortal pour Outlook. Le nombre le plus élevé (8) peut être configuré pour une recherche plus précise et des performances système améliorées. Valeur par défaut : 4
Numérotation par nom, recherche par extension locale uniquement	Lorsque cette option est activée, la fonction « composer par nom » est limitée au nœud actif (fonction locale). Lorsque cette option est décochée, l'ancienne fonction reste disponible ; elle prend en compte tous les utilisateurs du réseau, mais ne diffuse l'annonce qu'après la sélection d'un utilisateur local.

Paramètres	Description
Le cache de recherche dans l'annuaire expire dans	Définissez le nombre de minutes ou une plage de minutes pendant lesquelles la mémoire cache est utilisée lors de la recherche de contacts. La durée que vous pouvez régler est comprise entre 1 et 60 minutes. Lorsque la valeur est « 0 », cette fonction est désactivée.
Recherche par numéro de téléphone	Lorsque cette option est activée, vous pouvez effectuer des recherches dans les annuaires par numéro de téléphone.
TLS	
Utilisation de TLS pour les connexions client	Pour des raisons liées au réseau, il pourrait être nécessaire de désactiver la connexion client-serveur sécurisée. La modification de ce paramètre nécessite un redémarrage de l'application UC. Cela ne devrait être fait que dans des cas très spécifiques !
Présence	
Masquer son statut de maladie	Lorsque ce drapeau est activé, le statut de présence « malade » n'est plus disponible. Valeur par défaut : Désactivé
Nom d'utilisateur	
Désactiver la modification des noms	Lorsque cette option est activée, les utilisateurs ne peuvent plus modifier leur prénom et leur nom configurés. Valeur par défaut : Désactivé
Tableau mural	
Désactiver le tableau de bord	Lorsque cette option est activée, le tableau de bord mural n'est pas disponible.
Afficher les noms des agents dans la liaison de file d'attente myAgent	Lorsque cette option est activée, un nom s'affiche également, que l'utilisateur peut configurer, en plus du numéro de poste de l'agent. Le message « Hotdesk » s'affichera lorsqu'un utilisateur utilisera une extension autre que la sienne. Valeur par défaut : Désactivé.
Enregistrement en direct	
Enregistrement en direct	Lorsque cette option est activée, l'enregistrement des appels est possible. Valeur par défaut : Activé
Message de lecture avant l'enregistrement	Lorsque ce paramètre est activé, une annonce est diffusée avant le début de l'enregistrement. Valeur par défaut : Désactivé
Jouez un son de pip pendant l'enregistrement	Pour OpenScape Business S, lorsque cette option est activée, un signal sonore d'avertissement est émis pendant l'enregistrement. Valeur par défaut : Activé
Disponibilité des enregistrements en direct de la conférence	Lorsque cette option est activée, l'enregistrement des conférences est possible. Valeur par défaut : Désactivé

Paramètres	Description
Journalisation système	
Messages de suivi du journal (détaillés)	Lorsque cette option est activée, les messages de traçage sont enregistrés quotidiennement dans un fichier journal. Valeur par défaut : Désactivé
Journaux clients	
Chemin du journal client	Chemin de stockage des fichiers journaux du client (fichiers journaux de la suite UC)
Activer le téléchargement des journaux	Lorsque cette option est activée, les journaux du client sont stockés sur le disque dur du système de communication OpenScape Business S. Valeur par défaut : Activé
Activer la journalisation du client	L'activation de cette option permet l'enregistrement des journaux clients. Valeur par défaut : Activé
Notifications par e-mail	
Activer les notifications par e-mail des erreurs système	Lorsque cette option est activée, des notifications par e-mail seront envoyées aux destinataires saisis afin de les avertir à l'avance, par exemple, des niveaux critiques d'utilisation du disque dur ou des erreurs éventuelles. Valeur par défaut : Activé
Activer l'e-mail d'invitation myPortal	Lorsque cette option est activée, les utilisateurs de UC Suite recevront un e-mail d'invitation pour installer ou mettre à jour le client myPortal. Ce courriel est normalement envoyé à tous les utilisateurs de UC Suite disposant d'une adresse courriel valide dans l'annuaire des utilisateurs lors d'une nouvelle installation, lorsqu'une adresse courriel est ajoutée ou modifiée pour un utilisateur de UC Suite dans l'annuaire des utilisateurs ou après une mise à jour du logiciel OpenScape Business et la disponibilité d'une nouvelle version du client. Valeur par défaut : Activé
Bénéficiaires	Adresses électroniques des personnes auxquelles les notifications par courriel doivent être envoyées.
Conditions	
Envoyer des messages critiques	Lorsque cette option est activée, des notifications par e-mail sont envoyées pour les messages critiques (par exemple, les erreurs système). Valeur par défaut : Activé
Envoyer des notifications de plantage	Lorsque cette option est activée, des notifications par e-mail sont envoyées en cas de panne système. Valeur par défaut : Activé
Lors du signalement d'erreurs, veuillez envoyer les dernières lignes du fichier journal.	Définit le nombre de lignes d'un fichier journal à envoyer par e-mail. Valeur par défaut : 100

Paramètres	Description
Entretien	
Début de la maintenance du système à	Définit à quel moment les données suivantes sont supprimées quotidiennement lorsque les périodes de conservation individuelles ont expiré : • Messages • Informations sur les appels dans le journal d'appels (historique des appels) • Appels enregistrés avec myAgent (centre de contact) • Fax et courriels reçus et envoyés pour le centre de contact • Fichiers journaux Valeur par défaut : 2,00 heures
Message	
Conservez les messages de la boîte de réception pour	Durée de conservation en jours des messages vocaux dans la boîte de réception Valeur par défaut : 60
Continuez à jouer / lire les messages pour	Durée de conservation en jours des messages vocaux lus/écoutés Valeur par défaut : 30
Conserver les messages enregistrés pour	Durée de conservation en jours des messages vocaux enregistrés Valeur par défaut : 365
Conserver les messages supprimés pour	Durée de conservation en jours des messages vocaux supprimés Valeur par défaut : 30
Fax	
Conservez les fax de la boîte de réception pour	Durée de conservation en jours des fax dans la boîte de réception Valeur par défaut : 30
Lisez les fax pour	Durée de conservation en jours des fax lus Valeur par défaut : 30
Conservez les fax supprimés pour	Durée de conservation en jours des fax supprimés Valeur par défaut : 30
Continuez à envoyer des fax pour	Durée de conservation en jours des fax envoyés Valeur par défaut : 30
Maintenance des informations sur les appels	
Conserver l'historique des appels pour	Durée de conservation en jours des appels dans la revue Valeur par défaut : 30

Paramètres	Description
Conversation étroite après	Durée de conservation en jours des conversations à appel à contributions ouvertes dans la revue. Tous les appels sans réponse provenant ou destinés au même contact pendant cette période seront ajoutés à l'onglet « Appels en cours », liés à la même conversation. À l'issue de cette période, tous les appels d'une conversation sont automatiquement marqués comme terminés et supprimés de l'onglet des appels ouverts. Valeur par défaut : 3 Valeur maximale : 30
Centre de contact	Durée de conservation (en jours) des appels enregistrés avec myAgent et des fax et courriels reçus et envoyés pour le centre de contact Valeur par défaut : 30
Conservez l'enregistrement en direct des appels CC, les rappels, les e-mails et les fax pour	Durée de conservation en jours de toutes les données de communication associées aux appels, telles que les messages de rappel, les appels enregistrés en direct, les appels par fax et les courriels. Valeur par défaut : 30
Maintenance des fichiers journaux	
Conserver les informations de journalisation pour	Durée de conservation des fichiers journaux (en jours) Valeur par défaut : 10
Messagerie instantanée	
Conservez les messages instantanés pour	Durée de conservation des messages instantanés (en jours). Valeur par défaut : 30
Rapports	
Réinitialiser le mot de passe	Réinitialise le mot de passe administrateur de myReports au mot de passe par défaut.
Réinitialiser tous les mots de passe utilisateur	
Réinitialiser tous les mots de passe utilisateur	Réinitialise les mots de passe de tous les utilisateurs, accepte les mots de passe jusqu'à 6 caractères. **Remarque :** Dans ce cas, le mot de passe par défaut est fixé à 6 caractères (123456).
Messagerie vocale	
Langue de la messagerie vocale	Langue par défaut de la messagerie vocale pour les messages du menu et les annonces système internes
Ordre de lecture des messages vocaux	Définit l'ordre dans lequel les messages vocaux sont lus Valeur par défaut : Du plus récent au plus ancien
Ordre de lecture des messages vocaux : le plus récent en premier	Le message vocal le plus récent est affiché en premier.

Paramètres	Description
Ordre de lecture des messages vocaux : le plus ancien en premier	Le message vocal le plus ancien est affiché en premier.
Durée d'enregistrement des messages vocaux	Définit la durée maximale d'enregistrement d'un message vocal en secondes Valeur par défaut : 900
Mode messagerie vocale	Définit les fonctionnalités de la boîte vocale Valeur par défaut : Plein
Mode Messagerie vocale : Complet	Fonctionnalités complètes de la messagerie vocale
Mode Messagerie vocale : menu court	Une fois l'annonce, qu'elle soit basée sur le statut ou personnelle, faite, une mise en relation avec l'opérateur est proposée.
Mode Messagerie vocale : pas de menu Messagerie vocale	Une fois le message d'accueil diffusé, l'appelant est directement redirigé vers l'enregistrement vocal.
Autoriser uniquement le rappel de la messagerie vocale vers un numéro connu.	Lorsque cette option est activée, les appelants dont le numéro n'est pas enregistré dans le client UC ne pourront pas accéder à la messagerie vocale. Valeur par défaut : Activé
Ignorer l'invite « Veuillez laisser un message après le signal sonore ».	Lorsque cette option est activée, l'invite « veuillez laisser un message après le signal sonore » sera ignorée. Valeur par défaut : Désactivé
Cartographie des cartes de contact	
Microsoft : Disponible (vert)	Le statut UC de présence de cette ligne est attribué au statut Outlook Disponible (Vert).
Microsoft : Hors travail (jaune)	Le statut UC de présence de cette ligne est attribué au statut Outlook « Hors du travail (jaune) ».
Microsoft : Occupé (rouge)	Le statut UC de présence de cette ligne est attribué au statut Outlook Occupé (Rouge).
Microsoft : Hors service (gris)	Le statut UC de présence de cette ligne est attribué au statut Outlook Hors service (gris).

27.4.4.14 OpenScape Business, UC Suite > Profils

Description des paramètres des onglets :

- **Ajouter / Modifier**

Paramètres	Description
Profils	Les profils utilisateur enregistrent les paramètres des utilisateurs de UC Suite. Il est possible d'affecter plusieurs utilisateurs (membres) à un profil d'utilisateur. Tous les membres de ce profil ont (dans un premier temps) les mêmes paramètres. Il est possible de créer plusieurs profils, ce qui permet une préconfiguration différente pour les différents types de groupes d'utilisateurs.
Nom	Nom du profil (entrée libre)
Données personnelles	
Mes données personnelles	Données personnelles sélectionnées pour les utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Mes Préférences	
Apparence	Habillage et langue du UC Client des utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Notification	Notifications pour les utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Connexion Outlook	Intégration calendrier pour les utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Touches de raccourci	Activation et configuration des combinaisons de touches pour accéder aux différentes fonctions couramment utilisées via le clavier. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Divers	Retour automatique à l'état Présence "Bureau", méthode de transfert et durée de conservation du journal des appels pour les utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Règles d'appel	
Destinations de renvoi	Destinations de renvoi pour les appels entrants en fonction de l'état Présence pour les utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Communications	
Paramètres de messagerie vocale	Enregistrement des messages vocaux en fonction de l'état Présence pour les utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Notification MV	Communication pour les nouveaux messages vocaux à destination des utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Notification fax	Communication pour les nouveaux messages fax à destination des utilisateurs affectés. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Notifications d'appel manqués	Service de notification pour les appels manqués.

Paramètres	Description
Profils MV	
Profils MV	Standard automatique personnel pour les utilisateurs affectés. Les utilisateurs concernés doivent enregistrer une annonce à sélectionner. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Sensibilité	
Sécurité et accès	Autoriser l'écoute des messages Voix avec myAttendant ainsi que l'interrogation de la boîte vocale à partir du propre téléphone, sans mot de passe. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Visibilité de l'état de présence	Abonnés internes qui ont l'autorisation de voir l'état Présence. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
État de présence de la boîte vocale	Appelants internes ou externes qui doivent être informés de l'état Présence par des annonces automatiques de la boîte vocale. L'icône du cadenas indique si l'utilisateur est autorisé à modifier lui-même ces paramètres.
Favoris	
Favoris	Groupes Favoris avec une liste de contacts pouvant être attribués à l'utilisateur.

Description des paramètres des onglets :

- **Affecter les utilisateurs**

Paramètres	Description
Utilisateurs affectés	Utilisateurs pour lesquels le profil doit s'appliquer
Utilisateurs disponibles	Utilisateurs pour lesquels le profil peut s'appliquer

Description des paramètres des onglets :

- **Supprimer**

Paramètres	Description
Nom	Nom du profil (entrée libre)
Utilisateurs	Utilisateurs pour lesquels le profil doit s'appliquer

27.4.4.15 OpenScape Business UC Suite > Lignes d'en-tête de fax

Description des paramètres des onglets :

- **Modifier**
- **Ajouter**
- **Supprimer**

Paramètres	Description
Nom du modèle / Nom	Nom de la ligne d'en-tête (doit être univoque).
Texte	Il est possible d'ajouter un joker pour la date/l'heure, le nom de la société, le nom de l'utilisateur, le n° de Tél. de la société, le numéro de page ainsi que le nombre de pages.

27.4.5 Open Directory Service

Open Directory Service regroupe les fonctions pour la configuration de Directory Service.

27.4.5.1 Open Directory Service > Configuration de base

Paramètres	Description
Activer/Désactiver Open Directory Service	Valeur par défaut : désactivé
Paramètres de connexion du serveur LDAP	Informations d'identification pour la connexion du serveur de base de données externe. Open Directory Service doit être autorisé à accéder à la base de données externe, le cas échéant il faut ajouter un propre utilisateur dans le serveur.

27.4.5.2 Open Directory Service > Sources de données > Utilisateurs OpenScape Business

Description des paramètres des onglets :

- **Aperçu des sources de données configurées**

Paramètres	Description
Utilisateurs OpenScape Business	Répertoire interne de UC Suite. Le répertoire est attribué de manière permanente à l'Open Directory Service et ne peut être ni supprimé ni modifié.
Annuaire externe UC Suite	Source de données externe pour les systèmes UC Suite. Le répertoire est attribué de manière permanente à l'Open Directory Service et ne peut être ni supprimé ni modifié.
Répertoire global	Source de données de l'annuaire global pour les systèmes non UC Suite. Le répertoire est attribué de manière permanente à l'Open Directory Service et ne peut être ni supprimé ni modifié.
Numéros abrégés	Numéros d'appel abrégé centraux. Le répertoire est attribué de manière permanente à l'Open Directory Service et ne peut être ni supprimé ni modifié.
Ajouter/Modifier/Supprimer	Sources de données externes pour les informations de contact provenant de bases de données avec accès en lecture via ODBC.

Description des paramètres des onglets ::

- **Modifier la source de données**

Paramètres	Description
Nouvelle source de données	Les paramètres des sources de données ajoutées peuvent être modifiés ici.

27.4.5.3 Open Directory Service > Sources de données > LXV3

Paramètres	Description
Numéros abrégés	Numéros abrégés centralisés. Le répertoire est affecté de manière fixe à Open Directory Service fixe et ne peut pas être supprimé ou modifié.

27.4.5.4 Open Directory Service > Sources de données > LXV3

Paramètres	Description
Vue d'ensemble des sources de données configurées	Un mappage de sortie des données LDAP définit les champs du schéma de données d'Open Directory Service qui doivent être fournis via LDAP, par ex. à certains clients LDAP ou pour divers groupes de participants, qui ne doivent pas voir tous les détails, mais uniquement un sous-ensemble défini. L'affectation de sortie LDAP web est disponible par défaut et ne peut être ni effacée ni modifiée. Tous les champs du schéma de données d'Open Directory Service de la sortie LDAP y sont affectés de manière fixe. Vous pouvez configurer d'autres mappages de sortie de données LDAP.
Ajouter	Ajouter d'autres affectations de sortie. À l'aide du paramètre dc de la connexion LDAP, les clients LDAP peuvent accéder à un mappage de sortie de données LDAP définie, par ex. : dc=web.

27.4.5.5 Open Directory Service > Maintenance

Description des paramètres des onglets :

- **Maintenance**

Paramètres	Description
Contrôler / redémarrer Open Directory Service	Indication d'état de Open Directory Service (gris = désactivé, rouge = configuration incorrecte ou source de données non disponible, vert = activé)
Redémarrage	Redémarrage de Open Directory Service

27.4.6 Application Launcher

Application Launcher regroupe les fonctions pour la configuration d'Application Launcher.

27.4.6.1 Application Launcher

Paramètres	Description
Chargement du fichier de configuration	Un profil avec les données de configuration d'Application Launcher permet de configurer de manière simple et rapide Application Launcher sur tous les PC client. Une fois que Application Launcher a été entièrement configuré pour le premier utilisateur, vous pouvez, en tant qu'administrateur, mettre à disposition le profil avec les données de configuration de Application Launcher dans le système de communication. Ensuite, tous les utilisateurs peuvent effectuer la configuration de Application Launcher en important ce profil.
Profil	Type de fichier .xml autorisé

27.5 Intergiciel

Les fonctions de configuration de l'intergiciel sont regroupées sous les rubriques **Intergiciel**.

27.5.1 Lecteur de communication d'interphone

Description des paramètres des onglets :

- **Paramètres du lecteur de communication d'interphone**
- **Statistiques du lecteur de communication d'interphone**

Paramètres	Description
Activation	
Le service sera démarré automatiquement	Activation ou désactivation du périphérique de lecture des communications d'interphone.
Statistiques du lecteur de communication d'interphone	L'état du périphérique de communication d'interphone est affiché ici. Les données sont automatiquement mises à jour toutes les 5 minutes. Cependant, la page peut également être actualisée manuellement.

27.5.2 CSTA Message Dispatcher (CMD)

Description des paramètres des onglets :

- **Paramètres - CSTA Message Dispatcher (CMD)**
- **Statistiques - CSTA Message Dispatcher (CMD)**

Paramètres	Description
Activation	
Le service sera lancé automatiquement	Activation ou désactivation de CSTA Message Dispatcher (CMD). Le CMD établit la connexion entre les clients OpenScape Business TAPI 120 et le système de communication ; il est nécessaire pour la fonctionnalité.
Enregistrement automatique	

Paramètres	Description
Enregistrement auto. du client actif	Activation ou Désactivation de la connexion automatique des clients. Connexion automatique signifie que de nouvelles entrées dans la liste du pare-feu CTI sont possibles. Cela provoque la configuration automatique du pare-feu CTI. Lorsque tous les clients autorisés se sont connectés, il est possible de décocher la case ; il est alors impossible d'effectuer de nouvelles entrées dans le pare-feu CTI. Un PC peut être autorisé à contrôler un poste défini. Les licences TAPI/CTI doivent être attribuées en plus.
Pare-feu CTI	
Effacer	Les entrées identifiées par une case cochée dans la colonne Effacer sont retirées de la liste des clients autorisés dès que l'on clique sur le bouton **Interception**. La connexion est refusée lorsque l'enregistrement automatique n'est pas activé.
ID d'application	Nom du PC à partir duquel il est possible de contrôler un poste. Grâce à l'utilisation du nom de PC, il est possible d'utiliser également DHCP pour les PC OpenScape Business TAPI 120.
Numéro d'appel	Numéro interne du poste qui peut être contrôlé.
Statistiques - CSTA Message Dispatcher (CMD)	Il est indiqué ici l'état de CMD. En exploitation, il est possible de contrôler quels sont les OpenScape Business TAPI 120 qui sont connectés à CMD de sorte qu'il peut être nécessaire d'attribuer des licences. Les données sont automatiquement actualisées toutes les 5 minutes. Il est également possible d'actualiser manuellement la page.

27.5.3 Fournisseur de services CSTA (CSP)

Description des paramètres des onglets :

- **Paramètres - Fournisseur de services CSTA (CSP)**
- **Statistiques - Fournisseur de services CSTA (CSP)**

Paramètres	Description
Activation	
Le service sera lancé automatiquement	Activation ou Désactivation de CSTA Service Provider (CSP). CSP est nécessaire pour la suite UC, pour le serveur DSS (Gestionnaire de présences, uniquement en réseau), pour OpenScape Business TAPI 170 et pour les applications CSTA externes.
Accès CSTA	
ID utilisateur CSTA / **Mot de passe utilisateur CSTA**	OpenScape Business TAPI 170 et les applications CSTA externes ne peuvent se connecter à CSP qu'à l'aide du compte utilisateur configuré ici. Si aucun utilisateur CSTA n'est configuré, l'utilisation d'OpenScape Business TAPI 170 ou des applications CSTA externes n'est pas possible sur CSP.

Paramètres	Description
Statistiques - Fournisseur de services CSTA (CSP)	Il est indiqué ici l'état de CSP. On voit le nombre et le type d'applications reliées à CSP. Les applications inconnues sont représentées "par défaut". Il est possible de consulter l'état de la connexion avec les différents noeuds du réseau / le noeud local. Les données sont automatiquement actualisées toutes les 5 minutes. Il est également possible d'actualiser manuellement la page.

27.5.4 Serveur DSS

Description des paramètres des onglets :

- **Paramètres - Serveur DSS**
- **Statistiques - Serveur DSS**

Paramètres	Description
Activation	
Le service sera lancé automatiquement	Activation ou Désactivation du serveur DSS.
Statistiques - Serveur DSS	Il est indiqué ici l'état du serveur DSS. Les données sont automatiquement actualisées toutes les 5 minutes. Il est également possible d'actualiser manuellement la page.

27.5.5 Media Extension Bridge (MEB)

Description des paramètres des onglets :

- **Paramètres - Media Extension Bridge (MEB)**
- **Statistiques - Media Extension Bridge (MEB)**

Paramètres	Description
Activation	
Le service sera lancé automatiquement	Activation ou Désactivation de Media Extension Bridge.
Statistiques - Media Extension Bridge (MEB)	Il est indiqué ici l'état de MEB. Les données sont automatiquement actualisées toutes les 5 minutes. Il est également possible d'actualiser manuellement la page.

28 Annexe

Cette annexe donne des informations sur les langues supportées, les standards, les configurations et capacités, les fonctionnalités Euro-ISDN, les indicatifs pour l'activation et la désactivation des fonctionnalités, les codes de fonctionnalités via DTMF ainsi que les protocoles IP utilisés et les numéros de port.

28.1 Normes supportées

Vous obtenez ici des informations sur les normes supportées.

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

Routage IP

- 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 à Expedited Forwarding PHB (Per-Hop Behavior)

Services

- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 à Expedited Forwarding PHB (Per-Hop Behavior)

Codecs

- G.711
- G.729

VoIP sur 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
- RC 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

Autre

- RFC 959 FTP
- RFC 1305 NTPv3
- RFC 1951 DEFLATE

28.2 Fonctionnalités Euro-RNIS

Les fonctionnalités Euro-RNIS peuvent être utilisées sur tous les ports Euro-RNIS, du moment que le matériel existant (par ex. le téléphone ou la carte RNIS) est configuré en conséquence. Les fonctionnalités sont disponibles en permanence sur le réseau ou bien peuvent être activées/désactivées à l'aide d'un indicatif.

La disponibilité des fonctionnalités dépend de l'opérateur du réseau. Certaines des fonctionnalités indiquées sont payantes.

Sujet	Explication
Numéros multiples (MSN = Multiple Subscriber Number)	Il est possible d'attribuer plusieurs numéros de téléphone à chaque connexion multiposte. L'utilisateur peut attribuer ces numéros de téléphone aux différents terminaux en les configurant directement sur les terminaux.
Présentation de la ligne appelante (CLIP = Calling Line Identification Presentation)	Le numéro d'appel est transmis à l'appelé et s'affiche par ex. sur l'écran de son téléphone ou est enregistré dans la liste des appels s'il ne répond pas. Il est impossible de transmettre des numéros incorrects. La sélection directe à l'arrivée (SDA) de systèmes de télécommunication ne peut toutefois pas être contrôlée. La transmission du numéro d'appel peut être supprimée de façon permanente ou au cas par cas.
Refus de présentation de la ligne appelante (CLIR = Calling Line Identification Restriction)	La transmission du numéro d'appel peut également être désactivée de façon permanente ou au cas par cas. Le cas échéant, le numéro d'appel ne s'affiche que pour des abonnés B définis (Appels d'urgence, Police, Sapeurs-pompiers).
Identification des appels malveillants (MCID = Malicious Call Identification)	L'appelé peut faire identifier l'appelant anonyme par l'intermédiaire du poste opérateur, même lorsque la présentation de la ligne appelante est désactivée. Cette fonctionnalité est soumise à facturation.
Portabilité du terminal (TP = Terminal Portability)	Cette fonctionnalité vous permet de raccorder le terminal RNIS à une autre prise RNIS pendant une communication et de poursuivre l'entretien. La communication doit être parquée avant le changement de prise.

Sujet	Explication
Sous-adressage (SUB = Subaddressing)	Cette fonction soumise à facturation peut être utilisée en supplément des numéros de téléphone normaux. Le sous-adressage permet, en fonction de l'appelant, de commander un terminal pouvant être appelé (par ex. un programme sur un ordinateur).
Signalisation d'usager à usager (UUS = User-to-User-Signalling)	Cette fonctionnalité permet d'échanger des informations par le biais du canal D pendant l'établissement de la connexion et la déconnexion. La transmission est possible dans les deux sens.
Groupe fermé d'usagers (CUG = Closed User Group)	Si cette fonction est activée, aucun appel ne peut être effectué hors du groupe d'usagers (exception faite des numéros d'appel d'urgence 110 et 112). Il est également possible de bloquer des appelants externes.
Renvoi d'appel sur occupation (CFB = Call Forwarding Busy)	Cette fonction de renvoi d'appel permet, lorsque l'abonné est occupé, de transférer les appels sur un poste arbitraire joignable. Le transfert d'appel a lieu au niveau du central. Les deux canaux utiles restent ainsi libres.
Renvoi d'appel inconditionnel (CFU = Call Forwarding Unconditional)	Cette fonction de renvoi d'appel permet de transférer immédiatement les appels sur un poste arbitraire joignable. Le transfert d'appel a lieu au niveau du central. Les deux canaux utiles restent ainsi libres.
Renvoi d'appel sur non-réponse (CFNR = Call Forwarding No Reply)	Cette fonction de renvoi d'appel permet, au bout de 20 secondes (si l'appelé ne répond pas), de transférer les appels sur un poste arbitraire joignable. Le transfert d'appel a lieu au niveau du central. Les deux canaux utiles restent ainsi libres.
Avertissement (Indication d'appel en instance - CW = Call Waiting)	Un autre appel est signalé pendant une communication. Cependant, l'appelant entend la tonalité de retour d'appel. L'appel en instance peut être accepté, refusé ou simplement ignoré.
Va-et-vient (Hold = Call Hold)	La fonction Double appel permet d'établir une deuxième connexion pendant une communication. La commutation entre les deux connexions est assurée par la fonction intitulée Va-et-Vient. L'interlocuteur en attente ne peut pas écouter l'autre communication.
Conférence à trois (3PTY = Three Party Service)	Vous pouvez interconnecter deux communications en cours. Il est ainsi possible de tenir une conférence à trois participants.
Rappel automatique sur occupation (CCBS = Completion of Calls to Busy Subscriber)	Cette fonction peut être activée lorsqu'un abonné appelé est occupé. Un signal vous indique que la ligne de cet abonné est de nouveau libre. La connexion est établie lorsque vous décrochez le combiné.

Sujet	Explication
Information de taxation à la fin de l'appel (AOCE = Advice of Charge (End))	Vous pouvez programmer l'application de manière à afficher la taxation à la fin de la communication. Les remises et tarifs éventuellement consentis ne sont pas pris en compte.
Information de télétaxe (AOCD = Advice of Charge (During))	Vous pouvez programmer l'application de manière à afficher la taxation pendant la communication. Les remises et tarifs éventuellement consentis ne sont pas pris en compte.

28.3 Ports utilisés

Les composantes système d'OpenScape Business utilisent différents ports qui doivent, si nécessaire, être validés dans le pare-feu. Pour les ports des clients basés sur le Web (par ex. myPortal to go), il faut paramétrer un renvoi de port dans le routeur.

Une liste complète de tous les ports utilisés de OpenScape Business est disponible dans la « base de données de gestion d'interface » (IFMD) accessible depuis le portail partenaire de Unify (https://unify.com/en/partners/partner-portal.

Remarque : Les ports identifiés par O dans la liste ci-dessous sont facultatifs, c'est-à-dire qu'ils ne sont pas ouverts en permanence dans le pare-feu.

Description	TCP	UDP	Numéro de port	OpenScape E	OpenScape Business S
Composants du système					
Portail Admin (https)	X		443	X	X
Contrôles CAR Alive	X		12062	X	X
CLA	X		61740	O	O
Découverte auto CLA		X	23232	X	X
CLS	X		7780, 7790 (jusqu'au V3R3) 7780, 7791 (V3R3.1 et supérieur)	O	O
Programme d'installation Communications Client	X		8101	X	X
CSTA Message Dispatcher (CMD)	X		8900		X
CSTA Protocol Handler (CPH)	X		7004	X	X
Fournisseur de services CSTA (CSP)	X		8800		X

Description	TCP	UDP	Numéro de port	OpenScape E	OpenScape Business S
DHCP		X	67	X	
DLI	X		18443	X	X
DLSC	X		8084	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
Messagerie instantanée (http)	X		8101	X	X
JSFT	X		8771		X
JSFT	X		8772		X
Service de Cloud LAS	X		8602	X	
Serveur LDAP	X		389		X
Manager E	X		7000	X	
MEB SIP	X		15060		
Traversée de NAT (NAT-T)		X	4500	X	
NTP		X	123	X	
Openfire Admin (HTTPS)	X		9091		X
Utilitaire de mise à jour automatique OpenScape Business (http)	X		8101	X	X
OpenScape Business Multisite	X		8778		X
OpenScape Business myReports (http)	X		8101		X
Serveur d'état OpenScape Business	X		8808	X	X
Portail utilisateur OpenScape Business	X	X	8779		X
Postgres	X		5432	X	X
RTP (intégré)		X	29100-30530	X	X
RTP (serveur)		X	29100-30888	X	X
SIP (serveur)	X	X	5060	X	X
SIP TLS SIPQ (serveur)	X		5061	X	X
Abonné SIP TLS (serveur)	X		5062	X	X
SNMP (Get/Set)		X	161	X	X

Description	TCP	UDP	Numéro de port	OpenScape E	OpenScape Business S
SNMP (Traps)		X	162	X	X
VSL	X		8770-8780		X
Webadmin pour les clients	X		8803	X	X
Clients basés sur le Web					
Webbased Clients (http)	X		8801	X	X
Webbased Clients (https)	X		8802	X	X

Remarque : Pour des raisons de sécurité, il est recommandé d'utiliser exclusivement https pour les clients basés sur le Web et de configurer un renvoi de port (Port Forwarding) de TCP/443 externe vers TCP/8802 interne.

Certificat CLS

A partir de V3R3.1, un nouveau certificat CLS avec un nom commun (CN) mis à jour est fourni via un port nouvellement introduit. Il offre un algorithme de résumé amélioré et plus fort, ainsi que des entités légales mises à jour. Les systèmes sous licence en ligne via le mode CLS Connect nécessitent les deux conditions préalables suivantes :

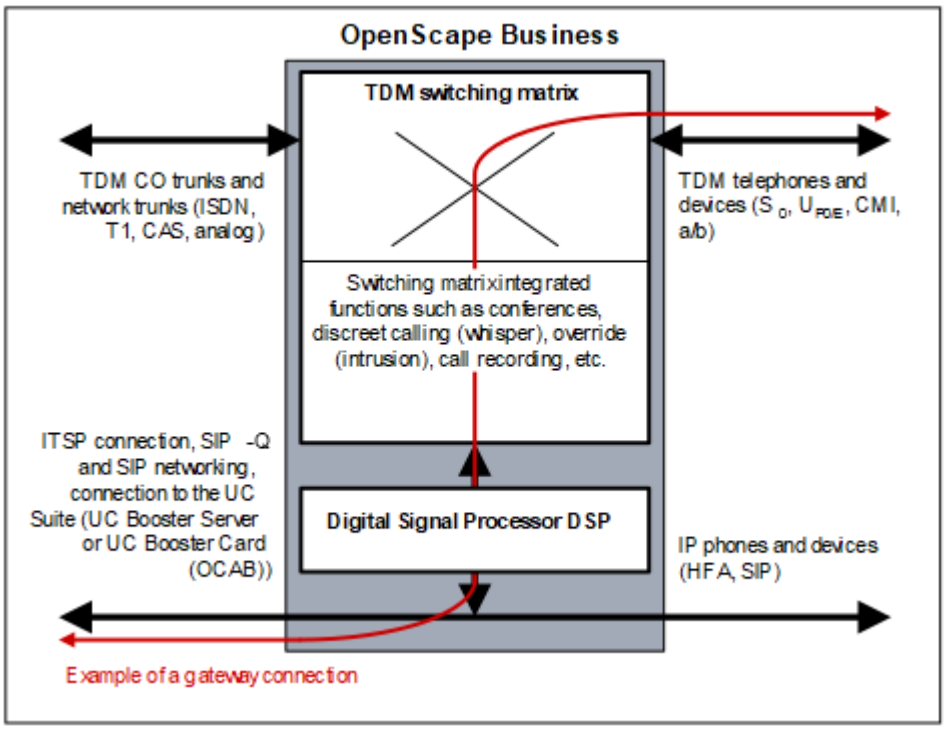
- L'adresse IP 188.64.16.4 est activée pour le trafic sortant dans le pare-feu.
- Les ports 7780 et 7791 sont activés pour le trafic sortant dans le pare-feu.

Le port 7790 précédemment utilisé peut être supprimé de la configuration du pare-feu après la mise à niveau vers V3R3.1 pour augmenter la sécurité.

28.4 Planification de projet des canaux DSP pour les systèmes de communication Unify OpenScape Business X5/X8

Les connexions entre téléphones / lignes IP et TDM sont des connexions passerelles pour lesquelles il faut disposer pour chacune d'elles d'un canal DSP (Digital Signal Processor). En outre, les canaux DSP sont requis lors de l'activation de la fonction de signalisation et de chiffrement de la charge utile (SPE).

Aucun canal DSP n'est nécessaire pour des connexions TDM pures et pour des connexions IP pures.



Les cartes mères des systèmes de communication OpenScape Business X3/X5/X8 offrent au maximum huit canaux DSP.

Si les canaux DSP d'une carte mère ne sont pas suffisants, des canaux supplémentaires peuvent être fournis en branchant une carte Booster de canal Voix (sous-carte OCCB1 ou OCCB3) :

- OCCBL : fournit jusqu'à 40 canaux DSP supplémentaires (canaux passerelle).
- OCCB3 fournit un maximum de 120 canaux DSP supplémentaires.

Le nombre de canaux DSP disponibles pour les connexions de passerelle est réduit par l'utilisation du codec G.729 et lors de l'utilisation de la signalisation et du chiffrement de la charge utile (SPE).

En fin de compte, le nombre de connexions de passerelle simultanées (connexions Voix simultanées avec transition IP-TDM) détermine si et quelle sous-carte OCCB doit être utilisée.

Avec une conférence UC-Suite et des téléphones IP, un système de communication OpenScape Business X3/X5/X8 peut inclure jusqu'à huit canaux DSP. Trois canaux DSP sont alloués par défaut aux trois codecs de musique d'attente par défaut. Ce nombre peut être diminué si vous utilisez moins de codecs pour musique d'attente. De plus, deux canaux DSP sont réservés à la configuration du cryptage de la signalisation et de la charge utile (SPE). Le reste des canaux DSP peut être alloué aux téléphones IP (un canal DSP par téléphone IP). Lorsque les canaux DSP disponibles sont épuisés, le nombre de canaux DSP peut être augmenté en utilisant les cartes OCCB (OCCB1 ou OCCB3 comme indiqué précédemment).

Conseil : Indication sur le nombre maximum des canaux DSP de la carte mère et des sous-modules OCCB, voir Limites de configuration imposées par le système.

En cas de sous-dimensionnement des canaux DSP, il peut se produire des goulots d'étranglement DSP qui se manifestent par des états Occupé lors de l'établissement de la connexion (tonalité Occupé lors de l'établissement de la connexion, affichage à l'écran `Actuellement impossible`).

S'il se produit un goulet d'étranglement DSP, il est établi une entrée dans le fichier journal d'événements (Journal des événements) du système de communication.

Lorsque des goulots d'étranglement DSP surviennent souvent, il faut prendre les mesures suivantes.

Si	Alors
Les canaux DSP de la carte mère sont utilisés.	Insérez le sous-carte OCCB1 ou OCCB3 dans la carte mère.
Les canaux DSP de la carte mère et du sous-module OCCB3 sont utilisés.	Insérez le sous-carte OCCB3 dans la carte mère.
Les canaux DSP de la carte mère et du sous-module OCCB3 sont utilisés.	Vérifiez si le système de communication ne peut être utilisé qu'avec le codec G.711. Cela augmente le nombre de canaux DSP au maximum. ***INFO :*** L'option **Utiliser exclusivement G.711** peut être activée par un administrateur avec le profil **Expert** en **Mode Expert** (**Téléphonie** > **Passerelle vocale** > **Paramètres du codec**).

Le tableau suivant fournit les valeurs d'orientation pour lesquelles le sous-carte OCCB, le cas échéant, doit être utilisé.

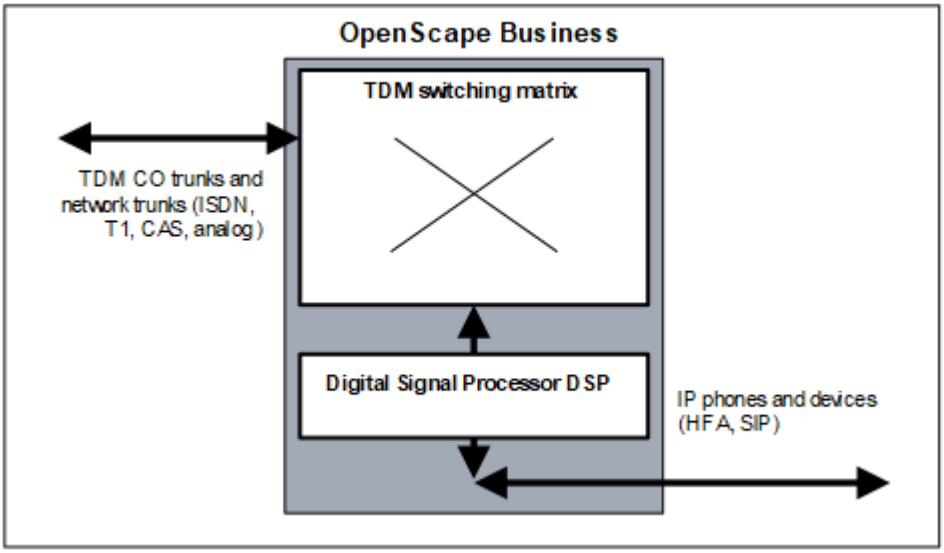
Indépendamment des canaux TDM. Lignes réseau et trunks réseau (RNIS, T1, CAS, analogique)	**Somme des canaux IP :** Connexion ITSP, mise en réseau SIP-Q et SIP	**Total des téléphones TDM et des équipements TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Somme des téléphones et appareils IP (HFA, SIP)**	**Quel sous-comité OCCB ?**	**Notes**
N'importe quel numéro	jusqu'à 16 0	N'importe quel numéro	0	Pas de sous-carte OCCB	Les conférences Smart VM et système sont traitées via la matrice de commutation.

Indépendamment des canaux TDM. Lignes réseau et trunks réseau (RNIS, T1, CAS, analogique)	**Somme des canaux IP :** Connexion ITSP, mise en réseau SIP-Q et SIP	**Total des téléphones TDM et des équipements TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Somme des téléphones et appareils IP (HFA, SIP)**	**Quel sous-comité OCCB ?**	**Notes**
			jusqu'à 8	Pas de sous-carte OCCB	Indépendamment des canaux TDM. Smart VM et les conférences système en combinaison avec les téléphones IP et les équipements IP ont besoin des ressources DSP, jusqu'à 40 simultanément.
			1 à 100	OCCB1	Indépendamment des canaux TDM. Smart VM et les conférences système en combinaison avec les téléphones IP et les équipements IP ont besoin des ressources DSP, jusqu'à 40 simultanément.
			> 100	OCCB3	Indépendamment des canaux TDM. Smart VM et les conférences système en combinaison avec les téléphones IP et les équipements IP ont besoin des ressources DSP, jusqu'à 120 simultanément.
	> 0	jusqu'à 8		Pas de sous-carte OCCB	
	> 0	1 à 100		OCCB1	Jusqu'à 40 simultanément
	> 0	> 100		OCCB3	Jusqu'à 120 simultanément
> 0	jusqu'à 8			Pas de sous-carte OCCB	La combinaison est essentiellement pertinente pour SIP-Q et UC Suite.

Indépendamment des canaux TDM. Lignes réseau et trunks réseau (RNIS, T1, CAS, analogique)	**Somme des canaux IP :** Connexion ITSP, mise en réseau SIP-Q et SIP	**Total des téléphones TDM et des équipements TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Somme des téléphones et appareils IP (HFA, SIP)**	**Quel sous-comité OCCB ?**	**Notes**
> 0	jusqu'à 9			OCCB1	La combinaison est essentiellement pertinente pour SIP-Q et UC Suite.
> 0	> 40			OCCB3	La combinaison est essentiellement pertinente pour SIP-Q et UC Suite.

Les exemples suivants fournissent des valeurs d'orientation pour lesquelles le sous-carte OCCB, le cas échéant, doit être utilisé.

OpenScape Business avec lignes réseau TDM et téléphones et équipements IP

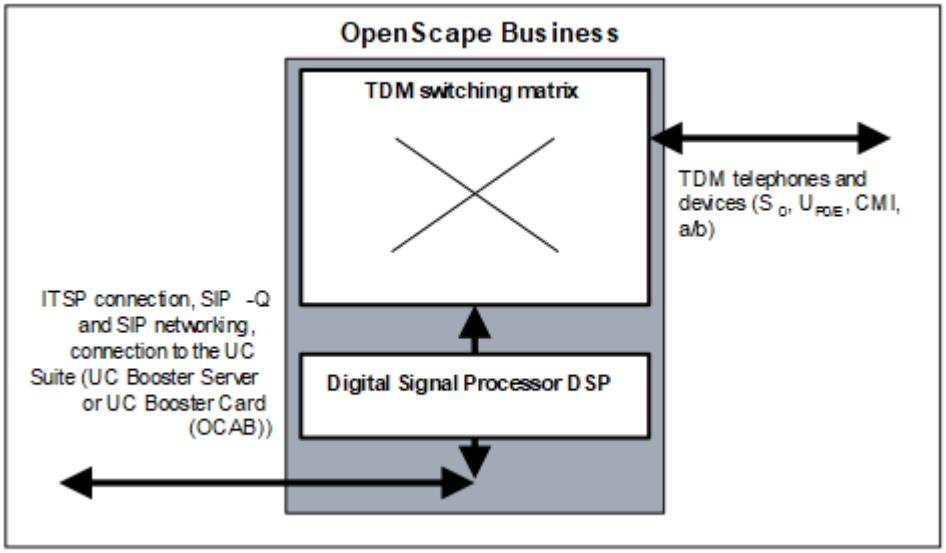


Si	**Alors**
OpenScape Business 2 avec : • 1 x réseau TDM (RNIS) • 20 x Téléphone IP (HFA, SIP)	Les canaux DSP sur la carte mère sont suffisants. Aucun sous-carte OCCB n'est requis.
OpenScape Business 2 avec : • 1 x réseau TDM (RNIS) • 100 x Téléphone IP (HFA, SIP)	Sous-module OCCB3 nécessaire. Alternativement, le sous-carte OCCB3 peut être utilisé.

Si	Alors
OpenScape Business 2 avec : • 2 x réseau TDM (RNIS) • 100 x Téléphone IP (HFA, SIP)	Sous-module OCCB3 nécessaire.
OpenScape Business 2 avec : • 4 x réseau TDM (RNIS) • 500 x Téléphone IP (HFA, SIP)	Sous-module OCCB3 nécessaire. ***REMARQUE :*** afin d'atteindre le nombre maximal de canaux DSP, seul le codec G.711 peut être utilisé dans cette configuration système.

Si le système de communication doit être équipé également de téléphones et équipements TDM (S_0, $U_{P0/E}$, CMI, a/b), il faut prendre en compte des canaux DSP supplémentaires.

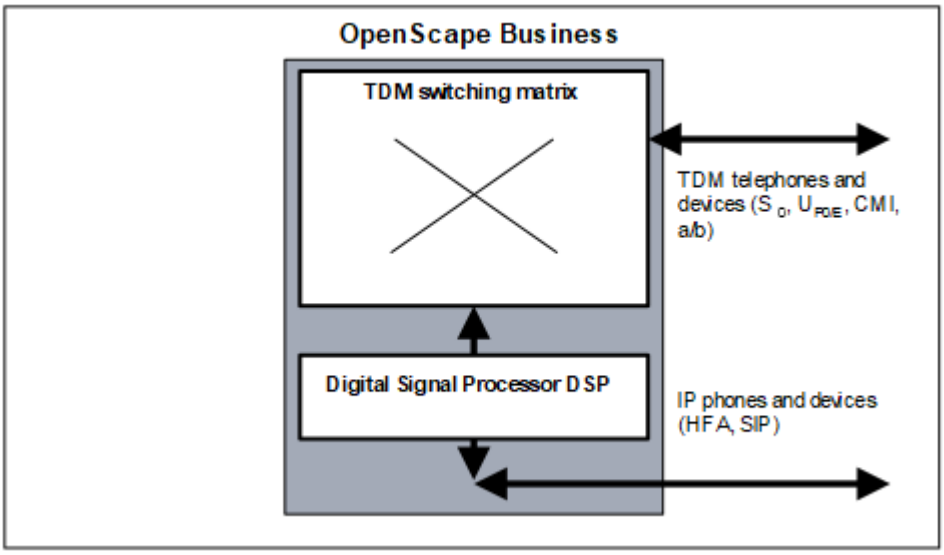
OpenScape Business avec connexion ITSP et téléphones et équipements TDM



Si	Alors
OpenScape Business 2 avec : • 6 x connexions ITSP (6 canaux B) • 20 x téléphone TDM (S_0, $U_{P0/E}$, CMI, a/b)	Les canaux DSP sur la carte mère sont suffisants. Aucun sous-carte OCCB n'est requis.
OpenScape Business 2 avec : • 30 x connexions ITSP (30 canaux B) • 100 x téléphone TDM (S_0, $U_{P0/E}$, CMI, a/b)	Sous-module OCCB3 nécessaire. Alternativement, le sous-carte OCCB3 peut être utilisé.

Si le système de communication doit être équipé également de téléphones et équipements TDM (S0, UP0/E, CMI, a/b), il faut prendre en compte des canaux DSP supplémentaires.

OpenScape Business avec téléphones et équipements TDM et téléphones et équipements IP



Si	Alors
OpenScape Business 2 avec : • 6 x téléphone TDM (S_0, $U_{P0/E}$, CMI, a/b) • 6 x Téléphone IP (HFA, SIP)	Les canaux DSP sur la carte mère sont suffisants. Aucun sous-carte OCCB n'est requis.
OpenScape Business 2 avec : • 100 x téléphone TDM (S_0, $U_{P0/E}$, CMI, a/b) • 100 x Téléphone IP (HFA, SIP)	Sous-module OCCB3 nécessaire.

Si le système de communication doit être équipé de jonctions TDM ou de jonctions IP, des canaux DSP supplémentaires doivent être pris en compte.

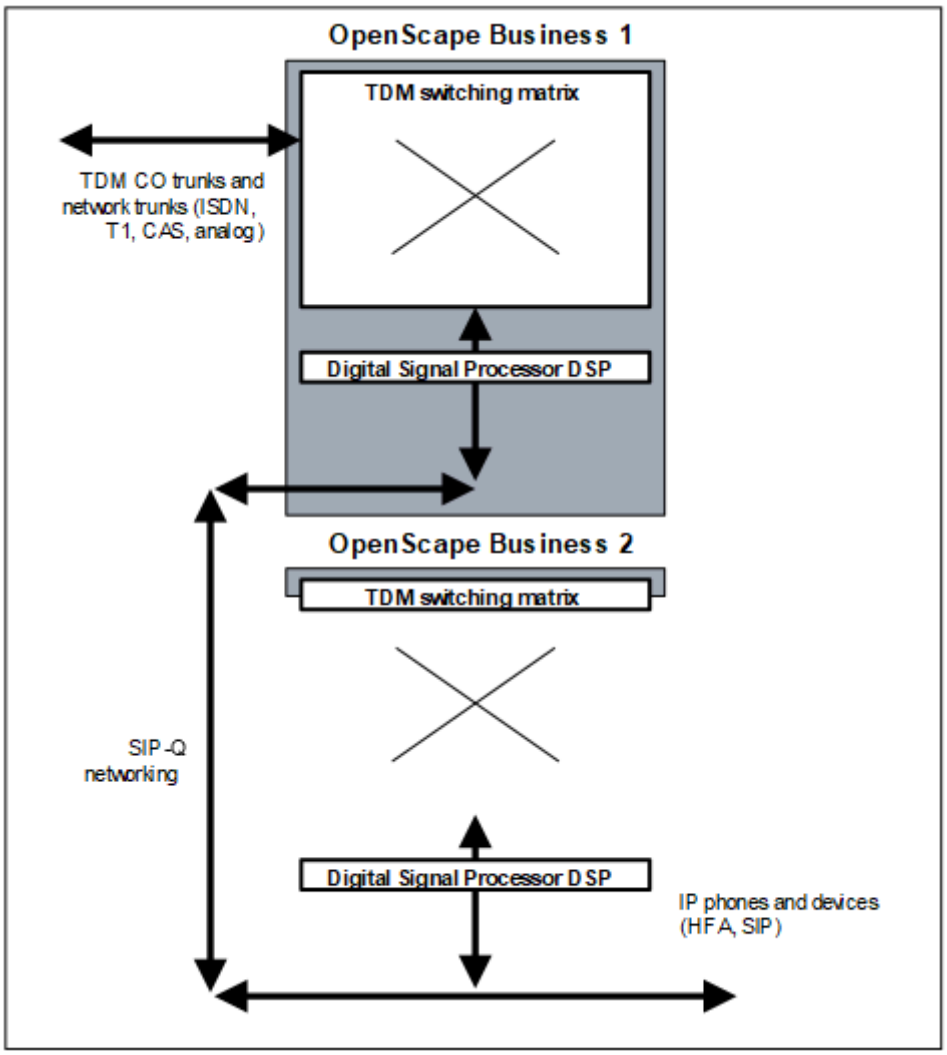
Mise en réseau SIP-Q OpenScape Business

Remarque : Cet exemple présente les exigences d'un deuxième système OpenScape Business en réseau. Les connexions du premier système ne sont pas représentées ici pour plus de simplicité. Cependant, les exigences du premier système, comme indiquées dans les exemples 1, 2 et 3, doivent également être prises en compte.

Le système de communication Unify OpenScape Business 1 agit comme une passerelle pour le bureau central TDM.

Les téléphones IP (HFA, SIP) ne sont connectés qu'au système de communication Unify OpenScape Business 2.

En fonction du nombre de téléphones IP sur le système de communication Unify OpenScape Business 2, les canaux DSP pour le système de communication Unify OpenScape Business 1 doivent être planifiés. Les canaux DSP sont requis exclusivement dans la passerelle TDM.



Si	Alors
OpenScape Business 1 avec : • 1 x réseau TDM (RNIS) OpenScape Business 2 avec : • 100 x Téléphone IP (HFA, SIP)	La sous-carte OCCB1 est requise dans Unify OpenScape Business 1. Alternativement, le sous-carte OCCB3 peut être utilisé. Aucun sous-comité OCCB n'est requis dans OpenScape Business 2.

Si	Alors
OpenScape Business 1 avec : • 2 x réseau TDM (RNIS) OpenScape Business 2 avec : • 100 x Téléphone IP (HFA, SIP)	Le sous-carte OCCB3 est requis dans OpenScape Business 1. Aucun sous-comité OCCB n'est requis dans OpenScape Business 2.
OpenScape Business 1 avec : • 4 x réseau TDM (RNIS) OpenScape Business 2 avec : • 500 x Téléphone IP (HFA, SIP)	Le sous-carte OCCB3 est requis dans OpenScape Business 1. ***REMARQUE :*** afin d'atteindre le nombre maximal de canaux DSP, seul le codec G.711 peut être utilisé dans cette configuration système. Aucun sous-comité OCCB n'est requis dans OpenScape Business 2.

Si le système de communication OpenScape Business 2 doit être équipé également de lignes TDM ou de téléphones et équipements TDM (S_0, $U_{P0/E}$, CMI, a/b), il faut prendre en compte des canaux DSP supplémentaires.

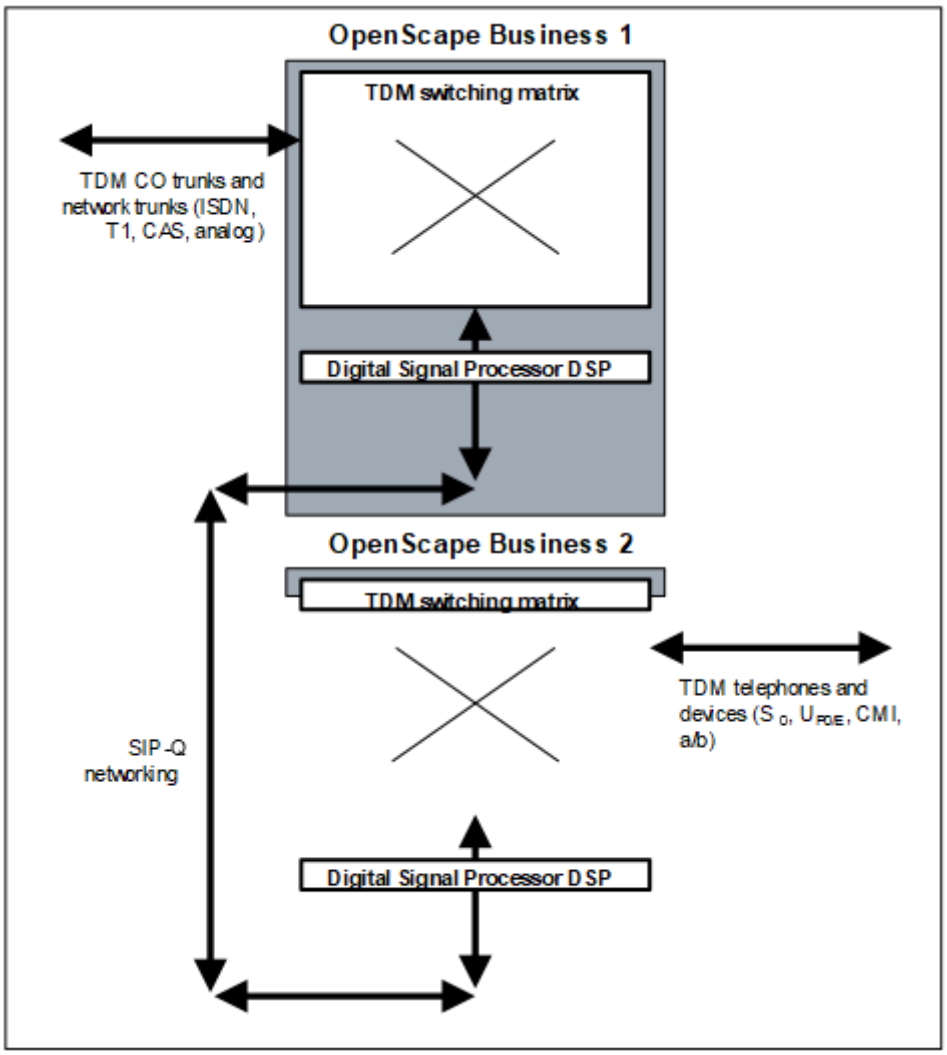
Mise en réseau SIP-Q OpenScape Business

Remarque : Cet exemple présente les exigences d'un deuxième système OpenScape Business en réseau. Les connexions du premier système ne sont pas représentées ici pour plus de simplicité. Cependant, les exigences du premier système, comme indiquées dans les exemples 1, 2 et 3, doivent également être prises en compte.

Le système de communication Unify OpenScape Business 1 agit comme une passerelle pour le bureau central TDM.

Exclusivement sur le système de communication OpenScape Business 2, des téléphones TDM (S_0, $U_{P0/E}$, CMI, a/b) sont raccordés.

Étant donné que des connexions de passerelle sont nécessaires dans les deux systèmes de communication (OpenScape Business 1 : TDM CO <-> Réseau SIP-Q, OpenScape Business 2 : Réseau SIP-Q <-> téléphone TDM), des canaux DSP sont nécessaires dans les deux systèmes.



Si	Alors
OpenScape Business 1 avec : • 1 x réseau TDM (RNIS) OpenScape Business 2 avec : • 100 x téléphone TDM (S_0, $U_{P0/E}$, CMI, a/b)	Sous-module OCCB3 nécessaire dans OpenScape Business 1 et OpenScape Business 2. Alternativement, le sous-carte OCCB3 peut être utilisé dans les deux cas.
OpenScape Business 1 avec : • 2 x réseau TDM (RNIS) OpenScape Business 2 avec : • 100 x téléphone TDM (S_0, $U_{P0/E}$, CMI, a/b)	Sous-module OCCB3 nécessaire dans OpenScape Business 1 et OpenScape Business 2.

Si le système de communication OpenScape Business 1 doit être équipé également de téléphones et équipements TDM (S_0, $U_{P0/E}$, CMI, a/b), il faut prendre en compte des canaux DSP supplémentaires.

OpenScape Business avec téléphones et équipements IP

Remarque : Cet exemple présente les exigences d'un deuxième système OpenScape Business en réseau. Les connexions du premier système ne sont pas représentées ici pour plus de simplicité. Cependant, les exigences du premier système, comme indiquées dans les exemples 1, 2 et 3, doivent également être prises en compte.

Si	Alors
OpenScape Business X5/X8 avec : • 7 x Téléphone IP (HFA, SIP)	Les canaux DSP sur la carte mère sont suffisants. Aucun sous-carte OCCB n'est requis.
OpenScape Business • 30 x Téléphone IP (HFA, SIP)	Subboard OCCB1 est requis. Alternativement, le subboard OCCB3 peut être utilisé.
OpenScape Business 2 avec : • 100 x Téléphone IP (HFA, SIP)	Sous-module OCCB3 nécessaire.

29 Glossaire

Le glossaire donne de brèves explications sur les termes utilisés (par ex. pour les protocoles et les normes).

29.1 Glossaire

10BaseT, 100BaseT, 1000BaseT

Il s'agit d'une spécification (IEEE. 802.3i)) pour les réseaux avec une transmission en bande de base de 10 Mbps sur un câble symétrique à quatre fils de 100 Ohms. 100BaseT, d'autre part, est utilisé pour des bandes passantes allant jusqu'à 100 Mbps et 1000BaseT pour des bandes passantes allant jusqu'à 1000 Mbps.

AES (Advanced Encryption Standard)

AES est un système de cryptage symétrique qui a été ratifié par l'Institut national des normes et de la technologie en tant que successeur des normes DES et 3DES antérieures. Il est utilisé pour les VPN, par exemple.

ADSL avec adresse IP dynamique

ADSL signifie Asymmetric Digital Subscriber Line et signifie que les bandes passantes d'Internet (téléchargement, en aval) et d'Internet (téléversement, Flux ascendant) sont différentes. La connexion téléphonique Internet classique est l'ADSL. Une adresse IP dynamique est suffisante si les services Web et de messagerie sont fournis par le fournisseur de services Internet.

Clients avec adresse IP fixe (facultatif)

ADSL signifie ligne numérique asymétrique d'abonné et signifie que les bandes passantes d'Internet (téléchargement, en aval) et d'Internet (téléversement, Flux ascendant) sont différentes. La connexion téléphonique Internet classique est l'ADSL. L'ADSL avec une adresse IP fixe est nécessaire si vous souhaitez exécuter votre propre serveur Web et de messagerie sur votre site.

AF-EF (Expédition accélérée - Expédition assurée)

Les codepoints AF et EF définissent les différentes priorités des paquets IP pour la QOS (Qualité de Service).

AF : garantit une bande passante minimale pour les données

EF : garantit une bande passante constante pour ces données.

Protocole de résolution d'adresses

Le protocole de résolution d'adresse (ARP) est un protocole réseau qui facilite l'attribution d'adresses réseau à des adresses matérielles. Bien qu'il ne soit pas limité aux protocoles Ethernet et IP, il est presque exclusivement utilisé en conjonction avec l'adressage IP dans les réseaux Ethernet.

Authentification

L'authentification est la vérification de l'identité d'une personne ou d'un PC. Le contrôle peut être effectué avec un simple nom d'utilisateur, par exemple, ainsi qu'avec une empreinte digitale.

Autorisé

L'autorisation est un mécanisme d'octroi de droits, par exemple, les droits d'accès dans un réseau de données.

Canal B

Un canal B est le chemin de transmission de la charge utile (voix, données) d'une connexion RNIS.

Champ d'occupation (BLF)

myPortal fournit un champ de lampe occupé (BLF) pour afficher l'état des appels des abonnés spécifiés.

Diffusion

Une diffusion est un message envoyé à tout le monde dans un réseau PC. Le message (c'est-à-dire un paquet de données) est transmis d'un point à tous les abonnés du réseau. Une diffusion est principalement utilisée dans un réseau de données si l'adresse du destinataire du message est inconnue.

CA (Autorité de certification)

L'AC est une organisation qui émet des certificats avec des signatures numériques. Des signatures numériques sont nécessaires pour un VPN (réseau privé virtuel), par exemple.

Interface capi (Common Application Programming Interface)

Capi est une interface logicielle standardisée conforme au RNIS. Capi permet le développement de logiciels RNIS sans nécessiter de connaissances sur le matériel RNIS spécifique au fabricant utilisé.

Centrex

Centrex (Central Office Exchange) assure les fonctions d'un système téléphonique via un RTPC ou un ITSP. Ceci est également connu sous le nom de système téléphonique virtuel, PBX hébergé (Private Branch Exchange) ou NetPBX.

CHAP (Challenge Handshake Authentication Protocol)

CHAP est un protocole d'authentification utilisé dans le cadre du protocole Point-to-Point.

Classes de service

La QoS est une procédure qui assure la qualité de transmission des données dans les réseaux IP.

Informations d'identification de l'appelant (CLIP)

Avec la transmission du numéro de terminal, le numéro de téléphone de l'appelant est affiché sur le terminal de l'appelé. L'appelé peut donc identifier l'appelant avant d'intercepter l'appel.

Calling Line Identification Restriction, COLR :

L'appelant supprime l'affichage de son numéro d'appel sur le terminal appelé. En conséquence, l'appelé ne peut pas identifier l'appelant avant d'intercepter l'appel.

COLP - Présentation de l'identification de la ligne connectée

Avec la présentation de l'identification de la ligne connectée, le numéro de l'appelé est affiché pour l'appelant si la connexion est réussie.

COLR (Restriction d'identification de la ligne connectée)

Avec la restriction d'identification de la ligne connectée, le numéro de l'appelé n'est pas affiché pour l'appelant, même si l'appelant a activé le COLP.

Confort de l'utilisateur

Confort de l'utilisateur est l'utilisateur standard du système de communication.

Comfort Plus

L'utilisateur Comfort Plus est l'utilisateur Advanced du système de communication. Contrairement à l'utilisateur Confort, l'utilisateur Confort Plus peut utiliser plus de fonctionnalités (telles que le fax, la mobilité et En conférence).

CorNet

CorNet est un protocole propriétaire pour la mise en réseau des systèmes de communication HiPath et OpenScape. Contrairement au QSIG généralement pris en charge, toutes les fonctionnalités spécifiques au fabricant des systèmes de communication HiPath et OpenScape sont intégrées dans CorNet.

CorNet-IP

CorNet-IP est une variante de protocole de CorNet qui permet la mise en réseau croisée de systèmes ou la connexion de téléphones système (tels qu'optiPoint) sur IP.

CorNet-NQ

Protocole de signalisation propriétaire basé sur QSIG pour interconnecter des systèmes de communication à un ou plusieurs systèmes PBX QSIG.

CSTA – Computer Supported Telecommunications Applications (Applications de télécommunications assistées par ordinateur)

CSTA est une interface de protocole pour les applications qui prennent en charge la norme de l'Association européenne des fabricants d'ordinateurs (ECMA). Les tâches de télécommunication sont contrôlées et surveillées à l'aide de SIP via CSTA.

CSV (valeurs séparées par des caractères)

Un fichier CSV est un fichier texte permettant de sauvegarder ou d'échanger des données simplement structurées. CSV signifie Character Separated Values, Comma Separated Values ou Colon Separated Values, puisque les valeurs individuelles sont délimitées par un caractère séparateur spécial tel qu'une virgule ou un point-virgule. Les fichiers CSV doivent être disponibles au format ANSI/ASCII.

CRL (Certificate Revocation Lists)

Une CRL ou une liste de révocation de certificat est une liste ou tous les certificats révoqués. Les LCR doivent toujours être générées par l'autorité de certification d'où proviennent les certificats.

Délai

Un retard a deux significations dans les télécommunications :

- Le délai par lequel un événement est reporté.
- Le temps écoulé entre la survenance d'un événement et l'apparition d'un événement de suivi attendu.

Passerelle dédiée (assignée en permanence

Si une passerelle dédiée est entrée dans le LCR pour un itinéraire, le routage via cette passerelle est appliqué. Toutes les règles contradictoires sont alors invalides pour le routage.

DHCP (Dynamic Host Configuration Protocol)

DHCP est une procédure par laquelle un PC se voit attribuer une certaine configuration IP (adresse IP, masque de sous-réseau, etc.) au démarrage.

DS (DiffServ, Services Différenciés)

DS est une procédure de gestion des paquets dans les réseaux de données. Le procédé de routage pour un paquet de données spécifique est spécifié ainsi qu'un niveau de service particulier en ce qui concerne la bande passante, la théorie de la mise en file d'attente et les décisions de rejet de paquet.

Algorithme Diffie-Hellman

L'algorithme Diffie-Hellman est utilisé pour l'échange de clés dans un VPN. Les données produites par cet algorithme sont configurées avec un ensemble spécifique de paramètres mathématiques. L'échange de clés ne fonctionne correctement que si les deux abonnés utilisent des valeurs identiques pour ces paramètres.

DLI (Service de licence de déploiement intégré)

DLI permet l'installation et la mise à niveau sans surveillance des téléphones IP.

DMZ (zone démilitarisée)

Une zone démilitarisée (DMZ) fait référence à un réseau de PC qui offre un certain nombre de fonctionnalités de sécurité pour accéder aux nœuds de réseau connectés (PC, routeurs, etc.).

DNS (Domain Name Service)

Résolution de noms sur Internet et dans le LAN. Le DNS traduit les noms des PC ou des pages Web en adresses IP pertinentes.

DSL (ligne d’abonné numérique)

DSL est une solution technologique pour fournir un accès Internet à large bande passante. Le téléphone Internet comble le fossé entre le préposé du fournisseur et la prise téléphonique du client.

DSS (Direct Station Server)

Les touches de fonction d'un téléphone ou d'un appareil complémentaire peuvent être programmées en tant que touches de sélection directe du terminal (DSS). Ceux-ci sont programmés avec le numéro de téléphone d'un abonné interne ou d'un groupe pour cela. Appuyer sur une touche DSS déclenche un appel immédiat vers la destination programmée.

DTMF (Dual Tone Multifrequency)

Voir DTMF.

EIM (messagerie instantanée d'entreprise)

EIM est un service de messagerie instantanée qui s'exécute sur des serveurs privés d'une entreprise sur des plateformes telles que le serveur de communications en direct.

Enterasys commute

Les commutateurs Enterasys sont produits par Enterasys Networks en tant que solutions réseau sécurisées. Les commutateurs empilables prennent en charge les fonctionnalités QoS et peuvent classer et hiérarchiser les applications Voix, vidéo et de données.

ESP (charge utile de sécurité encapsulée)

ESP est un protocole IPsec qui garantit le cryptage des paquets, l'intégrité des paquets ainsi que l'authenticité des paquets. Le contrôle d'intégrité et d'authentification ne s'étend pas à l'en-tête IP. Elle n'est effectuée que pour les données réelles (charge utile).

FoIP (Fax sur IP)

FoIP est un procédé de transmission de messages de télécopie sur un réseau IP.

FTP

Le protocole de transfert de fichiers (FTP) est un protocole réseau spécifié dans la RFC 959 pour la transmission de données via des réseaux TCP/IP.

Numéros fonctionnels

Les numéros fonctionnels (également appelés codes de fonction) sont des numéros MSN/DID ou des numéros pilotes, par exemple pour le stationnement, En conférence et l'AutoAttendant. Les numéros fonctionnels correspondent à des terminaux virtuels. Les numéros fonctionnels dans un inter-réseau doivent être uniques.

G.711

G.711 est une norme pour la numérisation des signaux audio analogiques. Il est utilisé dans la téléphonie classique en réseau fixe (technologie PCM). G.711 peut également être utilisé pour l'encodage de la voix en VoIP.

G.729AB

G.729 est un codec pour la compression de la voix dans les signaux numériques et est utilisé dans la téléphonie IP. G.729 est très gourmand en

CPU. Bien que légèrement inférieur en termes de qualité, G.729AB est une version quelque peu simplifiée et donc moins gourmande en CPU.

Passerelle /Modules de passerelle

Une passerelle est l'entrée et la sortie d'un réseau de communication, reliant généralement deux flux de trafic disparates.

GSM (Système mondial de communications mobiles)

Le GSM est une norme pour les réseaux mobiles numériques qui est principalement utilisée pour la téléphonie, mais aussi pour les transmissions de données à commutation de lignes et de paquets ainsi que pour les messages courts (SMS).

Transfert

Le terme transfert désigne le processus dans un réseau de communication cellulaire mobile dans lequel le téléphone mobile commute d'une cellule à une autre lors d'un appel ou d'une connexion de données. Le terme est également utilisé lors de la commutation entre GSM et UMTS avec un téléphone mobile bi-mode.

Valeur de hachage

Les valeurs de hachage ou de plage de dispersion sont généralement des valeurs évolutives à partir d'un sous-ensemble d'entiers naturels. Une valeur de hachage est également appelée « empreinte digitale » car il s'agit d'une identification virtuellement unique d'une quantité de la même manière qu'une empreinte digitale est une identification virtuellement unique d'une personne.

H.323

H.323 désigne un groupe de normes qui définissent une variété de types de supports pour les réseaux de paquets. Les normes couvrent la voix, les données, le fax et la vidéo, et définissent comment les signaux doivent être convertis de l'analogique au numérique et quelle signalisation doit être utilisée.

OpenScape Business Assistant

Unify OpenScape Business Assistant est utilisé pour administrer le système de communication. Il fournit tous les assistants pour le soutien rapide des tâches d'administration.

Services hébergés

Les services hébergés sont des services informatiques traditionnels tels que le courrier électronique, la messagerie instantanée (IM) et les communications unifiées (UC), qui sont fournis à une entreprise par un fournisseur d'accès Internet à partir d'un site distant, éliminant ainsi la nécessité pour l'entreprise d'exécuter et de gérer ces services sur ses propres serveurs sur site.

ICMP (Internet Control Message Protocol)

ICMP est utilisé dans les réseaux de données pour l'échange d'informations et de messages d'erreur à l'aide de l'IP du protocole Internet.

IDS (système de détection d'intrusion)

IDS est un système de sécurité qui surveille toutes les activités réseau entrantes et sortantes afin d'identifier d'éventuelles violations de la sécurité. Il s'agit à la fois d'intrusion (attaques provenant de l'extérieur de l'organisation) et d'abus (attaques provenant de l'intérieur de l'organisation).

NormesIEEE

Les normes IEEE sont un ensemble de spécifications définies par l'Institute of Electrical and Electronic Engineers (IEEE) (telles que Token Ring, Ethernet) pour établir des normes de mise en réseau communes entre les fournisseurs.

IEEE. 802.1p

IEEE. 802.1p est une norme IEEE pour réguler le transport de paquets de données avec différentes priorités dans les réseaux informatiques. Les paquets de données sont classés en classes de priorité de 1 à 7. La norme ne stipule que les priorités ascendantes de 1 à 7, mais ne traite pas de la façon dont les paquets de données individuels doivent être traités.

Protocole IKE

Le protocole IKE a deux tâches différentes. Commencez par créer une SA (association de sécurité) exclusivement utilisée par le protocole IKE (IKE-SA). L'IKE-SA existant est ensuite utilisé pour la négociation sécurisée de toutes les autres SA (SA de charge utile) pour la transmission de données de charge utile.

IM (messagerie instantanée)

La messagerie instantanée est une procédure d'échange en temps réel de messages texte sur Internet à l'aide d'ordinateurs, de Pocket PC et de téléphones mobiles. Les services de messagerie instantanée modernes permettent la VoIP et la vidéoconférence, les transferts de fichiers et le partage d'applications de bureau.

IP PBX

IP PBX est un système de communication qui prend en charge les connexions VoIP et les connexions voix normales sur les lignes téléphoniques traditionnelles.

IPSec

IPSec est un cadre de normes ouvertes pour assurer des communications privées et sécurisées sur des réseaux à protocole Internet (IP) grâce à l'utilisation de divers services et protocoles de sécurité.

FAI (Fournisseur d'Accès à Internet)

Un FAI est une entreprise qui fournit des services de connectivité Internet aux particuliers, aux entreprises et à d'autres organisations. Certains FAI sont de grandes sociétés nationales ou multinationales qui offrent un accès dans de nombreux endroits, tandis que d'autres sont limités à une seule ville ou région.

ITSP (Internet Telephony Service Provider, fournisseur de services de téléphonie sur Internet)

Un ITSP est une entreprise qui fournit des services de connectivité Internet aux particuliers, aux entreprises et à d'autres organisations.

DP (impulsion de cadran)

DP est la méthode de signalisation la plus ancienne utilisée pour la commutation téléphonique automatique. Aujourd'hui, le DP a généralement été remplacé par le DTMF.

Gigue

La gigue fait référence aux variations de retard des paquets dans les transmissions de voix. Un délai excessif entre l'envoi des paquets et leur arrivée à l'extrémité réceptrice entraîne une voix hachée difficile à comprendre.

ISD (numérotation rapide individuelle)

La numérotation rapide individuelle (ISD) permet d'enregistrer 10 numéros de numérotation rapide individuels externes sur chaque téléphone autorisé en plus de la numérotation rapide du système (SSD).

Numérotation abrégée centralisée

Les numéros de téléphone externes fréquemment requis peuvent être stockés dans la mémoire système du système de communication. Chaque numéro est représenté par un numéro abrégé qui est utilisé à la place du numéro de téléphone complet.

Latence

La latence est le temps nécessaire pour transporter un paquet de données d'une application à une autre, y compris le temps de transmission sur le réseau et pour préparer et traiter les données au niveau des dispositifs d'émission et de réception.

Routage automatique).

Vous pouvez utiliser la fonction de routage à moindre coût (LCR) pour spécifier le fournisseur que vous souhaitez utiliser, par exemple, pour les appels de jonction, les appels de téléphonie mobile ou les appels internationaux. Vous utilisez le système de communication pour définir le fournisseur le moins coûteux et effectuer tous les appels via ce chemin spécifique.

Chiffre par LIN (Location Identification Number)

Le LIN est un numéro unique à 16 chiffres maximum qui correspond au NANP (Plan de numérotation nord-américain) à 10 chiffres.

LWCA (Lightweight CA)

LWCA est une fonction de certification restreinte.

Canal de flux multimédia

Une passerelle multimédia peut mettre fin à des canaux RNIS B à commutation de circuits et utiliser les données de voix transportées pour générer des canaux de flux multimédia pour un réseau à commutation de paquets basé sur IP. Les canaux de flux multimédia comprennent une combinaison de médias audio, vidéo et T.120.

DTMF (Dual Tone Multifrequency)

La multifréquence à double tonalité (DTMF) est la méthode de numérotation en téléphonie analogique qui est principalement utilisée dans la technologie de

commutation aujourd'hui pour transmettre le numéro de téléphone au réseau téléphonique.

MIM (messagerie instantanée mobile)

MIM est un service de présence et de messagerie instantanée pour téléphones mobiles.

Mobility

Le terme mobilité désigne l'utilisation des Pocket PC et des téléphones mobiles et leur intégration dans le système de communication d'une entreprise.

Musique d'attente

La musique en attente (MOH) peut être jouée aux appelants qui ne peuvent pas être commutés immédiatement.

MSN (numéro d'abonné multiple)

Lors de la connexion de téléphones RNIS via un bus S0 (connexions point à multipoint), chaque téléphone RNIS (terminal RNIS) se voit attribuer un numéro d'abonné multiple (MSN) unique. Les terminaux RNIS sont accessibles via leurs MSN.

MULAP (Apparence de plusieurs lignes)

Les MULAP sont des groupes spéciaux dans lesquels plusieurs téléphones sont combinés. Un membre du groupe peut se voir attribuer plusieurs téléphones sous un seul numéro d'appel (MULAP Basic) ici. En outre, un tel groupe peut être utilisé pour mettre en œuvre des fonctionnalités spéciales requises pour la communication entre un exécutif et un secrétaire, par exemple, ou au sein d'équipes (Executive MULAP, Team MULAP).

Multi-Gateway

Dans le cas d'un réseau multi-passerelles, les appels sont acheminés via plusieurs passerelles différentes.

myAttendant

myAttendant est la console opérateur du système de communication.

myPortal

myPortal est le portail utilisateur basé sur Java qui permet aux abonnés d'accéder aux fonctions de communications unifiées. Outre les informations sur l'état de présence, l'aide à la numérotation pratique via les favoris et les annuaires, les abonnés peuvent également accéder aux messages vocaux et aux télécopies.

myPortal for Outlook

myPortal for Outlook est le portail utilisateur intégré à Microsoft Outlook qui permet aux abonnés d'accéder aux fonctions de communications unifiées. Il est analogue à myPortal. myPortal pour Outlook fournit également un numéroteur de bureau pratique.

NAC (contrôle d’accès au réseau)

NAC est une technologie qui prend en charge les défenses contre les virus et les vers au sein du réseau. Avec NAC, la conformité des terminaux aux directives est vérifiée lors de l'authentification. Si le scanner de virus n'est pas à jour, par exemple, ou si le système d'exploitation client n'a pas installé le dernier correctif de sécurité, l'appareil concerné est mis en quarantaine et reçoit les mises à jour actuelles jusqu'à ce qu'il réponde aux directives de sécurité applicables.

NAT (traduction d'adresses réseau)

NAT est une procédure permettant de remplacer une adresse IP dans un paquet de données par une autre. Il est utilisé pour mapper les adresses IP privées aux adresses IP publiques. Le masquage ou PAT (Port Address Translation) est le moment où les numéros de port sont également réécrits.

NTBA (Terminaison de réseau pour l'accès RNIS Basic)

Un NTBA (Network Termination for ISDN Basic Access), également connu sous le nom de NT (Network Termination), est le dispositif de terminaison du réseau pour l'interface de débit de base du RNIS. C'est le lien entre le réseau numérique de l'opérateur du réseau et les configurations RNIS côté abonné.

NTPM (Network Termination for Primary Rate Multiplex Access) (terminaison de réseau pour accès multiplex à débit primaire)

Un NTPM (Network Termination for Primary Rate Multiplex Access) est le dispositif de terminaison du réseau pour l'interface de débit primaire RNIS. C'est le lien entre le réseau numérique de l'opérateur du réseau et les configurations RNIS côté abonné.

OLSR - Protocole de routage d'état de liaison optimisé

L'OLSR est un protocole ad hoc spécial qui permet d'optimiser la capacité de routage manquante sur la couche OSI 2 sur la couche OSI 3.

ONS (One Number Service)

Numéro d'appel directement attribué à un utilisateur Une ou plusieurs ressources (téléphones) peuvent être attribuées à un utilisateur. Lorsqu'un utilisateur est appelé via son numéro ONS, l'appel est renvoyé vers le téléphone actuellement utilisé par cet utilisateur (par exemple, un téléphone mobile).

PAP (protocole d'authentification par mot de passe)

PAP est une procédure d'authentification basée sur le protocole point à point. Il est utilisé pour la numérotation dans un FAI. PAP transmet le mot de passe pour l'authentification en texte clair avec un ID utilisateur.

PBX (Private Branch Exchange)

Un PBX est un système de commutation qui interconnecte plusieurs terminaux tels que des téléphones, des télécopieurs et des répondeurs entre eux et également au réseau téléphonique public.

Pair

Un pair est le dispositif terminal de communication dans un réseau peer-to-peer. Lors de la communication, chaque pair met à disposition ses services et utilise les services de l'autre pair.

Pair à pair

Dans un réseau peer-to-peer, tous les PC ont des droits égaux et peuvent utiliser et également fournir des services sur le réseau.

Authentification de l'entité homologue

La corroboration que l'entité homologue dans une association est celle revendiquée.

Infrastructure à clé publique

En cryptologie, une PKI (infrastructure à clé publique) est un système permettant de générer, de distribuer et de vérifier des certificats numériques. Les certificats émis au sein d'une PKI sont utilisés pour protéger les communications informatiques.

PPP (protocole point à point)

PPP est une norme de l'IETF pour la transmission de paquets IP sur des lignes série. PPP est principalement utilisé pour la numérotation sur Internet.

PPPoE (protocole point à point sur Ethernet)

Le protocole PPPoE (PPP over Ethernet) permet l'utilisation du protocole réseau point à point sur une connexion Ethernet.

Clé pré-partagée

La clé pré-partagée est une clé qui est définie pour la configuration du tunnel (pour les VPN). Pour que les homologues VPN communiquant via le tunnel s'authentifient, le même mot de passe doit être utilisé pour les deux points de terminaison du tunnel.

PPTP (Point-to-Point Tunneling Protocol)

PPTP est une technologie utilisée pour configurer un réseau privé virtuel (VPN). Parce qu'Internet est essentiellement un réseau ouvert, PPTP est utilisé pour s'assurer que les messages transmis d'un nœud VPN à un autre sont sécurisés. PPTP permet aux utilisateurs de se connecter à leur réseau d'entreprise via Internet.

Présence

Le terme Présence fait référence à la capacité d'un système de communications unifiées à déterminer l'emplacement et le statut d'un utilisateur à tout moment. Cela facilite la réponse aux besoins de communication spécifiques d'un utilisateur par téléphone, e-mail, messagerie instantanée ou fax.

Serveurs de mandataire

Le serveur proxy est le lien de connexion entre une application client et un serveur Web. Il effectue la tâche de filtrage des demandes d'application client et soulage ainsi la charge sur le serveur Web.

RTPC (réseau téléphonique public commuté)

Comme son nom l'indique, le RTPC désigne un réseau téléphonique public commuté. Les réseaux publics peuvent appartenir à des entités privées ou publiques.

Qualité de service

Vous devez garantir une bande passante minimale pour la voix sur IP pendant toute la durée de la transmission. Si plusieurs applications avec des droits égaux fonctionnent via IP, la bande passante disponible pour un chemin de transmission est divisée. Dans ce cas, une connexion Voix peut subir des pertes de paquets qui peuvent réduire la qualité de la Voix. Il existe différentes façons de garantir la meilleure qualité possible pour la transmission ; ces méthodes sont collectivement appelées Qualité de Service (QoS).

Service d'accès à distance (RAS)

Un utilisateur RAS (Remote Access Service) est un abonné IP (par exemple, un télétravailleur) qui se connecte au système à distance et se comporte comme un Terminal IP interne. Cet abonné peut donc utiliser tout le périmètre fonctionnel du système de communication.

RJ45 (prise Jack 45 enregistrée)

RJ45 est un connecteur à huit broches qui est utilisé pour connecter un câble 10BaseT dans la technologie réseau, par exemple.

Itinérance

L'itinérance est la capacité d'un abonné de réseau mobile à passer automatiquement des appels ou à accéder à d'autres services de réseau mobile dans un réseau étranger, c'est-à-dire différent du réseau d'origine de l'abonné.

RTCP (protocole de contrôle en temps réel)

Le protocole de contrôle en temps réel (RTCP) est utilisé pour la négociation et la conformité des paramètres de qualité de service (QoS) grâce à l'échange périodique de messages de contrôle entre les émetteurs et les récepteurs.

RTP (protocole de transport en temps réel)

RTP est une norme de l'IETF pour le streaming de données multimédia en temps réel à l'aide du protocole Internet. En règle générale, RTP s'exécute sur le protocole UDP et utilise des ports UDP dynamiques négociés entre l'expéditeur et le destinataire de flux multimédias spécifiques.

Temps d'aller-retour :

RTT est l'intervalle de temps requis par un paquet de données pour se déplacer de la source à la cible et vice versa.

SA (Association de sécurité)

SA est une association de sécurité entre deux unités communicantes dans des réseaux informatiques. Il décrit comment les deux parties utiliseront les services de sécurité pour communiquer en toute sécurité entre elles.

SDSL (ligne d'abonné numérique symétrique)

SDSL est particulièrement adapté à la téléphonie Internet, aux applications intranet dans les entreprises avec des réseaux locaux, à la visioconférence et est, par exemple, conçu pour les télétravailleurs qui peuvent l'utiliser pour envoyer et recevoir des données avec la même bande passante. Contrairement à l'ADSL, SDSL utilise des bandes passantes identiques de et vers Internet.

Secure CLI

Secure CLI est une fonctionnalité de sécurité qui fournit des interfaces de ligne de commande et de transfert de données sécurisées à l'aide du protocole de transfert de fichiers sécurisé (SFTP).

SFTP (protocole de transfert de fichiers sécurisé)

SFTP est un protocole de sécurité pour le transport des enregistrements de données de connexion.

Client VPN ShrewSoft

Le client VPN ShrewSoft est un client VPN open source et gratuit avec une interface utilisateur graphique. Il comprend, entre autres, le support ISAKMP, Xauth et RSA, et les protocoles de cryptage AES, Blowfish et 3DES.

Single Gateway

Dans le cas d'un réseau à passerelle unique, les appels sont acheminés via une passerelle unique.

protocole d'initialisation de session

SIP est un protocole Internet standard défini dans la RFC 3261 pour l'établissement et la gestion des connexions Voix et des vidéoconférences sur un réseau IP.

SNMP (Simple Network Management Protocol)

SNMP est une procédure permettant d'obtenir des informations sur l'état des composants réseau et des PC.

Cryptage de la signalisation et de la charge utile (SPE)

La signalisation et le cryptage de la charge utile (SPE) servent à améliorer la sécurité lors de la transmission de données Voix. La charge utile VoIP et les flux de données de signalisation de et vers la passerelle et entre les téléphones IP sont cryptés.

SRTP (protocole de transport sécurisé en temps réel)

SRTP est un protocole RTP crypté. Il est particulièrement adapté à la transmission de données de communication sur Internet et est utilisé en téléphonie IP.

SSH (Secure Shell)

SSH est un protocole qui prend en charge la connexion à distance sécurisée, le transfert de fichiers sécurisé et la transmission TCP/IP sécurisée. Il peut crypter, authentifier et compresser automatiquement les données transmises.

SSL (Secure Socket Layer, couche de socket sécurisée)

SSL est un protocole de transport de documents sur Internet. Avec SSL, les données sont fournies avec une clé privée avant d'être transmises. Par convention, les URL qui nécessitent une connexion SSL commencent par https : au lieu de http :.

État

L'état, ainsi que le concept « Présence », indique si un abonné est disponible, occupé, hors ligne, etc., afin que les autres abonnés du système de communication sachent si cet abonné peut être atteint.

ÉTOURDISSEMENT (Traversée simple de l'UDP par NAT)

STUN est un protocole réseau permettant de détecter, d'identifier et de contourner les pare-feu et les routeurs NAT.

Survivability

La survivabilité est la capacité d'un interréseau à maintenir la continuité de service en présence de pannes au sein du réseau.

TAE (Telekommunikations-Anschluss-Einheit) - Norme allemande pour les fiches et prises téléphoniques

Un TAE est un type de connecteur pour les connexions téléphoniques analogiques avec l'interface a/b et pour les connexions RNIS pour brancher le NTBA dans la ligne principale. Il est utilisé pour connecter des téléphones analogiques, des télécopieurs et des systèmes téléphoniques RNIS.

TCP (Transmission Control Protocol)

TCP est un protocole qui régit la façon dont les données doivent être échangées par les PC. Tous les systèmes d'exploitation des PC modernes prennent en charge TCP et l'utilisent pour l'échange de données avec d'autres PC.

TFTP (Trivial File Transfer Protocol)

TFTP est un protocole de transfert de fichiers trivial qui ne prend en charge que la lecture et l'écriture de fichiers. De nombreuses fonctions prises en charge par le protocole Superordinate ne sont pas disponibles, par exemple, les fonctions d'attribution de droits, d'affichage de fichiers existants ou d'authentification d'utilisateur.

Telnet

Protocole qui relie deux PC afin de fournir une connexion de terminal au PC distant. Au lieu de composer le numéro sur le PC, l'utilisateur se connecte via Internet via Telnet. L'utilisateur lance une session Telnet, se connecte à l'hôte Telnet et se connecte. La connexion permet à l'utilisateur de travailler avec le PC distant comme s'il s'agissait d'un terminal qui lui est connecté.

Choisir type de service

TOS est un champ dans l'en-tête des paquets de données IP. Il est utilisé pour la priorisation de ces paquets et évalué pour la qualité de service, par exemple.

UCD (distribution uniforme des appels)

UCD permet de répartir uniformément les appels entrants dans le système de communication vers un groupe de terminaux (groupe UCD).

UDP (User Datagram Protocol)

UDP est un protocole réseau qui appartient à la couche Transport de la famille de protocoles Internet. UDP est responsable du routage des données transmises sur Internet vers la bonne application.

UMTS (Système Universel de Télécommunications Mobiles)

L'UMTS est une norme de réseau mobile de troisième génération avec laquelle des débits de transmission de données significativement plus élevés (384 kbit/s à 7,2 Mbit/s) peuvent être atteints par rapport aux normes de réseau mobile de la deuxième génération ou à la norme GSM.

Unified Communications

Les communications unifiées sont l'intégration de divers systèmes de communication, médias, appareils et applications dans un environnement (par exemple, la téléphonie IP, la téléphonie sur site et mobile, le courrier électronique, la messagerie instantanée, les applications de bureau, la messagerie vocale, le fax, les conférences et la messagerie unifiée).

Messagerie unifiée

La messagerie unifiée est l'intégration de différentes données de communication telles que le courrier électronique, les SMS, les télécopies, la téléphonie, etc., dans un magasin de messages uniforme. Ce magasin de messages est accessible par plusieurs appareils différents.

Reconnaissance de pause vocale (VAD)

VAD (détection de l'activité de la voix) est un algorithme de traitement de la parole permettant de détecter la présence ou l'absence de parole dans la transmission numérique de données audio.

Interface VCAPI

VCAPI est une interface capi virtuelle qui émule la présence d'une carte RNIS locale. Si une carte RNIS a été installée sur un PC du réseau interne, cette carte RNIS peut être mise à la disposition de tous les terminaux du réseau via l'interface VCAPI.

VDSL (Ligne d'Abonnement Numérique à Très Haut Débit)

VDSL est utilisé pour transférer des flux de données symétriques ou asymétriques à grande vitesse sur de courtes distances. Le VDSL est une alternative à l'ADSL et au SDSL qui offre en outre des vitesses de transmission plus élevées.

Voice over IP

La VoIP est la transmission de données de voix sur des réseaux basés sur IP.

VPN (réseau privé virtuel)

Un VPN utilise l'infrastructure publique d'Internet pour connecter des sites et fournir aux télétravailleurs un accès aux réseaux internes. Les partenaires

externes bénéficient d'un accès sécurisé au réseau de données interne à l'aide de mécanismes de cryptage et d'authentification.

WAN (réseau étendu)

WAN est la désignation pour les réseaux de données étendus tels qu'Internet, par exemple.

Gestion basée sur le Web (WBM)

Le Web based Management (Web admin) est une interface utilisateur basée sur le Web qui est affichée dans un navigateur Internet utilisant des pages HTML ou JAVA (pages Web) et un protocole Web (HTTP ou HTTPS).

Norme X.509 (certificat VPN)

X.509 est une norme UIT-T pour une infrastructure à clé publique et actuellement la norme la plus importante pour les certificats numériques.

Deuxième degré

Deuxième degré signifie qu'un terminal appelle et a déjà un deuxième appel en attente pour ce terminal.

Index

Special Characters

Écran, mode Expert 1463
Éditeur de règles 786, 825
Édition personnelle d'Openscape 80
Émissions perturbatrices 59
état de présence 490
événement 1272, 1273, 1273, 1274, 1274
    modifier les paramètres e-mail 1276
Événements
    signalisation d'alarme, mode Expert 1437

A

Abonné en ligne 1448
Abonné en ligne, mode Expert 1448
Abonnés
    configuration à l'aide des assistants 404
    IP 390
Abonnés
    Abonnés, mode Expert 1599, 1601
    Programmation des touches, mode Expert 1605
    Vue d'ensemble, mode Expert 1604
Abonnés IP 390
Abonnés Mobility Entry 550, 550
    conférence 548, 549, 551
    Conférences 542
Abonnés, mode Expert 1573, 1638, 1660
accès à distance
    Configurer un PC avec Windows 7 1307
Accès distant 1304
    activer via un accès Internet avec une adresse IP fixe 179, 232
    activer, par l'accès Internet avec adresse IP fixe 181, 181, 183, 234, 234, 235, 1308
    activer, par l'accès Internet sans adresse IP fixe 1309
    activer, via RNIS 1305
    Configuration PC 1306
    désactiver 1310
Accès distant au système de communication 1304
Accès Internet 321
    configuration 322
    configurer par le FAI par défaut PPTP 334
    configurer par le FAI préconfiguré 328
    configurer via le PPPoE standard du FAI 331
    par modem Internet externe 327
    par routeur Internet externe 323
Accès réseau
    accès réseau RNIS, configurer 361
Accès réseau RNIS
    configurer 361
Acheminement 610
Action automatique 1213
    arrêter le regroupement des positions non utilisées 1215
    arrêter notification DLS 1217
    démarrer notification DLS 714, 1217, 1220, 1220
    lancer le regroupement des positions non utilisées 1215
    modifier le regroupement des positions non utilisées 1214
    modifier notification DLS 1216
    notification DLS 1216
    regroupement des positions non utilisées 1214
Action automatique
    démarrer notification DLS 715, 715, 1222
action manuelle 1244
Actions
    actions automatiques, mode Expert 1444, 1445
    actions manuelles, mode Expert 1442
Actions, Mode Expert 1442
Activation des licences 263, 274
activation du logiciel 1190
activation, logiciel (voir activation du logiciel) 1190
Active Directory Service 1124
Actualisation de la licence 290
Adresse passerelle IP, mode Expert 1413
Adresses IP 1209
    afficher la présentation 1211
Adresses IP statiques, mode expert 1527
Affectation à un groupe VBZ, mode Expert 1643
Affecter le MSN, mode Expert 1637
Afficher la liste des numéros autorisés 712
Agent relais DHCP : configurer 305
Agents UCD, mode Expert 1659
Annonces de distribution des appels 703
Annonces de la boîte vocale relatives à l'état 554
Annonces pour la boîte vocale 554
Annuaire externe 519
Annuler un appel 612
Aperçu des messages 799
appel
    manqué 536
    programmé 536
appel de groupe 633
    boîte vocale 634
    NPD pour le membre du groupe 634
    Téléphones SIP 636
    type de sonnerie 636
Appel de groupe
    afficher le type Avertissement 651
    afficher le type Non réponse 651
    ajouter le type Avertissement 650
    ajouter le type Groupe 642
    ajouter le type Non-réponse 651
    effacer le type Avertissement 652

effacer le type Groupe 644
effacer le type Non réponse 652
modifier le type Avertissement 651
modifier le type Groupe 643
modifier le type Non réponse 651
type Avertissement, ajouter un membre 652
type Avertissement, effacer un membre 652
type Groupe, ajouter un membre 645
type Groupe, effacer un membre 645
type Non réponse, ajouter un membre 652
type Non réponse, effacer un membre 652
Appel flexible 622
Appel interphone 586
Appel interphone pour groupes 691
Appelle-moi 512
Appels d'urgence
conditions 766
Appels entrants
Groupes/Groupes de recherche, mode Expert 1610
mode Expert 1610
Renvois d'appels, mode Expert 1622
Appels entrants
Interception d'appel, mode Expert 1619
Membres du groupe, mode Expert 1614
Team/Top, mode Expert 1616
UCD, mode Expert 1619
Application Launcher
profil pour données de configuration 1128
Application Launcher 1126, 1698
Application Launcher, mode Expert 1697
Applications UC, mode expert 1598
Applications, mode Expert 1662, 1698
Arrêt de OpenScape Business X 1206
Assistants 93
authentification
participant à la conférence 476
Avertissement/Indication d'appel 614
avertissements
avertissement 47
Avertissements 45
attention 48
danger 46
remarques 48

B

Bandes passantes du LAN 991
boîte Fax 562
boîte vocale 554
Boîte vocale
annonces liées à l'état 554
enregistrer 554
interception d'appel 554
boîte vocale (UC Smart) 479
Boîte vocale, voir Messagerie vocale 554
bouclage numérique 1249
Bouclage numérique, mode Expert 1424
Boutons utilisateur 798
disposition 798
Branding, mode Expert 1412

C

Câblage pour raccordements LAN et WAN 57
Calendrier 785, 824
Calendrier de congés 786, 825
Calendriers, mode Expert 1683
canaux DSP 1707
Capacités 1371
Carrier Select Override 728
Carte mère, mode expert 1524
Carte mère, mode Expert 1446
Carte RNIS 395
CDP (Certificate Distribution Point) 969
Central Messagerie, inscription 335
Centre d'appels
ajouter une pause 876
charger annonce 858
définir les agents préférés 875
effacer une pause 877
enregistrer la règle en fichier PDF 864
enregistrer une annonce 857
imprimer règle 864, 864, 865
myReports 811
post-traitement simple, effacer le motif de post-traitement 878
procédure lors de la configuration 855
rapports 886
Rôles d'utilisateur myReports 811
télécharger règle 864, 865
Centre d'appels:configurer le pilote pour les messages fax entrants 872
Centre d'appels:exemple de configuration d'un centre d'appels 839
Centre de contact
utilisation des téléphones DECT 885
Centre de contact, mode expert 1674
Centre de contacts 785, 786, 786, 786, 807, 824, 825, 825, 825
activer la file d'attente 872
affecter agent à file d'attente 880
affichage des détails file d'attente 834
affichage mural/wallboard 834
agent 816
agents préférés 818
ajouter un calendrier 858
Ajouter une file d'attente 865
classe de discrimination (niveau d'autorisation) d'un agent) 817
clients 807
conditions pour l'exploitation 882
configurer l'abonné comme agent 857
configurer un groupe UCD 856
définir la valeur de consigne pour le niveau de service 873

définir les priorités des appelants VIP 873
désactiver la file d'attente 872
effacer les agents préférés 876
file d'attente 822
liste d'appels VIP 835
modèles de rapport prédéfinis 887
modifier la liste d'appels VIP 874
modifier un calendrier 862
modifier une pause 876
motifs de post-traitement 833
myAgent 808
niveau de discrimination d'un agent 816
niveau de service 834
pause 818
Post-traitement 833
post-traitement multiple, ajouter un motif de post-traitement 878
post-traitement multiple, effacer le code de post-traitement 880
post-traitement multiple, modifier le code de post-traitement 879
post-traitement simple, ajouter le code de post-traitement 877
post-traitement simple, modifier le code de post-traitement 878
priorités des appelants VIP 835
rappel d'agent 834
restrictions des fonctionnalités système 883
Sélectionner une file d'attente 869
solution de repli 836
supprimer agent file d'attente 881
supprimer un calendrier 863
Centre de contacts:configuration 839
Certificat CA DLSC, mode Expert 1493
Certificat client DLSC, mode Expert 1492
Certificat SecureTrace, mode Expert 1426
Certificat SPE, mode Expert 1496
Certificats actifs, mode Expert 1498
Certificats CA SPE, mode Expert 1496
Certificats configurés, mode Expert 1500
Certificats de serveur, mode Expert 1514
Certificats Peer, mode Expert 1500
Certificats VPN
afficher 950
générer un certificat Lightweight CA 949
générer une demande de certificat 951, 951
importer 952
importer un certificat CA de confiance 950
Charge utile
Equipements, mode Expert 1653
Media Stream Control (MSC), mode Expert 1653
Modules matériels, mode Expert 1654
Charge utile, Mode Expert 1653
Chargement du fichier, mode Expert 1684
Charger sur la passerelle, mode Expert 1407
charger vers la passerelle, mode Expert 1408
Chef/Secrétaire (voir configuration Chef/Secrétaire) 658
Chiffrement de la trace 1250
arrêter 1261, 1261
importer certificat à partir du fichier X.509 1262
importer fichier X.509 1262
interroger l'état 1261
lancer 1261
modifier le mot de passe 1261, 1261
circuit d'alimentation et connexion
OpenScape Business S 56
Serveur OpenScape Business UC Booster 56
Classes de priorisation 387
Classes de service
Abonnés, mode Expert 1638
Affectation à un groupe VBZ, mode Expert 1643
Jour : Groupes de discrimination, mode Expert 1639
Jours spéciaux, mode Expert 1645
Listes des numéros autorisés, mode Expert 1641
Listes des numéros interdits, mode Expert 1641, 1642
Matrice de connexions VBZ, Mode Expert 1643
Nuit : Groupes de discrimination, mode Expert 1640
Renvoi de nuit, mode Expert 1642
Classes de service, mode Expert 1541, 1546
Clés pré-partagées 947
client (UC Smart) 445
client (UC Suite) 489
Client de développement et licence (DLSC), mode Expert 1492
Client intelligent UC 445
Client IP (voir abonnés IP) 390
Client NCP
activer, désactiver 956
préparer 956
Client SIP 390
Client système 390
Clients IP, mode expert 1576
Clients IP, mode Expert 1604
Clients mobiles, mode expert 1601
clients PC 80
Clients UC Suite 489
Clients, configuration matérielle et logicielle 813
clients, prérequis matériels et logiciels 493, 809
CLIP No Screening 593
CLIR - Refus de présentation de la ligne appelante 591
CMD (CSTA Message Dispatcher) 1698
Code d'autorisation de licence (LAC) 274
Code d'autorisation de licence (LAC) 263
Code de verrouillage individuel 725
Codec audio 384
affecter les paramètres à une destination 385
configurer les paramètres 385
COLP - Présentation de l'identification de la ligne connectée 592
COLR - Non-identification de la ligne connectée 592
Communautés d'écriture, mode Expert 1440
Communautés de lecture, mode Expert 1439
Communautés, mode Expert 1439
Comportement en cas d'urgence 54, 54

Composant Trace
modifier 1267
Composante de licence Trace
modifier 1264
Composante de licence Trace, mode Expert 1430
composante de trace 1254
Composante de trace
afficher 1265
afficher les données détaillées 1266
arrêter 1266
arrêter toutes les composantes 1267
démarrer 1266
modifier 1267
Composante de trace M5T
afficher 1259
arrêter 1260
démarrer 1260
modifier 1260
Composante de Trace M5T 1250
Composante de trace M5T, mode Expert 1425
Composants Trace, mode Expert 1431
Composition de chiffres 578
Concept 44
conditions
renvoi d'appel basé sur une règle 513
conditions de fonctionnement (environnementales, mécaniques)
OpenScape Business S 62
OpenScape Business X5, X8 61
Serveur OpenScape Business UC Booster 62
conditions nécessaires pour Application Launcher 1127
Conditions nécessaires pour myReports 813
conférence 476, 542, 550, 550
Abonnés Mobility Entry 542
authentification 542
Directeur de conférence 542
extension 542
géré(e) par l'application 542
gestion par le téléphone 542
invitation automatique par e-mail 542
invitation automatique via rendez-vous Outlook 542
numéro d'accès 542
participant à la conférence 542
registre 542
salle de conférence virtuelle 542
Tonalité de conférence 542
Type 542
Conférence
abonnés Mobility Entry 548, 549, 551
AdHoc 548
ouverte 551
programmée 549
Conférence (UC Suite) 541
conférence ad hoc 476
Conférence Ad-hoc 548
conférence contrôlée par application 476
conférence gérée par l'application 543
Conférence ouverte 551
conférence permanente 476, 550
conférence programmée 476
Conférence programmée 549, 549
conférence, contrôlée par téléphone 476
conférence, gérée par téléphone 543
Conférence, mode Expert 1686
Conférences 550
configuration
annonces, mode Expert 1408
Configuration
branding, Mode Expert 1412
Configuration de port, mode Expert 1409
Configuration
Adresse passerelle IP, mode Expert 1413
musique d'attente (MoH), mode Expert 1407
SmartVM, Mode Expert 1409, 1410, 1410
Configuration chef/secrétaire 658
Ajouter 665
ajouter un membre 671
ajouter une boîte Fax 672
boîte Fax 660
effacer 667
modifier 666
modifier les propriétés d'un membre 672
modifier un membre 671
supprimer un membre 671
téléphones SIP 661
type son 660
Configuration de base
gestion de l'alimentation, mode Expert 1488
Gestion des ports, mode Expert 1480
lecteur, mode Expert 1485
Passerelle, mode Expert 1473
Système, mode Expert 1457, 1463, 1470, 1472
Configuration de base
Classes de service, mode Expert 1478
Date et heure, mode Expert 1479, 1479, 1479
DynDNS, mode Expert 1476, 1477
Passerelle, mode Expert 1474
Système, mode Expert 1466, 1471, 1472
Taxes, mode Expert : 1481, 1483, 1484
Configuration de base, mode Expert 1448, 1696
Configuration de port, mode Expert 1409
Configuration des événements, mode Expert 1435
Configuration des fournisseurs externes, mode expert 1672
Configuration du format Trace, mode Expert 1422
Configuration matérielle OpenScape Office MX
afficher 439
configuration team 654
boîte Fax 656
type de sonnerie 656
Configuration Team
Ajouter 662
ajouter un membre 668
ajouter une boîte Fax 670
effacer 664
effacer un membre 668
modifier 663

modifier la programmation des touches du téléphone 670
modifier les propriétés d'un membre 669
modifier un membre 669
Configuration, mode Expert 1407, 1441
Configurer le renvoi temporisé 482, 604
Conformité
normes internationales 61
normes US et canadiennes 60
Conformité CE 60
Connexion à l'agent CLA local;CLA
connexion locale 282, 283, 293
Connexion avec l'agent central CLA;CLA
connexion centrale 293
connexion d'un utilisateur mobile 899
Connexion LDAP 1127
connexion mobile 899
Connexions
Musique d'attente, mode expert 1645
SmartVM, Mode Expert 1649
Connexions, Mode Expert 1606
Consignes de sécurité 45
contact 536
Contrôler la connexion réseau 1228
par itinéraire de trace 1229
par ping 1228
Conventions de présentation des informations 45
Conversion de numéros en noms 594
Cordless
Dans l'ensemble du système, Mode Expert 1606
Station de base, Mode Expert 1609
Cordless
Multi-SLC, Mode Expert 1609
SLC, Mode Expert 1608
Coupure de la ligne pour un appel d'urgence 769
CRL (Certificate Revocation Lists) 948, 969
Cryptage de la signalisation et de la charge utile
activer l'assistance SPE 933
désactiver l'assistance SPE 933
Cryptage de la signalisation et de la charge utile (SPE) 931
Cryptage de la signalisation et de la charge utile, mode Expert 1495
CSP (CSTA Service Provider) 1699
CSTA Message Dispatcher (CMD) 1698

D

Dans l'ensemble du système, Mode Expert 1606
Date et heure, mode Expert 1479
Démon RPCAP 1271
activer 1272
désactiver 1272
Départements 534
Départements, mode Expert 1669
Déploiement des paramètres du téléphone, mode Expert 1485
Derniers baux actifs, mode expert 1529
Déroulement de la procédure de licence 273
Desk Sharing 899
DHCP Mode, mode Expert 1524
Diagnostic de la plate-forme, mode Expert 1445
Diagnostic des applications Carte mère, mode Expert 1446
Diagnostic des applications Paramètres développeur, mode Expert 1446, 1446
Diagnostic IP
Carte mère, mode Expert 1446, 1447, 1447
Diagnostic IP, mode Expert 1446
Diagnostics des applications, mode Expert 1446
Diffusion à un groupe 691, 691
transférer la communication 692
DISA, mode Expert 1466
Discrimination réseau 706
afficher la liste des numéros autorisés 712
afficher les numéros interdits 712
ajouter le numéro de téléphone aux numéros interdits 711
ajouter le numéro de téléphone dans les numéros autorisés 711
configurer 710, 710, 716, 717, 718
modifier le filtre pour les numéros interdits 712
Discriminations
Renvoi de nuit automatique, mode Expert 1644
Discriminations, mode Expert 1638
Distribution des appels (UCD)
configuration 692
DNS (Domain Name Service)
définir serveur 313
Données d'abonnés
importer 383
données de configuration 1181
données de configuration pour les diagnostics 1279
générer 1280
Données de diagnostic
télécharger 1246
Données du protocole d'admin, mode Expert 1441
DSL (Digital Subscriber Line) 321
DynDNS 312
DynDNS (Dynamic Domain Name Service) 335

E

e-mail
invitation à la conférence 476
E-mail
notification 487, 566
E-mail en SMS 568
E-mail, mode Expert 1435
Echange de numéro 623
Echangeur de messagerie 335, 336
définir 338
Editeur Cover Page 564
Edition numérotation (type GSM 579
Emission de la numérotation 728
sélectionner 729
En-tête ESP 937

enregistrement de l'appel en direct (enregistrement vocal) 601
Enregistrement MX 335
Enregistrer 540
ensemble de sauvegarde 1181
Entrée en tiers 616
entrées journal 1273
Environnement d'exécution Java (JRE) 106
environnement électrique
OpenScape Business S 56
Serveur OpenScape Business UC Booster 56
Environnements de serveur terminal et de serveur Citrix 490
Envoi d'e-mails 567
Equipement de réveil 626
Equipements, mode Expert 1653
Etat de l'abonné 1208
consulter 1209
Etat de l'établissement de la liaison 1208
consulter 1210
Etat de la ligne, mode Expert 1659
Etat des modules, mode Expert 1420
Etat des ports, des modules, mode Expert 1420
Etat du système de communication 1208
Etat ITSP 1208
interroger 1210
Etat Présence
renvoi d'appel 512
Etat Présence (UC Suite) 509
Etat VPN 1209
Evénements
E-mail, mode Expert 1435
Evénements
Configuration des événements, mode Expert 1435
Fichier-journal d'événements, mode Expert 1435
Journaux de diagnostic, mode Expert 1437
Tableau de réactions, mode Expert 1436
Evénements, mode Expert 1435
Event (événement)
afficher le tableau de réactions 1276
effacer le fichier-journal 1275
modifier la consignation des événements par LAN 1275
modifier les paramètres de réaction d'un événement 1277
modifier les paramètres de réaction de plusieurs événements 1277
télécharger fichier journal 1275
Eventail de la boîte vocale 554
EVM, mode expert 1584
exception
renvoi d'appel basé sur une règle 513
Exigences de protection anti-incendie 57
Exigences de protection contre la foudre 58
Exigences relatives au LAN 991

F

Facteurs de taxation, mode Expert 1483
Faisceaux 360, 366
affecter l'indicatif 370
affecter les noms 369
compléter le préfixe entrant 367, 372
configurer le n° de type départ 372
configurer le type de numéro 372
entrer le deuxième indicatif réseau 373
indiquer la direction du débordement 370
inscrire le numéro de l'installation 371
fax 554
T.38 571
Fax Printer (Imprimante fax 491
Fax Printer (Imprimante fax) 563
fichier audio 1174
Fichier audio 1177
Fichier CSV 380
Fichier de licence 263, 274
fichier image 1191
fichier journal 1273
Fichier PDF
message Fax 562
notification 566
Fichier son 1177
Fichier TIFF
message Fax 562
notification 566
Fichier WAV
notification 487, 566
Fichier Wave 1174
Fichier-journal d'événements, mode Expert 1435
Flag abonné
activer la protection contre les intrusions 653
désactiver la protection contre les appels interphones 587
Flag système
assistance SPE 933
interception après retour d'appel 650, 995
numéro A dans groupes d'interception / Pilotage / Destination de renvoi / Destination de renvoi temporaire 649
tonalité d'avertissement pour groupe d'interception 650
Flags LCR, mode Expert 1540
Fonction Chef (voir Configuration Chef/Secrétaire) 658
fonction d'équipe (voir Configuration Team) 654
Fonction Secrétaire (voir Configuration Chef/Secrétaire) 658
Fonctionnalités
voix, sur l'ensemble du réseau 990
Fonctionnalités Euro-RNIS 1703
Fonctionnalités QSIG, mode Expert 1636
Fonctions
myPortal 490
myPortal for Outlook 491
myPortal Smart 447
Format canonique de numéro d'appel 475
Format des numéros d'appel 475
Format sélectionnable de numéro d'appel 475
Fournisseur de service de téléphonie sur Internet (ITSP, Internet Telephony Service Provider) 151, 216, 341

Fournisseur de services CSTA (CSP) 1699
Fournisseur de services de téléphonie sur Internet (ITSP) 339, 339
Fournisseur de services de téléphonie sur Internet, mode expert 1553

G

Gare 1573
    Stations, mode expert 1576, 1579, 1580, 1581, 1583, 1584, 1585, 1601
Gares
    Station, mode expert 1586
Génération de certificats, mode Expert 1512
Gestion basée sur le Web 84
gestion de conférences 476
Gestion de l'alimentation, mode Expert 1488
Gestion des certificats, mode Expert 1498, 1514
gestion des conférences 543
Gestion des ports, mode Expert 1480
Gestion Inventory 1208
Gestionnaire E 102
groupe Boîte Fax
    ajouter un membre 690
    effacer un membre 690
Groupe Boîte Fax 686
    afficher 690
    Configuration 689, 690
    modifier 690
Groupe Boîte vocale 685
    afficher 687
    Ajouter 686
    ajouter un membre 688
    effacer 687
    effacer un membre 688
    Modifier 687
    modifier un membre 688
Groupe d'appel collectif
    activer le rejet des appels en instance pour les membres d'un groupe 653
    désactiver le rejet des appels en instance pour les membres d'un groupe 653
Groupe d'interception 631
    activer l'affichage du nom de l'appelant 649
    activer l'affichage du numéro de l'appelant 649
    activer l'interception des rappels 650, 995
    activer la tonalité d'avertissement 650
    affichage du nom de l'appelant 632
    affichage du numéro de l'appelant 632
    ajouter un membre 641
    configurer 641
    désactiver l'affichage du nom de l'appelant 649
    désactiver l'affichage du numéro de l'appelant 649
    désactiver l'interception des rappels 650, 995
    désactiver la tonalité d'avertissement 650
    effacer un membre 642
    interception d'appel à l'extérieur d'un groupe d'interception 632
    interception des rappels 632
    téléphones SIP 632
    tonalité d'avertissement 632
groupe de recherche 637
    messagerie vocale 638
    Téléphones SIP 640
    type de sonnerie 639
Groupe de recherche
    Ajouter 645
    ajouter un membre 648
    effacer 648
    effacer le membre 648
    modifier 647
Groupe de télécopieurs 3 399
Groupe Fax 395
Groupe Fax (voir groupe Boîte Fax) 686
Groupe Répondeur (voir groupe Boîte vocale) 685
groupe team 654
    boîte Fax 656
    type de sonnerie 656
Groupe Team
    Ajouter 662
    ajouter un membre 668
    ajouter une boîte Fax 670
    effacer 664
    effacer un membre 668
    modifier 664
    modifier la programmation des touches du téléphone 670
    modifier les propriétés d'un membre 669
    modifier un membre 669
Groupe Top 658
    Ajouter 665
    ajouter un membre 671
    ajouter une boîte Fax 672
    boîte Fax 660
    effacer 667
    effacer un membre 671
    modifier 666
    modifier les propriétés d'un membre 672
    modifier un membre 671
    téléphones SIP 661
    type de sonnerie 660
Groupes 631
Groupes de restriction de trafic 721, 722
    affectation des numéros KWZ 722
    affecter la ligne 723
    affecter les abonnés 723
Groupes, mode Expert 1669
Groupes/Groupes de recherche, mode Expert 1610

H

haut-parleur 399
Heure d'actualisation des noms DNS, mode Expert 1477
Hot Desking 899
Hotline 767

I

ICMP (Internet Control Message Protocol) 1228
IKE-SA 946
Image logicielle
    Logiciel système, mode Expert 1413, 1414
Image logicielle
    Logiciel système, mode Expert 1415
Image logicielle, mode Expert 1413, 1418
Image téléphone
    charger, mode Expert 1415
    diffusion par terminal, mode Expert 1416
    distribuer, mode Expert 1416
Indicatifs de service, mode Expert 1473, 1473
Indication d'appel/Avertissement 614
Informations de sécurité pour l'Australie 49
Informations de sécurité pour le Brésil 50
Informations de sécurité pour le Canada 53
Informations de sécurité pour les États-Unis 50
installation 104, 192
Instructions d'utilisation 44
Intégration d'Active Directory Service
    configurer 1125
Intégration d'Active Directory Service, mode Expert 1662
Interception d'appel, mode Expert 1619
Interception de communication à partir de la boîte vocale 554
Interconnexion SIP, mode expert 1566
Interface des services Web 1111
Interface primaire 737
Interfaces d'édition Trace, mode Expert 1423
Interfaces réseau 1524
    Carte mère, mode expert 1516, 1526, 1527, 1529
Interfaces réseau
    Carte d'application, mode Expert 1530, 1530, 1531
    Carte mère, mode Expert 1516, 1521, 1522, 1523, 1524, 1529
Interfaces réseau, mode Expert 1516
inventaire, OpenScape Business S 1212
inventaire, OpenScape Business X 1211
Inventory OpenScape Business S
    interroger 1213
Inventory OpenScape Office LX/HX
    interroger 295, 295
Inventory OpenScape Office MX
    interroger 295
inventory, OpenScape Business X3/X5/X8
    contrôler 1212
invitation
    conférence 476
Itinéraire de trace, mode Expert 1447
Itinéraire, mode Expert 1628
Itinéraires statiques 314
    Ajouter 315, 318, 319, 320
    effacer 316
Itinéraires statiques, mode expert 1532, 1533

J

Java 1127
Java Runtime Environment (JRE) 193
Jeu de sauvegarde 1182, 1182
    afficher 1183, 1183
    Rétablir 1189
    sauvegarde immédiate 1187
    sauvegarde planifiée 1188
jeu de sauvegarde à des fins de diagnostic 1280, 1280
Jour
    Groupes de discrimination, mode Expert 1639
journal
    durée de conservation 536
Journal (UC Smart) 474
journal (UC Suite) 536
Journal de diagnostic 1274
journal de trace client 1250
Journal de trace client
    afficher 1258
    effacer 1259
    modifier 1258
    ouvrir 1259
    télécharger 1259
Journal de trace client, mode Expert 1424
Journal de trace, mode Expert 1424
Journal diagnostic
    effacer 1279, 1279
    ouvrir 1278
    télécharger 1278
Journaux Client 1287
    télécharger 1291
Journaux de diagnostic, mode Expert 1437, 1442
Jours spéciaux, mode Expert 1645

L

LAN 1 (WAN), mode expert 1516
LAN 1, mode Expert 1530
LAN 2, mode Expert 1521, 1531
LAN 3 (Admin), mode Expert 1522
lancement d'un redémarrage d'OpenScape Business 1204
langue système pour la boîte vocale 554
langues 81
LCR
    Planification, mode expert 1541
LCR
    Classes de service, mode Expert 1541
    Flags LCR, mode Expert 1540
    Multisite, mode Expert 1546
    Règle de numérotation, mode Expert 1544
    Table de routage, mode Expert 1542
LCR (Least Cost Routing) 726
    attribuer/modifier une classe de discrimination 734
    classe de discrimination 734
    fonctionnalité 726, 726
    modifier la table de routage 733
    modifier le plan de numérotation 731

modifier les règles de numérotation 736
plan de numérotation 730
règles de numérotation 734
table de routage 732
LDAP, mode Expert 1470
lecteur de communication d'interphone 1698
Lecteur, mode Expert 1485
les stations 378
RNIS 395
Liaison large bande 321
Liaison système 1127
licence 250
Licence
activer à l'aide du fichier de licence 265
activez à l'aide du code d'autorisation de licence 265, 1352
actualiser 291
afficher les informations 284, 285, 285, 286, 286, 295
Lightweight CA 948
Lightweight CA, mode Expert 1497
Ligne directe après temporisation 767
Ligne privée 589
Ligne réseau du serveur SIP natif, mode Expert 1568
Ligne réseau RNIS
prise ciblée 738
Lignes 360
affecter le MSN 364
configurer la prise de ligne 371, 375, 376
modifier l'indicatif 363, 364, 364
modifier le faisceau 369
modifier le protocole 365, 365, 365
prise 367
Lignes d'en-tête de fax, mode Expert 1695
Lignes, mode Expert 1625
Lignes/Routage
Affecter le MSN, mode Expert 1637
Fonctionnalités QSIG, mode Expert 1636
Lignes, mode Expert 1625
Paramètres RNIS, mode Expert 1638
Lignes/Routage, mode Expert 1624
Limites de configuration 1371
liste des favoris 536
Liste des favoris
message instantané 478
Liste des favoris (UC Smart) 467
Liste des numéros interdits
afficher 712
Liste des sites, mode expert 1686
Listes des numéros autorisés, mode Expert 1641
Listes des numéros interdits, mode Expert 1641, 1642
logo de téléphone
charger, mode Expert 1417
LXV3, mode Expert 1697

M

Maintenance DLI, mode Expert 1444
Maintenance, mode expert 1407
Maintenance, mode Expert 1697
Mappage (état Présence UC Suite) 509
Marquage CE 59
Marqueur de test pour H.323 1251
Matériel, remplacement 290
Matrice de connexions VBZ, Mode Expert 1643
MCL Single Stage 737
MCL Two Stage 737
MEB (Media Extension Bridge) 1700
Media Extension Bridge (MEB) 1700
Media Stream Control (MSC), mode Expert 1653
Mediatrix 4102S 80
Membres du groupe, mode Expert 1614
Menus flexibles, mode Expert 1472
Message discret) 600
message instantané 552
Message instantané 478, 478, 478, 478, 552, 552
messagerie instantanée 552
Messagerie instantanée 799
messagerie vocale 554
messagerie vocale (UC Smart) 479
Messages
administration 799
messages fax 554, 799
Messages instantanés 799
messages vocaux 554, 799
Ministère de la Santé 1174
mise à jour 1190
Mise à jour
définie par l'utilisateur 1199
mise à jour du logiciel (voir mise à jour) 1190
Mise à jour via chargement de fichier, mode Expert 1414
Mise à jour via clé USB, mode Expert 1415
Mise à jour via Internet, mode Expert 1413
mise à jour, complète
commencer en arrière-plan 1197
Mise à jour, complète
démarrer avec affichage de la progression 1194, 1203
mise à jour, logiciel (voir mises à jour logicielles) 1190
mise à niveau 1190
Mise au rebut 55
Mise en garde 594
Mise en réseau
supprimer un noeud dans l'interconnexion de réseaux 1081
mises à jour automatiques 499
mises à jour logicielles 1190
Mobilité
effacer l'abonné 899
Mobilité :
configurer le téléphone mobile pour GSM 895
Mobilité IP 899
Mobility Entry 889
codes de fonctionnalité 889
Mode Expert, mode Expert 1406
Modèle de SMS 568
Modèles, mode Expert 1671

modem 399
Modem Internet 327
Modem RNIS 395
Modifier la matrice de connexions 724
Modules matériels, mode Expert 1654
MoH 1177
monAgent
  prérequis 809
MULAP chef 676
  afficher 682
  ajouter un membre 683
  effacer 682
  effacer un membre 683
  modifier 682
  modifier un membre 683
  Téléphones SIP 678
  type de sonnerie 677
MULAP Chef
  Ajouter 681
MULAP de base 673
  afficher 679
  Ajouter 679, 684
  ajouter un membre 680
  effacer 680
  effacer un membre 680
  modifier 679
  modifier un membre 681
  type de sonnerie 675
Multi Location (multi-emplacement) 984
Multi-SLC, Mode Expert 1609
Musique d'attente 1177, 1177
Musique d'attente (Music On Hold MoH) 703
Musique d'attente interne 1174
Musique d'attente pour UCD 703
Musique d'attente, mode expert 1645
musique en attente 1174
myPortal
  état de présence 490
  Fonctions 490
myPortal for Outlook
  Fonctions 491
myPortal Smart
  Fonctions 447
myReports
  réinitialiser le mot de passe administrateur 813
  rôles d'utilisateur 811

N

NAT (Network Address Translation) 926
NAT, mode Expert 1534
Ne pas déranger 612
Noeud, mode Expert 1565
Nom d'hôte, mode Expert 1516, 1530
Nom DNS 335
Non-identification de la ligne connectée - COLR 592
Normes 1701
Notification
  message Fax 566
  message Voix 487, 566
Notification DLS, mode Expert 1445
Notification par SMS 568
Nuit
  Groupes de discrimination, mode Expert 1640
Numéro abrégé individuel (KWI) 585
numéro d'appel
  conférence 476
Numéros abrégés, mode Expert 1472, 1697
Numéros de téléphone
  importer 383
Numéros de téléphone publics dans le réseau 994
Numéros SDA, mode Expert 1601
Numérotation
  ouverte 993
Numérotation
  fermée 993
Numérotation abrégée centralisée (KWZ) 581
Numérotation E.164 994
Numérotation KEYPAD 578
Numérotation par blocs 578
Numérotation via le bureau 491, 538
Numéroter à partir du presse-papiers 538

O

Objets CCV 786, 825
observateur d'événements 1249
Observateur d'événements
  afficher le journal 1258
  effacer le journal 1259
  modifier le journal 1258
  ouvrir le fichier-journal 1258
  télécharger le fichier-journal 1258
Open Directory Service 1127
  Maintenance, mode Expert 1697
  Sources de données, mode Expert 1696
Open Directory Service
  Configuration de base, mode Expert 1696
  Sources de données, Mode Expert 1697, 1697
Open Directory Service, mode Expert 1696, 1697
OpenScape Business Assistant 84, 86
OpenScape Business X5R
  mise à la terre de protection 1349, 1350
OpenScape Office, mode expert 1696
OpenStage 79
Opérateur principal 737
Opérateurs 737
Optimisation de route 994
optiPoint 79
Out of Service (hors service), mode Expert 1421

P

Padding 937
Paramètre global, mode expert 1524

Paramètres de base 1448
Déploiement des paramètres du téléphone, mode Expert 1485
Système, mode Expert 1467, 1473
Paramètres de la station, mode expert 1586
Paramètres du codec de destination, mode Expert 1552
Paramètres du codec, mode expert 1550
paramètres e-mail 1274
Paramètres réseau (LAN, WAN) 990
Paramètres RNIS, mode Expert 1638
Paramètres SecureTrace, mode Expert 1426
Paramètres SIP, mode Expert 1546
Paramètres SNTP, mode Expert 1479, 1479
Paramètres système, mode expert 1448
Parcage 595
pare-feu 1127
Pare-feu 923
Pare-feu applicatif, mode expert 1490
Partenaire RTC, mode Expert 1536
Passerelle vocale
Fournisseur de services de téléphonie sur Internet, mode expert 1553
Interconnexion SIP, mode expert 1566, 1568
Paramètres du codec, mode expert 1550
Passerelle vocale
Mise en réseau, mode Expert 1565, 1566
Paramètres du codec de destination, mode Expert 1552
Paramètres SIP, mode Expert 1546
Passerelle vocale, mode Expert 1546
Passerelle, mode Expert 1474
Path Replacement 994
Pause dans la numérotation 585
Permanente 550
Perturbations radio 59
Pilotage 610
PIN mobile 622
PIN pour activation du Shutdown 1206
Ping, mode Expert 1447
Plan de mise en réseau 983
plan de numérotation 107
Plan de numérotation 196, 378, 730
importer 383
modifier 382
supprimer 381
Plan de numérotation, mode expert 1541
Points de code AF/EF 387
Pools d'adresses IP, mode expert 1526
port 1127
Ports 924
configurer la validation de port 925, 1077
gestion des ports 925
Poste de portier / Ouverture de la porte 1088
Poste de travail alternatif 512
Préposé OpenStage 796
Prérequis pour myAgent 809
présence (UC Smart) 464, 464
Présence (UC Suite) 509, 509
Présentation de l'identification de la ligne connectée - COLP 592
Présentation de la ligne appelante - CLIP 590, 590
Priorisation des lignes réseau) 377
profil de trace 1252
Profil de trace
afficher 1256
afficher les données détaillées 1264
ajouter 1265
arrêter 1257
arrêter tous les profils 1265
démarrer 1257
Profil pour données de configuration de Application Launcher 1128
profils
créer nouveau profil 430
modification 433
Profils
abonnés 429
afficher les membres 431
afficher les profils 431
ajouter des membres 431
effacer les membres 432
exporter tous les profils 434, 919
exporter un profil 432
importer tous les profils 434, 919
importer un profil 432
Profils / Modèles, mode Expert 1599
Profils d'abonné 429
Profils de trace, mode Expert 1431
Profils des utilisateurs de UC Suite 505
Profils, mode Expert 1693
Profils:exporter tous les profils 434, 919
Profils:importer tous les profils 434, 919
programmation de touches 400, 401
Programmation des touches, mode Expert 1605
Protection appel PCV par ligne réseau 726
Protection contre les appels interphones pour abonné 586
Protection contre les appels interphones pour un abonné
activer 587
désactiver 587
Protection des données 59, 886
Protocole Admin 978
charger 978
modifier la langue 933, 934, 934, 935, 978
Protocole Admin, mode Expert 1441
Protocole ARP, mode Expert 1446
Protocole CSTA 1096
Protocole d’admin Configuration, mode Expert 1441
Protocole d’admin Données du protocole d'admin, mode Expert 1441
protocole de diagnostic 1244
Protocole de diagnostic 1244
télécharger 1246
Protocole PPP, mode Expert 1536
Public Key Infrastructure (PKI), mode Expert 1512

Q

Qualité de service QoS) 387
    configuration 389
Qualité de service, mode Expert 1478

R

Raccordement par câble 321
Raccourci clavier pour la numérotation via le bureau 538
rappel
    journal 536
Rappel 613
Rappel automatique 614
Rappel sur occupation 614
Rechargement d'OpenScape Business 1205
Recyclage 55
redémarrage d'OpenScape Business 1204
Redémarrer / Recharger
    Redémarrer / Recharger, Mode Expert 1438
Redémarrer / Recharger, Mode Expert 1438, 1438
Refus de présentation de la ligne appelante - CLIR 591
règle 513
Règle de numérotation, mode Expert 1544
Règle NAT
    configurer 926
    configurer avec le tableur NAT 927
    effacer 928
Règles actives, mode Expert 1509
Règles configurées, mode Expert 1511
Règles de numérotation 734
Règles NAT 926
Regroupement des positions non utilisées, mode Expert 1444
Rejeter les appels 611
Relocate 623
Remarques sur l'utilisation simultanée des clients myAgent et UC Suite 815
Rendez-vous 626
Renvoi d'appel 606
    en fonction de l'état 512
renvoi d’appel
    basé sur une règle 513
Renvoi de nuit automatique, mode Expert 1644
Renvoi de nuit, mode Expert 1642
Renvoi distinct/P.O./Hotline, mode Expert 1467
Renvoi temporisé 603, 608
Renvoi temporisé en réseau 609
Renvoi temporisé fixe 603
Renvoi temporisé sur occupation 603
Renvois d’appels, mode Expert 1622
Renvois, mode Expert 1660
Répertoire
    message instantané 478
Répertoire externe (LDAP) 523
Répertoire externe, mode Expert 1671
Répertoire interne (UC Smart) 466
Répertoire interne (UC Suite) 517
Répertoire système 468
Répertoire système (UC Suite) 525
Répertoire utilisateur, mode Expert 1666
Répertoires (UC Smart) 465
Répertoires (UC Suite) 514
Répétition de la numérotation 580
répondeur 399
Réponse sur appel interphone 586
Reprendre le jeton écriture, mode Expert 1446
réseau
    hétérogène, hybride 983
    homogène, natif 983
Réseau
    licence 990
Réseau d'entreprise 737
Réservation de ligne 588
restaurer 1181
Restore (voir Rétablir) 1189
Rétablir 1189
Retour d'appel 597
Routage 314
    Routage IP, mode expert 1532, 1532, 1533, 1534
Routage
    NAT, mode Expert 1534
    Routage IP, mode Expert 1533
    RTC, mode Expert 1535, 1536, 1536
Routage, mode Expert 1532, 1566
Routeur Internet 323
Routeur par défaut 314
    Configuration 314
Routeur par défaut, mode expert 1532, 1534
rpcap Daemon, mode Expert 1433
RTC, mode Expert 1535

S

SA de charge utile 946
salle de conférence virtuelle 476
sauvegarde 1181, 1181
    immédiat 1186
Sauvegarde
    programmée dans le temps 1188
Sauvegarde - immédiate 1187
sauvegarde des données (voir sauvegarde) 1181
Schéma des adresses IP 108, 196
Secure Trace, mode Expert 1425
Sécurité
    Pare-feu applicatif, mode expert 1490
    Sécurité Web, mode expert 1515
Sécurité
    Client de développement et licence (DLSC), mode Expert 1492, 1492, 1493
    Cryptage de la signalisation et de la charge utile, mode Expert 1495, 1496, 1496
    Sécurité SQL, mode Expert 1516
    SSL, mode Expert 1512, 1514, 1514
    VPN, Mode Expert 1496, 1497, 1498, 1498, 1500, 1500, 1501, 1502, 1502, 1505, 1509, 1511, 1512

Sécurité des données 59
Sécurité SQL, mode Expert 1516
Sécurité Web, mode expert 1515
Sécurité, mode Expert 1490
Security Associations SA 946
Security Checklist 923
Sélection de l'application 1662
Sélection de l’application 1663
Serveur de licences (CLS) 268, 291
modifier l'adresse IP 271, 282, 292
Modifier l’adresse IP 180, 233, 280, 287, 288, 288, 289
Serveur de licences central (voir serveur de licences) 291
Serveur Dial-In Control 737
Serveur DNS 313
Serveur DNS, mode Expert 1533
Serveur DSS 1700
Serveur FTP, mode Expert 1523
Serveur PKI
afficher 968
ajouter 968
Serveur, mode Expert 1686
Service à distance 1298
Service CallMe 512
Service d'appel d'urgence E911 770
Service de notification 487, 566
Service des données de crash du noyau
arrêter 1269
démarrer 1269
Service DynDNS 335
Configuration 336
configurer 357, 357, 358, 359, 921
Service DynDNS, mode Expert 1476
Services actifs, mode Expert 1501
Services configurés, mode Expert 1502
Shutdown
PIN pour activation 1206
Signalisation d'accident 54
signalisation d'alarme, mode Expert 1437
Signalisation des appels 589
Signature numérique 947
Single Location (mono-emplacement) 984
Site Of Operations, mode Expert 1662
SLC, Mode Expert 1608
SmartVM, Mode Expert 1409, 1410, 1410, 1649
SMS
notification 566
SNMP
Communautés, mode Expert 1439, 1439, 1440, 1440
Traps, mode Expert 1440
SNMP (Simple Network Management Protocol) 1229
afficher les communautés 1241
afficher les données détaillées d'un trap 1244
afficher les traps 1243
ajouter une communauté 1242
Bases de données d’informations de gestion MIB 1230
communautés 1230
effacer la communauté 1243
modifier la communauté 1242
traps 1230
SNMP, mode Expert 1439
Sortie console de trace, mode Expert 1446
SSDP (Plateforme de prestation de services intelligents) 1298
SSDP (Smart Services Delivery Platform)
configurer le PIN pour activer/désactiver le plugin Service 1304
configurer le plugin Service pour un réseau client avec proxy 1301
réinitialiser le plugin Service 1303
SSDP (Smart Services Delivery Platform)
désactiver le plugin Service 1303
SSL (Secure Socket Layer, couche de socket sécurisée) 969
activation d'un certificat 976
afficher les certificats 929, 930, 930, 975
effacer le certificat 975
exporter le certificat 975
générer le certificat autosigné 971
générer un certificat CA 971
générer une demande de certificat 973
importation d'un certificat de serveur 974, 974
importer un certificat étendu 976
Standard automatique 554
stations
analogique 399
Station, mode expert 1598
Stations analogiques, mode expert 1579
Stations d'entrée pour la mobilité
conférence 476
Stations de base, mode expert 1581
Stations de base, mode Expert 1418, 1418, 1609
Stations DECT, mode expert 1583
Stations RNIS, mode expert 1580
Stations UP0, mode expert 1573
Stations virtuelles, mode expert 1585
Stations, mode expert 1573
Statistiques
Statistiques de téléphonie, mode Expert 1659
Statistiques
statistiques de la passerelle, mode Expert 1657
statistiques de téléphonie, mode Expert 1658, 1659, 1659, 1660, 1660
Statistiques SNMP, mode Expert 1658
Statistiques d’équipements, mode Expert 1657
Statistiques MSC, mode Expert 1658
Statistiques SNMP, mode Expert 1658
Statistiques, mode Expert 1657
Statut de présence (UC Smart) 464
STUN (Simple Traversal of UDP through NAT) 358
Suite UC
activer l'enregistrement des journaux clients sur le disque dur du système 1290
Centre de contact, mode expert 1674

Configuration des fournisseurs externes, mode expert 1672
désactiver l'enregistrement des journaux clients sur le disque dur système 1290
Liste des sites, mode expert 1686
Serveur, mode Expert 1686
support de sauvegarde 1181, 1183
Support de sauvegarde
Ajouter 1184
effacer 1186
modifier 1186
support, sauvegarde (voir support de sauvegarde) 1183
Surnumérotation 581
surveillance d'appel, mode Expert 1428
survivabilité 1078
Système de communication
Éteindre 1206
Système, mode expert 1448

T

T.38 Fax 571
Table de routage 732
Table de routage, mode Expert 1542
tableau de réactions 1274
Tableau de réactions, mode Expert 1436
Tableur NAT 927
Taxes - Codes affaire, mode Expert 1484
Taxes - Format d'édition, mode Expert 1481
TCP- Dump, mode Expert 1432
TCP-Dump 1270
arrêter 1271
démarrer 1270
effacer 1271
team (voir Configuration Team) 654
Team/Top, mode Expert 1616
télécharger (voir mise à jour) 1190
Telefon-Logo
Verteilen, Experten-Modus 1417
Téléphone analogique 399
Téléphones 79
Téléphones RNIS 395
Téléphones sans fil 80
Téléphones SIP 80
téléphonie bi-mode 893
téléphonie par Internet 339
Téléphonie, mode Expert 1448
télétravail 913
Télétravail 512
Temporisations
surveillance d'un appel UCD sur une ligne analogique 705
surveillance d'un transfert avant réponse à un groupe UCD 704
Temporisations, mode Expert 1457
Terminaux RNIS 395
Texte en plusieurs langues 1173
Textes d'absence 618
Textes messages 618
Textes système, mode Expert 1659
Textes, mode Expert 1471
Thèmes, types de 44
Tonalité de conférence, activer/désactiver 608, 608
Touche d'appel direct 585
Touche DSS 585
touches de fonction
programme 442
Touches de fonction 400
Programme 401, 463
programmer 443, 444, 463, 487
Toutes les locations, mode Expert 1529
trace 1247
journal 1249
Trace
afficher la configuration du format 1257
afficher les interfaces d'édition 1258
effacer le fichier-journal 1255
modifier la configuration du format 1257
modifier les interfaces d'édition 1258
télécharger le fichier-journal 1254
Trace
effacer le fichier journal 1255
Trace de pile H.323
effacer le fichier-journal 1264
modifier la configuration 1262, 1262
modifier les modules 1263
ouvrir le fichier-journal 1263
télécharger le fichier-journal 1263
Trace de pile H.323, mode Expert 1427
trace des composants de la licence 1252
Trace du serveur média
arrêter 1270
démarrer 1269
trace:configuration du format 1247
trace:interfaces d'édition 1248
traces
surveillance d'appel, mode Expert 1428
Traces
rpcap Daemon, mode Expert 1433
Traces du serveur média, mode Expert 1434
Traces
Bouclage numérique, mode Expert 1424
Composante de licence, mode Expert 1430
Composante de trace M5T, mode Expert 1425
Composants Trace, mode Expert 1431
Configuration du format Trace, mode Expert 1422
Interfaces d'édition Trace, mode Expert 1423
Journal de trace client, mode Expert 1424
Journal de trace, mode Expert 1424
Profils de trace, mode Expert 1431
Secure Trace, mode Expert 1425, 1426, 1426
TCP- Dump, mode Expert 1432
Trace de pile H.323, mode Expert 1427
Traces du serveur média, mode Expert 1434
Traces, mode Expert 1421
Transférer à un groupe à partir d'une diffusion 692

Transférer les communications téléphoniques 596
transfert de logiciel 1190
transfert, logiciel (voir transfert de logiciel) 1190
Transmission d'informations personnalisées sur le numéro d'appel 593
Trap Communautés, mode Expert 1440
Traps, mode Expert 1440
Troncs/Routage
Itinéraire, mode Expert 1628
Tunnel IPSec 946
Tunnels actifs, mode Expert 1502
Tunnels configurés, mode Expert 1505

U

UC Application
redémarrage 1207, 1207
UC Smart
Configuration de base 1664
État 1665
Gestion des utilisateurs 1665
UC Smart
appeler l'état 1297
état 1297
UC Smart, mode Expert 1663
UC Suite
activer l'enregistrement des journaux système individuellement par abonné 1289
configurer les notifications par e-mail pour les erreurs système 1294
désactiver l'enregistrement des journaux système individuellement par abonné 1289
maintenance 1286
Répertoire utilisateur, mode Expert 1666
surveillance 1286
télécharger les journaux Client 1291
UC Suite 1666
activer l'enregistrement de la journalisation client sur l'ensemble du système 1288
activer l'enregistrement des journaux système 1288
Calendriers, mode Expert 1683
Chargement du fichier, mode Expert 1684
Conférence, mode Expert 1686
configurer la durée de conservation des données de centre d'appels 1297
configurer la durée de conservation des fichiers journal 1296
configurer le chemin d'archivage pour fichiers journal client 1290
configurer le moment de la maintenance 1296
Départements, mode Expert 1669
désactiver l'enregistrement de la journalisation client sur l'ensemble du système 1289
désactiver l'enregistrement des journaux système 1288
effectuer immédiatement la maintenance du système 1296
Groupes, mode Expert 1669
Journaux Client 1287
Journaux système 1287
Lignes d'en-tête de fax, mode Expert 1695
maintenance 1294
Modèles, mode Expert 1671
notification 1292
notification par e-mail 1292
Profils, mode Expert 1693
Répertoire externe, mode Expert 1671
UC Suite, mode Expert 1666
UCD 692, 693
agent UCD 695
AICC (Automatic Incoming Call Connection) 699
ajouter un agent UCD 696
annonces 703
Configuration 694
configurer un groupe UCD 694
débordement 701
durée du post-traitement 697
effacer un agent UCD 696
état de l'abonné 695
file d'attente 700
groupe UCD 693
libération des appels UCD arrivant via des lignes analogiques 705
libération des appels UCD arrivant via des lignes analogiques, modifier l'heure de libération 705
modifier la file d'attente 700
modifier la musique d'attente (Music On Hold MoH) 703
modifier la priorité des appels externes 698
modifier la priorité des appels internes 698
modifier le débordement 701
modifier le délai de post-traitement 697
modifier les annonces 703
prendre automatiquement les appels UCD 699
prendre automatiquement les appels UCD, activer 699
prendre automatiquement les appels UCD, désactiver 699
priorité des appels externes 698
priorité des appels internes 698
renvoi de nuit 702
transférer à un groupe UCD 704
transférer à un groupe UCD, modifier le délai de retour d'appel 704
UCD (Uniform Call Distribution, distribution uniforme des appels) (voir UCD) 692
UCD, mode Expert 1619
Utilisateur en ligne 1310
démarrer 1311
départ 1227
Utilisateur RAS 390
Utilisateurs de UC Smart
modifier les données 463, 487
Utilisateurs de UC Smart
Modifier les données 463
utilisateurs de UC Suite
modifier l'état de présence 503
utilisateurs de UC Suite
modifier la longueur du mot de passe 504

Mot de passe:changer 504
Utilisateurs de UC Suite 499
configurer en tant qu'agent 503
modifier les données 502
réinitialiser 502
Utilisation conforme des systèmes de communication et du serveur 55

V

Va-et-vient 596
Valeurs maximales
Fonctionnalités 1379
Verrouiller le téléphone 725
Verrouiller les services (uniquement LX) 931
VPN
authentification 947
bandes passantes 936
certificats 948
clients 953
VPN - Mécanismes de sécurité VPN 946
VPN - Règles
afficher les règles spéciales actives 965
afficher toutes les règles actives 964
afficher toutes les règles configurées 965
ajouter pour le sens opposé 967
ajouter une règle configurée 966
effacer 967
modifier 966
VPN - Services actifs
afficher le service spécifique 958
afficher tous les services 958
VPN - Services configurés
afficher tous les services 959
effacer 960
modifier 959
renommer 960
VPN - Tunnels actifs
afficher 961
afficher les règles 961
VPN - Tunnels configurés
afficher 962
afficher les règles 962
ajouter 962
VPN (Virtual Private Network) 935
End-to-Site 936
Site-to-Site 936
VPN, Mode Expert 1496

W

WAN 335
WBM 84
page d’accueil 84
Web Services 1127

© 2026 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.